SAVONIA-AMMATTIKORKEAKOULU
LIIKETALOUS, KUOPIO

MICROSOFT WINDOWS SERVER 2008 -TIETOTURVA

Timo Knuutinen
Tradenomin opinnäytetyö
Tietojenkäsittelyn koulutusohjelma

Marraskuu 2009

SAVONIA-AMMATTIKORKEAKOULU
LIIKETALOUS, KUOPIO
Koulutusohjelma, suuntautumisvaihtoehto (jos on)

Tietojenkäsittelyn koulutusohjelma

Tekijä(t)

Timo Knuutinen

Työn nimi

Microsoft Windows Server 2008 -tietoturva

Työn laji	Päiväys	Sivumäärä
Opinnäytetyö	18.11.2009	75 + 1

Työn ohjaaja(t)	Toimeksiantaja
Pekka Granroth	Savonia-ammattikorkeakoulu

Tiivistelmä

Tämän opinnäytetyön tavoitteena oli tutkia ja testata Microsoftin Windows Server 2008 -käyttöjärjestelmän keskeisimpiä tietoturvaominaisuuksia keskittyen erityisesti Network Access Protection -suojausominaisuuteen.

Opinnäytetyöprosessi alkoi marraskuussa 2009 ja valmistui lokakuun 2009 lopussa. Opinnäytetyön toimeksiantaja Savonia-ammattikorkeakoulu toimitti työtä varten tarvitun laitteiston ja käyttöjärjestelmän.

Tämä opinnäytetyö jakaantuu kahteen osioon, joista ensimmäisessä eli teoriaosassa esitellään Server 2008 -käyttöjärjestelmän keskeiset tietoturvaominaisuudet. Toisessa eli käytäntöosassa käydään läpi opinnäytetyön teknistä vaihetta ja tuodaan esille työhön liittyvät havainnot ja lopputulokset. Raportin käytäntöosa soveltuu myös ohjeistukseksi samankaltaisen palvelinympäristön asentamiseen ja käyttämiseen.

Tästä opinnäytetyöstä käyvät ilmi Windows Server 2008 -käyttöjärjestelmän tietoturvaominaisuuksien lisäksi käyttöjärjestelmän ja sen keskeisten palvelinroolien asentaminen ja toiminta.

Opinnäytetyölle asetetut tavoitteet liittyen tietoturvaominaisuuksien tutkimiseen ja niiden käyttämiseen täyttyivät. Työssä luotu virtuaalipalvelinympäristö toimi hyvin ja mahdollisti työn teknisen onnistumisen.

Asiasanat

Windows Server 2008, käyttöjärjestelmä, tietoturva, palvelin, virtuaalisointi

Huomioitavaa

SAVONIA UNIVERSITY OF APPLIED SCIENCES
UNIT OF BUSINESS AND ADMINISTRATION, KUOPIO
Degree Programme, option

Degree Programme in Computer Science

Author(s)

Timo Knuutinen

Title of study

Data security of Windows Server 2008

Type of project	Date	Pages
Thesis	18.11.2009	75 + 1

Supervisor(s) of study

Pekka Granroth

Executive organisation

Savonia University of Applied Sciences

Abstract

The objective of this thesis was to examine and test the essential data security features of the Microsoft Windows Server 2008 operating system. The main focus was on the security feature Network Access Protection.

The work of the thesis began in November 2008 and was completed by late October 2009. Savonia University of Applied Sciences supplied the server hardware and the operating system.

The thesis is divided into two parts, the first containing a basic introduction to the essential data security features and the second detailing the deployment and usage of those features in the thesis. The second part can also be used as a guide when installing and using a similar server environment.

In addition to the essential data security features this thesis also focuses on the installation and functions of the Windows Server 2008 operating system and its vital server roles.

The objectives set for the thesis, concerning the examination and usage of the data security features, were achieved. The virtual server environment created for the thesis functioned well and made the technical implementation of the project successful.

Keywords

Windows Server 2008, operating system, data security, server, virtualization

Note

LYHENTEET JA ERIKOISMERKIT

EAP	EAP on lyhenne sanoista Extensible Authentication Protocol eli laajennettava autentikointiprotokolla. EAP:ta käytetään yleisimmin tunnistettaessa lähiverkkoon pyrkiviä tietokoneita. EAP itsessään on varsin rajallinen protokolla, joten siitä on kehitetty useita suojatumpia eri versioita, kuten PEAP (Protected EAP).
EM	Enforcement method eli pakotusmetodi tarkoittaa metodia, jota käytetään NAP-järjestelmäominaisuuden kanssa.
Hypervisor	Hypervisor on ohjelmistokerros, joka luo eristetyn toimintaympäristön, partition, virtuaalikoneille sekä hallinnoi ja valvoo virtuaalikoneiden pääsyä fyysisen isäntäkoneen laitteistoresursseihin.
HV	HV on virtuaalisoinnissa hypervisorin ja isäntäkoneen yhdistävä tekninen silta.
IC	Integration Component mahdollistaa kommunikaation virtuaalikoneiden ja hypervisorin välillä sekä virtuaalikoneiden keskinäisen kommunikaation.
NAP	Network Access Protection on järjestelmä, jonka avulla voidaan valvoa ja säätää lähiverkkoon pyrkivien tietokoneiden pääsyä verraten niiden terveystilaa määritettyihin asetuksiin.
NAP Agent	Network Access Protection -ominaisuuden komponentti, joka kerää työasemakoneiden tietoja ja välittää niitä eteenpäin NAP EC:lle.
NAP EC	Network Access Protection Enforcement Client on niin sanottu asiakasohjelma, joka toimittaa työaseman tietoja SHV-komponentille.
RODC	Read-only Domain Controller eli vain lukuoikeudella varustettu toimialueen kontrolleri. Osa Server 2008:n uudistettua aktiivihakemistopalvelinroolia.

SHA System Health Agent on jokaisessa Network Access Protection -tietoturvaominaisuutta käyttävässä tietokoneessa sijaitseva komponentti, joka kerää kyseisen koneen terveydentilatietoja.

SHV System Health Validator on palvelinkomponentti, joka vastaanottaa NAP EC:ltä saadut työaseman terveystiedot ja toimittaa ne eteenpäin terveydentilapalvelimelle.

TLS TLS eli Transport Layer Security on kryptografinen turvallisuusprotokolla, jota käytetään muun muassa Internet-verkossa estämään datakommunikaation vakoilua, häirintää ja väärentämistä. SSL-protokollan (Secure Sockets Layer) seuraaja.

VID Virtualization Infrastructure Driver toimittaa eri hallintapalveluja virtuaalikoneille isäntäkoneelta.

VMBus Virtual Machine Bus on virtuaaliväylä, jonka kautta VSP lähettää laitetietoja virtuaalikoneille sekä välittää virtuaalikoneiden keskinäistä kommunikaatiota.

VMWP Virtual Machine Worker Process on virtuaaliteknologia Hyper-V:n käyttämä isäntäkoneen hallinnointipalvelu Hyper-V:n kautta luodulle virtuaalikoneelle.

VSC Virtualization Service Client on virtuaalinen laitteistoilmentymä, jonka kautta isäntäkoneen laitteistoa voidaan käyttää virtuaalikoneessa.

VSP Virtualization Service Provider toimittaa virtuaalikoneille isäntäkoneen laitteiston emuloituna.

WMI Windows Management Instrumentation on Windows-käyttöjärjestelmien tiedon ja toimintojen hallinnan infrastruktuuri.

SISÄLLYS

1 JOHDANTO

Tämän opinnäytetyön tavoitteena oli asentaa Windows Server 2008 -käyttöjärjestelmä palvelintietokoneeseen ja tutkia järjestelmän tietoturvaominaisuuksia, keskittyen erityisesti Network Access Protection -verkkosuojausominaisuuteen. Tietoturvaominaisuuksien tutkiminen työn keskeisenä sisältönä oli aiheena erittäin mielenkiintoinen sekä oman oppimisen että tulevan työelämän kannalta. Työn virallisena toimeksiantajana toimi Savonia-ammattikorkeakoulu ja sen tietohallinto, jossa yhteyshenkilöni työn eri vaiheissa oli Timo Kinnunen.

Tämä raportti käsittelee Windows Server 2008 -käyttöjärjestelmää sekä teoriatasolla että käytännössä tutkimustyöni kautta. Raportin käytäntöosio soveltuu myös ohjeistukseksi kyseisen käyttöjärjestelmän ja sen keskeisten toimintojen asentamiseen ja käyttöön.

Yritin kirjoittaa opinnäytetyöni raportin mahdollisimman selkeäksi ja ymmärrettäväksi, joskin osa termeistä ja teknologioista vaatii hieman aiempaa perehtymistä.

2 MICROSOFT WINDOWS SERVER 2008

2.1 Yleiskatsaus

Microsoft Windows Server 2008 on opinnäytetyöni raportin kirjoitushetkellä (helmi-maaliskuussa 2009) uusin Windows Server -käyttöjärjestelmäperheen jäsen. Se julkaistiin 27. helmikuuta 2008 edellisen sukupolven Windows Server 2003 -käyttöjärjestelmän korvaajaksi. Työasemakäyttöjärjestelmä Windows Vistan tavoin Windows Server 2008 käyttää Windows NT 6.0 Service Pack 1 -käyttöjärjestelmän ydintä (kernel).

Tulevissa kappaleissa käyn hieman läpi Server 2008 -käyttöjärjestelmän eroja verrattuna Server 2003 -järjestelmään. Olen laatinut erilliset osiot tärkeimmiksi kokemistani aihekokonaisuuksista, jotka seuraavat tämän luvun jälkeen.

2.2 Käyttöjärjestelmän eri versiot

Windows Server 2008 -käyttöjärjestelmästä on olemassa yhdeksän erilaista versiota. Näiden versioiden lisäksi jokainen versio on saatavilla sekä 32- että 64-bittisille suoritinkannoille. Seuraavaksi käyn läpi niiden oleellisimpia ominaisuuksia ja käyttötarkoituksia.

2.2.1 Datacenter ja Enterprise

Datacenter- ja Enterprise-versiot käyttöjärjestelmästä ovat toiminnallisuudeltaan ja ominaisuuksiltaan hyvin samanlaiset. Kummatkin ovat tarkoitettu pääosin isoille yrityksille ja organisaatioille. Kummassakin on kaikki käyttöjärjestelmää varten kehitetyt ominaisuudet, joista osa muista versioista puuttuu. Näiden kahden version

keskeisin ero on palvelinlaitteiston tuettujen suorittimien määrässä, Datacenter-versiossa palvelinkoneessa voi olla peräti kuusikymmentäneljä moniydinsuoritinta, kun taas Enterprise tukee vain kahdeksaa vastaavaa suoritinta. Keskusmuistin tuettu määrä on massiivinen, peräti kaksi teratavua. Opinnäytetyöni kannalta ei olisi ollut merkitystä, kumpaa versiota olisin käyttänyt, mutta päädyin Enterprise-versioon.

Ollessaan suurille yrityksille ja organisaatioille suunnattuja tuotteita kummatkin järjestelmän versiot ovat kalliita, maaliskuun 2009 alussa hinta liikkui lähes viiden tuhannen euron luokassa (Moonsoft Oy:n verkkokaupan hinnasto, 2009). Tähän hintaan sisältyy kylläkin 25 lisenssiä, joten yksittäiselle kappaleelle hinta ei ole järin suuri. Suurten yritysten tuotteeksi tämän tekee myös juuri se, että sitä myydään ainoastaan näin suurilla lisenssimäärillä.

2.2.2 Standard

Standard-versio Windows Server 2008:sta on hieman rajatumpi, kuin Datacenter ja Enterprise. Se tukee maksimissaan neljällä moniydinsuorittimella ja korkeintaan 32 gigatavun keskusmuistilla varustettua laitteistoa. Keskeisin puute kahteen kattavimpaan järjestelmäversioon verrattuna on Failover clustering -konfiguraatiotietojen hajauttamisominaisuuden puuttuminen. Hintaa tällä versiolla on hieman yli tuhat euroa (Moonsoft Oy:n verkkokaupan hinnasto, 2009).

2.2.3 Web Server

Microsoft tarjoaa uudesta palvelinkäyttöjärjestelmästään myös pelkän Web Server -vaihtoehdon eli pelkillä webpalvelin-ominaisuuksilla varustetun rajallisen käyttöjärjestelmän. Laitteiston tuki on hyvin samanlainen, kuin Standard-versiossakin. Web Server -version saa ostettua noin viidellä sadalla eurolla (Moonsoft Oy:n verkkokaupan hinnasto, 2009).

2.2.4 Muut versiot

Microsoft on tehnyt omat versionsa Windows Server 2008 -järjestelmästä myös HPC-supertietokoneille, joita käytetään esimerkiksi autonvalmistajien keskuudessa (Microsoft Corporation 2009); sekä Intelin kehittämille Itanium-pohjaisille suorittimille. Kumpikin soveltuu hyvin ominaisuuksiensa puolesta sovellus- ja teknologiakehitystyön rungoksi, joskaan perinteisen ”peruspalvelimen” rooliin niistä ei juuri ole. Koska näiden versioiden tarkoitusperä on muussa kuin tietojärjestelmän ylläpitämisessä, esimerkiksi uudet Hyper-V- ja Network Access Protection -ominaisuudet puuttuvat molemmista.

3 KESKEISET OMINAISUUDET

3.1 Hyper-V

Hyper-V on Microsoftin kehittämä käyttöjärjestelmien virtuaalisointijärjestelmä 64-bittisille Windows Server 2008 -käyttöjärjestelmille. Hyper-V on mahdollista asentaa erilliseksi palvelinrooliksi, kuten itse tein opinnäytetyössäni, jonka kautta pystytään asentamaan ja hallinnoimaan useita eri virtuaalikoneita. Virtuaalikoneiksi voidaan asentaa toisia Windows Server -palvelinkäyttöjärjestelmiä, Windows-työasemajärjestelmiä, kuten XP ja Vista; tai kolmannen osapuolen käyttöjärjestelmiä kuten Linux. Microsoft julkaisi lokakuun 2008 alussa Windows Server 2008 -käyttöjärjestelmästä ilmaisen Hyper-V Server -version, jonka toiminnallisuus pohjautuu Server Core -versioon, eikä näin ollen sisällä graafista käyttöliittymää. Tämä versio on käytännöllinen, mikäli käytössä on useampia fyysisiä palvelimia, sillä Hyper-V Serverin hallintaan tarvitaan toinen palvelinkone tai Windows Vista -käyttöjärjestelmällä varustettu työasema. Käytännöllisyys tulee esiin palvelinversion minimaalisessa tietoturvahyökkäyspinta-alassa, koska järjestelmässä ei ole ylimääräisiä ominaisuuksia asennettuna.

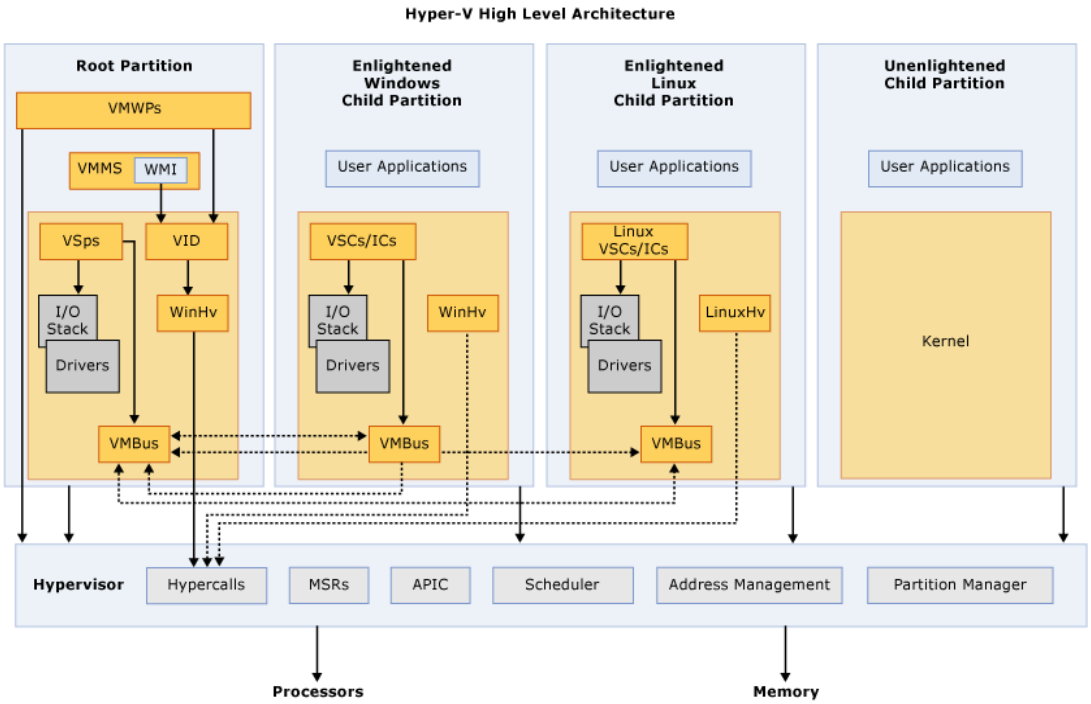
Virtuaalisoinnin kätevyys ja edut tulevat esiin erityisesti hieman pienemmillä yrityksillä tai organisaatioilla. Erilaisiin tarkoituksiin soveltuvat palvelimet, kuten vaikka DHCP-palvelin ja aktiivihakemistopalvelin, on syytä pitää asennettuina eri tietokoneille mahdollisten ongelma- ja vahinkotapausten vuoksi. Tämä taas tulisi kalliiksi, kun pitäisi ostaa useita fyysisiä palvelinkoneita. Tämän tilanteen kiertämiseksi kehitettiin virtuaalisointijärjestelmät, joiden kautta pystytään virtuaalisoimaan eri käyttöjärjestelmiä ja asentamaan fyysisen koneen kiintolevylle useampi virtuaalikone, jolloin selvitään vähemmillä laitteistoinvestoinneilla.

Aiemmat virtuaalisointijärjestelmät ovat olleet vaativia fyysisen isäntäkoneen laitteistolle. Isäntäkoneen keskusmuisti- ja suoritintarve on ollut hyvin suuri, jotta virtuaalikoneet ovat toimineet sujuvasti. Nämä järjestelmät ovat olleet usein

kolmannen osapuolen valmistamia, kuten VMWare, ja ne on tarvittu asentaa erikseen. Microsoftin Hyper-V on kehitetty käyttämään vähemmän isäntäkoneen resursseja, jolloin toiminta on jouhevampaa. Ollessaan Microsoftin tuote, Hyper-V integroituu Windows Server 2008 -käyttöjärjestelmään helposti ja pystyy käyttämään täysin osaa isäntäkoneen resursseista, kuten verkkokorttia ja DVD-asemaa. Käytännössä katsoen on kuitenkin suositeltavaa, että fyysisessä palvelinkoneessa on reilu määrä keskusmuistia ja kiintolevytilaa sekä virtuaalikoneiden, että isäntäkoneen käytössä.

Itse virtuaalikoneiden puolella laitteisto ja niiden ajurit ovat virtuaalisia, kuten käyttöjärjestelmäkin. Hyper-V sisältää valtavan määrän eri laitteistoajureita itsessään, joten useammanlaisten laitteiden simulointi onnistuu. Hyper-V:n alla toimivilla virtuaalikoneilla ei kuitenkaan ole suoranaista pääsyä isäntäkoneen suorittimelle, vaan ne käyttävät virtuaalista näkymää suorittimesta.

Fyysisen isäntäkoneen ja Hyper-V:n yhdistää toisiinsa hypervisor. Hypervisor on eräänlainen ohjelmistokerros, joka luo eristetyn toimintaympäristön, partition, virtuaalikoneille sekä hallinnoi ja valvoo virtuaalikoneiden pääsyä fyysisen isäntäkoneen laitteistoresursseihin.



Kuva 1 Hyper-V-arkkitehtuuri

Kuvaa 1 puretaan auki seuraavasti.

1. Root Partition on isäntäkoneen juuriosio.
2. VMWP eli worker-prosessi tarjoaa virtuaalikoneen isäntäkoneen hallinnointipalvelun jokaiselle Hyper-V:n kautta luodulle virtuaalikoneelle. Kyseinen prosessi kommunikoi sekä hypervisorin että VID:n kanssa.
3. VID toimii virtuaalisoinnin infrastruktuurin ajurina eli se toimittaa eri hallintapalveluja virtuaalikoneille.
4. VMMS-prosessi käyttää myös VID:iä ja se ylläpitää virtuaalikoneiden toimintaa käyttäen WMI-pohjaisia sovelluksia. VID on samalla toiminta-alusta WinHV:lle,
5. WinHV on tekninen silta isäntäkäyttöjärjestelmän ajurien ja hypervisorin välillä.
6. Hypervisor kommunikoi virtuaalikoneen vastaavan Win/Linux/ym. HV:n kanssa ja mahdollistaa ajurien käytön.
7. VSP-prosessi eli virtuaalisoinnin palveluntarjoaja sijaitsee isäntäkoneessa ja tuottaa virtuaalikoneille emuloidut laitteet, jotka pohjautuvat fyysisen isäntäkoneen konkreettiseen laitteistoon.
8. Arkkitehtuurin loppupuolella on virtuaaliväylä VMBus, jonka kautta VSP lähettää laitetietonsa virtuaalikoneille, ja jonka kautta samassa verkossa olevat virtuaalikoneet kommunikoivat keskenään.
9. Virtuaalikoneen puolella VSP:tä vastaavat prosessit ovat VSC ja IC, joista ensimmäinen on virtuaalikonepalvelun asiakas, client, joka on virtuaalinen laitteistoilmentymä, jonka avulla isäntäkoneen fyysisiä laitteistoresursseja voidaan käyttää.
10. IC puolestaan mahdollistaa kommunikaation hypervisorin ja mahdollisten muiden virtuaalikoneiden välillä.

Hyper-V toimii ainoastaan 64-bittisessä Windows Server 2008 -käyttöjärjestelmässä, jonka kolme pääversiota Enterprise, Datacenter ja Standard ovat kaikki tuettuja. Virtuaalikoneiden enimmäismäärä riippuu paljolti siitä, minkälainen isäntäkoneen laitteisto on ja paljonko isäntäkoneen keskusmuistia asettaa käyttöön per virtuaalikone. Windows Server 2008:n Enterprise- ja Datacenter-versiot tukevat molemmat yhteensä maksimissaan kahta teratavua (kaksi tuhatta gigatavua) keskusmuistia, joten suurellakin keskusmuistimäärällä varustettuja virtuaalipalvelimia

saa käyttöönsä lukemattomia. Standard-versio tukee keskusmuistia vain 32 gigatavuun asti.

