



Patrik Sundgren

Windows Server 2008 -infrastrukturi

Metropolia Ammattikorkeakoulu
Insinööri
Tietotekniikka
Opinnäytetyö
8.2.2011

Alkulause

Tämä insinööryö on tehty Metropolia ammattikorkeakoululle keväällä 2010.

Haluan esittää erityiskiitoksen työtä ohjanneelle yliopettaja Janne Saloselle, jonka neuvot ja kannustukset auttoivat työn ja opintojeni suorituksessa erittäin paljon.

Haluan omistaa tämän työn perheelleni ja erityisesti rakkaalle vaimolleni, jonka korvaamattoman tuen ansiosta tämä työ on olemassa.

Helsingissä 8.2.2011

Patrik Sundgren

Tekijä Otsikko	Patrik Sundgren Windows Server 2008 -infrastruktuuri
Sivumäärä Aika	35 sivua 8.2.2011
Tutkinto	Insinööri
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Tietoverkot
Ohjaaja	Yliopettaja Janne Salonen
<p>Tämä työ käsittelee Windows 2008 -verkkoinfrastruktuuri-kurssin materiaalin suunnittelua ja testausta. Työ toteutettiin Metropolia Ammattikorkeakoululle keväällä 2010.</p> <p>Työn alussa esitellään työssä käytetty virtuaalisointiohjelmisto ja toiminta, sekä Windows Server 2008:n ominaisuuksia. Työssä käydään läpi virtuaaliympäristön luonti sekä Windows Server 2008 -palvelinten konfigurointia. Konfigurointi tapahtuu Windows Server 2008 infrastructure -materiaalin harjoitustöiden pohjalta. Työssä käydään läpi eri harjoitustyöt ja pohditaan niiden sopivuutta Windows 2008 -verkkoinfrastruktuuri-kurssin materiaaliiksi.</p> <p>Työssä testattiin myös virtuaalikoneiden minimivaatimuksia ja niiden riittävyyttä harjoitustöiden suorittamisen osalta.</p> <p>Kun kaikki harjoitustyöt käytiin läpi, koottiin valituista harjoitustöistä harjoitustyöpaketti kurssia varten.</p>	
Avainsanat	Windows Server 2008, palvelin, virtuaaliympäristö

Author Title	Patrik Sundgren Windows Server 2008 infrastructure
Number of Pages Date	35 pages 8 Feb 2011
Degree	Bachelor of engineering
Degree Programme	Information Technology
Specialisation option	Data Networks
Instructor	Janne Salonen, Principal Lecturer
<p>This thesis deals with the planning and testing of course materials for the Windows Server 2008 infrastructure course for Metropolia University of Applied Sciences. The work was carried out in spring 2010.</p> <p>The study begins with an introduction to Virtual PCs, a computer virtualization program for Windows operating systems and the Windows Server 2008 operating system. The key features of both software are reviewed. The thesis concentrates on the configuration exercises of the Windows Server 2008 operating systems. In addition, the minimum requirements of the virtual machines are tested.</p> <p>After completing all of the exercises in the Windows Server 2008 material, the exercises that seems best suited for the Windows Server 2008 infrastructure course were chosen to be included in the exercise package for the course.</p>	
Keywords	Windows Server 2008, virtual machines

Sisällys

Alkulause

Tiivistelmä

Abstract

1	Johdanto	1
2	Työkalut	2
2.1	Microsoft Virtual PC 2007	2
2.2	Windows Server 2008	4
2.2.1	Ominaisuudet	4
2.2.2	Palvelinroolit	5
2.2.3	Server Core	5
2.2.4	Active Directory	6
2.2.5	Hyper-V	7
2.2.6	Server Manager	8
3	Suunnittelu	10
4	Toteutus	11
4.1	Alustan valmistelu	11
4.2	Windows Server 2008 -asennus	14
4.3	Verkon luominen	15
4.4	DNS-palvelin	17
4.5	GlobalNames Zone	19
4.6	DHCP-palvelin	21
4.7	Telnet	23
4.8	NAT-palvelin	24
4.9	VPN-palvelin	25
4.10	Palomuri	26
4.11	DHCP NAP	27
4.12	WSUS	29
4.13	Lisäasetuksia	30
4.13.1	Tietojen kirjaus	30
4.13.2	Tiedostojen salaus	31

4.13.3 Kansioden jakaminen	31
4.13.4 Varmuuskopiointi	32
4.14 Kurssiympäristön luonti	33
5 Yhteenveto	34
Lähteet	36

1 Johdanto

Insinööriyön lähtökohtana on tutustua Microsoftin viralliseen Windows Server 2008 Network Infrastructure -materiaaliin, käydä läpi aineiston harjoitustyöt ja niiden pohjalta rakentaa Windows 2008 -verkkoinfrastruktuuri (MCP/MCITP) -kurssin sisällölle sopiva harjoitustehtäväpaketti. Harjoitustehtävien toimivuus on tarkoitus testata käytännössä, jotta kurssin läpivienti onnistuu ongelmitta. Kurssille on alustavasti suunniteltu, että osallistujien määrä olisi 25 opiskelijaa. Heille kaikille materiaali käydään läpi samassa tahdissa, ja ensimmäisillä harjoitustunneilla osallistun opastukseen sekä mahdollisten ongelmatilanteiden ratkaisuun.

Insinööriyön alussa esittelen työssä käytettyjä ohjelmistoja sekä Windows Server 2008 -käyttöjärjestelmän keskeisimmät toiminnot. Esittelyn jälkeen tarkastellaan ohjelmistojen ja käyttöjärjestelmien asennusta sekä tutustutaan materiaalin harjoitustöihin.

Lopussa käydään läpi työssä esiintyneitä ongelmatilanteita sekä kurssilla käytävän materiaalin suunnitteluvaihe, mitä tehtäviä kurssilla tehdään ja mitkä tehtävät jätetään mahdollisesti pois kurssin sisällöstä.

2 Työkalut

Kaikki työssä käytetyt palvelinkoneet toteutettiin virtuaalisesti. Virtuaalikoneiden alustana toimi Microsoft Virtual PC 2007. Kaikki virtuaalikoneet olivat kokoonpanoltaan toisiaan vastaavat. Koneissa oli 512 MB RAM keskusmuistia (Random Access Memory) sekä 20 GB kovalevymuistia. Nämä asetukset olivat vähittäisvaatimukset koneisiin asennettavalle käyttöjärjestelmälle. Virtuaalikoneisiin asennettiin x86-bittinen Windows Server 2008 Enterprise -käyttöjärjestelmä täysillä vakioasetuksilla (Standard Full Installation).

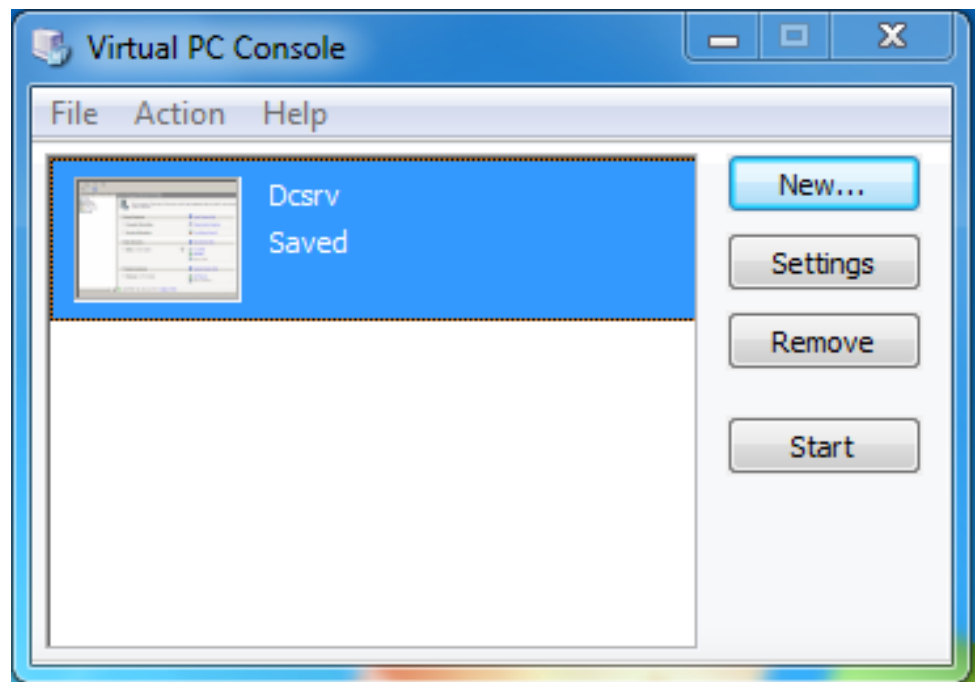
Työ toteutettiin täysin virtuaalisessa ympäristössä. Työssä käytettiin Microsoft Virtual PC 2007 -virtuaalikoneita, joihin jokaiseen oli asennettu Windows Server 2008 Enterprise (x86) -käyttöjärjestelmä. Virtuaalikoneita oli kolme kappaletta.

Työasema, jolla virtuaaliympäristö toteutettiin, käytti Windows 7 Ultimate (x64) -käyttöjärjestelmää. Koneessa oli Intel Core Duo E6750 (266 GHz) -prosessori, 2 GB RAM keskusmuistia sekä 500 GB kovalevymuistia, josta käytössä oli noin puolet.

2.1 Microsoft Virtual PC 2007

Virtual PC on virtualisointiohjelma Microsoft Windowsille. Sillä voidaan virtualisoida tietokoneita ja niihin liittyviä tietokonelaitteistoja. Virtual PC -virtuaalikoneisiin voidaan asentaa tuettuja Microsoft Windows -käyttöjärjestelmiä. Jotkin muut käyttöjärjestelmät, kuten Linux, saattavat toimia Virtual PC:n virtuaalikoneissa, mutta ne eivät ole virallisesti tuettuja käyttöjärjestelmiä. Samoin myös Virtual PC -asennus onnistuu muissakin kuin Microsoft-käyttöjärjestelmissä, mutta näihin ei ole olemassa virallista tukea. Virtuaalikoneet toimivat kuten normaalit tietokoneet, mutta ne eivät vie fyysistä tilaa ja niitä voidaan luoda yhdelle fyysiselle koneelle tai

palvelinkoneelle useita. Näin pystytään säästämään sekä tilaa että rahaa. Esimerkiksi käyttäjän tarvitessa työssään samanaikaisesti useita tietokoneita riittää, kun yhdelle tietokoneelle tai palvelinkoneelle luodaan useampia virtuaalitietokoneita. Käyttäjä ei täten tarvitse montaa fyysistä konetta, joiden osat maksavat ja jotka vievät fyysistä tilaa käyttäjän työpisiteellä. Ainoana rajoittavana tekijänä on, että kaikkien virtuaalikoneiden yhteenlasketun muistin määrä ei voi ylittää fyysisen tietokoneen muistin määrää, sillä virtuaalikone varaa itselleen muistin fyysisen koneen muistista. Tämä pätee sekä keskusmuistissa että kovalevymuistissa. Fyysinen tietokone varaa itselleen muistin määrästä sen verran, että se kykenee toimimaan normaalisti. Vapaaksi jäävä muisti on virtuaalikoneiden käytettävissä. [1.]



Kuva 1. Virtual PC Console -ikkuna

Virtuaalikoneet luodaan yksitellen Virtual PC Consolessa. Virtual PC Consolessa määritellään koneen asetukset kohta kerrallaan. Määrittelyjen jälkeen valmis kone näkyy Virtual PC Consolen ikkunassa, josta se käynnistetään ja josta sitä pystytään myös muokkaamaan. Käynnistetty kone tulee näkyviin uudessa ikkunassa ja näyttää samalta kuin tavallisen fyysisen koneen monitorinäkylässä.

Tämän jälkeen konetta käytetään kuin mitä tahansa fyysistä tietokonetta. Virtuaalikoneille voidaan asentaa kaikkia ohjelmia, joita tavalliselle tietokoneelle voidaan asentaa. [1.]

2.2 Windows Server 2008

Windows Server 2008 on helmikuussa 2008 ilmestynyt, palvelinkäyttöön tarkoitettu käyttöjärjestelmä. Se on Windows Server 2003 -käyttöjärjestelmän seuraaja, jonka ilmestymisestä oli ehtinyt kulua jo lähes viisi vuotta. Windows Server on rakennettu Windows NT 6.x:n pohjalta, kuten Windows Vista- sekä uusin Windows 7 -käyttöjärjestelmä. Tästä syystä se sisältää paljon samoja arkkitehtuurisia ja toiminnallisia ominaisuuksia kuin Windows Vista. Lähdekoodin pohjan samankaltaisuuden johdosta Windows Server 2008 sisältää samoja teknisiä, tieturva- sekä hallintaominaisuuksia, jotka tulivat uusina ominaisuuksina Windows Vista -käyttöjärjestelmään sen ilmestyttyä. [2.]

2.2.1 Ominaisuudet

Uudessa Windows Server -käyttöjärjestelmässä on paljon ominaisuuksien parannuksia edeltäjänsä nähden.

- Paranneltuun verkon pinoon (stack) on sisällytetty paikalliset IPv6, langattoman verkon, nopeuden ja turvallisuuden parannukset.
- Levykuva-asennuksia, tiedostojen takaisinsaantia, diagnosointi-, raportointi- ja monitorointityökaluja on parannettu.
- Uudet turvallisuusominaisuudet, kuten BitLocker ja ASLR.
- Paranneltuun Windows-palomuuri on lisätty oletuksena seuraavia turvallisuusominaisuuksia: .NET Framework 3.0 -tekniikka, Windows Communication Foundation, Microsoft Message Queuing ja Windows Workflow Foundation. [2.]

2.2.2 Palvelinroolit

Windows Server 2008 -käyttöjärjestelmässä on useita eri palvelinrooleja, joita muokkaamalla palvelimesta saadaan suurin mahdollinen hyöty. Windows Server 2008 käyttöjärjestelmässä on kaikki seuraavat palvelinroolit:

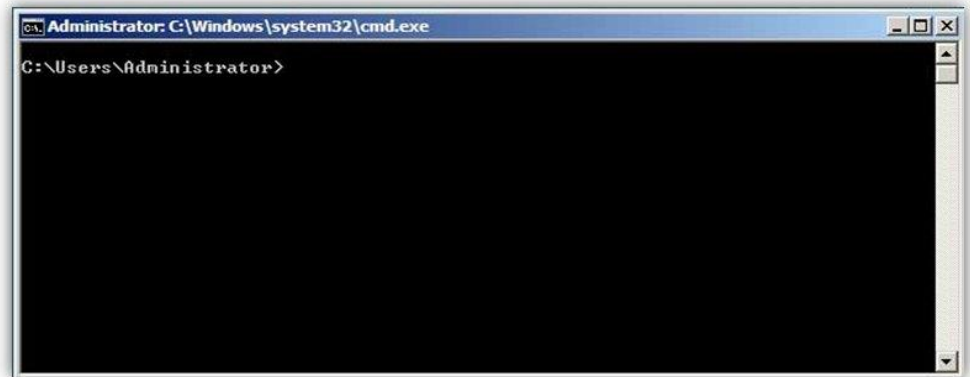
- Active Directory Certificate Services
- Active Directory Domain Services
- Active Directory Federation Services (ADFS)
- Active Directory Rights Management Services
- Application Server
- Dynamic Host Configuration Protocol (DHCP) Server
- DNS Server
- Fax Server
- File Services
- Hyper-V
- Network Policy and Access Services
- Print Services
- Universal Description
- Discovery and Integration (UDDI)
- Web Server (IIS)
- Windows Deployment Services (WDS).

Näiden pääpalvelinroolien alta löytyy useampia pienempiä rooliasetuksia, joita pystytään asentamaan palvelinkoneille yksittäin ilman koko palvelinroolipaketin asennusta. [3.]

2.2.3 Server Core

Windows Server 2008 sisältää vaihtoehtoisen asennusmahdollisuuden nimeltään Server Core. Server Core on asennuspaketti, joka on huomattavasti pienempi kuin Windows Server 2008 -oletusasennuspaketti. Siihen ei kuulu lainkaan Windows Explorer -komentoriviä. Kaikki palvelimen konfigurointi ja ylläpito suoritetaan komentoriviliittymästä (command prompt)

tai vaihtoehtoisesti kytkemällä kone toiseen tietokoneeseen, josta halutut konfiguroinnit voidaan suorittaa Windows Management Consolen avulla. [2.]



Kuva 2. Command prompt -komentoriviliittymä

Asennuspakettiin on kuitenkin liitetty muutamia toimintoja, kuten Windows Notepad sekä muutamia ohjauspaneelin ominaisuuksia, kuten Sijainti-asetukset. [2.]

Server Coreen ei ole liitetty .NET Framework-, Internet Explorer-, Windows PowerShell- eikä monia muitakaan ominaisuuksia, jotka eivät ole välttämättömiä Server Coren toiminnan kannalta. Palvelinkonetta, johon on asennettu käyttöjärjestelmä Server Core -ominaisuudella, voidaan käyttää ainoastaan yksinkertaisimmat perusroolit omaavana palvelimena. Näitä palvelinrooleja ovat Domain controller/Active Directory Domain Services, ADLDS (Active Directory Lightweight Directory Services), DNS-palvelin, DHCP-palvelin, tiedostopalvelin, tulostuspalvelin, Windows Media -palvelin, IIS 7web -palvelin sekä Hyper-V -virtuaalipalvelin. [2.]

2.2.4 Active Directory

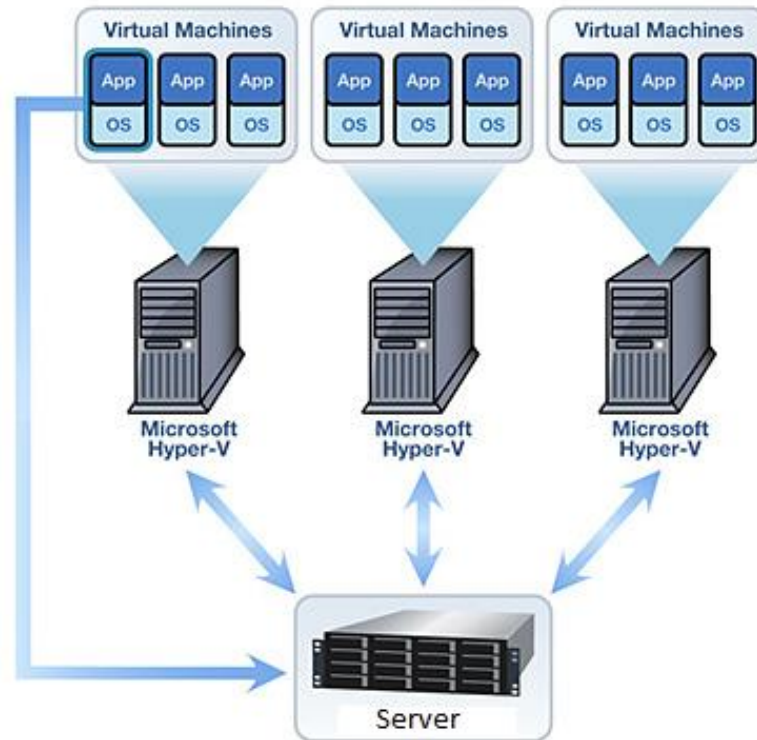
Active Directoryn rooleja on laajennettu tunnistus, sertifiointi ja oikeuksien hallinta Windows Server 2008 -käyttöjärjestelmässä. Aikaisemmassa Windows Server 2003 -versiossa palvelimen ylläpitäjä pystyi keskitetysti hallitsemaan tietokoneita, ryhmiä ja niiden käyttäjiä sekä asentamaan so-

velluksia usealle tietokoneelle samanaikaisesti. Nämä toiminnot ovat uudessa Windows 2008 Server -käyttöjärjestelmässä nimetty yhdeksi keskitetyksi ADDS-palveluksi (Active Directory Domain Services). Active Directoryyn on lisätty useita muita palveluja, joita ovat muun muassa ADFS (Active Directory Federation Services), ADLDS (Active Directory Lightweight Directory Services), ADAM (Active Directory Application Mode), ADCS (Active Directory Certificate Services) sekä ADRMS (Active Directory Rights Management Services). [2.]

Ylläpitäjällä on mahdollisuus uusien tunnistus- ja sertifiointipalveluiden ansiosta keskitetysti hallinnoida käyttäjätilejä sekä digitaalisia sertifikaatteja, jotka antavat käyttäjille oikeuden käyttää määriteltyjä palveluita ja järjestelmiä verkossa. [2.]

2.2.5 Hyper-V

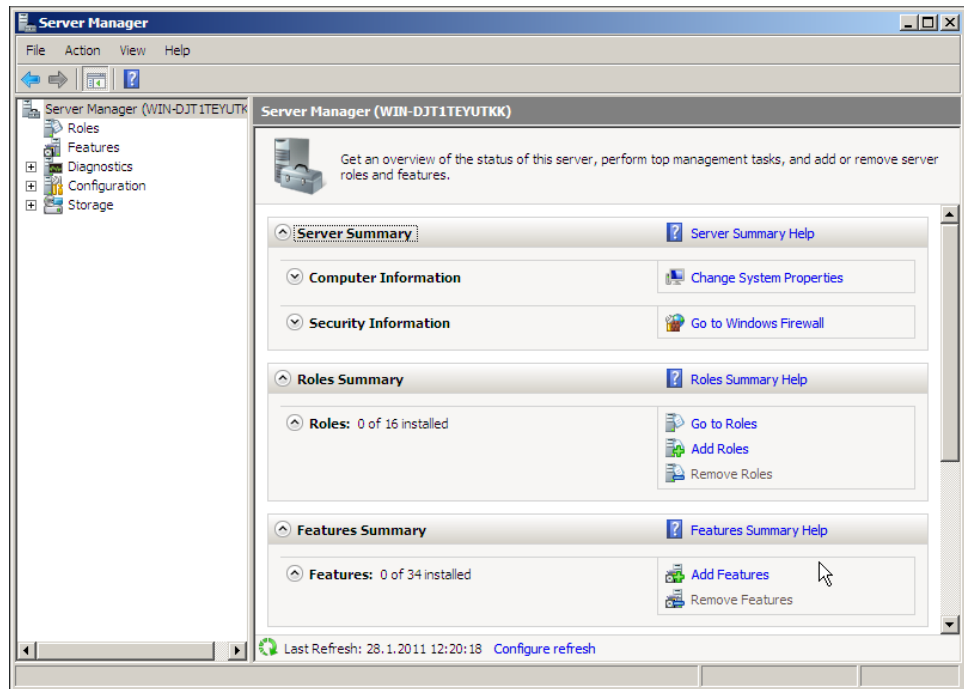
Hypervisorin pohjautuva Hyper-V-virtualisointijärjestelmä on keskeinen osa Microsoft-virtualisointia. Se virtualisoi palvelimen käyttöjärjestelmän kernel-tason. Toisin sanoen se pystyy jakamaan yhden fyysisen palvelinkoneen moneksi pienemmäksi tietokoneosioiksi, jotka toimivat itsenäisinä palvelimina. Virtualisoiuihin palvelimiin pystytään edelleen luomaan omia tietokoneosioita. [2.]