Windows Server 2008 -käyttöjärjestelmän uusista palvelinrooleista Hyper-V on monessa määrin kaivatuin uudistus, sillä juuri virtuaalipalvelimien käyttöön monet tahot, Microsoft mukaan lukien, kehottavat palvelinmaailmassa siirtymään (Ou, 2006; Microsoft 2009).

3.2 Server Core

Server Core on rajoitetulla toiminnallisuudella varustettu Windows Server 2008 -käyttöjärjestelmän asennusvaihtoehto, joka tarjoaa kevytkäyttöisen ja tietoturvahyökkäyspinta-alaltaan minimaalisen vaihtoehdon käyttöjärjestelmän täydelliselle asennukselle.

Server Core on nimensä mukaisesti ”palvelimen ydin” ja tarjoaa vain muutamia palveluita ja palvelinrooleja asennettavaksi. Se sisältää hyvin suppean komentopohjaisen käyttöliittymän, jonka kautta voi asentaa palvelinrooleja ja -palveluja, sekä suorittaa rajallisia hallinnointitehtäviä komentojen ja ohjelmointiskriptien avulla. Käyttöjärjestelmän hallintaan voidaan käyttää myös toiselle tietokoneelle asennettua erillistä etähallintatyökalua, kuten Microsoft Management Consolea (MMC). Heinäkuun 2009 alussa ainoa etähallintaan sopiva käyttöjärjestelmä on täydellinen asennus Windows Server 2008 -käyttöjärjestelmästä.

Server Coren tukemia palvelinrooleja ovat tiedostopalvelin (File Server), DHCP-palvelin, DNS-palvelin, mediapalvelut (Media Services), aktiivihakemisto ja tulostuspalvelin.

Tämän asennusvaihtoehdon edut tavalliseen asennukseen verrattuna voidaan jakaa seuraaviin:

- vähäisempi huolto- ja hallintatarve
    - käyttöjärjestelmään asennetaan vain palvelinroolien tarvitsemat ominaisuudet.

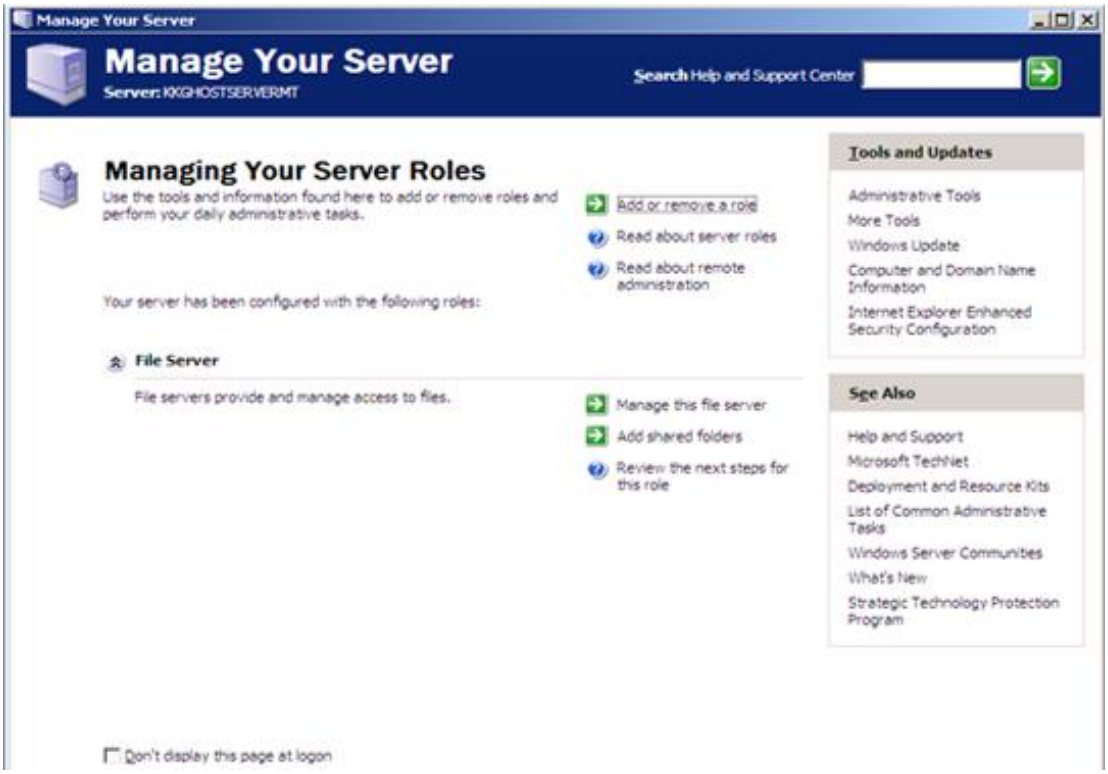
- järjestelmän tarvitsema kiintolevymäärä
    - Server Core vaatii enimmillään vain noin kolme gigatavua kiintolevytilaa, kun täydellinen asennus vähintään 10 gigatavua.
- hyvin minimaalinen tietoturvahyökkäyspinta-ala
    - koska palvelimelle ei pysty asentamaan paljoa, Palvelimen rajallisten ominaisuuksien ja asennusvaihtoehtojen vuoksi sen hyökkäyspinta-alakin on pieni.

Server Core sopii oivasti käyttöjärjestelmäksi palvelinkoneeseen, jonka toimintaa valvotaan ja kontrolloidaan etätietokoneelta. Tämä on varsin kätevä asennusvaihtoehto isommalle yritykselle/organisaatiolle, jolla on käytössään esimerkiksi useampi aktiivihakemistopalvelin. Server Corea käyttämällä organisaation aktiivihakemistoa voidaan jakaa useammalle palvelimelle, mutta joita hallinnoidaan pelkästään yhden tietokoneen kautta.

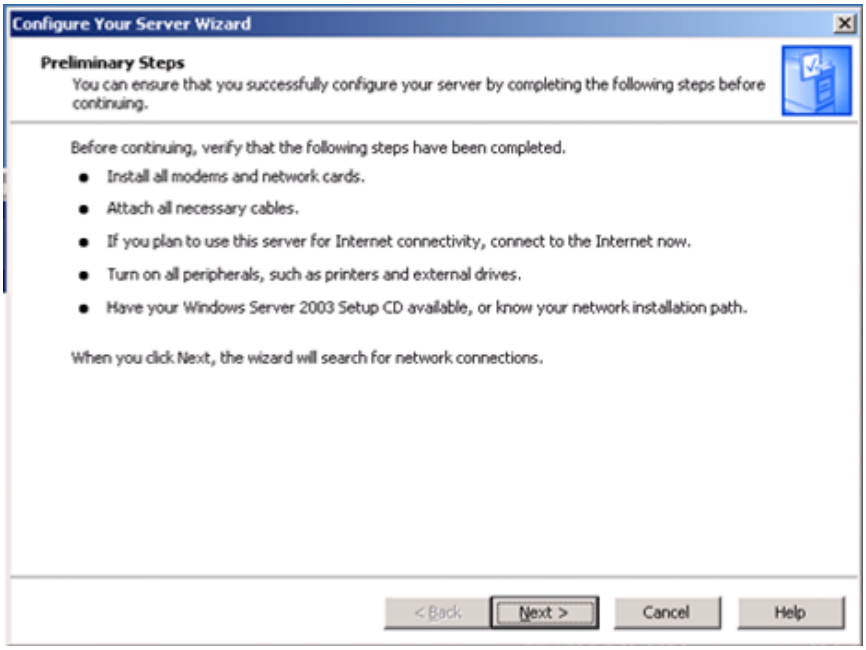
Server Core ei puolestaan sovi käytettäväksi, mikäli organisaatiossa tai yrityksessä käytetään vain yhtä palvelinkonetta, tämä palvelinasennusvaihto kun tarvitsee toisen tietokoneen Server Coren hallintaan.

3.3 Server Manager

Yksi Windows Server 2008 -käyttöjärjestelmän uusista ominaisuuksista on Server Manager -hallinnointityökalu, joka yhdistää aiemmista Windows Server -käyttöjärjestelmistä Manage Your Server- ja Security Configuration Wizard -ominaisuudet, joita molempia käytettiin erillään hallinnoidessa palvelinkonetta. Server Manager on osittain myös edistyneempi versio Windows Server 2003 -käyttöjärjestelmän Configure Your Server -työkalusta, jota Server 2003 käyttää asennettaessa uusia palvelinrooleja.



Kuva 2 Windows Server 2003: Manage Your Server

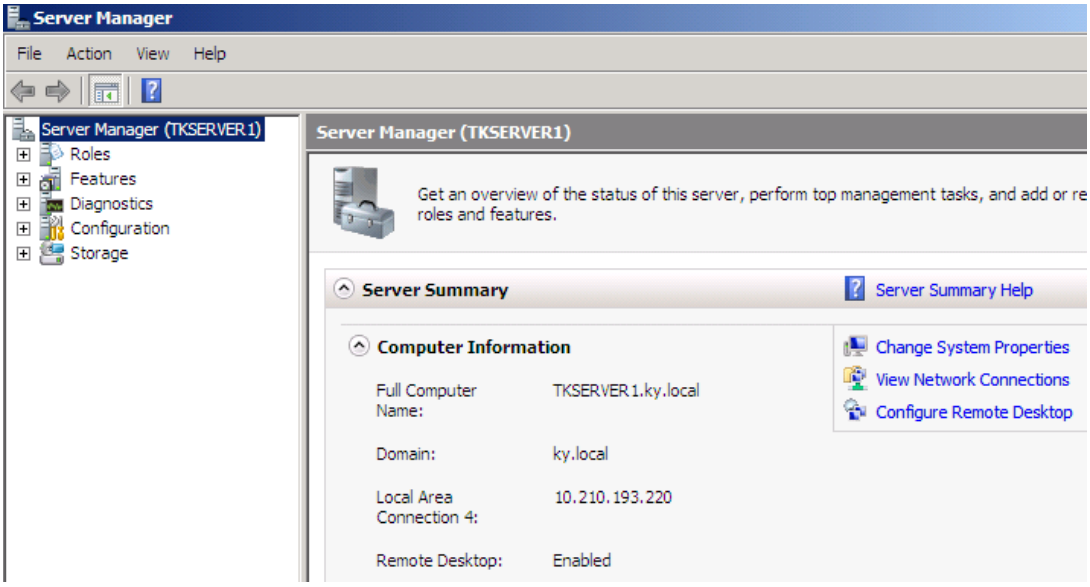


Kuva 3 Windows Server 2003: Configure Your Server

Aikaisemmissa Windows Server -versioissa palvelinkonetta pystyttiin siis hallinnoimaan osittain Manage Your Server -hallinnointityökalun avulla, mutta eri toimintojen tekeminen, kuten vaikkapa uuden palvelinroolin asentaminen avasi toisen erillisen työkalun, jolla toiminto oikeasti suoritettiin. Yllä olevat kuvat ovat kaapattu

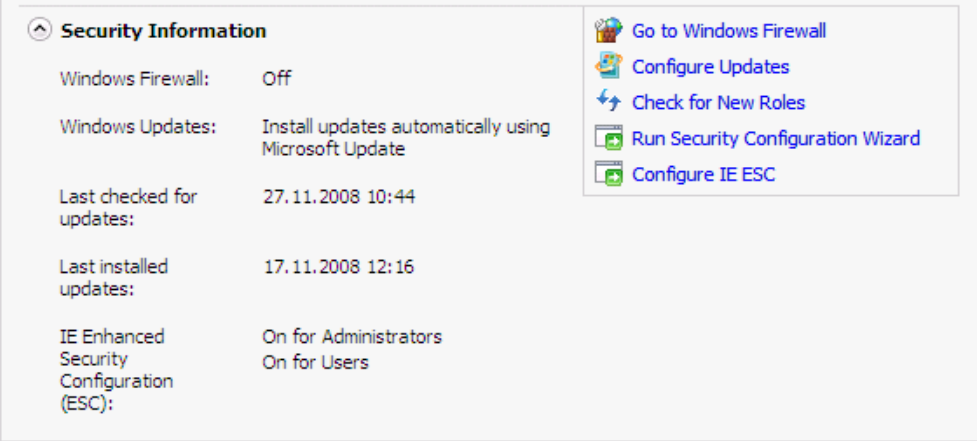
Savonia-ammattikorkeakoulun eräästä palvelinkoneesta, johon on asennettu Tiedostopalvelin (File Server). Uuden palvelinroolin lisääminen (Add or remove a role) avaa siis Configure Your Server Wizard -työkalun.

Windows Server 2008:n Server Manager siis kokoaa hyvin yhteen eri toimintoja ja näyttää suoraan pääikkunassa useimmat oleelliset tiedot, kuten palvelinkoneen nimen, toimialueen, IP-osoitteen, palomuuriasetukset sekä oleellisesti asennetut palvelinroolit ja -toiminnot (Features).



Kuva 4 Windows Server 2008: Manage Your Server, Server Summary

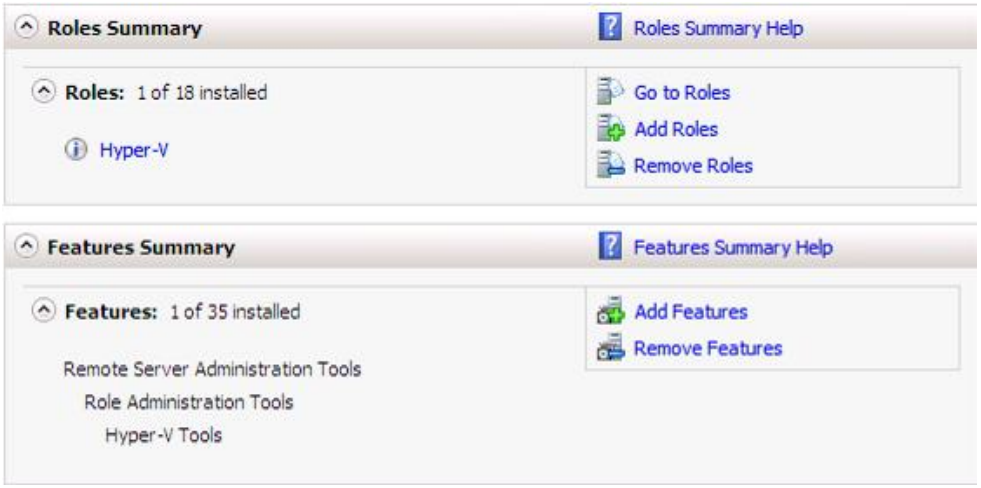
Olen käyttänyt kuvakaappauksissani itse fyysisen palvelimen käyttöjärjestelmän Server Manager -työkalua. Server Summary -kohta näyttää oleellisia tietoja, kuten palvelinkoneen nimen, toimialueen (Savonia-ammattikorkeakoulun ky.local) ja IP-osoitteen Server Summary antaa myös mahdollisuuden muuttaa järjestelmän asetuksia, kuten juuri nimen ja toimialueen; muuttaa verkkoasetuksia, sekä muokata etätyöpöytäyhteysasetuksia.



Kuva 5 Windows Server 2008: Server Manager, Security Information

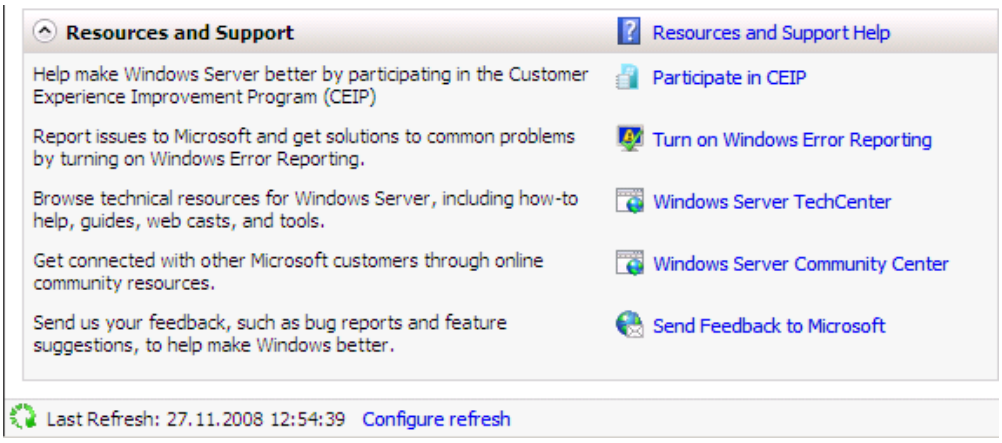
Security Information -kohta puolestaan esittää palvelinkoneen tietoturva-asetukset. Käyttöjärjestelmän oma palomuuri on poistettu käytöstä, koska Savonialla on käytössään oikeat fyysiset palomuurilaitteistot. Tämä valikkoruutu tarjoaa mahdollisuuden säätää palomuuriasetuksia, käyttöjärjestelmän päivityksiä, Internet Explorer -webselaimen ESC-suojausasetuksia, etsiä uusia palvelinrooleja sekä suorittaa Security Configuration Wizard.

Internet Explorerin ESC-ominaisuus asettaa palvelimelle ja itse IE-selaimelle hyvin tarkat ja korkeat suojausasetukset, joiden kautta pyritään estämään tietoturvahyökkäykset Internet-sivustojen ja ohjelmien scriptien välityksellä. Käytännössä tämä ominaisuus asettaa web-selaimen turvallisuusvyöhykkeet (Security Zones) hyvin korkeiksi, jolloin valtaosa Internet-sivustojen käyttämistä sovelluksista ja ominaisuuksista eivät toimi. Käyttäjä voi itse määrittää sivustoja, joiden katsotaan olevan luotettavia, jolloin turvallisuusvyöhyke on hieman matalampi, mutta silti karsii pois joitain ominaisuuksia, kuten selainlaajennuksia (esimerkiksi Java) ja animaatioita. Tämän ominaisuuden voi halutessaan asettaa pois käytöstä, joskaan Microsoft ei suosittele tätä (Server Manager: Help-tiedosto).



Kuva 6 Windows Server 2008: Server Manager, Roles ja Features

Roles Summary -kohta kertoo käyttäjälle, mitä palvelinrooleja koneelle on asennettu. Koska kuvakaappaukseni ovat Savonian verkossa olevasta palvelimesta, ainoastaan yksi rooli, virtuaalisointirooli Hyper-V, on asennettu. Oikean reunan painikkeilla päästään joko selaamaan asennettujen palvelinroolien tarkempia tietoja ja sekä lisäämään että poistamaan rooleja.



Kuva 7 Windows Server 2008: Server Manager, Resources and Support

Viimeisenä kohtana Server Managerissa on Resources and Support -kohta, josta voi säätää halutessaan päälle tai pois Microsoftin Customer Experience Improvement Program -asiakastyytyväisyysohjelmaan, jolloin halutessaan voi auttaa kehittämään Windows Server -käyttöjärjestelmää. On myös mahdollista käyttää Windows Error Reporting -työkalua, jonka avulla voi raportoida kokemiaan ongelmia Microsoftille ja saada helpommin ratkaisuja niihin. Resources and Support -kohta tarjoaa myös linkit äärimmäisen hyödyllisiin ja informatiivisiin Windows Server TechCenteriin ja

Community Centeriin, joista ensimmäisessä on koottu valtavasti tietoa ja ohjeita liittyen Windows-käyttöjärjestelmäperheiden toimintaan ja jälkimmäisessä voi keskustella Serveriin liittyvistä ongelmistaan ja ratkaisuistaan muiden käyttäjien kesken.

Server Managerin jokaisen osakokonaisuuden yhteydessä on myös kyseistä kokonaisuutta käsittelevä opastusmateriaali Help, jossa neuvotaan erittäin selkeästi, mitä milläkin ominaisuudella voi tehdä ja miten ottaa palvelimesta kaikki hyöty irti.

Server Manager on kokonaisuutena erittäin hyödyllinen ja kätevä työkalu, jolla pystyy hallinnoimaan moniulotteisesti koko palvelinkäyttöjärjestelmää.

3.4 Aktiivihakemisto

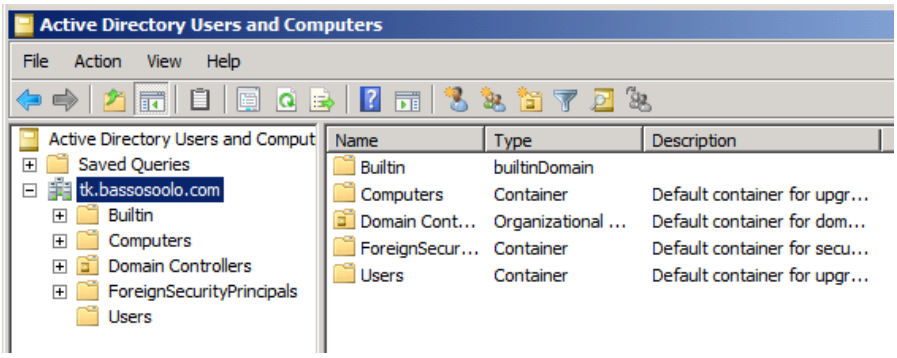
Aktiivihakemisto on Microsoftin kehittämä käyttäjätietokanta ja hakemistopalvelu, jonka avulla pystytään hallitsemaan tietoa lähiverkon käyttäjistä, tietokoneista ja erilaisista verkkoresursseista sekä niitä jakamaan eri sovellusten ja käyttäjien kesken. Aktiivihakemistorooli otettiin käyttöön ensimmäisen kerran Windows 2000 -käyttöjärjestelmän Server-versiossa 2000-luvun taitteessa ja on sen jälkeen kuulunut keskeisenä osana Windows Server -käyttöjärjestelmiin.

Windows Server 2008 -käyttöjärjestelmässä aktiivihakemistoa on kehitetty eteenpäin edellisestä Server 2003-versiosta. Microsoftin mukaan keskeisimmät uudistukset koskevat Federation Services (AD FS), Lightweight Directory Services (AD LDS) ja Rights Management Services (AD RMS) -palvelurooleja. AD FS -roolin avulla pystytään luomaan laajennettava ja turvattu useiden käyttöjärjestelmien välillä toimiva tunnistuspalvelu. AD LDS on nimensä mukaisesti erittäin kevyt ja karsittu versio laajemmasta AD DS -ominaisuudesta, joskin se pohjautuu erilaiseen tietokantapohjaan. AD RMS -roolilla voidaan suojata sovelluksia ja tiedostoja kuten intranet-sivustoja ja sähköpostiviestejä. Nämä ominaisuudet ovat itsessään laajoja kokonaisuuksia enkä katsonut oleelliseksi sisällyttää niitä opinnäytetyöprosessiini.