Kuva 3. Hyper-V –virtualisointi

2.2.6 Server Manager

Windows Server 2008 -käyttöjärjestelmään on sisällytetty uusi hallintatyökalu Server Manager. Se vastaa Manage Your Server- ja Security Configuration Wizard -palveluita, jota sisältyivät Windows Server 2003-käyttöjärjestelmään. Server Manager on paranneltu versio Windows Server 2003:ssa olleesta Configure My Server –palvelusta, joka käynnistyy oletuksena aina, kun Windows Server 2003 käynnistetään. Toisin kuin edeltäjässään, Server Manager on muutakin, kuin aloituspisteenä toimiva palvelu.



Kuva 4. Server Manager -aloitusikkuna

Server Manageriin on kerätty kaikki ne toimenpiteet, joita käyttäjät haluaisivat suorittaa palvelimelle, kuten etäkäyttöönoston asennus ja palvelinroolien lisäys. Käytännössä kaikki palvelimeen tehtävät konfiguroinnit eli muutostyöt pystytään tekemään suoraan Server Manager -ikkunan kautta. Server Manager on keskeisin osa Windows Server 2008 -palvelimen konfigurointia. [2.]

3 Suunnittelu

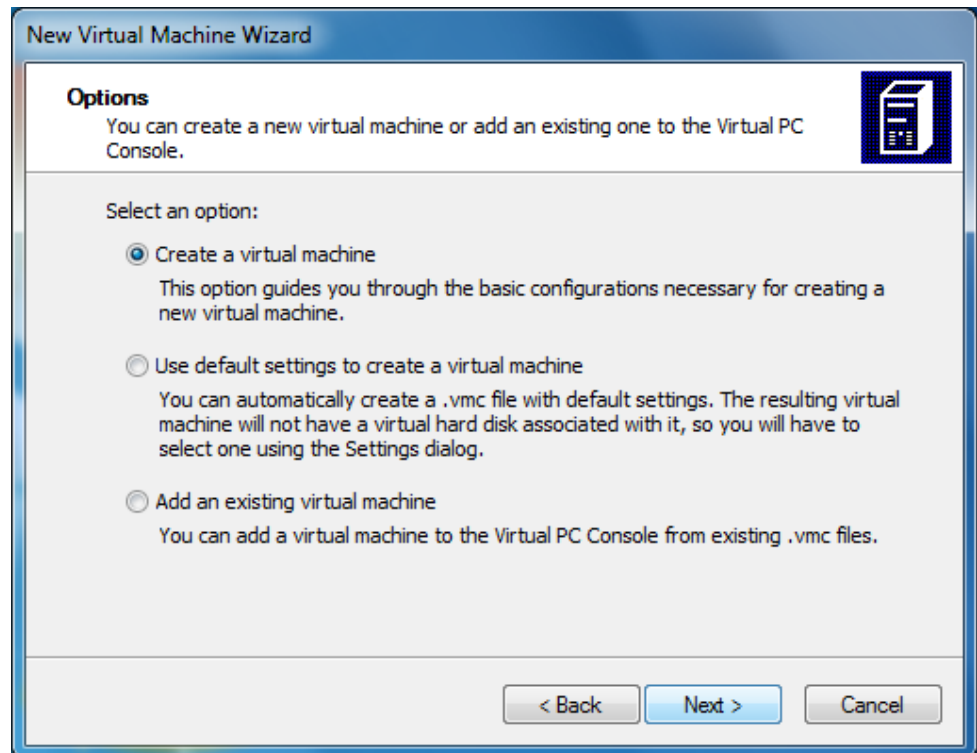
Tarkoituksena on, että kurssin alkaessa jokaisella opiskelijalla on käytössään kolme virtuaalikonetta, joiden kokoonpano on kaikissa sama ja ennalta määrätty. Koneet nimetään etukäteen jokaiselle samoiksi materiaaleissa annetuilla nimillä, erona ainoastaan koneen perässä oleva liukuva numerointi (1-25). Ensimmäinen virtuaalikone on nimetty Dcsrv#, toinen virtuaalikone on Boston# ja kolmas virtuaalikone on Binghampton#, joissa merkki # kuvaa numerointia.

Kaikkiin koneisiin asennetaan ennakkoon Windows Server 2008 -käyttöjärjestelmä perusasetuksilla. Koneisiin ei asenneta mitään muita ohjelmia, eikä käyttöjärjestelmään tehdä alustavia konfigurointeja. Opiskelijat eivät asenna käyttöjärjestelmiä itse vaan aloittavat työskentelyn valmiiksi asennetuilta koneilta. Materiaalin harjoitustehtävät käydään läpi ja tarkastetaan niiden toimivuus käytännössä. Mikäli materiaalin harjoitustehtävistä löytyy tehtäviä, jotka eivät sovellu kurssin virtuaaliympäristössä toteutettaviksi, jätetään ne pois lopullisesta kurssin harjoitustyömateriaalista. Kaikista mahdollisesti pois jätettävistä tehtävistä keskustellaan erikseen työtä ohjaavan opettajan kanssa.

4 Toteutus

4.1 Alustan valmistelu

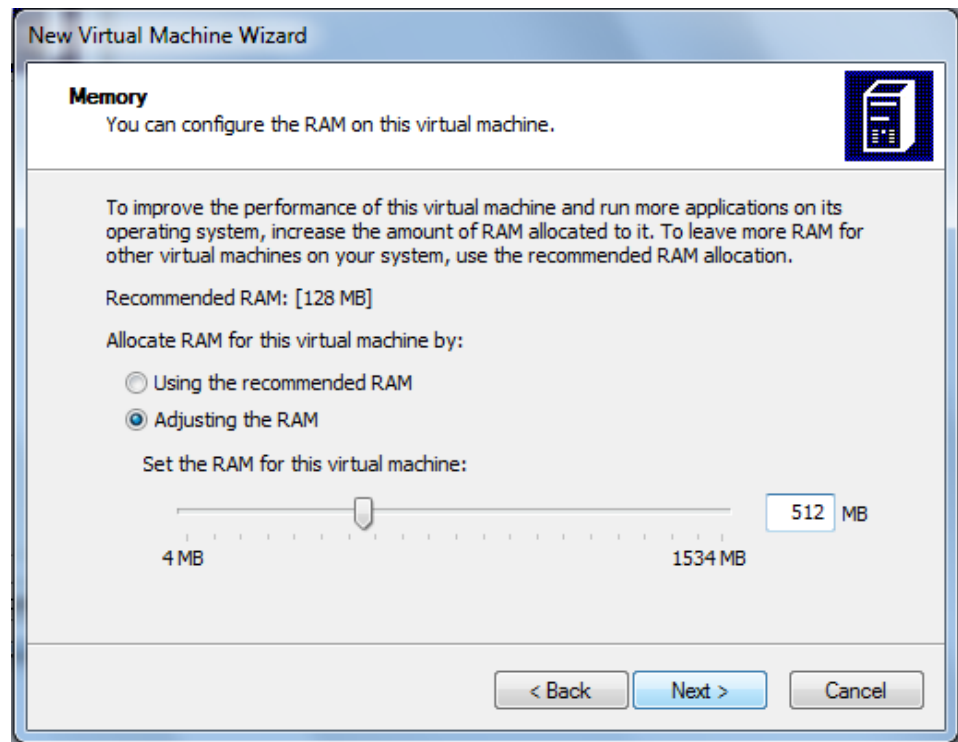
Alustana käytettävä Virtual PC asennettiin koneelle. Asennus suoritettiin ohjelman oletusasetuksilla. Virtual PC Console -ikkunassa luotiin tarvittavat virtuaalikoneet yksi kerrallaan.



Kuva 5. Virtual PC -virtuaalikoneen luonti

Koneet ja niiden kokoonpanot määriteltiin itse alusta alkaen käyttämättä ohjelman ehdottamia oletusasetuksia. Koneiden luonnissa määriteltiin ensin virtuaalikoneen nimi. Nimen määrittämisen jälkeen valittiin käytettävä käyttöjärjestelmä. Virtual PC antaa mahdollisuuden valita käytettävä käyttöjärjestelmä, mutta mikäli oikeaa käyttöjärjestelmää ei ole, listassa on käyttöjärjestelmäksi valittava Other (muu).

Koska käyttämäämme Windows Server 2008-käyttöjärjestelmää ei löytynyt, listalta valittiin määritelmäksi Other. Tämän jälkeen valittiin käytettävän keskusmuistin määrä.



Kuva 6. Virtuaalikoneen muistin koon määrittely

Alin mahdollinen muistin määrä, jolla järjestelmä toimii, oli 512 MB. Tämä valittiin myös käytettäväksi virtuaalikoneissa, jotta virtuaaliympäristöä pyörittävän tietokoneen muisti riittää kaikkien virtuaalikoneiden tarpeisiin. Muistin määrä rajattiin mahdollisimman vähäiseksi myös sen takia, että kurssille toteutettavat virtuaalikoneet eivät kuormittaisi liikaa kurssilla käytettävää alustaa. Keskusmuistin määrittelyn jälkeen koneille luotiin omat virtuaalikovalevymuistit. Kovalevymuistin määräksi valittiin niin ikään alin mahdollinen muistin määrä, joka oli 20 GB. Näiden määrittelyjen jälkeen virtuaalikone oli valmis käynnistettäväksi. Kaikki kolme konetta luotiin ennen koneiden käynnistystä.

Luotujen virtuaalikoneiden kokoonpanot:

Virtuaalikone1

- Nimi: Dcsrv
- Keskusmuisti: 512 MB
- Kovalevy muisti: 20 GB

Virtuaalikone2

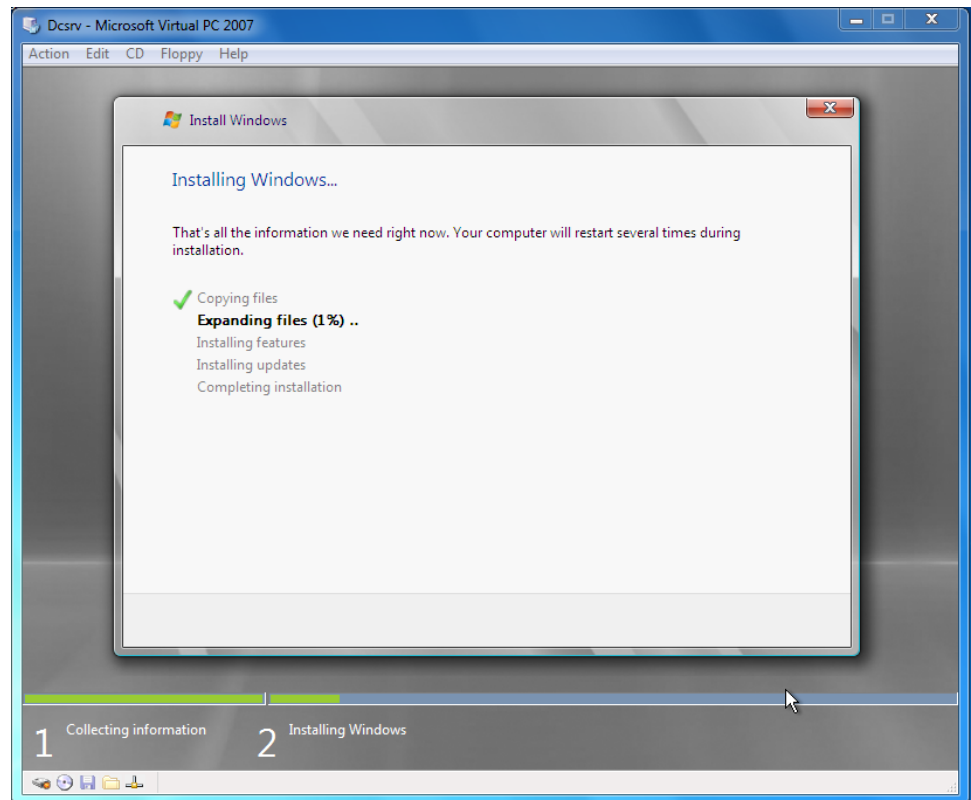
- Nimi: Boston
- Keskusmuisti: 512 MB
- Kovalevy muisti: 20 GB

Virtuaalikone3

- Nimi: Binghampton
- Keskusmuisti: 512 MB
- Kovalevy muisti: 20 GB

4.2 Windows Server 2008 -asennus

Kun kaikki virtuaalikoneet oli luotu, asennettiin jokaiseen x86-bittinen Windows Server 2008 Enterprise -käyttöjärjestelmä täysillä perusasetuksilla (Standard Full Installation). Käyttöjärjestelmät asennettiin käyttäen Windows Server 2008 -levy kuvaa.



Kuva 7. Windows Server 2008 -asennus virtuaalikoneelle

Käyttöjärjestelmän asentaminen koneelle vaati salasanan luomista. Tätä toimintoa ei voitu ohittaa, kuten tavallisissa tietokonekäyttöjärjestelmissä. Jokaiselle virtuaalikoneelle asetettiin sama salasana, jotta koneisiin kirjautuminen olisi mahdollisimman ongelmaton.

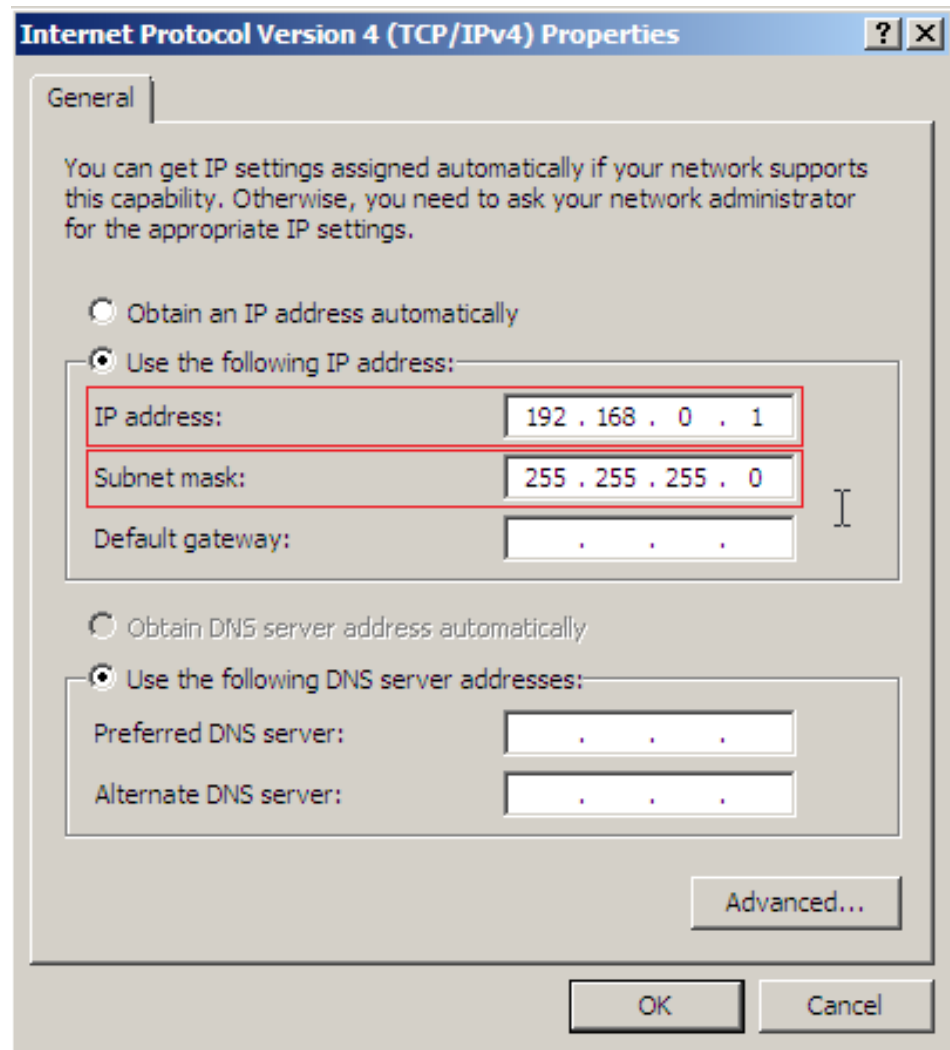
Koska käyttöjärjestelmä halutaan perusasetuksilla ilman alustavia palvelinrolien konfigurointia, käyttöjärjestelmä asennettiin oletusasetuksilla jokaiseen koneeseen ilman ylimääräisiä lisäasetuksia. Käyttöjärjestelmien asennus kesti noin 15-20 minuuttia jokaista konetta kohden. Kun käyttöjärjestelmät oli saatu asennettua, päästiin käymään läpi kurssille suunniteltua materiaalia.

4.3 Verkon luominen

Jotta koneet voisivat kommunikoida keskenään, oli niihin asetettava jokaiseen oma IP-osoite ja varmistettava yhteyksien toimivuus.

IP-osoite (Internet Protocol) on numerosarja, joka yksilöi jokaisen verkkoon kytketyn tietokoneen. IP-protokolla on alin yhtenäinen Internetin protokolla, ja kaikki verkon tietoliikenne kulkee IP-paketteina. IP-osoitteen perusteella IP-paketti löytää perille haluttuun osoitteeseen ja palauttaa samalla vastauksen, ovatko lähetetyt IP-paketit menneet perille. [5.]

IP-osoitteita on eri versiona. Yleisin käytössä oleva IP-osoitteiden versio on Ipv4 (Internet Protocol version 4), jossa IP-osoite on 32-bittinen. Tämä tarkoittaa, että erilaisia osoitteita on $4\,294\,967\,296$ kappaletta (2^{32}). IP-osoite on ilmaistu neljässä numeroiden sarjassa, esimerkiksi 192.168.0.0. Osoitteiden numerot kuitenkin päättyvät aina viimeistään numeroon 255. [6.]



Kuva 8. IP-osoitteen määrittäminen koneelle

Osoitteiden rajallisuuden vuoksi osoitekantaa on laajennettu Ipv6-versioon. Tässä osoite on 128-bittinen, jolloin osoitteiden määrä on paljon suurempi. Versioon on myös lisätty muita ominaisuuksia, joita Ipv4 ei sisältänyt. IPv6-osoitteet eivät myöskään näytä samalta kuin IPv4-osoitteet. IPv6-osoite jakautuu kahdeksaan heksadesimaalisarjaan, kuten esimerkiksi 2001:0db8:85a3:08d3:1319:8a2e:0370:7334. [7.]

Koneisiin asetettiin IP-osoitteet ohjeistuksen mukaisesti. Samalla koneissa käynnistettiin File share -toiminto. File share -toiminto mahdollistaa erilaisten tiedostopakettien jakamisen koneiden kesken.

IP-pakettien kulku varmistettiin lähettämällä ping-komento jokaisesta koneesta toisiin koneisiin. Ping-komento suoritetaan käyttöjärjestelmän

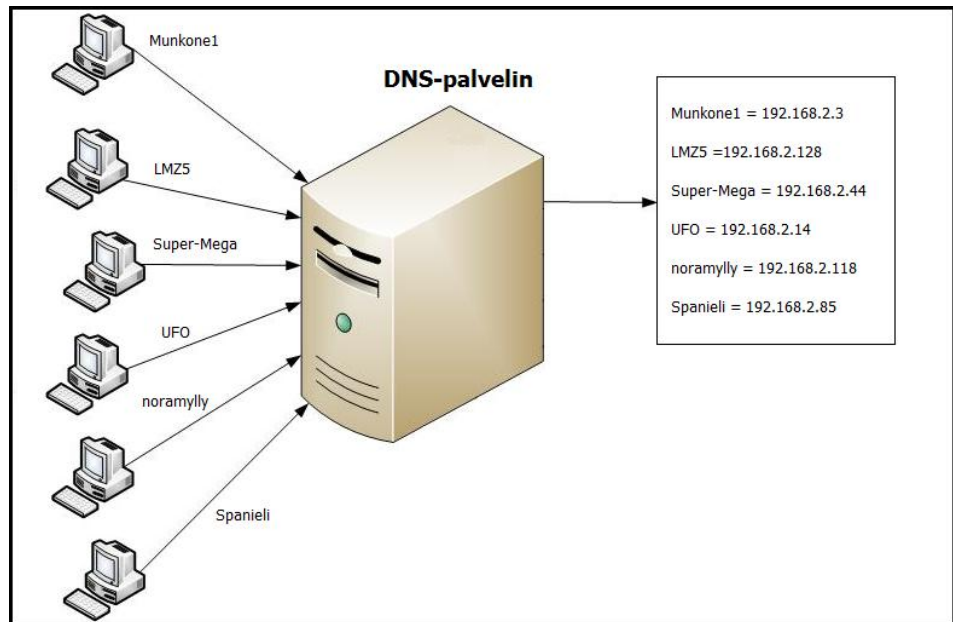
Command prompt t-ikkunassa. Ping-komento lähettää halutulle laitteelle ICMP (Internet Control Message Protocol) echo request -paketin, johon toinen tietokone vastaa omalla echo reply -paketilla. Näin saadaan varmistettua, että koneiden välinen linkki toimii.

Tämän jälkeen koneisiin asetetaan Network Discovery, joka etsii samassa verkossa olevia tietokoneita ja laitteita. Se myös kertoo, onko verkon muissa koneissa samaa tunnistustoimintoa käytössä. Tämä helpottaa esimerkiksi tiedostojen ja kirjoittimien jakamista verkossa. Network Discoveryn käyttöönoton jälkeen verrattiin Ipv4:n ja Ipv6:n eroja eri tilanteissa lähettämällä ping-komentoja IP-osoitteella sekä koneen nimellä. Ping-komento nimellä epäonnistui IPv4-protokollaa käytettäessä. Ipv6 tukee myös ping-komennon lähettämistä koneen nimellä. Tämä ominaisuus puuttuu kokonaan Ipv4-versiosta.