Toimiakseen kunnolla aktiivihakemisto tarvitsee DNS-palvelinroolin asennettuna samalle fyysiselle tai virtuaalipalvelimelle, kuin mihin aktiivihakemisto on asennettu. DNS-palvelinrooli parantaa järjestelmän loogista rakennetta, toisin sanoen aktiivihakemiston toimialueen käyttäjät ja verkkoresurssit saavat helpomman muistettavan ja tunnistettavan nimen. Esimerkkinä mainittakoon tilanne, jossa järjestelmänvalvoja asettaa tietokoneelle nimen TESTIPC-1 ja IP-osoitteen 193.193.193.193. Ilman aktiivihakemiston kanssa toimivaa DNS-palvelinroolia konetta ei tunnisteta toimialueen sisällä nimellä TESTIPC-1, vaan pelkällä numeerisella osoitteella.

Eräs mielenkiintoisimpia uudistuksia aktiivihakemistossa on RODC eli Read-Only Domain Controller. RODC on pelkästään lukuoikeudella varustettu toimialuekontrolleri, johon ei siis pysty tallentamaan tietoa. Asennettaessa RODC esimerkiksi etätoimipisteen palvelinkoneelle nopeutetaan sekä käyttäjien kirjautumista sekä pienennetään tietoturvariskiä.

Aktiivihakemistopalvelinroolin asennuksen valmistuttua sen varsinainen käyttö alkaa valitsemalla Administrative Toolsin alta Active Directory Users and Computers.



Kuva 8 Aktiivihakemisto

3.4.1 Aktiivihakemiston sertifikaattipalvelut

Aktiivihakemiston sertifikaattipalvelut tarjoavat sertifikaatti-infrastruktuurin, jonka avulla pystytään jakamaan sertifikaatteja eri palvelujen ja protokollien käyttöön.

Esimerkkejä näistä ovat virtuaalilähiverkot, Internet Protocol Security (IPsec) ja opinnäytetyössäni tutkima Network Access Protection (NAP). Sertifikaattipalvelut voidaan asentaa palvelinkoneelle, johon on asennettu joko Windows Server 2000-, 2003- tai 2008-käyttöjärjestelmä, joskaan 2008-käyttöjärjestelmää vanhemmat versiot eivät välttämättä tue kaikkia ominaisuuksia. Sertifikaattipalvelut toimivat hyvin rajallisesti Windows Server 2008:n Server Core- ja Itanium-pohjaisissa käyttöjärjestelmissä.

Sertifikaattipalvelut käyttävät Windows Server 2008 -käyttöjärjestelmään implementoitua Cryptography Next Generation (CNG) -kryptografista alustaa, jonka avulla pystytään luomaan ja muokkaamaan kryptografisia algoritmeja. CNG pohjautuu alun perin Yhdysvaltain valtion kehittämiin Suite B -kryptografisiin algoritmeihin, joita voidaan käyttää tiedon kryptaamisessa, digitaalisissa allekirjoituksissa, sertifikaattien avainpalveluissa ja hajakoodituksessa.

Opinnäytetyötä tehdessäni asensin aktiivihakemiston sertifikaattipalvelut, mutta loppujen lopuksi en tarvinnut niitä missään vaiheessa. Konfiguroidessani Network Policy Serveriä luulin virheellisesti, että tämä palvelinrooli tarvitaan, kun samanaikaisesti luulin tarvitsevani myös RADIUS-palvelinta ja VPN:ää, jotta NPS toimisi kunnolla. Loppujen lopuksi kävi ilmi, että käyttämälläni verkkoratkaisulla en tarvinnut kumpaakaan, joten kyseinen palvelurooli jäi ilman käyttöä.

Mikäli olisin valinnut käyttämäkseni NAP-pakotusmetodiksi IPsec-vaihtoehdon, sertifikaattipalvelut olisivat olleet välttämättömät. IPsec-metodissa jokaiselle lähiverkkoon laskettavalle työasemalla tai palvelimelle myönnetään erityinen turvallisuussertifikaatti, josta käy ilmi tietokoneen terveystila.

3.5 DNS-palvelinrooli

Domain Name System eli DNS on järjestelmä, jonka pääasiallinen tehtävä on nimetä toimialueisiin rekisteröityjä tietokoneita ja verkkopalveluja. DNS muuttaa tietokoneen numeerisen osoitteen eli IP-osoitteen käyttäjäystävälliseen ja ymmärrettävään muotoon, esimerkiksi yksi opinnäytetyössäni käyttämäni virtuaalipalvelin oli IP-

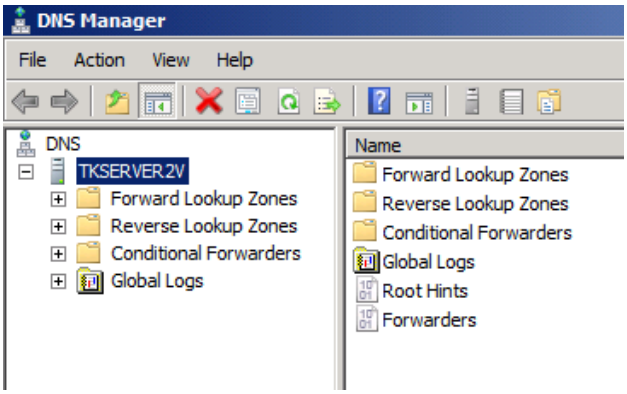
osoitteeltaan 193.210.210.210 ja kansankieliseksi nimeksi sai TKSERVER2V. DNS:ää käytetään TCP/IP-pohjaisissa verkoissa, joista yleisimmin tunnettu on Internet.

Windows Server 2008 -käyttöjärjestelmän DNS-palvelinrooli noudattaa Request for Comments -standardia (RFC), jonka avulla se pystytään haluttaessa implementoimaan osaksi toista RFC-yhteensopivaa DNS-palvelua.

DNS-palvelinroolia on kehitetty integroitumaan paremmin muiden Microsoftin verkkopalveluiden ja palvelinroolien, kuten aktiivihakemiston ja DHCP-palvelimen kanssa. Aktiivihakemiston toimialuepalvelut vaativat vähintään yhden DNS-palvelimen asentamista, jolloin ne on sijoitettava samalle fyysiselle tai virtuaalipalvelimelle. Näiden kahden palvelinroolin symbioosiin liittyy myös eräs oivallisimmista DNS-palvelinuudistuksista. Isossa yritysympäristössä DNS-palvelimen käynnistäminen on raskas prosessi, joka Server-käyttöjärjestelmien aiemmissa versioissa on ollut kaikkeen tietoverkon toimintaan vaikuttavaa. Aiemmin DNS-palvelin on kyennyt vastaamaan eri prosessien ja sovellusten lähettämiin kyselyihin vasta, kun kaikki verkon hallinta-alueet (zone) ovat kokonaan ladattuja. Server 2008:ssa DNS-palvelin lataa tietoa hallinta-alueilta käyttäen eri säikeitä ja näin mahdollistaa eri prosessien ja sovellusten kyselyihin (query) vastaamisen, vaikka kaikkia hallinta-alueita ei olisikaan vielä ladattu kokonaan.

Asennettaessa RODC-aktiivihakemistopalvelinta esimerkiksi etätoimistoon, samalle palvelimelle voidaan asentaa DNS-palvelinrooli, joka voidaan määrittää käyttämään uutta ensisijaista lukuoikeudella varustettua verkon hallinta-aluetta (Primary Read-Only Zone). Tämä uudistus takaa, että kyseinen DNS-palvelin saa käyttöönsä suoremmin ja nopeammin käyttöönsä aktiivihakemistosta tarvitsemansa hallinta-alueet, koska RODC on samalla palvelimella.

Windows Server 2008 -käyttöjärjestelmän DNS-palvelinrooli tukee nykyisen IPv4-osoiteavaruuden lisäksi uutta IPv6-avaruutta. En perehtynyt opinnäytetyössäni teoriatasoa enemmän IPv6:een saati sen hyödyntämiseen palvelinympäristöissä, koska työni keskeisin ominaisuus Network Access Protection ei tue vielä tässä vaiheessa kyseistä teknologiaa.



Kuva 9 DNS-palvelimen hallintatyökalu DNS Manager

Opinnäytetyössäni käyttämässä verkkoratkaisussa käytin osittain mallina Savonia Business -koulutusyksikön verkkostrategiaa, johon tutustuin ollessani kyseisen yksikön Helpdeskissä työharjoittelussa. Käytännössä tämä verkkoratkaisu tarkoittaa, että liitettäessä työasemaa tai palvelinkonetta lähiverkkoon ne saavat automaattisesti DHCP-palvelimelta sekä IP-osoitteen, että DNS-palvelimen osoitteen.

3.6 Network Access Protection

Network Access Protection eli lyhyesti NAP on eräs keskeisimmistä uudistuksista Microsoftin Windows Server 2008 -käyttöjärjestelmässä. NAP on tietoturvariskejä pienentävä järjestelmä, jonka avulla pystytään valvomaan ja kontrolloimaan lähiverkkoon pyrkivien työasemien ja palvelimien pääsyä. NAP käyttää Network Policy Server -palvelinroolia ”tukikohtanaan”, ja erillisten järjestelmäkomponenttien kanssa se pystyy kontrolloimaan, mitkä koneet päästetään kiinni lähiverkkoon.

NAP:n toiminta pohjautuu erilaisten terveyskäytänteiden tai -sertifikaattien käyttöön, joissa määritellään esimerkiksi virustorjuntaohjelmaan, palomuuriin ja muihin tietoturvaohjelmiin tai -ominaisuuksiin liittyvät asetukset, jotka toimialueelle pyrkivästä tietokoneesta on löydyttävä.

NAP-ominaisuutta käyttöön otettaessa valitaan pakotusmetodi (enforcement method). Pakotusmetodi on menetelmä, jonka kautta NAP:ia käytetään. Ominaisuuden tukemia

metodeja ovat VPN, IPsec, 802.1X ja opinnäytetyössäni käyttämä DHCP. Jokaisesta metodista on seikkaperäisempi osio tämän luvun jälkeen.

NAP on sisäänrakennettu ominaisuus Windows Server 2008:n lisäksi myös työasemakäyttöjärjestelmä-Vistassa, ja sitä on mahdollista käyttää myös Service Pack 3:lla varustetussa Windows XP -käyttöjärjestelmässä. Aiemmat palvelin- ja työasemakäyttöjärjestelmät, kuten Windows Server 2003 tai Windows 2000, eivät ole tuettuja.

On suotavaa mainita, että NAP ei itsessään ole työkalu, jolla suojataan yrityksen/organisaation tietoverkkoa ja jolla korvataan palomuurit tai virustorjuntaohjelmat. Se on pikemminkin järjestelmä, joka varmistaa, että kyseiset ohjelmat ja ominaisuudet ovat säädettyjen terveyssertifikaattien määritysten mukaisia. Kansan kielellä NAP:lla siis varmistetaan, että esimerkiksi virustorjuntaohjelmiston päivitykset ovat ajan tasalla.

Pääpiirteissään Network Access Protection -ominaisuuden toiminta tiivistyy seuraavaan:

1. SHA-komponentti kerää tiedot koneen terveydentilasta.
2. NAP Agent -ohjelma kokoaa tiedot datapaketiksi ja lähettää ne NAP EC:lle, client-ohjelmalle, joka on asennettuna jokaiselle työasemalle.
3. NAP EC lähettää tiedot NPS-palvelimen SHV-komponentille ja anoo pääsyä lähiverkkoon.
4. SHV toimittaa tiedot eteenpäin terveydentilapalvelimelle.
5. Terveydentilapalvelin vertaa saatuja tietoja määritettyihin asetuksiin ja lähettää joko myönteisen tai kielteisen vastauksen takaisin riippuen verkkoon pääsyä anoneen tietokoneen terveydentilasta.
6. Mikäli verkkoon pääsemistä yrittänyt työasema ei vastaa terveyssertifikaatin asetuksia, ohjataan se rajattuun verkkoon, jossa sen käytössä ovat vain päivityspalvelut, kuten Windows Update tai erillinen päivityspalvelin. Päivityksen jälkeen prosessin vaiheet käydään uudestaan läpi niin pitkään, kunnes työasema vastaa määritettyä standardia.

Verkkotoimialueen jäsenyys on välttämätöntä, riippumatta valitusta pakotusmetodista. Opinnäytetyössäni käyttämä virtuaalityöasema oli työtä varten luodun toimialueen

”tk.bassosoolo.com” jäsen. Toimialueen jäsenyys on välttämätöntä siitä syystä, että lähiverkkoon pyrkiessään tietokone ja kirjautumista yrittävä käyttäjä täytyy tunnistaa jollain tavoin. Tässä yhteydessä tämä tapa on hakea tiedot sekä käyttäjästä että tietokoneesta organisaation aktiivihakemistosta, jonne tiedot kaikista organisaation luoduista käyttäjätunnuksista ja tietokoneobjekteista tallennetaan. Aktiivihakemistosta osana tietoturvaa enemmän kappaleessa 4.5 Aktiivihakemisto.

NAP-ominaisuutta ei siis voida käyttää, mikäli organisaatiossa vaikkapa vierailee luennoitsija, jonka tarvitsee käyttää kannettavalla tietokoneellaan organisaation verkkoresursseja. Tällaisessa tapauksessa on hyvä säätää erillinen turvallisuuskäytäntö (vieras)käyttäjille, joille voidaan määritellä pääsy rajattuun verkkoon ja rajattuihin resursseihin.

NAP vaatii toimiakseen Windows Server 2008 -käyttöjärjestelmällä varustetun palvelintietokoneen, johon NPS-palvelinrooli tulee ensin asentaa. Käytetystä pakotusmetodista riippuen NPS-palvelinroolin voi yhdistää esimerkiksi DHCP-palvelinroolin kanssa, kuten tein omassa opinnäytetyössäni. Työasemapuolella tuettuja käyttöjärjestelmiä ovat ainoastaan Windows Vista ja Windows XP Service Pack 3, joista molemmista vaaditaan vielä Professional/Enterprise-versiot. Myös syksyllä 2009 ilmestyvä Windows 7 on tuettujen käyttöjärjestelmien listalla; opinnäytetyöni teknistä osaa tehdessäni kyseisestä käyttöjärjestelmästä ei ollut julkaistu minkäänlaista versiota.

3.6.1 NAP EC: DHCP

Suunnitellessani opinnäytetyöni toteuttamista Network Access Protectionin osalta tein päätöksen käyttää pakotusmetodina DHCP:tä. Tämä johtui pääosin Savonia-ammattikorkeakoulun mahdollisesta tulevasta NAP-järjestelmän käytöstä sekä Savonian verkkorakenteesta. IPSec, 802.1X ja pääosin myös VPN ovat Timo Kinnusen kanssa käydyn keskustelun perusteella organisaatiossa niin vähäisessä käytössä, että koin opinnäytetyön tulosten merkityksellisyyden kannalta käytännöllisimmäksi tavaksi tutustua NAP:iin DHCP-pakotusmetodin kautta.

Itse termi DHCP (Dynamic Host Configuration Protocol) tarkoittaa verkkoprotokollaa, jonka pääasiallinen toiminto on jakaa IP-osoitteita tiettyyn lähiverkkoon kuuluville tietokoneille ja muille verkkolaitteille, kuten verkkotulostimille. Lähiverkko käyttää määriteltyä IP-osoiteavaruutta, esimerkiksi alkaen 193.210.210.1 ja päättyen 193.210.210.255, josta voidaan jakaa IP-osoitteita verkkolaitteiden käyttöön.

DHCP-metodia käyttämällä NAP toimii seuraavalla tavalla. Esimerkissäni puhun työasemakoneesta, mutta sama pätee myös palvelinkoneeseen.

Ensimmäisenä työaseman NAP-client lähettää DHCP-palvelimelle viestin terveydentilastaan (SoH). DHCP välittää viestin eteenpäin NAP-terveyskäytäntöpalvelimelle (NAP Health Policy Server, HPS), joka puolestaan arvioi työaseman terveydentilan verraten sitä käytettävään terveyspolitiikkaan ja lähettää vastauksen takaisin DHCP-palvelimelle. Mikäli työaseman terveydentila vastaa politiikan asetuksia, DHCP-palvelin antaa työasemalle IPv4-osoitteen ja täysivaltaisen pääsyn organisaation toimialueen resursseihin.

Mikäli tämä ei taas toteudu ja terveyskäytäntöpalvelin lähettää kielteisen viestin DHCP-palvelimelle, DHCP-palvelin antaa joko yhteyden rajattuun verkkoon ja niin sanotut päivitysohjeet työasemalle tai järjestelmänvalvojan määrityksistä riippuen evää yhteyden kokonaan, mikä tosin ei ole järin suositeltavaa, mikäli työasemalle halutaan antaa mahdollisuus päästä toimialueelle. Yhteyden evääminen voi olla sopiva vaihtoehto, mikäli työasemaa halutaan tutkia tai huoltaa paikallisesti ilman verkkoresursseja. Tätä voidaan pitää myös vaihtoehtona, jos työaseman terveydentilaa ei jostain syystä saada päivitettyä sertifikaatin vaatimalle tasolle.

Rajatussa verkossa ollessaan työasema siis saa IPv4-osoitteen DHCP-palvelimelta, joskin verkkoyhteys tässä tilassa on yleensä ainoastaan päivityspalvelimille, jälleen järjestelmänvalvojan asetukset voivat vaikuttaa tähän. Seuraavaksi päivityspalvelimet lähettävät tarvittavat päivitykset työasemalle, jonka jälkeen työaseman NAP-client päivittää terveydentilatietonsa.

Prosessi lähtee tässä vaiheessa alusta eli työaseman NAP-client lähettää pyynnön yhdessä päivitettyjen terveydentilatietojensa kanssa DHCP-palvelimen kautta NAP-

terveyskäytäntöpalvelimelle, joka tutkii tilanteen uudelleen. Mikäli työaseman terveydentilassa on vieläkin jotain ristiriitaista, äskeiset vaiheet käydään läpi uudelleen.

DHCP-pakotusmetodi vaatii hieman säätämistä NAP:ia pyörittäviltä palvelinkoneilta, joskin kätevänä vaihtoehtona on mahdollista suorittaa kaikki tarvittavat prosessit samalta fyysiseltä tai virtuaaliselta palvelimelta, kun vain asentaa tarvittavat NPS- ja DHCP-palvelinroolit.

Jokaisessa pakotusmetodissa on omat hyvät ja huonot puolensa, niin myös DCHP-pakotusmetodissa. Ensimmäinen huomaamani seikka on ”terveystarkastuksen” aikaväli. NAP pystyy tekemään teoriassa lähes reaaliaikaista tarkastusta työasemien ja palvelimien terveydentilasta, mikäli niissä kesken kaiken tapahtuu muutoksia, esimerkiksi järjestelmänvalvoja käy asettamassa Windowsin oman palomuurin pois päältä. Tällaisessa tilanteessa NAP Agent havaitsee tehdyn muutoksen ja raportoi siitä terveyskäytäntöpalvelimelle, joka taas muutoksen huomatessaan käskee DHCP-palvelinta pudottamaan työaseman rajattuun verkkoon. Tämä kuulostaa erittäin hyvälle ominaisuudelle, mutta DHCP-pakotusmetodin kanssa toimii hieman epäloogisesti.

Tässä pakotusmetodissa terveystarkastukset ovat nimittäin sidottuja DHCP-palvelimen IP-osoitteiden vuokrausaikaan eli ajanjaksoon, minkä tietty annettu IP-osoite on voimassa, esimerkiksi 24 tuntia. Toisin sanoen työaseman terveydentila voi olla lähes vuorokauden sopimattomassa tilassa, ennen kuin asialle tehdään jotain. Tätä aikaväliä voi tietty säätää itse DHCP-palvelimelta lyhyemmäksi, mutta siinäkin on pidettävä varansa, ettei aikaväliä määritä liian lyhyeksi. Isommissa organisaatioissa liian lyhyt vuokrausaikaväli voi hidastaa työasemien verkkoresurssien käyttöä ja koko verkkoliikennettä, koska uusimisprosessi kuormittaa verkkoa.

DHCP-enforcement vaatii myös Network Policy Server (NPS) -instanssin organisaation (yhdelle) DHCP-palvelimelle, joko välittäjäpalvelinroolin (Proxy) tai itse NPS-palvelinroolin asennettuna ja konfiguroituna.

Palvelinpuolelta huomasin myös erään mahdollisen käytännön ongelman. Oman työkokemukseni pohjalta olen huomannut, että oikeassa yritysympäristössä osa

palvelinkoneista on säädetty käyttämään kiinteää IP-osoitetta, jolloin DHCP-palvelimen toiminta ei koske kyseisenlaista palvelinkonetta. Tällöin koko DHCP-pakotusmetodia käyttävä NAP ohitetaan, kun kiinteää IP-osoitetta käyttävä palvelinkone ei missään vaiheessa tee NAP-protokollan ensimmäistä vaihetta eli ota yhteyttä DHCP-palvelimeen. Tämä ei välttämättä ole varsinainen ongelma, sillä palvelinkoneita tarkkaillaan muutenkin tarkemmin ja syvällisemmin niiden suorittamien prosessien ja tehtävien vuoksi, kuin tavallisia työasemia.

DHCP-pakotusmetodin etuja muihin metodeihin verrattuna on sen käyttöönoton helppous ja yhteensopivuus myös muiden pakotusmetodien kanssa. Se ei vaadi erityisiä muutoksia DHCP-palvelimelle tai organisaation DHCP-arkkitehtuuriin.

Kokonaisuutena DHCP-pakotusmetodi ei ole varmin ja luotettavin mahdollinen vaihtoehto, mikäli sen toteuttaja ei ota kaikkia osakokonaisuuksia huomioon. Esimerkiksi mikäli työntekijällä on pääsy työasemansa verkkoasetuksiin ja mahdollisuus muuttaa siten IP-osoite kiinteäksi, koko metodi ohitetaan. DHCP-pakotusmetodi saadaan kyllä luotettavaksi ja toimivaksi ratkaisuksi, mikäli käyttäjien oikeuksia rajoitetaan eri ryhmäkäytäntöjen avulla.

3.6.2 NAP EC: VPN

Termi VPN tulee sanoista Virtual Private Network ja on kahden tai useamman eri verkon välinen, näennäisesti yksityinen verkko. VPN-pakotusmetodi käyttää tyypillistä VPN-etäyhteyttä, jossa etätietokoneen (VPN client) ja VPN-yhdyskäytävän (gateway) välinen kommunikaatio kryptataan.

VPN-pakotusmetodin prosessi on hyvin samanlainen, kuin vastaavassa DHCP-metodissa, tosin muutama ero löytyy. Ensimmäinen konkreettinen ero on, että käyttäjän yrittäessä muodostaa etäyhteyttä työasemassa oleva NAP-client ottaa DHCP-palvelimen sijasta yhteyttä VPN-palvelimeen. Toinen eroavaisuus on siinä, että NAP-client lähettää seuraavaksi käyttäjän autentikointitiedot NAP-terveyskäytäntöpalvelimelle. Mikäli käyttäjä tunnistetaan, vasta sen jälkeen NAP-client lähettää työaseman terveydentilatiedot samalle palvelimelle.