4.4 DNS-palvelin

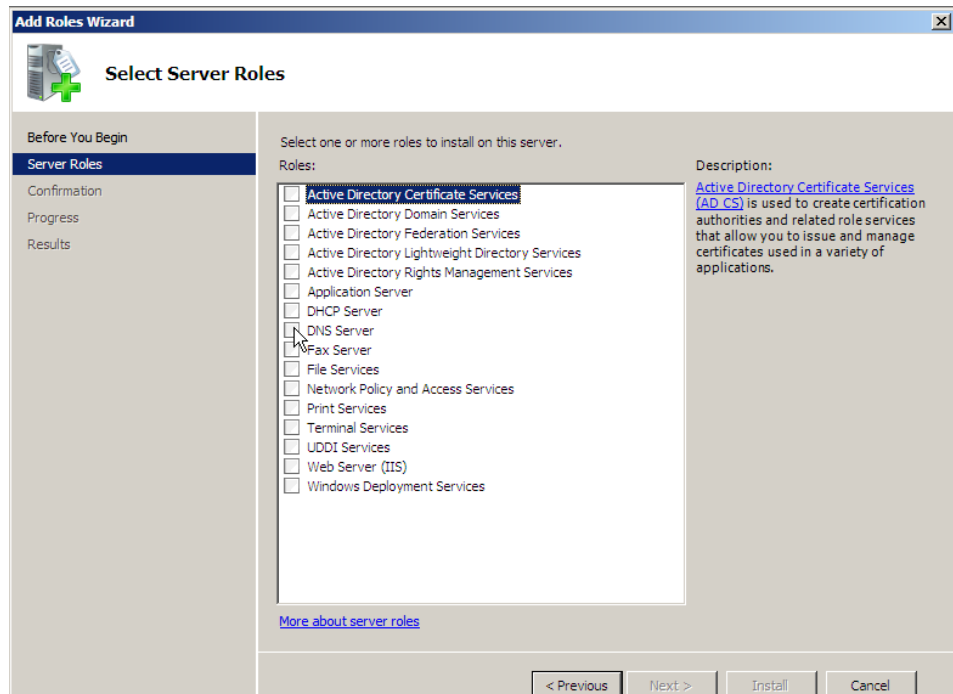
DNS eli Domain Name System on hierarkkinen nimeämisjärjestelmä jaettussa tietokannassa, joka muuntaa koneiden verkkotunnuksia IP-osoitteiksi. Esimerkiksi yksityisessä verkossa oleva DNS-nimipalvelin muuntaa laitteiden nimet numeeriseen muotoon ja pitää kirjaa verkossa olevista laitteista.

Se myös lähettää ylläpitämäänsä tietoa verkon muille koneille. DNS-palvelin toimii eräänlaisena puhelinluettelona, johon on listattu verkon koneiden nimet ja numeeriset tiedot. [8.]



Kuva 9. DNS-palvelimen toiminta

Kaikki palvelinroolien lisäykset tehdään Windows Server 2008 Server Manager -ikkunasta. Roolien luonti onnistui helposti ohjatulla Add Roles Wizardilla.



Kuva 10. DNS-palvelinroolin lisäys

Luotiin Dcsrv-koneella uusi toimialue (domain) nimeltä Nwtraders.msft, jossa Dcsrv toimii toimialueen ylläpitäjänä. Koneen nimi muuttui asetusten muuttamisen jälkeen muotoon dcsrv.nwtraders.msft, koska kone oli nyt osana toimialuetta. Samalla Dcsrv-koneesta tehtiin DNS-palvelin, joka pitää kirjaa verkon laitteiden nimistä ja osoitteista.

DNS-palvelimelle luotiin käyttäjäryhmä Domain Users. Luotuun ryhmään luotiin käyttäjätili ylläpitäjän oikeuksilla, jota tarvitaan myöhemmissä harjoitustehtävissä. Tilille annettiin nimi: patrik.sundgren.

Kun palvelu oli saatu toimintakuntoon, liitettiin muut virtuaalikoneet Boston ja Binghampton samaan toimialueeseen. Jotta toimialueeseen lisäys onnistuisi, oli koneiden Command prompt-ikkunaan kirjoitettava seuraavat komennot:

- netsh interface ip set dnsserver "local area connection" static 192.168.0.1
- netsh onterface ipv6 set dnsserver "local area connection" static fd00::1.

Nämä komennot konfiguroivat Boston- ja Binghampton-palvelinkoneet etsimään Nwtraders.msft-toimialuetta ja lähettämään kyselyn Dcsrv-palvelinkoneelle. Tämän jälkeen valittiin haluttu toimialue, joka tässä tapauksessa oli Nwtraders.msft. Koneet lisättiin onnistuneesti toimialueeseen. Dcsrv-kone tunnisti verkosta löytyneet uudet laitteet, jotka oli lisätty toimialueeseen.

4.5 GlobalNames Zone

GlobalNames Zone eli GNZ on Microsoftin uusi toiminto, jonka tarkoituksena on korvata Microsoftin vanha NetBIOS tietokonenimipalveluna toimiva WINS-palvelinjärjestelmä. WINS toimii siis vastaavanlaisena nimipalvelimena NetBIOS-nimille kuin DNS-palvelin toimialuenimille. Sen tehtävänä on olla keskitetty nimipalvelu verkko-osoitteille.

Koska WINS-palvelua käyttävät eivät voi siirtyä helposti uuteen, esimerkiksi DNS-palvelun piiriin, on GNZ tehty helpottamaan tätä siirtymistä. Koska GNZ-palvelu vastaa WINS-palvelua, voidaan siirtyä käyttämään DNS-palvelua joustavasti menettämättä jo olemassa olevia tietokantoja. [9.]

Dcsrv-koneelle luotiin Forward Lookup Zone -alue nimeltä GlobalNames. Alueeseen lisättiin tietue jolle annettiin nimi mail. Tietue mail näkyy GlobalNames Zones -välilehdellä. Tietueen toimivuus testattiin lähettämällä Boston koneesta komento ping mail. Komento palautti onnistuneen paluuviestin.

Dcsrv-koneelle luotiin levyosio, jonka toimintaa muokattiin niin, että se toimii Nwtraders.msft-alueen tiedon varastointiosiona. Levyosiolle tallentuvat kaikki verkon laitteiden tiedot, jotka DNS-palvelin löytää ja tallentaa. Osio luotiin command prompt -ikkunassa seuraavalla komennolla:

- `dnscmd . /createdirectorypartition DNSpartitionA.nwtraders.msft`

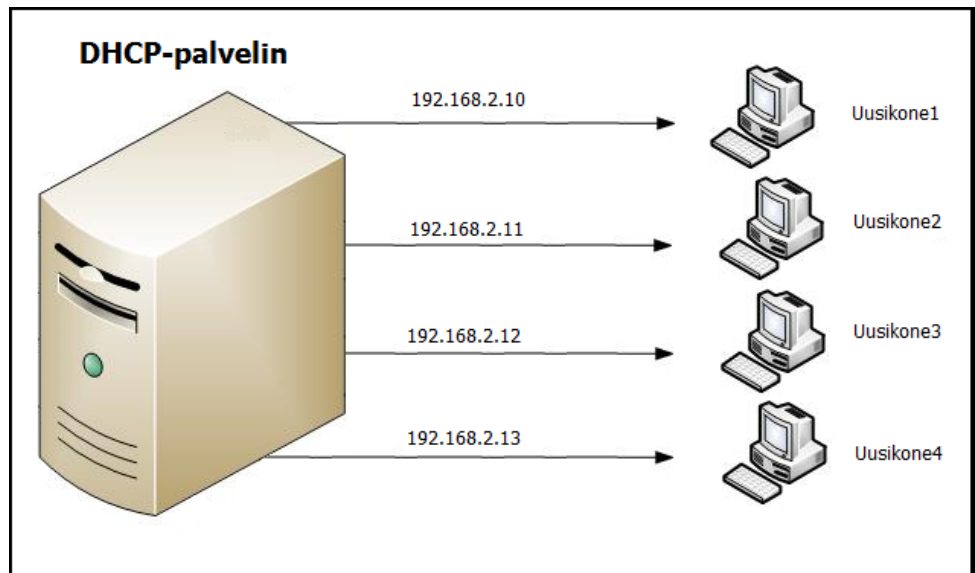
Osion luonnin jälkeen muokattiin kansion tietoja niin, että se toimii Nwtraders.msft-toimialueen tiedon varastointiosiona. Osioon lisättiin myös toiminto, joka mahdollistaa toimialueella olevien toisten DNS-palvelimien tietojen varastoinnin. Näin ollen, jos muita DNS-palvelimia lisätään toimialueelle, voidaan niiden tiedot lisätä yhdellä komennolla.

Boston-koneelle luotiin toissijainen DNS-alue, joka liitettiin Dcsrv-palvelimella toimivaan Nwtraders.msft-toimialueeseen. Dcsrv-palvelimella toissijaiselle alueelle sallittiin lupa toimia Nwtraders.msft-toimialueella. Toissijaiselle toimialueelle lisättiin myös toiminto, joka salli Zone-tietojen lähettämisen Dcsrv-palvelimen GlobalNames-alueelle.

Jotta Boston-palvelimelle pystyttäisiin lisäämään Dcsrv-palvelimen nimi-palvelimen rekisteritiedot, piti Dcsrv-palvelimen asetuksia muuttaa siten, että se myöntää Boston-palvelimen toissijaisen alueen käyttää sen nimi-palvelimen rekisteritietoja. Kun muutokset oli tehty, näkyi Boston-palvelimen tiedoissa myös Dcsrv-palvelimen nimirekisteri.

4.6 DHCP-palvelin

DHCP (Dynamic Host Configuration Protocol) on protokolla, jonka tehtävänä on jakaa toimiva IP-osoite palvelimen alaiseen lähiverkkoon liitettäville koneille. Jotta kone voi olla osana lähiverkkoa, pitää sen IP-osoitteen kuulua samaan verkko-osoiteavaruuteen.