Tämän metodin etuihin voidaan lukea sen käyttöönoton helppous sekä työasema- että palvelinpuolella. Kaikki tarvittavat ohjelmistokomponentit ovat valmiiksi asennettuina niissä Windows-käyttöjärjestelmissä, joiden kanssa Network Access Protection toimii. Se on myös ainoa konkreettinen NAP-metodi, jota voidaan käyttää etäkäyttäjien kanssa. Etäkäyttäjiksi voidaan käsittää esimerkiksi työntekijät, jotka vaikkapa työmatkoillaan työskentelevät kannettavilla tietokoneilla ja tarvitsevat yrityksensä/organisaationsa verkkoresursseja; tai kotoa käsin työskentelevät työntekijät.

Vaikka VPN-pakotusmetodi ei vaadikaan ulkoisia ohjelmistokomponentteja asennettavaksi, palvelinpuolella täytyy ottaa käyttöön Windows Server 2008:n Routing and Remote Access -ominaisuus.

VPN-enforcementin terveydentilatarkastus toimii DHCP-kollegaansa nopeammin. Tarkkaa tarkastusväliaikaa en ole lukemistani dokumenteista löytänyt, mutta Microsoftin TechNet-ohjeistuksen mukaan tarkastus tapahtuu ”aktiivisesti”. Mikäli työasema havaitaan sopimattomaksi kesken yhteyden, VPN-metodi asettaa IP-pakettisuodattimet kyseiselle yhteydelle ja asettaa työaseman rajattuun verkkoon.

VPN-enforcementin eduksi voidaan katsoa sen tuki maailmanlaajuisesti käytetyille EAP-autentikointimetodeille (Extensible Authentication Protocol eli laajennettava autentikointiprotokolla), joista esimerkkinä mainittakoon Cisco Systemsin, Microsoftin ja RSA Securityn yhteistyön tulos PEAP (Protected EAP). Yksi yleisimmistä ja tuetuimmista PEAP-muodoista on PEAPv0/EAP-MSCHAPv2, jota tukevat muun muassa Microsoftin, Cisco Systemsin ja Linuxin työasema- ja palvelinimplementaatiot (Ou, 2007).

3.6.3 NAP EC: IPsec

IPsec on lyhenne sanoista Internet Protocol Security ja tarkoittaa käytännössä protokollaryhmää, jotka suojaavat Internet-protokollaa (IP) autentikoimalla ja kryptaamalla jokaisen databittijonon IP-paketin.

IPsec-pakotusmetodi käyttää hieman eri ohjelmistokomponentteja toiminnassaan. NAP:ia ylläpitävässä NPS-palvelinroolissa täytyy olla asennettuna myös Health Registration Authority (HRA) -ominaisuus, jota muut pakotusmetodit eivät vaadi. HRA:n asentaminen vaatii myös Web-palvelinroolin asentamisen samalle fyysiselle palvelimelle. Jos käytössä oleva HRA ja terveyskäytäntöpalvelin sijaitsevat eri palvelimilla, tulee HRA-palvelimesta tehdä RADIUS-client. Mikäli kyseiset palvelinroolit taas sijaitsevat samalla palvelimella, äskeistä ei tarvitse tehdä.

HRA toimii DHCP- ja VPN-palvelinten tavoin niitä vastaavissa pakotusmetodeissa, eli välittää client-koneiden terveydentilatietoja eteenpäin terveydentilapalvelimelle. Toisin kuin aiemmin esitellyissä metodeissa, IPsecissä terveystietojen lähettämisen tekee NAP-clientin sijasta työasemilta ja palvelinkoneilta löytyvä prosessi IPsec Relying Party EC.

Tämäkin metodi käyttää rajattua verkkoa sopimattomien koneiden eristämiseen muusta verkosta. IPsec eroaa kuitenkin siinä, että työaseman terveydentilan arvioinnin jälkeen HRA joko myöntää sille turvallisuussertifikaatin tilan ollessa kunnossa ja täten pääsyn verkkoon, tai eristää koneen rajattuun verkkoon päivitysprosessia varten. IPsec onkin ainoa näistä neljästä pakotusmetodista, jossa työasemalle myönnetään erikseen sertifikaatti sen terveystilasta.

3.6.4 NAP EC: 802.1X

802.1X-pakotusmetodi eroaa muista muutamassa seikassa. Ensimmäinen ja ehkä oleellisin eroavaisuus on itse 802.1x, joka on virallisesti IEEE 802.1X Port Based Authentication eli porttikohtainen todentaminen. IEEE on lyhenne Institute of Electrical and Electronics Engineers -nimestä, joka on kansainvälinen tekniikan alan järjestö. Sen oleellisimpia tehtäviä on tietotekniikan alan standardien määrittely. 802.1X-standardia käytetään IEEE 802-pohjaisten verkkoratkaisujen kanssa eli toisin sanoen pääosin Ethernet- ja WLAN-verkkojen kanssa. Mitä 802.1X siis tekee, on luvattoman verkkoliikenteen estäminen liityntäpisteen kautta, joka on useimmiten kytkimen portti. Lähiverkkoon liittymistä yrittävän tietokoneen eli clientin ja

liityntäpisteen eli autentikaattorin välisessä kommunikaatiossa käytetään EAP-protokollaa, jonka tuloksena tietokone joko autentikoidaan ja päästetään lähiverkkoon tai pääsy evätään.

Eräitä keskeisimpiä eroja muihin pakotusmetodeihin ovat yhteyden muodostuksessa tarvittava kytkin ja muutamat palvelinroolit, joita muissa ei tarvita. Käytettävän kytkimen on oltava datalinkkitason 2 tai 3 kanssa yhteensopiva, tuettava 802.1X-porttikohtaista todentamista ja RADIUS-tunnelointia VLAN-määrityksiä varten. Myös kytkimen VLAN-asetusten ja porttien konfigurointi vaaditulle toimintatasolle on suoritettava, ennen kuin sitä voidaan käyttää tässä pakotusmetodissa.

Kuten muissakin pakotusmetodeissa, tiettyyn lähiverkkoon pyrkivillä työasemilla ja palvelimilla täytyy olla NAP-pakotusclient, joko osana käyttöjärjestelmää tai erillinen sovellus. Uudemmissa Windows-käyttöjärjestelmissä (Windows XP, Vista, Server 2003, Server 2008) kyseinen client on valmiiksi asennettuna. Tässä pakotusmetodissa client tunnetaan nimellä EAPHost NAP EC.

802.1X-pakotusmetodiprosessi alkaa työaseman tai palvelimen ottaessa yhteyden joko lähiverkon Ethernet-kytkimeen tai langattoman verkon liityntäpisteeseen (Action Point, AP). NAP-client lähettää tiedot joko sen hetkisestä käyttäjästä tai tietokoneesta NAP-terveydentilapalvelimelle. Tässä pakotusmetodissa terveydentilapalvelin toimii myös tunnistautumisen varmentavana AAA-palvelimena (Authentication, Authorization and Accounting). Mikäli käyttäjätiedot eivät täsmää aktiivihakemistosta noudettuihin tietoihin verrattuna, yhteysyritys katkaistaan.

Tästä eteenpäin tietokoneiden kommunikoinnissa käytetään eri EAP-protokollia. Käyttäjätietojen ollessa kunnossa terveydentilapalvelin lähettää vastauspyynnön NAP-asiakkaalle sen terveydentilatiedoista, johon NAP-asiakas sitten vastaa lähettämällä tietonsa palvelimelle. Tietojen ollessa kunnossa liityntäpiste suorittaa loppuun 802.1X-autentikoinnin ja sallii käyttäjälle ja tietokoneelle pääsyn oikeaan lähiverkkoon ja sen verkkoresursseihin.

Terveystietojen ollessa puutteellisia tietokone määritellään sopimattomaksi ja eristetään rajattuun verkkoon joko suodattamalla sen käyttöön rajatut IP-määritykset

tai asettamalla se omaan virtuaaliseen lähiverkkoonsa (VLAN). Kummassakin tapauksessa sillä on yhteys ainoastaan päivityspalvelimille.

Käytettäessä 802.1X-pakotusmetodia terveyspolitiikkaan sopivat ja sopimattomat koneet siis voidaan erottaa muista metodeista poiketen eri virtuaalilähiverkkoihin. Toisin sanoen, sopivat koneet pääsevät oikeaan lähiverkkoon ja käyttämään kaikkia annettuja verkkoresursseja, kun taas sopimattomat lähetetään rajattuun lähiverkkoon odottamaan päivitysoperaatioita. Tällä tavalla voidaan estää hyvin tehokkaasti sopimattomien koneiden mahdollisten virusten tai muiden haittaohjelmien pääsy oikean lähiverkon puolelle.

Eräs 802.1X:n lisävaatimus muihin pakotusmetodeihin verrattuna on tarve aktiivihakemiston sertifikaattipalvelulle, joka on asennettava palvelinrooliksi vähintään yhdelle palvelinkoneelle. Tämän pakotusmetodin käyttämä TLS-autentikaatio PEAP-protokollalle vaatii NPS-palvelimelle luottamussertifikaatin, jonka sertifikaattipalvelin sitten toimittaa ja jonka perusteella asiakaskoneet luottavat NPS-palvelimeen.

3.6.5 Pakotusmetodien yhteensopivuus

	IPsec	802.1x	VPN	DHCP
IPsec		Kyllä	Kyllä	Kyllä
802.1X	Kyllä		Ei	Kyllä
VPN	Kyllä	Ei		Ei
DHCP	Kyllä	Kyllä	Ei	

Taulukko 1 Pakotusmetodien yhteensopivuus

Kuten taulukosta 1 käy ilmi, IPsec-metodia voidaan käyttää yhdessä jokaisen muun metodin kanssa, kun taas VPN ei sovellu muiden kuin IPsecin kanssa yhteen. Opinnäytetyöni kannalta tämä oli lievä pettymys, sillä olisin halunnut kokeilla yhdistää DHCP- ja VPN-pakotusmetodien käytön.

4 WINDOWS SERVER 2008 KÄYTÄNNÖSSÄ

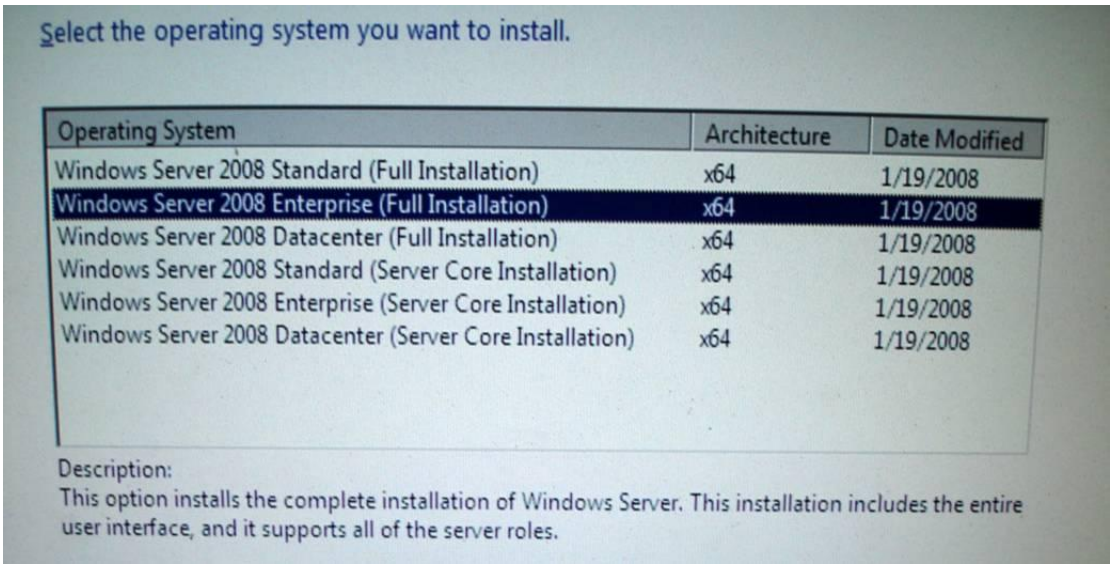
4.1 Käyttöjärjestelmän asentaminen

Opinnäytetyöni tekninen osio lähti käyntiin marraskuun loppupuolella saadessani uuden palvelintietokoneen käyttööni. Koneessa ei ollut alkuperäisenä mitään käyttöjärjestelmää, joten opinnäytetyöni tekninen osio alkoi sen asentamisella.

Ensimmäisenä käyttöjärjestelmävaihtoehtona mietin Hyper-V Server -versiota, jonka olisi saanut ladattua Microsoftin verkkosivuilta ilmaiseksi. Asiaan hieman tarkemmin perehdyttyäni huomasin kuitenkin, ettei kyseinen versio soveltuisi työhöni. Hyper-V Server on käytännössä erittäin rajallinen käyttöjärjestelmä ja vaatii hallinnointia varten toisen tietokoneen. Tässä toisessa tietokoneessa tulee vielä olla joko kaupallinen, kaikilla ominaisuuksilla varustettu versio Windows Server 2008:sta tai Windows Vista, joiden erillisellä Hyper-V Manager MMC -hallintaohjelmistolla Hyper-V Serveriä sitten pyöritetään (Microsoft 2008). Käytännöllisistä syistä hylkäsin tämän käyttöjärjestelmäversion asentamisen.

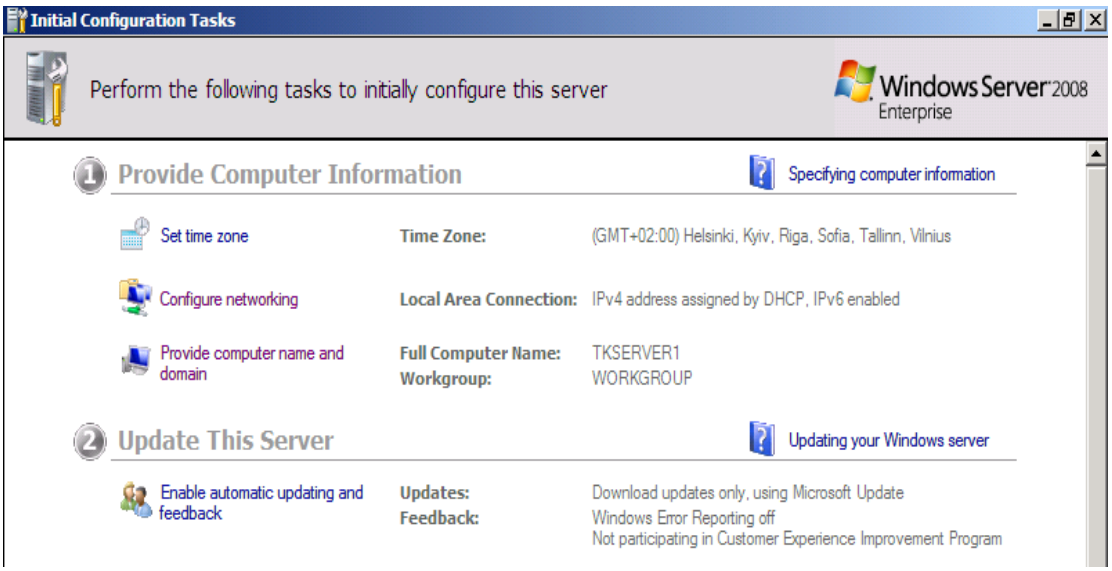
Seuraava vaihtoehto oli joko Enterprise tai Datacenter, joista kummankin hankkiminen oli mahdollista Savonia-ammattikorkeakoulun ja Microsoftin kaupallisen yhteistyön johdosta. Tietojenkäsittelyopiskelijana minulla oli mahdollisuus ladata molemmat versiot sisältävä asennuspaketti Microsoftin MSDNAA-palvelun kautta.

Ominaisuuksiensa ja toiminnallisuutensa puolesta kummatkin versiot olisivat käyneet opinnäytetyötäni varten yhtä hyvin, valitsin kuitenkin Enterprise-version ajatellen lähinnä opinnäytetyöni pientä mittakaavaa, Datacenter kun on enemmän suuryritysten versio.



Kuva 10 Käyttöjärjestelmän asennus

Käyttöjärjestelmän asentaminen itsessään ei ollut vaikea toimenpide, järjestelmä käynnistetään asennuslevyltä ja valitaan haluttu käyttöjärjestelmäversio asennusohjelman näyttäessä vaihtoehdot.



Kuva 11 Initial Configuration Tasks -hallintatyökalu

Salasanan vaihtamisen ja onnistuneen sisäänkirjautumisen jälkeen käyttäjälle tulee ensimmäiseksi esiin Initial Configuration Tasks -konsoli-ikkuna. Sen kautta käyttäjä voi vaihtaa järjestelmän asetuksia, kuten tietokoneen nimen, verkkoasetukset ja verkkotoimialueen jäsenyyden. Oletuksena palvelintietokone saa satunnaisesti generoidun nimen, jonka muutin TKSERVER1-nimiseksi. Windowsin asennuksen

jälkeen liitin koneen Savonian verkkotoimialueeseen päivitysten ja tulevien virtuaalikoneiden verkkoyhteyden vuoksi.

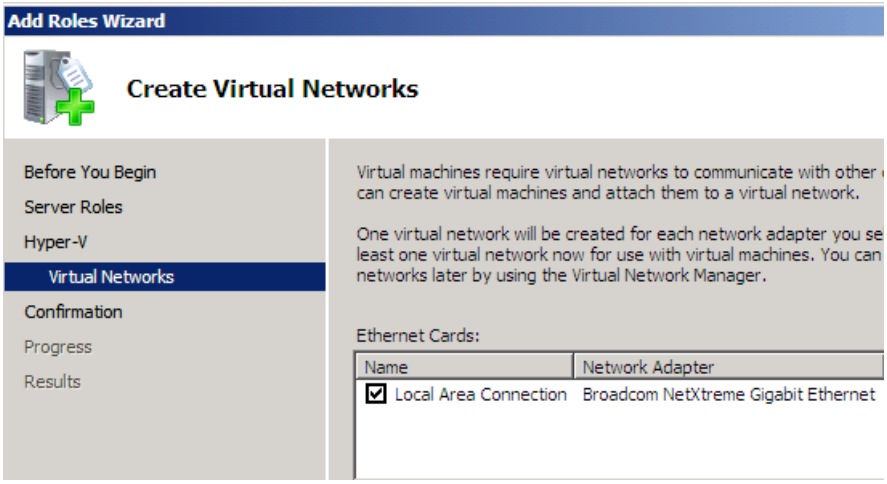
4.2 Hyper-V käytännössä

4.2.1 Hyper-V:n asentaminen

Hyper-V oli eräs keskeisimmistä käyttämistäni Windows Server 2008 -käyttöjärjestelmän uusista ominaisuuksista. Hyper-V mahdollisti itse fyysisen palvelinkoneen pitämisen pelkkänä isäntänä oikealle testijärjestelmälleni, joka isännöinnin lisäksi välitti niille verkkoyhteyden.

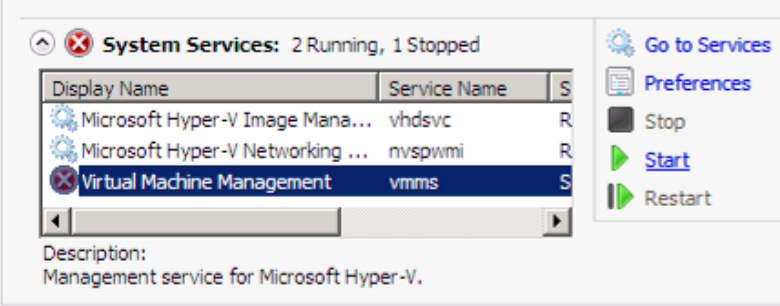
Ennen Hyper-V-palvelinroolin asentamista tulee BIOS:n puolelta Virtualization Technology -asetus määrittää Enabled-tilaan, mikä on oletuksena pois päältä. Tämä asetus mahdollistaa ylipäätään virtuaalisointiteknologian käytön.

Asensin Hyper-V-palvelinroolin valitsemalla Server Manager -työkalusta uuden palvelinroolin asentamisen. Ensimmäinen konkreettinen huomioni oli, että palvelinroolin asennuksen yhteydessä samalla luodaan fyysisen palvelinkoneen verkkokortin virtuaalinen ilmentymä eli virtuaaliverkkokortti. Tätä virtuaaliverkkokorttia käytetään myöhemmin luotavan virtuaaliverkon kanssa, jonka kautta virtuaalikoneet puolestaan saavat eri verkkoresursseja käyttöönsä.



Kuva 12 Virtuaaliverkkokortin tekeminen

Asennuksen valmistuttua käynnistin palvelinkoneeni uudestaan, jonka jälkeen huomioin, ettei Hyper-V:n toimintaa ohjaava prosessi vmms.exe (Virtual Machine Management Service) ei käynnistynyt automaattisesti. Prosessin sai kuitenkin helposti käyntiin valitsemalla Server Managerista Hyper-V-roolin alta System Services ja painamalla Start-painiketta vmms.exen kohdalla.



Kuva 13 Virtual Machine Management Service -prosessin käynnistäminen

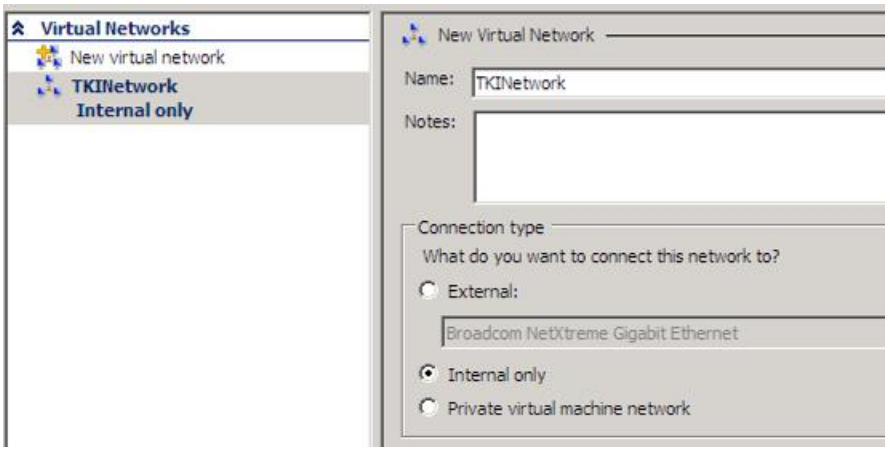
Huomioitavaa tämä on siinä mielessä, että vmms.exe-prosessin ollessa pysäytetyssä tilassa Hyper-V-palvelinrooli ei toimi ollenkaan. Kyseinen ongelma ilmeni opinnäytetyöprosessini aikana vain tämän kerran.