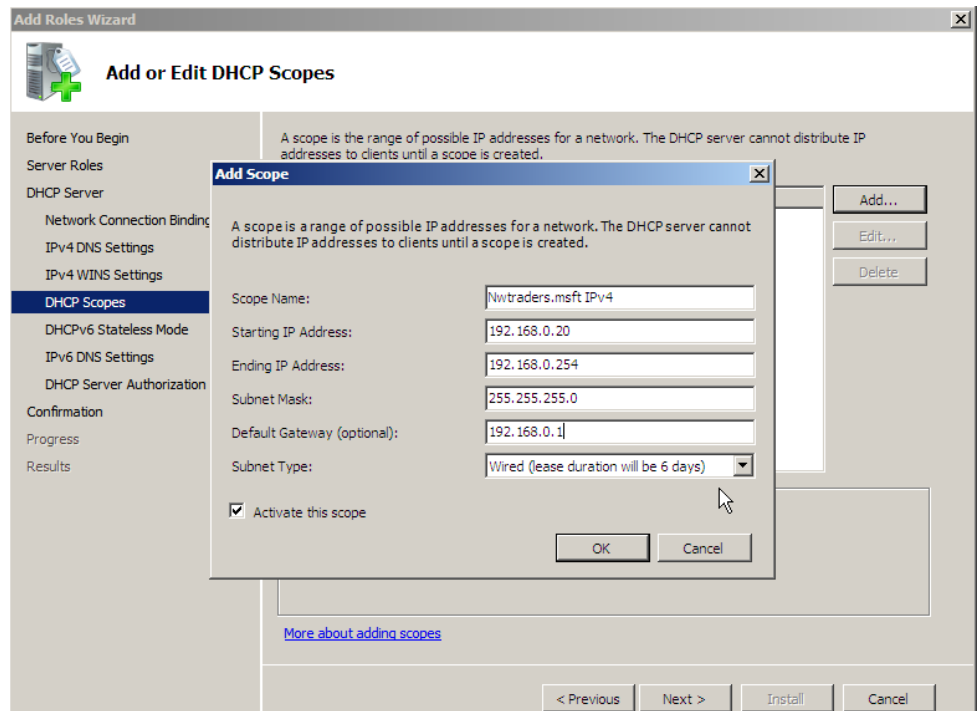


Kuva 11. DHCP-palvelimen toiminta

DHCP-palvelin voi sopivien IP-osoitteiden lisäksi jakaa myös muita tietoja, kuten esimerkiksi nimipalvelimen tai oletusyhdyskäytävän (default gateway) IP-osoitteen tai muita oleellisia verkko-osoitetietoja. DHCP-protokolla ei kuitenkaan reitity laitteilta toisille. Kaikkien laitteiden on hankittava DHCP-palvelimelta saatavat tiedot suoraan DHCP-palvelimelta. [10.]

Dcsrv-koneeseen lisättiin DHCP-palvelinrooli. Koneeseen määriteltiin verkko-osoiteavaruus, jonka sisältä DHCP-palvelin jakaa verkko-osoitteita. Koneeseen asetettiin seuraavat määritelmät:

- verkko-osoiteavaruuden nimi: Nwtraders.msft IPv4
- ensimmäinen IP-osoite: 192.168.0.20
- viimeinen IP-osoite: 192.168.0.254
- aliverkkomaski: 255.255.255.0
- default gateway: 192.168.0.1.



Kuva 12. DHCP-palvelimen määrittäminen

Jotta DHCP-palvelimen tiedot siirtyisivät palvelimelta verkon Boston- ja Binghampton-koneisiin, oli näissä koneissa kytkettävä DHCP-palvelu päälle. Palvelu saatiin toimintaan seuraavilla komennoilla:

- netsh interface ipv4 set address "local area connection" dhcp
- netsh interface ipv4 set dnsserver "local area connection" dhcp.

Näiden komentojen jälkeen tarkastettiin Boston- ja Binghampton-palvelinkoneilta ip config -komennolla, ovatko osoitetiedot päivittyneet koneisiin.

Dcsrv-palvelinkoneelle asetettiin DHCP-rajaus osoitteille, jotka ovat osoitteiden 192.168.0.199 ja 192.168.0.211 välillä. Nämä osoitteet ovat DHCP-palvelimen jakamien osoitteiden ulkopuolella, eikä niitä jaeta eteenpäin. Näin tehdään, jos halutaan varata tiettyjä IP-osoitteita toimialueen muita palveluita varten.

4.7 Telnet

Telnet on verkkoympäristössä päätelaitteiden välille luotavien yhteyksien protokolla. Telnet-yhteyttä käytetään esimerkiksi oltaessa yhteydessä palvelimeen tavalliselta tietokoneelta. Telnet on yksinkertainen protokolla, jonka ansiosta sen käyttö on hyvin laajaa. Telnetin heikkouksia ovat muun muassa se, ettei se salaa lainkaan liikennettä ja sen tietoturva on erittäin alhainen. Näistä syistä esimerkiksi sille asetetut salasana ovat nähtävissä selväkielisenä, mikäli verkkoliikennettä satutaan seuraamaan. [11.]

Boston-palvelinkoneelle asennettiin Telnet palvelin- ja tilaaja-asetukset palvelimen Server Manager -ikkunasta. Asennuksen jälkeen Telnet-asetuksiin määriteltiin Telnet-ryhmä, joka nimettiin Domain Admins nimeksi.

Dcsrv-koneelle tehtiin GPO (Group Policy)- sekä IPsec Policy (IP Security Architecture) -toimintamallit, joiden tarkoituksena oli toimia salauksena luoduille Telnet-yhteyksille. Toimialueelle luotiin GPO-toimintamalli, joka nimettiin IPsec GPO.

Tämän sisälle luotiin uusi IPsec-toimintamalli, jonka asetuksiin tehtiin seuraavat muutokset:

- IPsec nimi: Nwtraders IPsec Policy
- Kuvaus: This IPsec Policy encrypts Telnet traffic.

IPsec-toimintamalliin määriteltiin haluttavat asetukset, jotta muodostettavat Telnet-yhteydet olisivat salattuja. Asetukset nimettiin seuraavasti:

- Require High Authentication and Encryption
 - Edellytetään korkeaa oikeuksien todennusta sekä salausta
- Require AH authentication and 3DES encryption
 - Edellytetään IPsec AH (Authentication Header) todennusta sekä Triple-DES salausta.

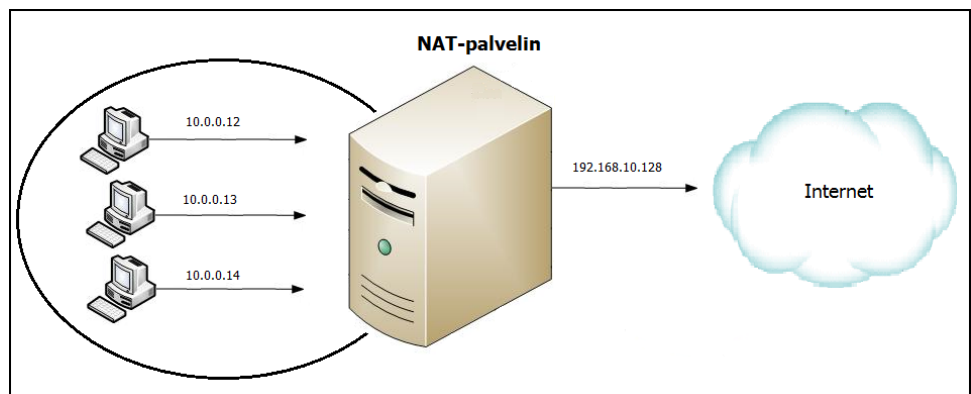
Seuraavaksi testattiin Telnet-yhteyksien toimivuutta. Boston-koneen command prompt-ikkunaan annettiin seuraava komento:

- telnet Binghampton.

Telnet-yhteys Binghampton-palvelinkoneen omaan Telnet-palvelimeen onnistui ongelmitta.

4.8 NAT-palvelin

NAT eli Network Address Translation on toiminto, jolla saadaan muunneltua verkon koneiden IP-osoitteita siirryttäessä toimialueelta toiselle. Esimerkiksi jos yhtiön omassa yksityisessä lähiverkossa on 50 tietokoneita, joiden kuluttamaa IP-osoiteavaruutta halutaan rajoittaa ja toisaalta halutaan estää ulkopuolisia näkemästä yhtiön IP-osoiteavaruutta, voidaan ottaa käyttöön NAT pitämään oman yksityisen lähiverkon osoitteet erillään verkon ulkopuolisista osoitteista. Eli kaikki koneet, jotka käyttävät lähiverkon ulkopuolisia verkkoja, käyttävät yhtä NAT- toiminnolla määriteltyä IP-osoitetta. [12.]



Kuva 14. NAT-palvelimen toiminta

Dcsrv-koneelle lisättiin NAT-palvelinrooli Server Managerin verkkoasetuksista. Tämän jälkeen verkossa olevat koneet Boston ja Binghampton oli saatava uuden IP-osoitetoimintaperiaatteen piiriin, joten niiden IP-osoitteet oli uusittava.

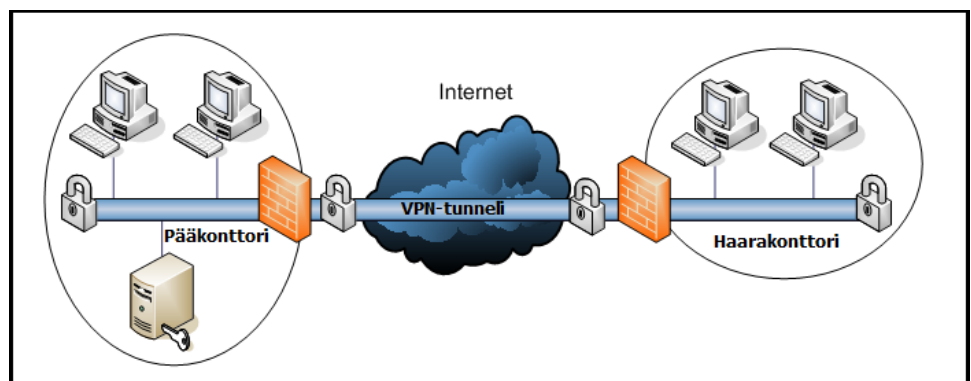
Tämä tehtiin molempien koneiden command prompt-ikkunassa seuraavilla komennoilla:

- ipconfig /release
- ipconfig /renew.

Näillä komennoilla ensin vapautettiin IP-osoite, jonka jälkeen kone haki uuden osoitteen NAT DHCP -palvelimelta. Tarkastettiin, että koneiden IP-osoitteet olivat asetuksien mukaiset.

4.9 VPN-palvelin

VPN (Virtual Private Network) on tapa, jolla yksityisiä lähiverkkoja pystytään yhdistämään internetin yli ja pitämään niiden välinen liikenne salatuna. Esimerkiksi, jos yrityksellä on useampia konttoreita ja niiden sisäiset verkot halutaan yhdistää, onnistuu se VPN-ratkaisulla. Kahden tai useamman yksityisen verkon välille luodaan niin sanottu VPN-tunneli, joka toimii yhteyskäytävänä verkkojen välillä. [13.]