4.2.2 Uuden virtuaalikoneen ja -lähiverkon luominen

Seuraava keskeinen vaihe opinnäytetyöni toteuttamisessa oli virtuaalikoneiden asentaminen ja toimintaan saattaminen sekä myös virtuaalilähiverkon luominen.

Periaatteessa on sama, kummassako järjestyksessä nämä tekee, joskin on loogisempaa luoda ensin virtuaalilähiverkko ja vasta sitten siihen liittyvät virtuaalikoneet. Sanottava kyllä on, että tein ajattelemattomuuttani itse juuri päinvastoin.

Uuden virtuaaliverkon luominen tapahtuu Hyper-V Manager -työkalua käyttämällä. Työkalun Action-valikosta valitaan Virtual Network Manager. Avautuvan asennusikkunan kautta voidaan valita verkon ja yhteyden tyyppi, sekä nimi. Sekä verkon että yhteyden tyyppivaihtoehdot ovat samat, ulko-, sisä- tai yksityinen verkko. Opinnäytetyössäni käytin ulkoverkkoa ja yksityistä verkkoa. Ulkoverkko nimensä mukaisesti mahdollistaa yhteyden ulkomaailmaan oikeisiin verkkoihin. Tällaisesta verkosta esimerkkinä opinnäytetyössäni käyttämä Savonia-ammattikorkeakoulun verkko. Yksityisverkkoa käytetään monesti yritysten sisäisissä verkkoratkaisuissa, joissa verkon työasemien ja palvelimien näkyminen ulkopuoliseen verkkomaailmaan halutaan rajata. Sisäverkkoa testasin hyvin lyhyesti työni alkuvaiheilla, joskin toimeksiantajani yhteyshenkilön Timo Kinnusen neuvosta hylkäsin sen käytön ja vaihdoin yksityiseen verkkoon.



Kuva 14 Uuden virtuaalilähiverkon luominen

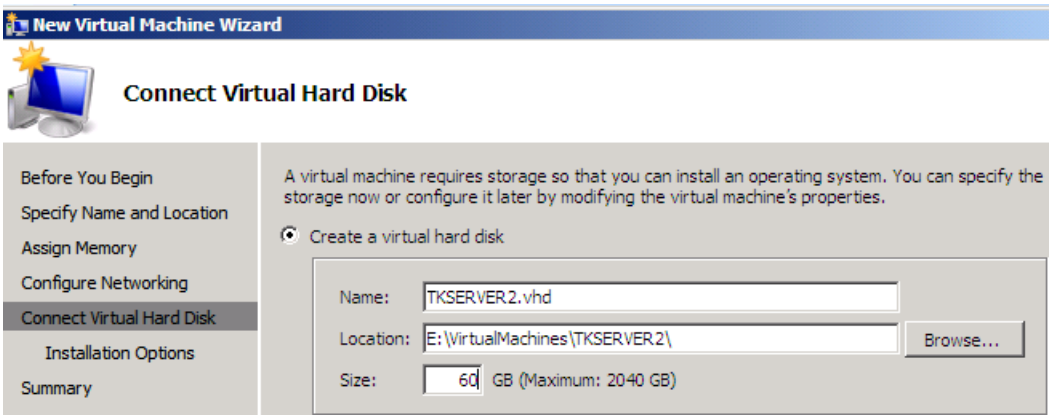
Virtuaaliverkkojen luominen oli minulle aivan uusi asia, enkä aluksi oikein tiennyt, mitä niistä minun pitäisi käyttää. Tästä todisteena kuva 14, jossa loin sisälähiverkon, mitä käyttämällä uskoin saavani virtuaalikoneet kommunikoimaan keskenään. Tämä verkkoratkaisu ei toiminut, joten muutin kyseisen verkon tyypin yksityiseksi verkoksi.

Kahden erityyppisen verkon ollessa käytössä virtuaalikoneeni käyttivät myös kahta eri virtuaaliverkkoadapteria, joista toinen ohjasi ulospäin menevää verkkoliikennettä ja toinen yksityisverkon eli virtuaalikoneiden välistä liikennettä.

Loin seuraavaksi kaksi tarvitsemaani virtuaaliverkkoa, joista toinen toimi ulkoverkkona ja toinen opinnäytetyössä käyttämieni virtuaalikoneiden yksityissisäverkkona. Käytin virtuaaliverkkojen niminä TKPNetwork sisäverkolle ja TKENetwork ulkoverkolle.

Uusien virtuaalikoneiden tekeminen tapahtuu myös Hyper-V Manager -työkalun kautta. Kätevimmin tämän työkalun, kuten muutkin palvelin- ja palvelurooleihin liittyvät työkalut, löytää Administrative Tools -valikon kautta.

Uuden virtuaalikoneen luominen on hyvin opastettua. Asennustyökalun kautta määritetään kaikki olennaiset seikat, kuten koneen nimi, virtuaalisen kiintolevyn koko ja sen sijainti fyysisellä palvelinkoneella sekä käytettävä virtuaaliverkko.



Kuva 15 Uuden virtuaalikoneen asennusohjelma

Käytin opinnäytetyössäni yhteensä kolmea virtuaalitietokonetta, joista kaksi oli palvelinkoneita ja yksi työasema, jota käytin virtuaaliverkkoympäristöni testaamiseen. Nimesin virtuaalipalvelimet nimillä TKSERVER2V ja TKSERVER3V. Virtuaalityöaseman nimenä toimi TKWSXP1V. Opinnäytetyössä käyttämästäni nimeämislogiikasta on enemmän luvussa 4.8 Tietokoneiden nimeämis- ja salasanakäytäntö.

Asetin jokaisen virtuaalikoneen keskusmuistin määräksi 1024 megatavua ja kiintolevyn suuruudeksi 60 gigatavua. Näillä määrityksillä sekä fyysinen isäntäkone, että kaikki kolme virtuaalikonetta toimivat yhtäaikaisessa käytössä loistavasti.

Taulukko 2 Virtuaalipalvelimien palvelinroolit

Virtuaalikoneen nimi	Palvelinroolit
TKSERVER2V	Aktiivihakemisto, DNS-palvelin, WSUS-palvelin
TKSERVER3V	DHCP-palvelin, NPS-palvelin

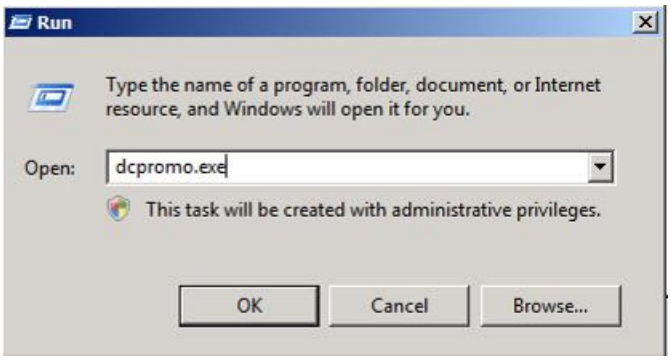
Kaikkein pelkistetyimmässä muodossaan kaikki käyttämäni palvelinroolit saa asennettua yhdelle palvelinkoneelle, joskin käytettävyys- ja tietoturvasyistä roolien jakaminen eri palvelimille, ovat ne sitten fyysisiä tai virtuaalisia, on Microsoftin Server 2008 -turvallisuusohjedokumentin (Microsoft, 2008) mukaan suositeltavaa.

4.3 Aktiivihakemisto

Virtuaalikoneiden ollessa toimintakunnossa seuraava vaihe opinnäytetyöprosessiani oli asentaa aktiivihakemisto ja sen rinnalle DNS-palvelinrooli.

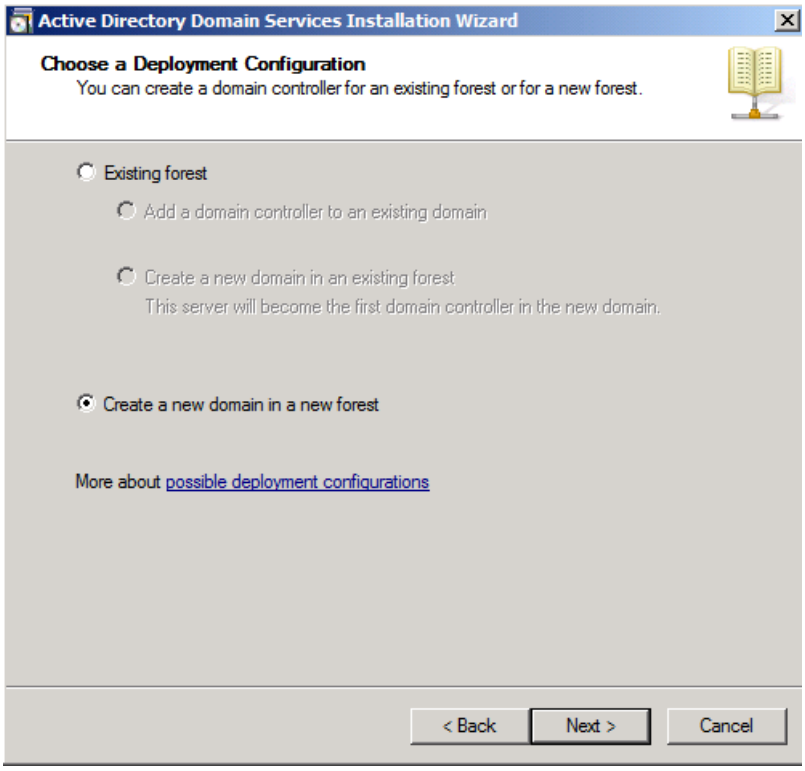
Opinnäytetyössäni luoma ja käyttävä aktiivihakemisto oli osittain mallinnettu Savonia-ammattikorkeakoulun (erityisesti silloisen Liiketalouden yksikön) aktiivihakemistoratkaisusta. Oma aktiivihakemistoni poikkesi tietysti paitsi kooltaan myös sisällöltään. Savonian aktiivihakemistossa käyttäjiä ja erilaisia käyttäjä- ja koneryhmiä oli satoja, kun taas itse loin vain oleellisimmat testikäyttäjät ja ryhmät, joihin käyttäjiä sitten lisäsin.

Ensimmäinen vaihe aktiivihakemistopalvelimen luomisessa oli asentaa Server Managerin kautta aktiivihakemiston toimialuepalvelu -ominaisuus (Active Directory Domain Services). Samassa yhteydessä valitsin asennusvalikosta myös DNS-palvelinroolin.



Kuva 16 Aktiivihakemiston konfigurointityökalun suorittaminen

Seuraavaksi aktiivihakemistopalvelin pitää vielä konfiguroida, mikä tapahtuu suorittamalla Dcpromo.exe-ohjelma. Tämä aukaisee asennusohjelman, jossa määritellään keskeiset toimialueeseen liittyvät tiedot ja asetukset.



Kuva 17 Uuden toimialuemetsän luominen

Tässä vaiheessa aktiivihakemiston konfigurointia on mahdollista liittää luotava toimialue olemassa olevaan toimialuemetsään, mikäli sellainen on jo luotu aiemmin. Tämä oli kuitenkin ensimmäinen lajiaan, joten valitsin uuden toimialueen ja metsän luovan vaihtoehdon.

Annoin aktiivihakemiston tulevalle toimialueelle viralliseksi nimeksi (FQDN eli fully qualified domain name) tk.bassosoolo.com. Tuossa vaiheessa opinnäytetyöni tekovaihetta en oikein käsittänyt, mihin etuliite nimessä vaikutti; noudatin asennusohjelman esimerkkiä, vaikka käsittääkseni etuliitteen olisi voinut jättää poiskin.

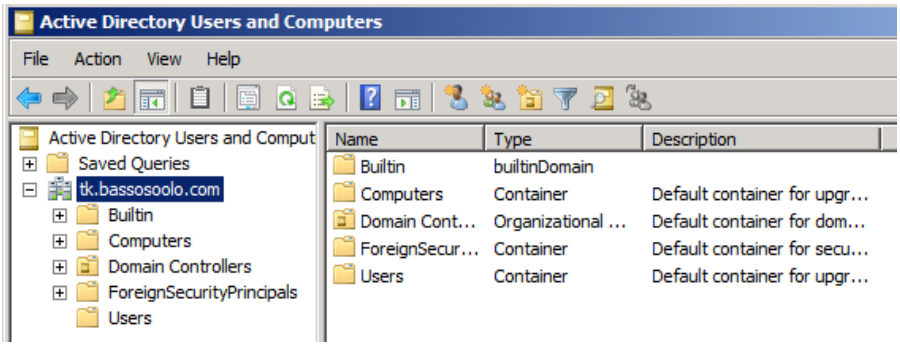
Kuva 18 Toimialueen nimeäminen

Loput asennusohjelman kohdista olivat valmiiksi esimääriteltyjä, joskin niitä olisi voinut halutessaan muuttaa; koin järkevimmäksi suorittaa asennuksen oletusvaihtoehtoja käyttäen. Nämä asennusohjelman kohdat käsittelivät toimialuemetsän toiminnallisuustasoa (forest functional level) ja aktiivihakemiston konkreettista asennuspolkua palvelinkoneen kiintolevyllä.

Kuva 19 Aktiivihakemiston asennus

Aktiivihakemiston asennus on tämän jälkeen valmis. Tästä alkaakin vasta virallinen työ aktiivihakemiston kanssa. Lähtötilanteessa (kuva 20) aktiivihakemisto ei pidä

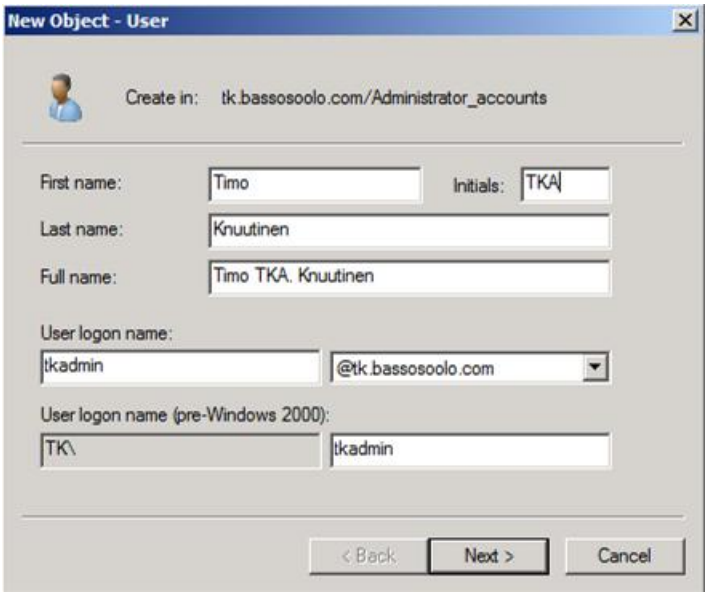
sisällään muuta, kuin valmiiksi siihen sisällytetyt komponentit ja kansiot, joista on onneksi helppo ottaa mallia ja lähteä luomaan tarvitsemiaan elementtejä.



Kuva 20 Lähtötilanne uuden aktiivihakemiston kanssa

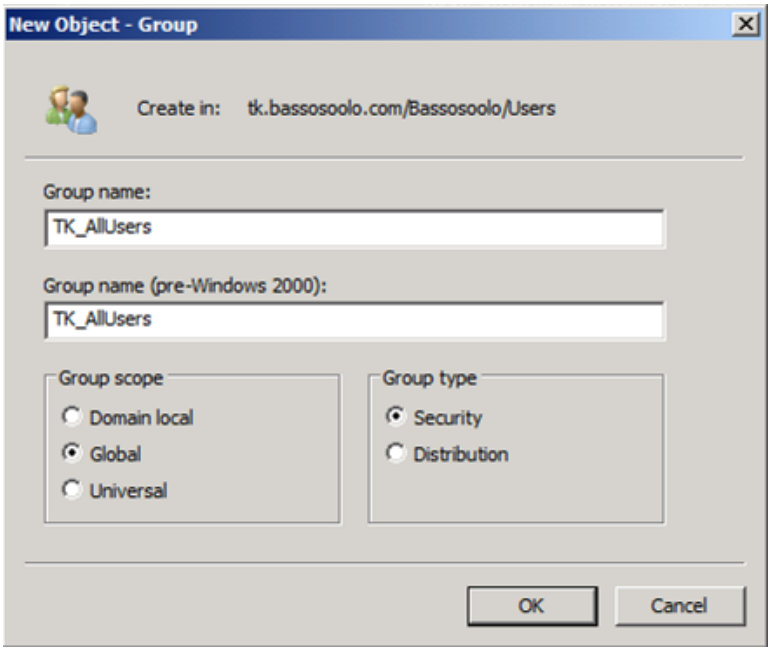
Loin kuvassa 20 näkyvän tk.bassosoolo.com-toimialuerakenteen alle Administrator_accounts ja Bassosoolo-organisaatioryhmät. Administrator_accounts-ryhmään sain mallin Savonia-ammattikorkeakoulun aktiivihakemistorakenteesta, jossa vastaavaan ryhmään oli lisätty kaikki mahdolliset järjestelmänvalvojatunnukset. Omassa työssäni kyseinen ryhmä ei välttämättä olisi ollut tarpeellinen järjestelmänvalvojatunnusten vähäisen määrän vuoksi. Kyseisen ryhmän luominen helpottaa kyllä käyttäjähallintaa, mikäli järjestelmänvalvojatunnuksia on useampia. Tässä tapauksessa lisätään kaikki järjestelmänvalvojat jäseniksi vain siihen ja kyseinen ryhmä Server 2008:n esiluotuihin Domain- ja Enterprise Admins -käyttäjäryhmiin.

Oleellinen osa aktiivihakemistoa ja keskeinen syy sen olemassaoloon ovat käyttäjät, jotka käyttäjätunnuksillaan kirjautuvat yrityksen/organisaation toimialueverkkoon. Omassa opinnäytetyössäni käytin siis fiktiivistä Bassosoolo-organisaatiota ja tämän käyttäjiksi loin kolme eri käyttäjää, joista jokainen kuului hieman eri käyttäjäryhmiin ja täten sai hieman erilaisia verkko-oikeuksia ja -resursseja käyttöönsä.



Kuva 21 Uuden käyttäjätunnuksen luominen

Uuden käyttäjän luominen tapahtuu samaan tapaan riippumatta siitä, minkälaisen käyttäjän luo, toisin sanoen järjestelmänvalvoja ja peruskäyttäjä luodaan samalla kaavalla.



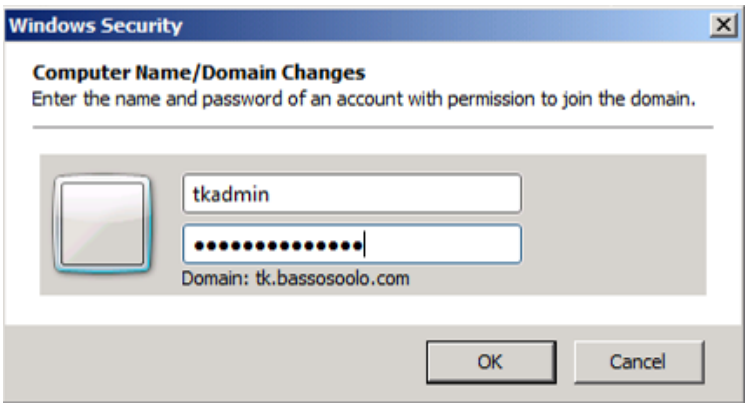
Kuva 22 Uuden ryhmän luominen

Uuden ryhmän luominen tapahtuu myös hyvin samaan tapaan. Kuvassa x loin kaikki käyttäjät sisältävän TK_AllUsers-käyttäjäryhmän. Vaihtoehtoina ryhmän luomisessa

ovat sekä ryhmän käyttöalue (scope) ja tyyppi. Domain local -vaihtoehto voi sisältää jäseniä eri toimialueilta, mutta niiden käytettävissä olevat resurssit rajoittuvat vain siihen toimialueeseen, jossa ne luodaan. Global puolestaan voi sisältää jäseniä vain sen omalta toimialueelta, joskin ne saavat resursseja useammalta samassa toimialuemetsässä sijaitsevalta toimialueelta. Universal-vaihtoehto antaa puolestaan mahdollisuuden lisätä ryhmään jäseniä useilta eri toimialueilta ja päästä useiden toimialueiden resursseihin. Ryhmätyypeistä Distribution-vaihtoehtoa voidaan käyttää vain sähköpostilistojen luomiseen, Security mahdollistaa oikeuksien antamisen eri resursseihin.

Valitsin näistä vaihtoehdoista kaikkiin luomiini ryhmiin Global käyttöalueeksi ja tyypiksi Security, jotka ovat itse asiassa oletuksena valittuina.

Työaseman tai palvelinkoneen liittäminen toimialueeseen on eräs ensimmäisiä vaiheita, jossa tarvitaan toimialuekelpoista järjestelmänvalvojatunnusta. Kuvassa x käytin aiemmin luomaani ”tkadmin”-tunnusta autentikoimaan liittymistä; tällä estetään aiheettomien tietokoneiden pääsy lähiverkkoon.



Kuva 23 Toimialueeseen liittyminen

Liitin TKSERVER3V-palvelimen lisäksi toimialueelle Windows XP -virtuaalityöaseman, jolla suoritin käytännön testauksia. TKSERVER2V-palvelin oli toimialueen jäsen automaattisesti sen ollessa itse aktiivihakemistopalvelin.

Aloitin aktiivihakemiston toiminnan testaamisen työaseman puolella hyvin yksinkertaisella toimenpiteellä, syöttämällä ensin satunnaisia kirjaimia

käyttäjätunnukseksi ja salasanaksi sekä sen jälkeen kokeilemalla aiemmin luomaani tunnusta.

Kuva 24 Epäonnistunut kirjautuminen

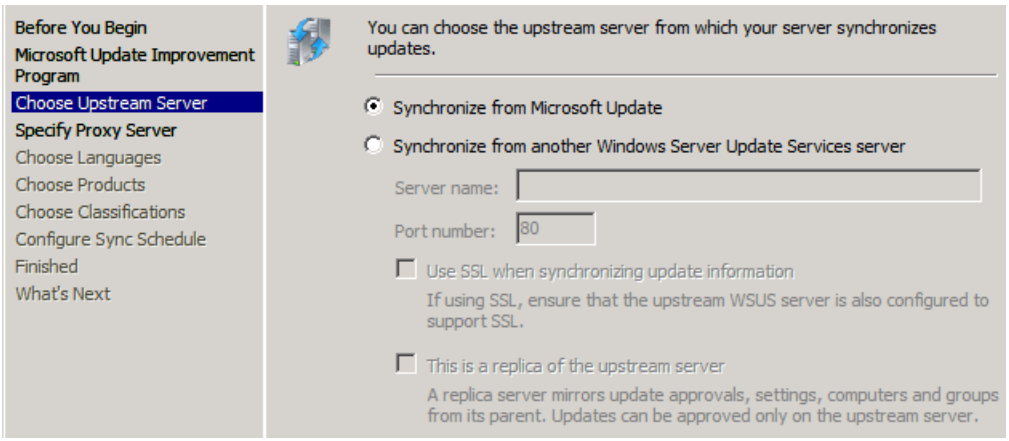
Yrittämällä kirjautua olemattomalla tunnuksella, tuloksena on ilmoitusteksti, jossa kehoitetaan tarkastamaan tunnus, salasana sekä toimialue.

Kuva 25 Onnistunut kirjautuminen

Onnistuneen kirjautumisen jälkeen käyttäjälle alkaa latautua Windows-käyttöympäristö.

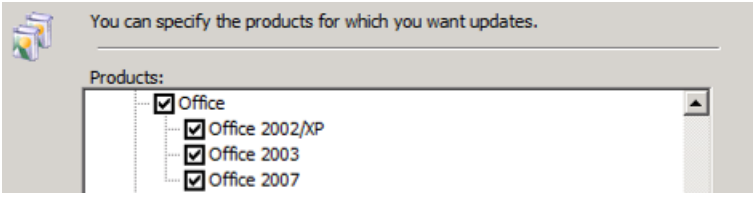
4.4 Windows Server Update Services

Osana opinnäytetyöni teknistä prosessia oli myös kokeilu päivityspalvelun luomisesta ja käyttämisestä. Server Manager -työkalua käyttäen asensin Windows Server Update Services (WSUS) -palvelinominaisuuden TKSERVER2V-virtuaalipalvelimelle.



Kuva 26 WSUS-palvelimen asentaminen

Asennuksen yhteydessä voi valita ladattavien päivitysten lähteen, mikäli haluaa käyttää useampaa palvelinta tai välityspalvelinta. Työni kannalta ainoa vaihtoehto oli käyttää oletuksena valittua Microsoft Update -järjestelmää. Vaihtoehdosta riippumatta halutut päivitykset ladataan asennetulle WSUS-palvelimelle, josta ne sitten asetuksista riippuen joko automaattisesti tai manuaalisesti siirretään ja asennetaan työasemakoneille.



Kuva 27 WSUS-päivitysten määrittäminen

WSUS-palvelimen työkalukonsoli antaa vapaasti valita saatavilla olevista päivityksistä halutut, useimmista päivityksistä on myös lokalisoituja kieliversioita saatavilla. Määritin työssäni ladattavaksi vain keskeiset järjestelmäpäivitykset sekä Microsoft Office -tuoteperheeseen liittyvät päivitykset.

WSUS-hallintakonsolilla on mahdollista luoda eri tietokoneryhmiä, joihin voi kohdistaa eri toimintoja, aktiivihakemiston tapaan. Loin testityöasemaani varten ryhmän WinXPs, vaikka yhtä konetta käyttäessä olisi selvinnyt ilman kyseisen ryhmän luomistakin. Eri tietokoneryhmät helpottavat päivityspalvelimenkin puolella eri tietokoneiden hallintaa, jakamalla ne vaikkapa juuri käyttöjärjestelmän mukaan.

Ennen kuin päivityspalvelinta voidaan käyttää Windowsin päivitysten jakelemisessa, on tehtävä muutama keskeinen säätö ryhmäkäytäntöjen puolelle, tarkemmin asiasta osiossa 4.5 Ryhmäkäytännöt.

4.5 Ryhmäkäytännöt

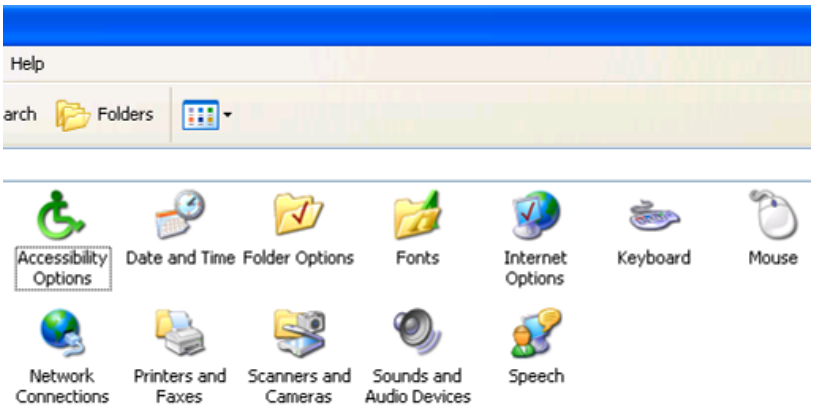
4.5.1 Käyttäjiä koskevat ryhmäkäytännöt

Kuva 28 Virtuaalityöasemakäyttäjän työpöytänäkymä

Opinnäytetyötä toteuttaessani koin järkeväksi luoda vain kaksi käyttäjätunnuksia koskevaa ryhmäkäytäntöä, ensimmäisenä TK_AllUsersGPO, johon kaikki käyttäjät kuuluvat. Loin toiseksi käytännöksi TK_BasicUsersGPO-objektin, johon kuuluvat niin sanotut peruskäyttäjät, joiden työaseman käyttöä on syytä rajata sekä mahdollisen heikomman teknisen taitotason, että työtehtävien vuoksi. Käytännössä tämä tarkoittaa sitä, että luomalleni tk.bassosoolo.com-toimialueelle kirjautuessa järjestelmä tarkastaa, kuuluuko käyttäjä pelkästään toiseen GPO:hon vai molempiin. Mikäli hän

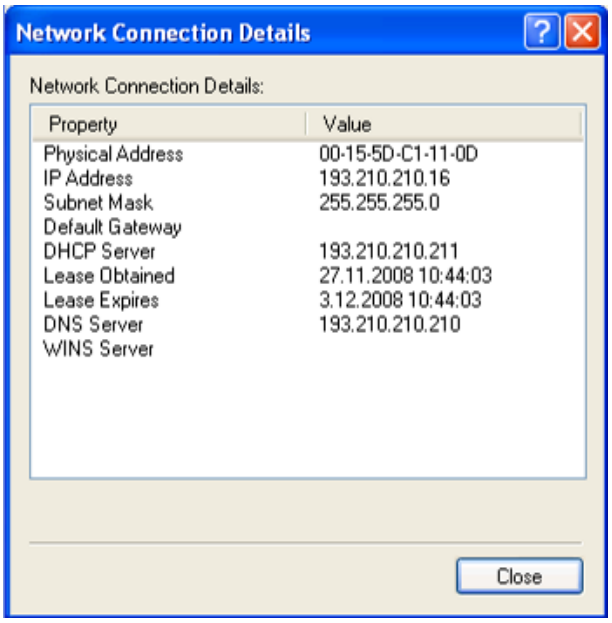
kuuluu vain ”kaikkiin käyttäjiin”, hän saa käyttöönsä enemmän oikeuksia. Jos taas käyttäjä kuuluu myös peruskäyttäjiin, sovelletaan osittain molempia käytäntöjä, jolloin TK_BasicUsersGPO:sta haetaan ensin käyttäjää koskevat määritykset ja sen jälkeen katsotaan onko TK_AllUsersGPO:ssa vielä joitain määrityksiä, joita ei ole asetettu ensimmäisessä. Tällä tavalla säästää hieman vaivaa, kun tietyt asetukset määritetään vain kerran koskemaan kaikkia käyttäjiä ja asetetaan sitten toisella GPO:lla lisämääritteitä.

TK_AllUsersGPO määrittää käyttäjille muun muassa työpöydän taustakuvan, Start-valikon alivalikot ja toiminnot sekä työaseman Ohjauspaneelin kuvakkeet ja toiminnot. TKBasicUsersGPO karsii puolestaan pois käytöstä muutamia ominaisuuksia, joten peruskäyttäjän toimintaympäristö on melko pelkistetty. Peruskäyttäjä pääsee säätämään muutamia työaseman toimintaan liittyviä asetuksia, esimerkiksi mikäli on tarvetta säätää hiiren liikeherkkyyttä tai verkkoyhteyden toimintaan liittyvän ongelmatilanteen sattuessa,



Kuva 29 Peruskäyttäjän Ohjauspaneeli

Peruskäyttäjän käyttörajoituksiin kuuluvat myös verkkoasetukset. TK_BasicUsersGPO- ryhmäkäytännöllä on määritelty, että käyttäjällä ei ole oikeuksia muuttaa verkkoasetuksia, vain tarkastella niitä ja ilmoittaa järjestelmänvalvojalle tiedot eteenpäin mahdollisessa ongelmatilanteessa.

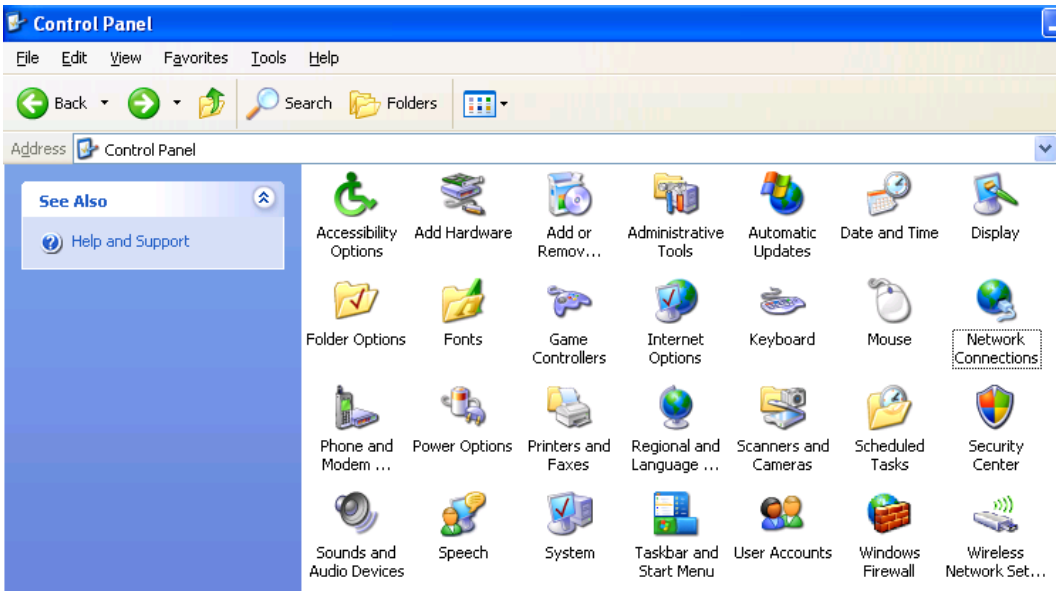


Kuva 30 Peruskäyttäjän verkkoyhteystiedot

Seuraavaksi esittelen lyhyesti, miten eri ryhmäkäytäntöjen piiriin kuuluvat käyttäjät näkevät ja kokevat työaseman käyttöjärjestelmän.

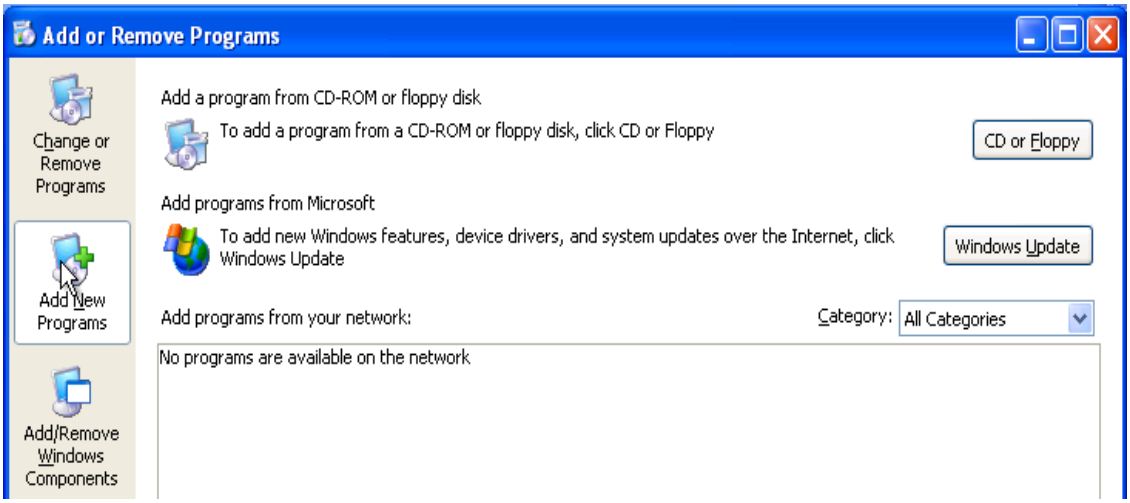
Kuva 31 Työasemalle kirjautuminen laajemmilla oikeuksilla

Kirjaudutaan samalle toimialueelle ainoastaan TK_AllUsersGPO-ryhmäkäytännön piiriin kuuluvan testihenkilö Ilkka Kirvesahon tunnuksella. Käyttäjälle avautuva Windowsin työpöytä on näkymältään hyvin identtinen TKBasicUsersGPO-käyttäjienkin kanssa.



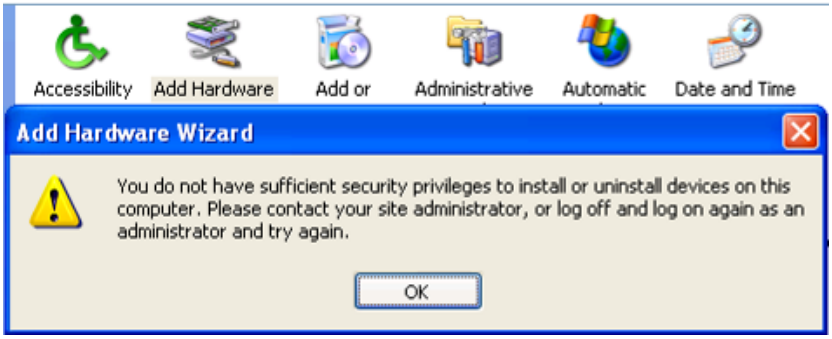
Kuva 32 Edistyneempien käyttäjien Ohjauspaneeli

Erot tulevat paremmin näkyviin Ohjauspaneelin puolella. Oletuksena siis on, että edistyneempien käyttäjien ryhmään kuuluvat henkilöt ymmärtävät tietokoneen toiminnasta enemmän ja osaavat näin ollen tehdä mahdollisia muutoksia tietäen, mitkä niiden seuraukset ja vaikutukset ovat.



Kuva 33 Uusien ohjelmien asennus

Edistyneemmillä käyttäjillä on oikeus asentaa työasemalle tarvitsemiaan ohjelmia, peruskäyttäjillä ohjelmienasennusvalikkoa ei saa edes näkyviin.



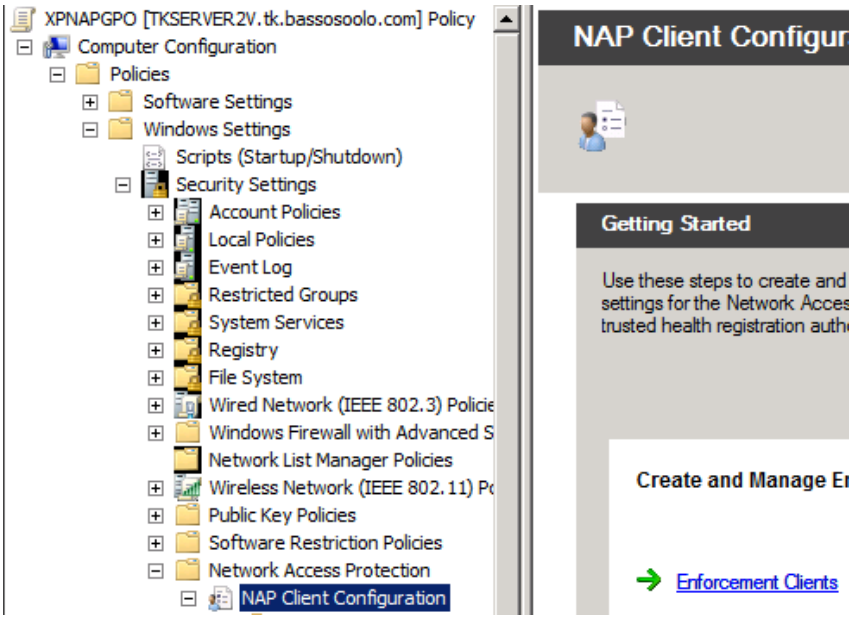
Kuva 34 Laitteen lisääminen

Määritin kuitenkin, että laitteistopuolen lisäykset tai poistot suoritetaan pelkästään järjestelmänvalvojien toimesta. Mikäli peruskäyttäjät tarvitsevat joitain erityisohjelmia, niiden asennus hoidetaan luonnollisesti myös järjestelmänvalvojien toimesta.

4.5.2 Ryhmäkäytännöt ja NAP

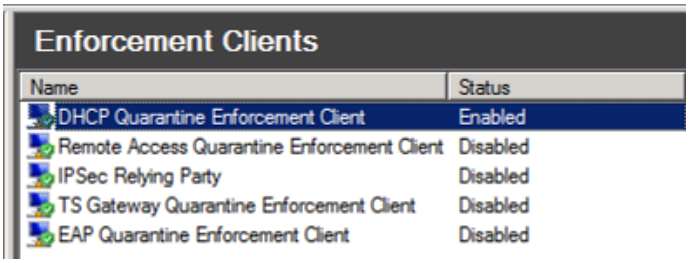
Opinnäytetyöni kannalta keskeinen ominaisuus Network Access Protection vaatii myös hieman säätöä ryhmäkäytäntöjen puolelle toimiakseen kunnolla. Windows Server 2008 -käyttöjärjestelmän ryhmäkäytäntöominaisuuteen on itseensä sisällytetty esiluodut käytännöt NAP:ia koskien, jotka kuitenkin täytyy käydä määrittämässä toimintaan.

Loin uuden ryhmäkäytännön nimeltään XPNAPGPO, johon tein ainoastaan NAP-ominaisuutta koskevat säädöt.



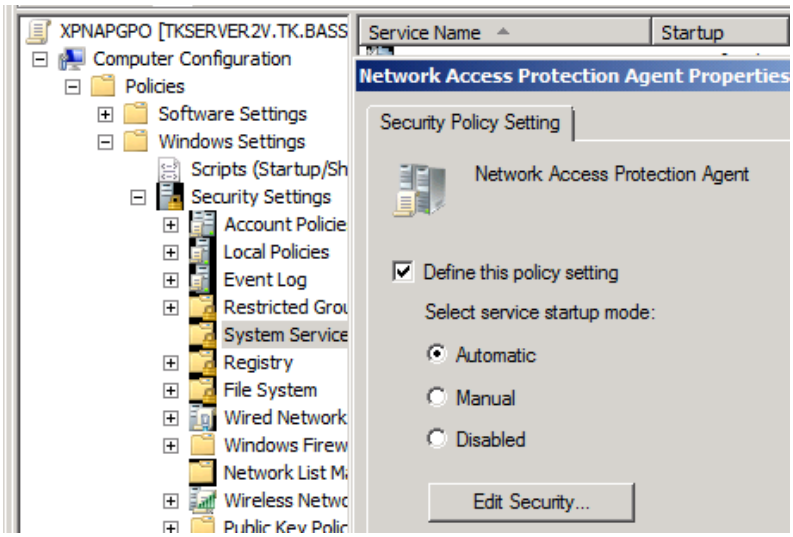
Kuva 35 XPNAPGPO:n muokkaaminen

Ryhmäkäytännön muokkaaminen aloitetaan valitsemalla Enforcement Clients. Tästä aukeaa lista NAP-ominaisuutta tukevista metodeista, joista jokainen on oletuksena pois päältä. Asetin DHCP-metodin päälle oman NAP-tutkimukseni pohjautuessa siihen.



Kuva 36 NAP:n pakotusmetodin clientin määrittäminen

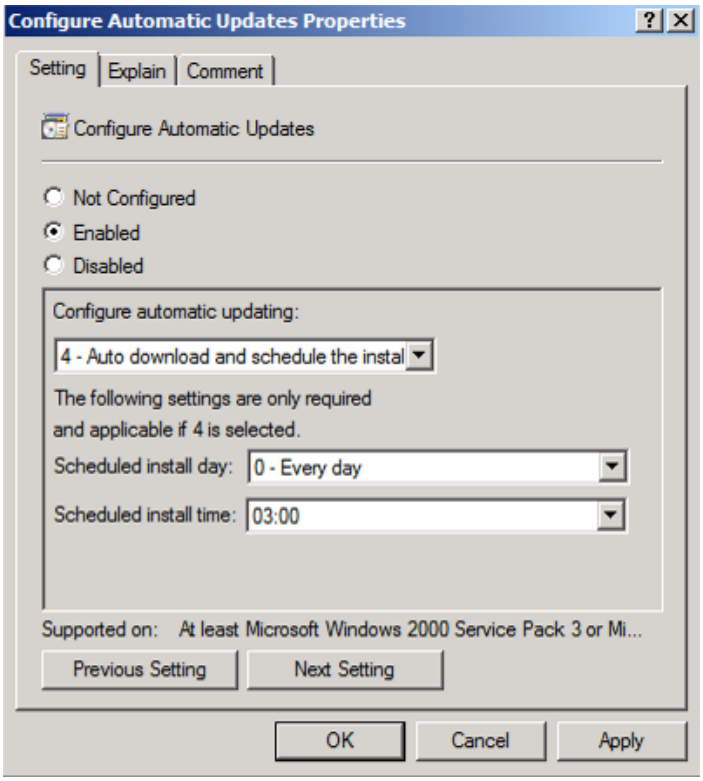
Loin myös uuden tietokoneryhmän nimeltään XP NAP Clients, johon asetin testityöasemani kuulumaan. Isommassa mittakaavassa vastaavanlaisen ryhmän jäseneksi on järkevää määrittää isompi tietokoneryhmä, esimerkiksi kaikki Windows XP -käyttöjärjestelmällä varustetut työasemat.