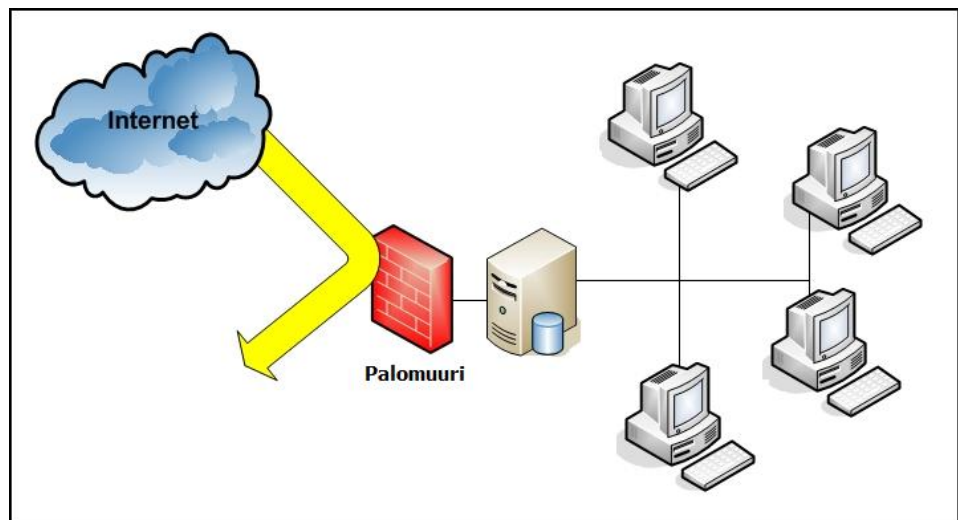
Kuva 15. Esimerkki VPN-tunnelista yrityksen toimipisteiden välillä

Dcsrv-palvelinkoneen Server Manager -ikkunan kautta luotiin uusi käyttäjäryhmä nimeltä VPN Users. Tämän lisäksi luotiin käyttäjätili nimeltä VPNUser, jolle annettiin harjoitustehtävän ohjeistuksen mukaan monimutkainen salasana. Käyttäjätili VPNUser liitettiin aikaisemmin luotuun Domain Users-ryhmään ja juuri luotuun VPN Users -ryhmään. Dcsrv-palvelinkoneelle lisättiin VPN-palvelinrooli.

Tämän jälkeen siirryttiin Boston-palvelinkoneelle ja luotiin siitä VPN client -kone, jolla otettiin yhteys Dcsrv-palvelinkoneelle luotuu VPN-palveluun. Boston-koneen asetuksista otettiin käyttöön VPN ja asetettiin Dcsrv-palvelinkoneen yhteysosoite sen määränpääksi. Tämän jälkeen testattiin luodun VPN-tunnelin yhteyttä lähettämällä ping-komento Dcsrv-palvelinkoneen yhteysosoitteseen. Ping-komento palautui onnistuneesti.

4.10 Palomuuuri

Palomuuuri on laite tai ohjelmisto, jonka tehtävänä on eristää ja suodattaa suojattavan verkon tai tietokoneen sekä vaaralliseksi luokiteltavan suojaamattoman verkon välisiä yhteyksiä. Useimmiten palomuuria tarvitaan avoimesta internet yhteydestä tulevilta hyökkäyksiltä suojautumista varten. Palomuurilaitteissa ja ohjelmistoissa on sääntöjä, joilla voidaan sisään tulevista liikenteestä suodattaa pois kaikki ei-toivottu liikenne.



Kuva 16. Palomuuuri torjuu ei-toivotun liikenteen internetistä

Nykyisin on yleistä, että suodatetaan myös jossain määrin ulospäin suuntautuvaa liikennettä. Varsinkin yritykset suodattavat oman sisäisestä verkosta lähtevän liikenteen tietosuojan turvaamiseksi. [14.]

Seuraavissa materiaalin harjoituksissa ei erikseen mainittu, mille koneelle kyseisiä konfigurointeja tulisi tehdä, joten päädyin tekemään muutokset tähänastisissa tehtävissä koneiden välisen lähiverkon keskuspalvelinkoneena toimineelle Dcsrv-palvelinkoneelle. Tehtävät tehtiin Dcsrv-palvelinkoneelle myös sen takia, että siihen oli jo ennakkoon lisätty Telnet-palvelinrooli, jonka lisäystä edellytettiin tehtävien alussa.

Koska Telnet-roolia ei tarvinnut lisätä Dcsrv-palvelinkoneelle, siirryttiin suoraan Windows-palomuurin lisäämiseen Telnet-palvelimen roolisääntöihin. Palomuurin toiminta varmennettiin yrittämällä sulkea toiminto Telnet-yhteyden kautta toiselta koneelta. Palomuuuri esti kyseisen toimenpiteen ja sulkemisyritys epäonnistui. Palomuuuri toimi oikein.

Seuraavassa osiossa lisättiin palvelinkoneelle myös ulkopuolelle lähtevän liikenteen suodatus. Suodatuksen tarkoituksena oli kieltää Internet Explorer -selaimen internetyhteyden luomisyhteykset. Palvelinkoneen palomuuriasetuksiin lisättiin toiminto, joka estää sovelluksen internetyhteyden.

Yhteyden toimimattomuutta oli tarkoitus testata yrittämällä siirtyä Internet Explorer -selaimella osoitteeseen <http://www.microsoft.com>, mutta koska internetyhteyttä ei ollut virtuaalikoneissa, tätä ei pystytty varmentamaan. Tämän jälkeen lisättiin vielä uusi rooli, joka antaa Internet Explorer-selaimelle oikeuden käyttää internettiä. Tässä kohtaa harjoitusta Internet Explorerilla yritettäisiin uudelleen siirtymistä edellä mainittuun osoitteeseen. Tätä ei myöskään pystytty testaamaan internetyhteyden puuttuessa. Vaikka kurssilla käytettävillä koneilla ei ole internetyhteyttä, harjoitus päätettiin kuitenkin jättää kurssin harjoitustyöksi.

4.11 DHCP NAP

NAP (Network Access Protection) on toiminto, jolla pystytään lisäämään verkon turvallisuutta asettamalla verkossa oleville koneille turvallisuus-ehdot.

NAP mahdollistaa turvallisuuteen liittyvien vähittäisvaatimusten asettamisen verkon ylläpitäjän toimesta. Määritelmänä voi olla muun muassa tietyt käyttöjärjestelmä-, ohjelmisto- tai virustorjuntapäivitykset.

Ilman vaadittuja päivityksiä koneelta evätään pääsy koko verkkoon tai sen tiettyihin osiin. Jos koneessa on kaikki vaaditut päivitykset, on käyttäjällä verkon koko käytettävyys. NAP on otettu ensi kertaa käyttöön Windows Server 2008 -käyttöjärjestelmässä. [15.]

Tehtävänä oli lisätä verkon palvelimelle DHCP- ja NAP-palvelinroolit. Muutokset oli tarkoitus tehdä Dcsrv-palvelinkoneelle. Koska Dcsrv-palvelinkoneelle oli jo aikaisemmassa harjoitustehtävässä lisätty DHCP-palvelinrooli, ei tämän lisääminen ollut tarpeellista. NAP-palveluun tarvittava toimialue saatiin lisättyä DHCP-palvelinasetuksista DHCP Scopes -sivulta.

Alue sai seuraavat määritelmät:

- Nimi: NAP Clients
- IP-osoiteväli: 192.168.1.10 – 192.168.1.100
- Aliverkkomaski: 255.255.255.0
- Default Gateway: 192.168.1.1.

Kun toimialue oli saatu määriteltyä, avattiin Server Managerin Add Roles-valikosta Configure NAP. NAP-asetukset määriteltiin siten, että NAP otettiin käyttöön DHCP-palvelimessa perusasetuksilla ja DHCP-palvelimen nimi olisi Dcsrv. Samalla Dcsrv-palvelinkoneen IP-osoite määriteltiin verkkoon hyväksytyksi osoitteeksi. Kun NAP-palvelu oli saatu toimintavalmiuteen, lisättiin siihen haluttuja toimintatapoja eli sääntöjä, joita edellytettiin verkon muilta koneilta.

Ensin asetuksiin lisättiin sääntö, joka pakottaa NAP-toiminnon käyttöön-oton verkkoon liitetyiltä koneilta. Mikäli kone ei vastaa pakotteeseen tai sen lähettäminen ei onnistu, asetetaan kyseinen kone karanteeniin. Kun asetukset olivat valmiit, kokeiltiin niiden toimivuutta lisäämällä Boston-palvelinkoneeseen NAP-palvelu ja uusimalla sen IP-osoite.

Tämän jälkeen tarkasteltiin command prompt -ikkunassa verkon NAP-asetuksia ja lähetettiin ping-komento Dcsrv-palvelinkoneen IP-osoitteeseen yhteyden varmistamiseksi. Seuraavaksi lähetettiin ping-komento NAP-palveluun määriteltyyn default gateway-osoitteeseen.

Heti ping-komennon lähettämisen jälkeen kone ilmoitti, ettei siinä ole yhteyden luomiseksi vaadittua virussuojausta. Tämä määritelmä tuli lisättyjen NAP-perusasetuksien mukana. NAP-asetuksiin pystytään lisäämään ehtoja aina, kun sellainen koetaan tarpeelliseksi. Jotta Boston-palvelinkone voisi ottaa yhteyden NAP-palveluun määriteltyyn default gateway -osoitteeseen, näitä asetuksia oli muutettava. NAP-asetuksia korjattiin siten, että niistä poistettiin virustorjuntaohjelman edellytys.

Boston-palvelinkoneelta yritettiin uudestaan lähettää ping-komento NAP default gateway -osoitteeseen. Tämän asetuksen poistamisen jälkeen ping-komento palautui onnistuneesti.

4.12 WSUS

WSUS (Windows Server Update Service) on palvelu, jolla pystytään päivittämään Microsoft Windows käyttöjärjestelmiä ja muita Microsoft-ohjelmistoja keskitetysti. WSUS on paikallisesti hallinnoitava palvelu, jonka avulla verkon ylläpitäjä pystyy jakamaan verkon hallinnoitaville laitteille tarvittavia päivityksiä ja hotfix-korjauksia Automatic Updates -palvelun kautta. Jos esimerkiksi yhtiön verkossa huomataan tietyllä ohjelmiston tai käyttöjärjestelmän päivityksellä korjattavissa oleva virhe, pystyy ylläpitäjä lisäämään päivityksen WSUS-palvelun kautta asentumaan kaikkiin hallinnoitaviin koneisiin. Tällöin vika saadaan korjattua mahdollisimman nopeasti.[16.]

WSUS piti erikseen ladata internetistä Microsoftin sivuilta <http://www.microsoft.com/wsus>. Ladattu lisäosa asennettiin Dcsrv-palvelinkoneelle, joka toimii verkon päähallintakoneena. Asennuksen jälkeen Dcsrv-palvelikoneeseen lisättiin WSUS-palvelinrooli.

WSUS-asetuksiin määriteltiin päivitysten oletussijainniksi Dcsrv-palvelin, jonka kautta verkon muut koneet saavat tarvittavat käyttöjärjestelmäpäivitykset. Päivitysten latausasetuksia muutettiin siten, että verkon laitteet lataavat päivitykset ja ilmoittavat käyttäjälle että ne on asennettava.

Toimivuutta testattiin lisäämällä päivityksiä Boston-palvelinkoneelle. Boston-palvelinkone ilmoitti saaduista päivityksistä reilun 5 minuutin jälkeen asetusten lisäämisestä.

4.13 Lisäasetuksia

Materiaalin loppupuolella olevat harjoitustehtävät olivat lähinnä pieniä lisäyksiä ominaisuuksiin ja palvelinten toiminnan hienosäätöä. Osa harjoitustehtävistä päätettiin jättää pois niiden ollessa tarpeettomia kurssin onnistumisen kannalta.

Osa harjoituksista ei pystyttäisi toteuttamaan virtuaaliympäristössä, kuten verkkokirjoittimien hallinnointitehtävät. Jotain tehtäviä haluttiin kuitenkin jättää, jotta tulevaisuudessa palvelinten kanssa työskentelevät opiskelijat tietäisivät, miten ongelmatilanteiden selvittämistä auttavia ominaisuuksia voidaan lisätä palvelinkoneisiin.