Kuva 37 NAP-lisäasetusten määrittäminen

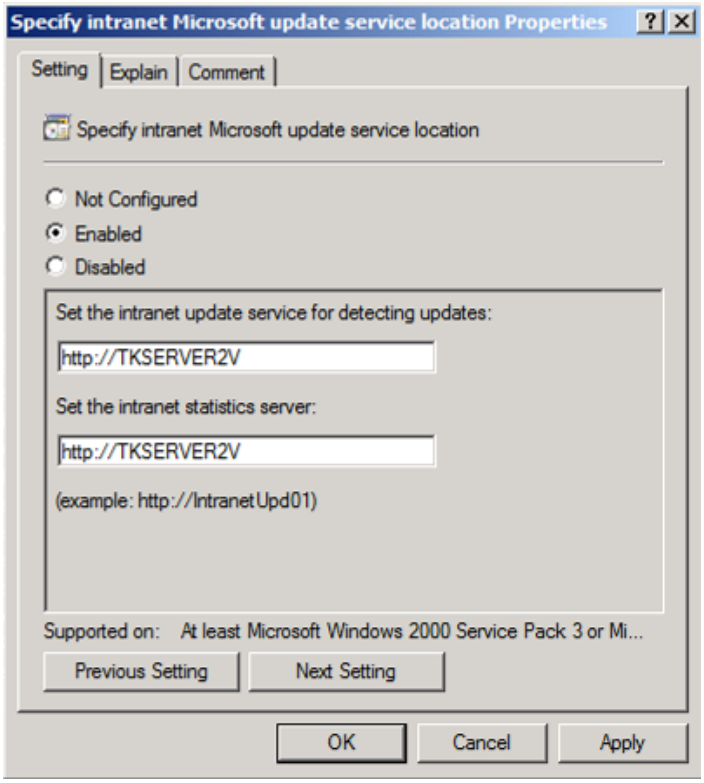
NAP-asetuksista on määritettävä päälle Network Access Protection Agent, jonka käynnistymisen määritin automaattiseksi. Toinen keskeinen asetus on Windows Security Center, joka on asetettava Enabled-tilaan. Tämä asetus muokataan valitun ryhmäkäytännön alta, jonka alikansiorakenteesta valitaan Administrative Templates, Windows Components ja viimein Security Center.

Ryhmäkäytäntöobjektista XPNAPGPO täytyy vielä säätää muutama kohta, jonka jälkeen järjestelmä on valmis siirtämään ja asentamaan päivityksiä Windows XP -työasemille.



Kuva 38 Automaattisten päivitysten asetusten muokkaaminen

Asetin työssäni päivitysten lataamis- ja asennusväliksi yhden päivän sekä asennusajaksi kello kolme aamuyöstä, joskin näitä asetuksia voi säätää hyvin vapaasti. Oikeassa toimintaympäristössä nämä asennukset on hyvä ajoittaa mahdollisimman hiljaiseen ajankohtaan, jolloin mahdolliset uudelleenkäynnistykset eivät häiritse kenenkään työtä.

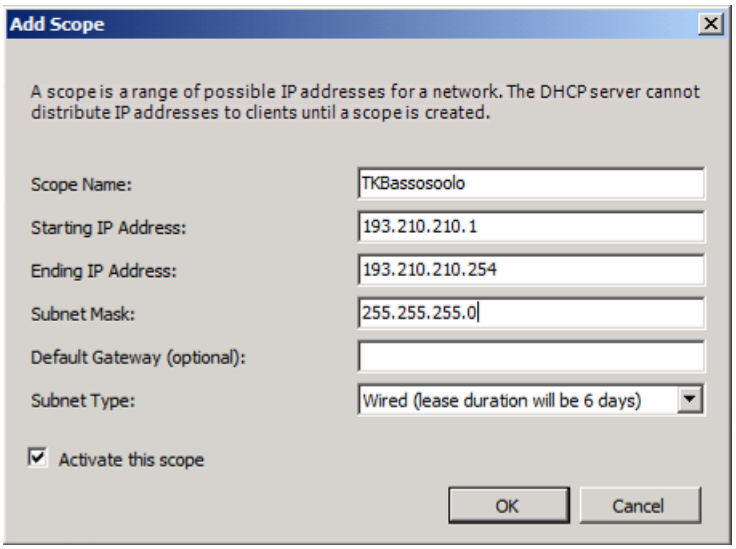


Kuva 39 WSUS-palvelimen verkko-osoitteen määrittäminen

Oleellisin asetus on päivityspalvelimen verkko-osoitteen määrittäminen. Osoitepoluksi voi määrittää lyhyesti päivityspalvelimen DNS-nimipalvelimelle syötetyn nimen, tässä tapauksessa TKSERVER2V.

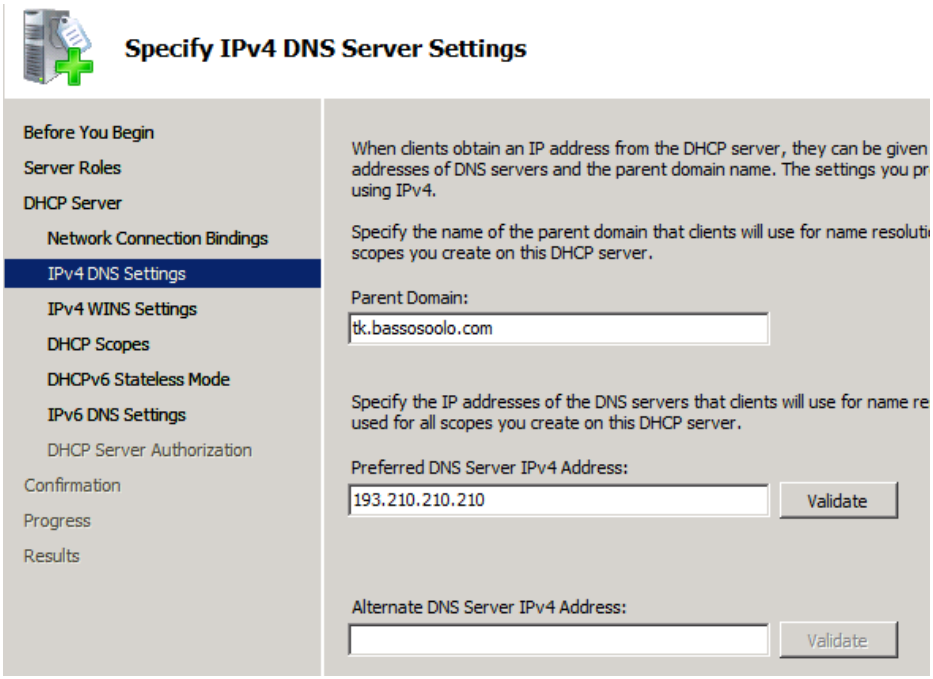
4.6 DHCP

Asensin virtuaalipalvelin TKSERVER3V:lle DHCP-palvelinroolin. Määritin lähiverkkoni IP-osoiteavaruuden käyttöalueeksi välin 193.210.210.1 ja 193.210.210.254 ja aliverkon maskiksi 255.255.255.0. Pärjäsin näillä määrityksillä loistavasti, koska käytössäni oli muutenkin vain kolme konetta.



Kuva 40 DHCP-käyttöalueen asetukset

DHCP-palvelinroolin asennus tapahtuu muiden palvelinroolien tapaan käyttämällä Server Manager -työkalua, jonka avustuksella määritetään kaikki tarvittavat tiedot toimivan DHCP-kokonaisuuden luomiseksi.



Kuva 41 DHCP-palvelinroolin asentaminen

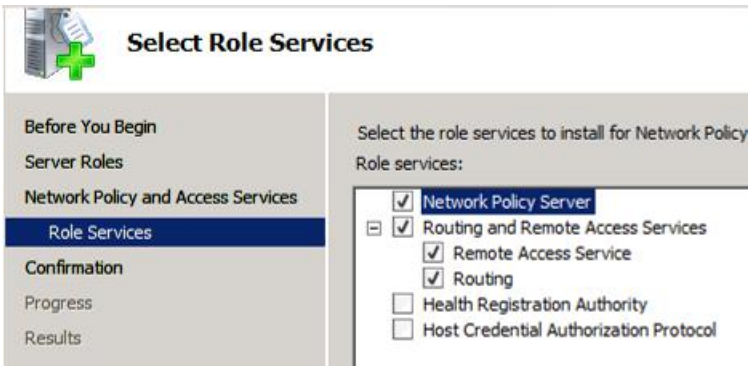
Asennusohjelman kautta määritetään palvelimen käyttöön tuleva IP-osoite, toimialueen nimi, DNS-palvelimet, DHCP-käyttöalue sekä sen käyttämä IP-osoitetyyppi. Windows Server 2008:n DHCP tukee siis sekä IPv4-osoiteavaruutta sekä sen korvaajaksi kehitettyä IPv6-avaruutta. Asentaessani DHCP-palvelinroolia määritin

IPv6-tilan pois päältä tutkimani NAP-palvelinominaisuuden takia. Tähän oli kaksi eri syytä. Ensimmäinen oli yksinkertaisesti se, ettei NAP tue IPv6-osoiteavaruuden käyttöä ja toisena se, että DHCP:n käyttö oli suorassa yhteydessä NAP-ominaisuuden implementointiin.

4.7 Network Access Protection

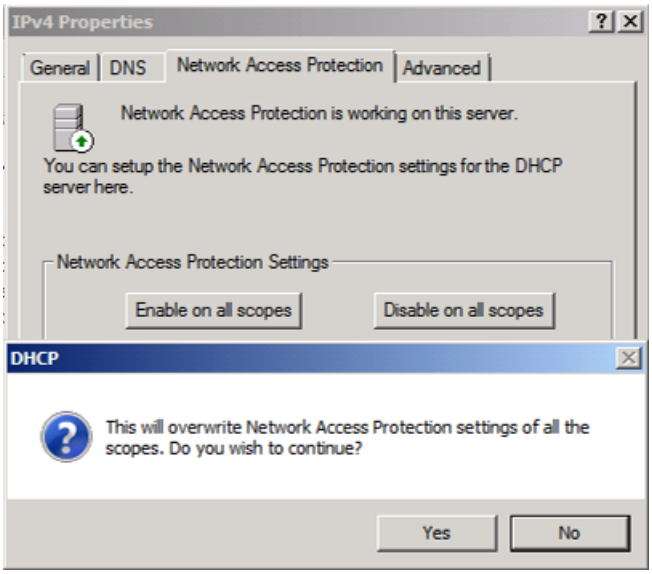
4.7.1 NAP: Palvelin

Network Access Protection otetaan käyttöön asentamalla ensin Network Policy and Access Services -palvelinrooli, joka asennetaan itsenäisenä kokonaisuutena Server Managerin kautta. Asensin palvelinroolin TKSERVER3V-virtuaalipalvelimelle, joka toimi myös DHCP-palvelimena. Roolin asentamisen yhteydessä annetaan muutama vaihtoehto eri ominaisuuksista, joita voi halutessaan asentaa palvelun yhteyteen. Oleellisin palvelu on Network Policy Server, eli palvelinrooli, jonka kautta kaikki NAP:iin liittyvät toimenpiteet kulkevat. Routing and Remote Access Services (RRAC) eli reititys- ja etäyhteyspalvelurooli, Health Registration Authority (HRA) ja Host Credential Authorization Protocol (HCAP) liittyvät eri NAP-pakotusmetodeihin. RRAC on oleellinen käytettäessä VPN-pakotusmetodia. HRA on IPSec-pakotusmetodin kanssa käytettävä NAP-komponentti, joka noutaa terveyssertifikaatit asiakaskoneilta. HCAP puolestaan on kytköksissä Cisco Systemsin 802.1X-pohjaisen NAP-ratkaisun asiakasautentikointiin. En asentanut yhtään näistä kolmesta roolista, koska käyttämäni pakotusmetodi on DHCP-pohjainen.

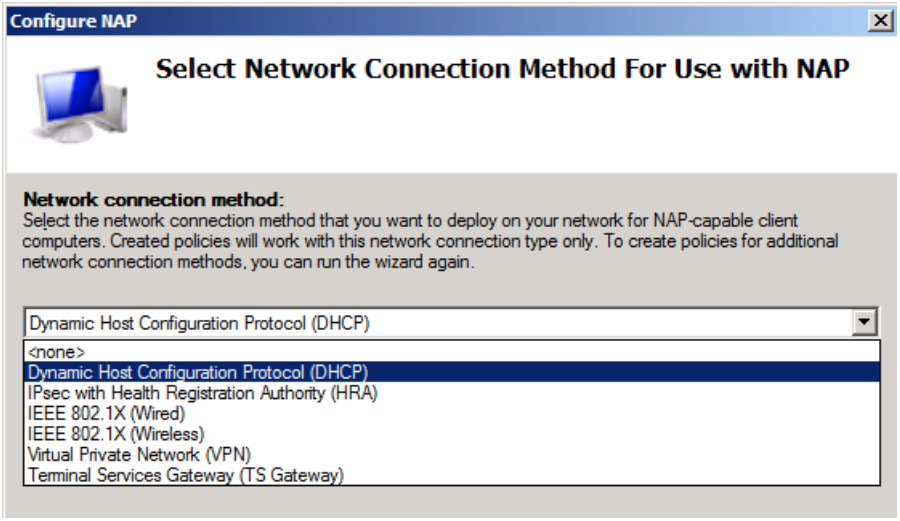


Kuva 42 Network Policy and Access Services -asennus

Asennuksen valmistuttua Network Policy Server -työkalu käynnistetään Start-valikon Administrative Tools -alavalikosta. Kuvassa 42 asetin päälle NAP-asetukset kaikilla DHCP-käyttöalueilla, joskaan käytössäni ei ollut kuin yksi. Järjestelmä kysyy tätä tehdessä hieman harhaanjohtavasti edellisten NAP-asetusten korvaamisesta uusilla, vaikka aiempia asetuksia ei olekaan.



Kuva 43 Network Access Protectionin konfigurointi



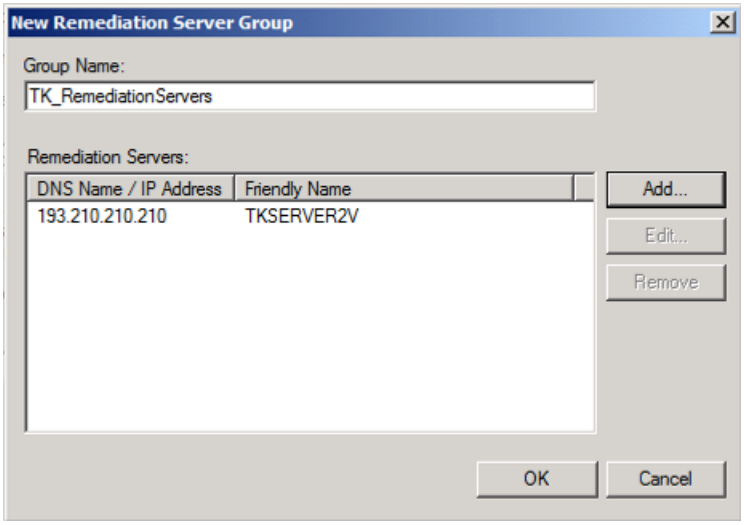
Kuva 44 Pakotusmetodin valitseminen

Seuraava askel Network Policy Server -sovelluksen puolella on valita oletuksena esiin tulevalta Getting Started -lehdeltä Configure NAP. Avautuva konfigurointiohjelma antaa valita käyttöön yhden kaikista tuetuista pakotusmetodeista; omassa opinnäytetyössäni valitsin DHCP-vaihtoehdon.

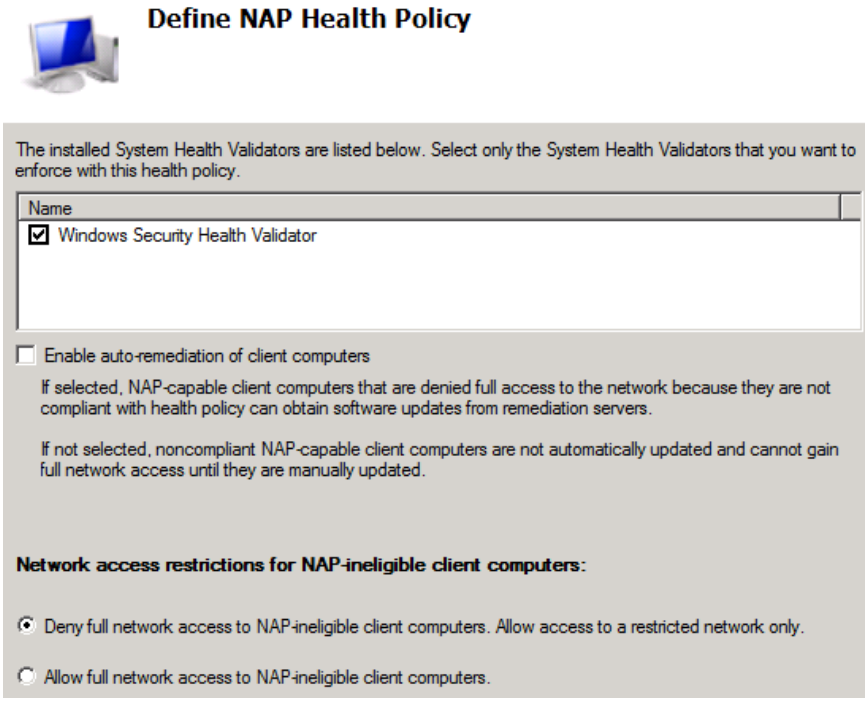
Konfigurointiohjelma antaa monia vaihtoehtoja käytettävien asetusten suhteen. NAP voidaan määritellä käyttämään erillistä DHCP-palvelinta, mikäli palvelinroolit eivät sijaitse samalla palvelimella. NAP-asetukset voidaan myös määritellä koskemaan vain tiettyjä tietokoneryhmiä, esimerkiksi palvelintietokoneet voidaan joko jättää ulkopuolelle tai sisällyttää pelkästään ne. Omaa NAP-ympäristöä luodessani asensin tietoisesti sekä NAP- että DHCP-palvelinroolit samalle palvelinkoneelle, joskin tein päätöksen tästä pohjautuen käyttämieni virtuaalipalvelimien kuormituksen tasaamiseen ennen NAP-asennukseen perehtymistä. Tämä oli jälkikäteen ajateltuna onnistunut päätös, sillä mikäli DHCP-palvelinrooli on eri palvelimella kuin NAP, kyseinen palvelin pitää konfiguroida RADIUS-asiakaskoneeksi ja asentaa vielä lisäksi Network Policy Server -palvelinrooli. Määritin myös NAP:n koskemaan kaikkia DHCP:n piirissä olevia tietokoneita, jo niiden vähäisen lukumäärän perusteella.

NAP on määriteltävä seuraavaksi käyttämään jotain tiettyä DHCP-käyttöaluetta. Edellisiä Server-käyttöjärjestelmäversioita edistyneemmän järjestelmäkomponenttien välisen integraation myötä NAP-järjestelmä tunnistaa käyttöalueen syöttämällä annettuun kenttään DHCP-palvelimen käyttöalueen nimeksi annetun nimen, omassa työssäni TKBassosoolo.

Keskeinen osa Network Access Protection -ominaisuutta on tarkistaa toimialueelle kirjautuvan tietokoneen terveydentila verrattaessa sitä asetettuun standardiin. Mikäli kone ei täytä vaatimuksia, sen on päivitettävä itsensä standardin tasolle. Tähän tarvitaan Remediation Server eli päivityspalvelin. Osana NAP:n konfigurointia on luoda päivityspalvelin tai useampia. Palvelimet määritetään syöttämällä niiden DNS-nimet tai IP-osoitteet. Tarvitsin omassa työssäni vain yhden päivityspalvelimen, joten asetin virtuaalipalvelimeni TKSERVER2V:n suorittamaan tätä tehtävää. Mikäli päivityspalvelimia on useampia, kuten isommissa organisaatioissa ja yrityksissä voi olla, ne voidaan yhdistää ryhmiin, jolloin niitä on helpompi hallita.

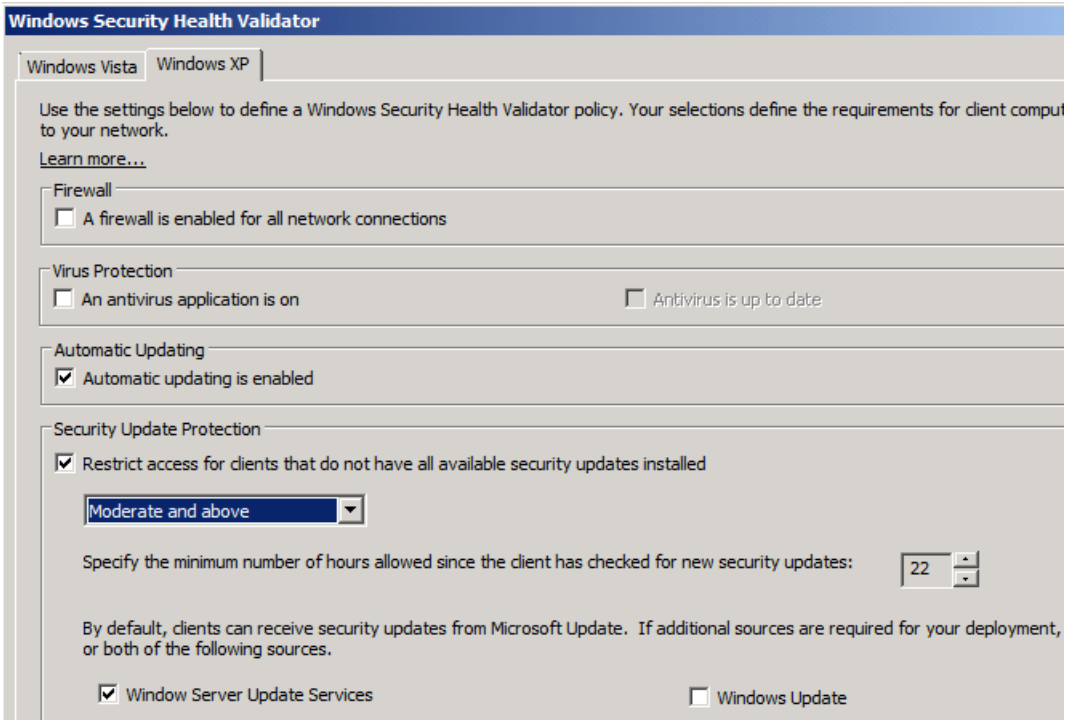


Kuva 45 Päivityspalvelimen määrittäminen



Kuva 46 NAP-terveyspolitiikan asettaminen

Network Access Protectionia pyörittävään palvelimeen on asennettava myös Windows Security Health Validator (SHV), tietokoneen turvallisuustilan validoiva komponentti. SHV:tä muokkaamalla ja käyttämällä voidaan määritellä käytetty terveystilastandardi ja miten sitä vastaamattomia tietokoneita käsitellään. Huomion arvoista kuvassa x on ”Enable auto-remediation of client computers” -asetusruutu, joka on tarkoituksella jätetty tyhjäksi. Tämän asetuksen tarkoitus selitetään tarkemmin luvussa 4.7.2 NAP: Työaseman testaaminen.



Kuva 47 SHV:n määrittäminen

Validointiasetuksista säätövaraa on tietokoneen palomuuriin, virustentorjuntaohjelmistoon, automaattisiin päivityksiin ja tietokoneen ”eristykseen” liittyen. Opinnäytetyössäni määritin oleellisina säätöinä, että toimialueelle pyrkivän tietokoneessa tulee olla automaattinen päivitystoiminto päällä ja asennettuna tulee olla vähintään tärkeysasteikoltaan kohtalaiset päivitykset. Asetin myös päivitysten lataamisen tapahtuvan Windows Server Update Services (WSUS) -palvelimelta Windows Update -verkkopalvelun sijasta.

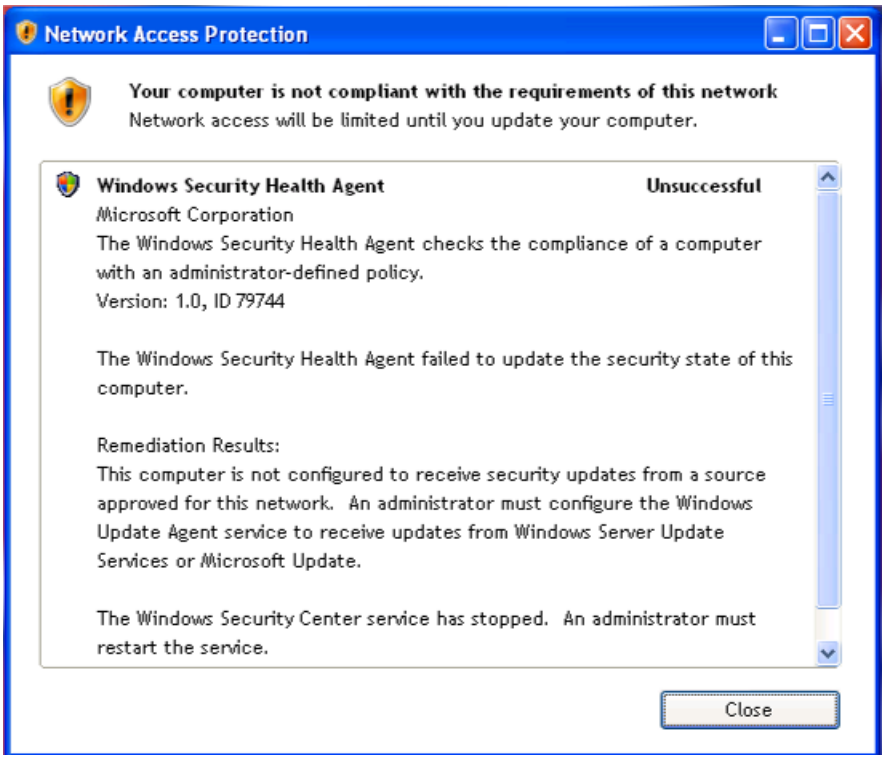
4.7.2 NAP: Työaseman testaaminen

Lähdin testaamaan Network Access Protectionin toimivuutta liittämällä luomaani tk.bassosoolo.com-toimialueeseen testityöaseman, jossa Windowsin automaattinen päivitystoiminto on kytketty kokonaan pois päältä ja oleellisia päivityksiä jätetty asentamatta. Palvelinpuolella tehtyjen asetusten mukaan työaseman pitäisi jäädä ”eristysverkkoon” siksi aikaa, kunnes sen tila on päivitetty vastaamaan validointiasetuksia.

Suoritin testaamista kahdella eri tavalla. Ensimmäisessä skenaariossa auto-remediation eli automaattinen terveydentilan korjaaminen on NAP-palvelinasetuksista pois päältä, jolloin terveydentila-asetusten mukaiset muutokset on tehtävä käsin. Jälkimmäisessä skenaariossa muutin tämän asetuksen automaattiseksi. Ennen testaamiseen ryhtymistäni otin työasemasta ”järjestelmäkaappauksen” (snapshot), joka tallentaa käyttöjärjestelmän tilan ja säädöt tietyllä hetkellä. Jälkimmäistä skenaariota aloittaessani palautin testityöasemani tilan vastaamaan tilannetta ennen ensimmäisen skenaarion aloittamista (rollback).

Kuva 48 NAP-ilmoitus työaseman terveydentilasta

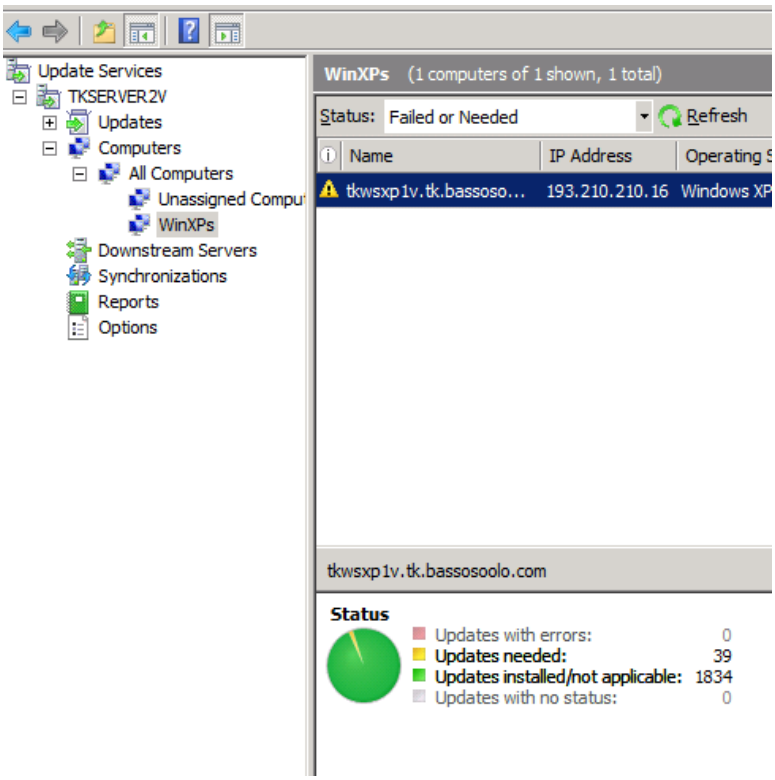
Kirjauduin tk.bassosoolo-toimialueelle käyttäen testihenkilö Esco Petäjän käyttäjätunnusta. Päällisin puolin käyttäjälle latautuva työpöytänäkymä näyttää hyvin samalle, kuin tavallisestikin. Windowsin alapalkkiin kellon viereen ilmestyy pieni keltainen kuvake, jonka päälle hiiren kursorin viemällä esiin tulee ilmoitus, että käytettävä verkkoyhteys on rajattu kunnes työasema päivitetään.



Kuva 49 Yksityiskohtaisempi NAP-ilmoitus

Kaksoisklikatessa alapalkin keltaista kuvaketta esiin aukeaa kuvassa 49 näkyvä ikkuna. Koska määritin päivitysasetuksen tapahtuvaksi manuaalisesti, SHA ei pysty automaattisesti päivittämään terveydentilaa. Tästä muodostuikin omassa työssäni lievä kompastuskivi manuaalisen päivittämisen suhteen. Luomieni toimialuekäyttäjien tunnukset olivat oikeusmäärittelyiltään samankaltaisia kuin työni toimeksiantajan käyttäjien, eli tunnuksilla on melko vähän oikeuksia tehdä työasemia koskevia muutoksia tai päivityksiä. Manuaalisessa päivitystilanteessa tarvitaan käyttää paikallisen tai verkkojärjestelmänvalvojan tunnusta tekemään muutoksia, joka taas ei isommassa mittakaavassa ole järkevää, mikäli päivitettäviä koneita on paljon.

Seuraava vaihe manuaalisessa päivityksessä on käydä päivityspalvelimen puolella asettamassa päivitykset asentumaan automaattisesti tietylle koneryhmälle.



Kuva 50 Työasemaobjekti päivityspalvelimella

Katsottaessa aiemmin luotua tietokoneryhmää WinXPs nähdään, että ryhmän jäseneksi on tullut testityöasema TKWSXP1V.

Toisen skenaarion lähtötilanne oli päinvastainen, kuin aiemmassa. Tässä asetin automaattisen terveydentilan korjaamisen päälle, jolloin käyttäjäinteraktiota pitäisi olla vähemmän. Näin itse asiassa olikin, testaamismielessä jopa liian vähän. En tiedä, oliko tarkoituksenmukaista, että järjestelmä ei missään vaiheessa ilmoittanut käyttäjälle työaseman terveydentilasta, vaan päivitykset ladattiin ja asennettiin hyvin nopeasti käyttäjän kirjautuessa sisään. Tällöin käyttäjän päästessä Windowsin työpöytänäkymään työaseman terveydentila oli jo päivitetty. Tämä on tietysti kyseisen päivitysmetodin tarkoituskin, joskin jonkinlainen tietoikkuna olisi ollut testitilanteessa tervetullut. Varmistin päivitysten asentumisen onnistumisen selaamalla läpi päivityspalvelimen lokitiedot siltä varalta, että NAP-palvelin olisikin päästänyt läpi virheellisen työaseman.

Jälkikäteen ajateltuna olisin voinut testata automaattista päivitysten asentamista kooltaan suuremmilla päivityksillä, esimerkiksi asentamalla testityöaseman käyttöjärjestelmäksi Windows XP:stä vain Service Pack 2 -järjestelmäpäivitys

sisältävä versio ja asentaa päivityspalvelimen kautta sitten uudempi Service Pack 3, jolloin päivitysten lataaminen ja asentaminen olisi kestänyt pidempään ja automaattisen terveydentilan korjaamisen olisi ehkä havainnut paremmin.

4.8 Tietokoneiden nimeämis- ja salasanakäytäntö

Käytin opinnäytetyöni fyysisen ja virtuaalilaitteiston nimeämisessä seuraavanlaista käytäntöä. Jokaisen nimen kaksi ensimmäistä kirjainta ovat TK omista nimikirjaimistani, seuraavaksi koneen tyyppi eli palvelin tai työasema, tietokoneen järjestysnumero ja mikäli kyseessä on virtuaalikone, kirjain V aivan lopussa. Esimerkkinä tästä opinnäytetyössä käyttämäni virtuaalipalvelin, jonka nimeksi asetin TKSERVER2V.

Käyttämäni virtuaalityöaseman TKWSXP1V nimeämisessä käytin samankaltaista logiikkaa. Kaksi ensimmäistä kirjainta siis tulevat nimikirjaimistani, kolmas ja neljäs ovat lyhenne englanninkielen sanasta workstation eli työasema, viides ja kuudes puolestaan kuvastavat asennettua käyttöjärjestelmää eli Windows XP:tä. Lopuksi numero yksi kuvaa työaseman numeerista järjestystä ja viimeinen kirjain virtuaalipalvelimien tapaan virtuaalikonetta. Alkuperäisessä suunnitelmassani aioin asentaa vielä yhden Windows Vista -käyttöjärjestelmällä varustetun virtuaalityöaseman, jonka nimessä XP-osan olisi korvannut Vista, mutta rajasin sen lopulta pois opinnäytetyöni kasvaneen laajuuden vuoksi

Salasanojen suhteen käytin seuraavanlaista logiikkaa. Otin salasanojen nimeämispohjaksi jääkiekon NHL-liigan kauden 1976-1977, jolloin Montreal Canadiens rikkoi monia jääkiekkoon liittyviä ennätyksiä. Esimerkiksi fyysisen palvelimen käyttöjärjestelmän järjestelmänvalvojan salasana oli ”76guy77laFleur”, jossa numeeriset arvot viittaavat kyseiseen kauteen, ”guy” ja ”laFleur” tulevat Canadiensin silloisen tähtipelaajan Guy LaFleurin nimestä.

5 TOTEUTUSYMPÄRISTÖ

5.1 Tarvekartoitus

Aloitin opinnäytetyöni aiheen suunnittelun perehtymällä Windows Server 2008 -käyttöjärjestelmän laitteistollisiin vaatimuksiin. Vaatimuksia tutkimalla minulle kävi selväksi, että vaikka koulutusyksikölläni ja samalla toimeksiantajallani oli teoreettinen mahdollisuus tarjota käyttööni suorituskyvyltään ja teknisiltä ominaisuuksiltaan sopiva tietokone, se olisi tarkoittanut kyseisenkaltaisen tietokoneen siirtämistä pois tietojenkäsittelyn opetuksesta. Näin ollen ainoa konkreettinen ratkaisu oli uuden tietokoneen hankkiminen.

Seuraava vaihe oli keskustella opinnäytetyöni ohjaavan opettajan sekä koulutusyksikköni koulutuspäällikön kanssa palvelintietokoneen hankkimisesta, jonka seurauksena laadin kirjallisen hankintaehdotuksen (liite 1). Koulutuspäällikön hyväksyttyä hankintaehdotuksen keskustelimme LiKun ATK-tukihenkilö Panu Pennasen kanssa palvelinkoneen teknisistä yksityiskohdista, minkä mukaisen laitteiston hän sitten tilasi.

5.2 Laitteisto ja toteutusympäristö

Opinnäytetyössäni käyttämä tekninen laitteisto koostui seuraavanlaisesta kokonaisuudesta. Itse keskusyksikkö oli Fujitsu Siemens -merkin Primergy TX 120 -malli. Palvelimen suorittimena toimi Intel Xeon 3070 -tuplaydinsuoritin, joka koostuu kahdesta kellotaajuudeltaan 2.66 gigahertsin suorittimesta. Keskusmuistia palvelimessa oli kaksi 2048 megatavun (eli kahden gigatavun) muistikampaa, jolloin muistin kokonaismäärä oli neljä gigatavua. Koneessa oli myös kaksi 146 gigatavun suuruista kiintolevyä.

Opinnäytetyön alkuvaiheessa olin hieman epävarma, mitä Windows Server 2008 -käyttöjärjestelmän versiota tulisin käyttämään. Konkreettisina vaihtoehtoina olivat opinnäytetyön tekohetkellä uusi ja ilmainen Hyper-V Server ja kaupallinen Enterprise-versio. Timo Kinnusen kehotuksesta kokeilin ensin asentaa testausmielessä Hyper-V Server-version. Heti alkuun kävi ilmi, ettei tämä versio sopisi työni toteuttamiseen, sillä sen toiminta on äärimmäisen rajallista, ja sen hallintaan tarvitaan käytännössä toinen palvelintietokone tai työasema. Näin ollen ainoaksi konkreettiseksi vaihtoehdoksi jäi Enterprise-versio (teknisesti Enterprise, 6.0 Build 6001), jonka asensin korvaamaan Hyper-V Server -version. Käytin käyttöjärjestelmän hankkimiseen Microsoftin MSDNAA-verkkopalvelua, jonka kautta sain tarvitsemani Enterprise-version, joka puolestaan mahdollisti Hyper-V-virtualisointiominaisuuden käytön.

Toteutusympäristönä toimi fyysisesti yksi työhuone Savonia-ammattikorkeakoulun Technopolis-teknologiakeskuksen tiloissa. Työhuoneessa käytössäni oli palvelintietokoneen lisäksi Savonia-ammattikorkeakoulun lähiverkko sekä dokumentointiin ja tiedonhankintaan käyttämäni tavallinen Windows XP -käyttöjärjestelmällä varustettu työasema.

6 POHDINTA

Opinnäytetyöprosessi erosi hyvin paljon verraten aiempiin kurssien harjoitustöihin ja yleisestikin opiskeluun. Teknisen osion suorittaminen oli erityisesti alkuun melko haasteellista, joskin palkitsevaa.

Yksi suurimpia haasteita opinnäytetyön tekemisessä oli se, mitä työhön sisällyttää ja mitä jättää pois. Tähän oman vaikeutensa toi vielä seikka, että käyttöjärjestelmä lukuisine ominaisuuksineen oli minulle täysin uusi tuttavuus, eivätkä kaikki käyttöjärjestelmän toimintaan liittyvät oleelliset palvelinroolit ja -ominaisuudet tuntuneet eroavan paljon toisistaan.

Haastavaa oli myös itse kirjoitustyö ja tämän raportin kokoon saattaminen. Valtaosa lähdeaineistoista oli englanninkielisiä, joista osa oli kirjoitettu hyvin teknistä sanastoa käyttäen. Joinakin päivinä ainoaksi edistykseksi saattoi jäädä jonkun tekstikokonaisuuden kääntäminen ja erityisesti sen ymmärtäminen. Silti tästä tuli vahva onnistumisen tunne, kun viimein ymmärsi asian ja jota kykenee nyt käyttämään tulevaisuuden työtehtävissä.

Itse prosessi kesti alkuvalmisteluista teknisen osion valmiiksi saattamiseen noin puolitoista kuukautta. Tämän raportin valmistuminen viivästyi melko huomattavasti suunnitellusta useiden elämäntilanteeseeni kohdistuvien muutosten myötä; kaiken kaikkiaan kirjoitusprosessi vei aikaa noin kolme kuukautta, joskin se jakaantui yli puolen vuoden ajalle.

Kokonaisuutena olen tekemääni tekniseen ja kirjalliseen työhön tyytyväinen. Palvelinkäyttöjärjestelmien maailma on erittäin laaja ja monimutkainen, joskin toivon tämän työn auttavan muita ymmärtämään perusasioita Windows Server 2008 -käyttöjärjestelmästä, sen toiminnasta ja mielestäni oleellisimmista tietoturvatekijöistä.

Loppusanoina haluaisin kiittää rakasta avovaimoani Miraa kaikesta tuesta ja rakkaudesta, jonka avulla jaksoin tehdä tämän työn loppuun. Myös vanhempani, hyvä ystäväni ja kollegani Jarkko Hyvärinen, opinnäytetyöohjaajani Pekka Granroth,

Savonia-ammattikorkeakoulun tietohallinnon yhteyshenkilöni Timo Kinnunen, bänditoverini Timo ja Matti sekä nelijalkaiset ystäväni Nelli, Pedro, Rudy ja Cassius ansaitsevat erityisen kiitoksen. Ilman teitä tätä työtä ei olisi.

Tärkeänä osana työprosessiani oli myös loistava musiikki, kiitos The Isley Brothers, Curtis Mayfield, Bobby Womack ja monet muut mahtavat soul- ja funkyhtyeet ja -artistit.

LÄHTEET

Fetty, P. & Microsoft 2008

Designing and Architecting a Network Access Protection (NAP) solution. Microsoft PowerPoint -tiedosto. Luettu marraskuussa 2008.

Granroth, P. 2007

Windows Vista and ”Longhorn”, New operating systems – new security concepts. Microsoft PowerPoint -tiedosto. Luettu marraskuussa 2008.

Microsoft Corporation 2009

Ferrari Takes Windows HPC Server for a Spin. Verkkodokumentti. Luettu 4.3.2009.
http://www.hpcwire.com/offthewire/Ferrari_Takes_Windows_HPC_Server_for_a_Spin.html

Microsoft Corporation 2008

Microsoft Hyper-V Server: Frequently Asked Questions -verkkosivu. Luettu 23.11.2008.
http://www.microsoft.com/servers/hyper-v-server/faq.mspx

Microsoft Corporation 2008

Microsoft TechNet -verkkosivusto. Luettu loka-joulukuussa 2009.
http://technet.microsoft.com/en-gb/default.aspx

Microsoft Corporation 2008

Windows Server® 2008 Security Guide Version 1.0. Microsoft Word -tiedosto. Luettu marraskuussa 2009.

Moonsoft Oy

Verkkokaupan web-sivut. Luettu 4.3.2009.
http://www.moonsoft.fi/products/000562.aspx

Online IP Subnet Calculator 2008

Verkkosivu. Luettu 10.12.2008

http://www.subnet-calculator.com/subnet.php?net_class=C

Ou, G. 2006

Ultimate wireless security guide –verkkodokumentti. Luettu 27.11.2008.

http://articles.techrepublic.com.com/5100-10878_11-6148543.html

Ou, G. 2006

Introduction to server virtualization -verkkodokumentti. Luettu 22.11.2008.

http://articles.techrepublic.com.com/5100-10878_11-6074941.html

Tulloch, M. & Windows Server Team 2007

Introducing Windows Server 2008. Microsoft Press. Redmond, Washington, Yhdysvallat.

LIITE 1 Palvelinkoneen hankintaehdotus

Timo Knuutinen
Särkiniementie 30 A 302
70700 Kuopio
28.9.2009

Esa Viklund
Koulutuspäällikkö
Savonia-ammattikorkeakoulu
Presidentinkatu 1
70100 Kuopio

Käymämme keskustelu 3.11.2008

Keskustelimme 3.11.2008 mahdollisesta tietokoneen keskusyksikön hankinnasta Savonia-ammattikorkeakoulun Microteknian toimitiloihin. Tietokoneen tämänhetkinen tarve olisi opinnäytetyöni toteuttaminen. Opinnäytetyöni aiheena on tutkia Microsoft Windows Server 2008 -palvelinkäyttöjärjestelmän tietoturvaominaisuuksia ja kuinka niitä voidaan käyttää hyödyksi Savonia-ammattikorkeakoulun tuleviin tarpeisiin. Työni aikatauluna olisi aloittaa työ mahdollisimman pian ja saattaa se valmiiksi tammikuun 2009 alkupuolella.

Nykyhetkellä koulutusyksiköllämme on kyseistä tarvetta varten tarpeeksi tehokkaita tietokoneita vain opetuskäytössä yhdessä luokassa; mikäli kyseisestä luokasta siirrettäisiin yksi kone opinnäytetyöni toteutusta varten, vaikeuttaisi tämä usean opiskelijan työtä ja oppimista.

Tarvittavanlainen tietokone tulisi maksamaan korkeintaan 1500 euroa. Opinnäytetyöni valmistuttua kyseistä tietokonetta voitaisiin käyttää muiden opiskelijoiden vastaavanlaisissa opinnäytetöissä sekä opetuspuolella Pekka Granrothin kursseilla.

Windows Server 2008 -käyttöjärjestelmään ammattikorkeakoululla on tarvittava lisenssi ja asennusmedia, muut mahdollisesti tarvittavat ohjelmistot voin saada ammattikorkeakoulun Tietohallintokeskuksen kautta.

Ehdotankin hankittavaksi yhden tehokkaan tietokoneen, jota opiskelijat voivat käyttää jatkossa palvelinaiheisten opinnäytetöidensä tekemiseen sekä tietojenkäsittelyn laitteistopuolen opetuksessa. Mikäli koulu puoltaa hankintaa, voimme keskustella tietokoneen laitteistollisista yksityiskohdista enemmän Savonian Helpdeskin Panu Pennasen kanssa.

Ystävällisin terveisin

Timo Knuutinen
opiskelija
kk44559
Savonia-ammattikorkeakoulu, LT05S