4.13.1 Tietojen kirjaus

Dcsrv-palvelinkoneelle lisättiin Windows Event Collector Service, jonka tehtävänä on kerätä ja kirjata tietoja palvelimen toiminnasta. Tämä helpottaa ongelmatilanteiden selvityksessä, sillä kirjaustiedostoista voidaan vikatilanteiden sattuessa tarkistaa, mitä palvelinkoneelle on tehty ja mitä muutoksia sen toiminnassa on tapahtunut. Tämän jälkeen lisättiin Boston-palvelinkoneelle sen omien kirjaustiedostojen edelleenlähetys Dcsrv-palvelinkoneelle. Näin verkon muiden palvelinkoneiden kirjaustiedostoja pystytään seuraamaan keskitetysti.

Boston-palvelinkoneen kellonaikaa ja päivämäärää muutettiin. Tämän jälkeen tarkastettiin, tallentuiko sen omaan kirjaustiedostoon tehtyjen muutosten tiedot. Kun tiedot oli tarkastettu, siirryttiin Dcsrv-palvelinkoneelle ja tarkastettiin sen vastaanottamat kirjaustiedot.

Kirjaustietojen saapuminen Dcsrv-palvelinkoneelle kesti muutaman minuutin. Tiedoston tiedoista näkyi Boston-palvelinkoneelle tehdyt muutokset.

4.13.2 Tiedostojen salaus

Dcsrv-palvelinkoneelle tehtiin kaksi uutta käyttäjätiliä EFSUser sekä DRA. Molemmat liitettiin Domain Admins -ryhmään. Koneelle kirjauduttiin EFSUser-käyttäjänä. Koneelle luotiin tekstitiedosto, jolle annettiin nimi Encrypted. Tiedosto muutettiin salattuun muotoon tiedoston asetuksista. Tämän jälkeen kirjauduttiin uudestaan koneelle DRA-käyttäjätillillä. DRA-käyttäjänä yritettiin avata EFSUserin salaamaa tekstitiedostoa. DRA-käyttäjätillille ei oltu määritelty oikeuksia tiedostoon, joten kone ilmoitti ettei tiedoston käyttöön ole oikeuksia.

4.13.3 Kansioden jakaminen

Dcsrv- ja Boston palvelinkoneille luotiin File Service- ja Distributed File System -palvelinroolit. Dcsrv-palvelinkoneelle luotiin DFS-nimialue, jolle annettiin nimi Public. Dcsrv-palvelinkoneelle lisättiin asetuksiin tieto, että DFS-nimialueeseen kuuluu myös Boston-palvelinkone. Dcsrv-palvelinkoneen C-asemalle luotiin Files-niminen kansio, joka jaettiin nimialueen koneiden kesken. Tarkoituksena oli saada jaettu kansio toimimaan siten, että kaikki sinne lisätyt tiedostot kopioituisivat suoraan Boston-palvelinkoneelle vastaavaan kansioon. Jotta sama kansio saataisiin luotua Boston-palvelinkoneelle, annettiin sen command prompt-ikkunassa seuraavat komennot:

- mkdir C:\Files
- icacls C:\Files\ /grant users:M
- net share Files=C:\Files /GRANT:Users,READ /GRANT:Administrators,FULL /CACHE:None.

Näiden komentojen jälkeen saatiin luotua jaettu yhteys kansioden välille. Toiselta palvelinkoneelta luotiin kansioon tekstitiedosto, jolle annettiin nimi Text File. Tiedostoon kirjoitettiin sanat Hello World. Tiedoston luonnin jälkeen siirryttiin toiselle palvelinkoneelle ja tarkastettiin, onko juuri luotu tekstitiedosto kopioitunut toisen palvelinkoneen kansioon. Tiedosto kopioitui muutamassa sekunnissa.

4.13.4 Varmuuskopiointi

Viimeisessä harjoitustehtävässä oli tarkoituksena luoda varmuuskopio tekstitiedostosta, tehdä siihen muutoksia ja palauttaa muutosten jälkeen alkuperäisen tekstitiedoston sisältö.

Dcsrv-palvelinkoneen työpöydälle luotiin kansio, jolle annettiin nimi Before. Koneen C-asemasta tehtiin varjokopio command prompt -ikkunan kautta seuraavalla komennolla:

- vssadmin create shadow /For=C:.

Kopioinnin jälkeen tekstitiedoston nimi muutettiin muotoon After. Tämän jälkeen palautettiin tallennettu varjokopio. Palautuksen jälkeen tiedoston nimi oli jälleen Before.

Dcsrv-palvelikoneen tiedostot haluttiin varmuuskopioida tietyinä ajankohtana, joten sen asetuksiin lisättiin varmuuskopion tuottaminen noin 10 minuutin päähän asetusten lisäämisestä, jonka jälkeen tarkastettiin, oliko varmuuskopiota koneen C-asemasta tehty. Varmuuskopiointi onnistui ongelmitta.

4.14 Kurssiympäristön luonti

Avustavalle lehtorille Tapio Wikströmille lähetettiin tiedot koneiden koonpanosta ja nimeämispolitiikasta, kun kaikki harjoitustehtävät oli testattu ja varmistettu, että virtuaalikoneiden vaatimat tehot riittävät niiden suorittamiseen. Lehtori Wikström loi koulun palvelinkoneelle kaikki tarvittavat virtuaalikoneet, nimesi ne ohjeistuksen mukaisesti sekä asensi virtuaalikoneisiin käyttöjärjestelmät. Koulun virtuaalikoneisiin asennettiin Windows Server 2008 R2 -versio.

5 Yhteenveto

Työn alussa asetetut tavoitteet luoda toimiva ympäristö Windows Server 2008 -käyttöjärjestelmä-kurssia varten, sekä koota materiaalin harjoitustehtävistä toimiva kokonaisuus kurssin sisällöksi, saavutettiin ajallaan.

Valmis materiaali takasi tehdyille työlle tietyn varmuuden siitä, ettei suurempia ongelmia tulisi esiintymään. Suurempia ongelmia ei esiintynyt, mutta pieniä hienosäätöä vaativia tilanteita kuitenkin oli muutamia.

Suurin huomioitava asia tuli kuitenkin siitä, ettei materiaalin alussa mainittu, että kahteen palvelinkoneeseen Boston sekä Binghampton tulisi tehdä samat konfiguroinnit harjoitustehtävien edetessä. Harjoitusten puolivälissä vain mainittiin, että Binghampton koneelle tehtävät konfiguroinnit jatkuvat siitä mihin Boston-palvelinkoneella jäätiin. Alun harjoitustehtävissä keskityttiin konfiguroimaan ainoastaan Dcsrv- ja Boston-palvelinkoneita. Mainintaa siitä, että Bostonille tehtävät konfiguroinnit tulisi tehdä myös Binghampton-koneelle, ei ollut missään. Tämä luonnollisesti aiheutti ongelmia tehtävien suorittamisessa. Tästä syystä kurssin harjoitustehtävämateriaaliin lisättiin joka harjoitustehtävän jälkeen maininta, että Boston-palvelinkoneelle tehtävät toimenpiteet olisi tehtävä myös Binghampton-palvelinkoneelle.

Materiaali oli erittäin selkeää ja helposti ymmärrettävää, mutta muutamissa kohdissa ei ollut erikseen mainittu, että koneille annettavissa komennossa saattaisi esiintyä esimerkiksi useampia välilyöntejä sanojen tai komentojen välissä, joita materiaalin tekstistä oli vaikea erottaa. Tämä aiheutti muutamaan otteeseen hieman päänvaivaa. Nämä kohdat korjattiin myös kurssin materiaaliin lisämerkinnöillä.

Muita pienempiä ongelmia esiintyi lähinnä palvelinkoneiden omassa toiminnassa. Vaikka harjoitustehtävissä suoritettujen asetusten muutokset tai lisäykset eivät vaatineet palvelinkoneiden uudelleenkäynnistystä toimiakseen, osoittautui se välttämättömäksi useissa tilanteissa.

Ilman uudelleenkäynnistystä palvelinkoneisiin asetetut ominaisuudet eivät lähteneet toimimaan tai palvelinkoneet jämähtivät paikoilleen.

Olin mukana seuraamassa ensimmäisen kurssin tunteja, eikä ongelmia ilmennyt lainkaan. Myöskään tätä seuranneilta kursseilta ei tullut yhtään ilmoitusta ongelmista. Muutamilla pienillä muutoksilla saatiin kurssista toimiva ja tarkoituksenmukainen kokonaisuus.

Lähteet

- [1.] Microsoft Virtual PC 2007 [verkkodokumentti]. [Viitattu 26.12.2010]. Saatavissa: http://en.wikipedia.org/wiki/Virtual_PC.
- [2.] Windows Server 2008 [verkkodokumentti]. [Viitattu 26.12.2010]. Saatavissa: http://en.wikipedia.org/wiki/Windows_Server_2008.
- [3.] Windows Server 2008 Roles [verkkodokumentti]. [Viitattu 26.12.2010]. Saatavissa <http://www.windowsitpro.com/article/john-savills-windows-faqs/q-what-are-the-server-roles-in-windows-server-2008-.aspx>.
- [4.] Windows Server 2003 [verkkodokumentti]. [Viitattu 26.12.2010]. Saatavissa: http://en.wikipedia.org/wiki/Windows_Server_2003.
- [5.] Internet Protocol [verkkodokumentti]. [Viitattu 27.12.2010]. Saatavissa: http://en.wikipedia.org/wiki/Internet_Protocol.
- [6.] IPv4 [verkkodokumentti]. [Viitattu 27.12.2010]. Saatavissa: <http://en.wikipedia.org/wiki/IPv4>.
- [7.] IPv6 [verkkodokumentti]. [Viitattu 27.12.2010]. Saatavissa: <http://en.wikipedia.org/wiki/IPv6>.
- [8.] DNS [verkkodokumentti]. [Viitattu 28.12.2010]. Saatavissa: http://en.wikipedia.org/wiki/Domain_Name_System.
- [9.] GNZ [verkkodokumentti]. [Viitattu 28.12.2010]. Saatavissa: <http://www.petri.co.il/windows-DNS-globalnames-zone.html>.
- [10.] DHCP [verkkodokumentti]. [Viitattu 28.12.2010]. Saatavissa: <http://en.wikipedia.org/wiki/DHCP>.
- [11.] Telnet [verkkodokumentti]. [Viitattu 28.12.2010]. Saatavissa: <http://en.wikipedia.org/wiki/Telnet>.
- [12.] NAT [verkkodokumentti]. [Viitattu 7.1.2011]. Saatavissa: <http://en.wikipedia.org/wiki/NAT>.
- [13.] VPN [verkkodokumentti]. [Viitattu 7.1.2011]. Saatavissa: <http://en.wikipedia.org/wiki/VPN>.
- [14.] Palomuri [verkkodokumentti]. [Viitattu 14.1.2011]. Saatavissa: http://en.wikipedia.org/wiki/Firewall_%28computing%29.
- [15.] NAP [verkkodokumentti]. [Viitattu 14.1.2011]. Saatavissa: http://en.wikipedia.org/wiki/Network_Access_Protection.

- [16] WSUS [verkkodokumentti]. [Viitattu 16.1.2011]. Saatavissa: <http://en.wikipedia.org/wiki/WSUS>.