Antti Koivisto

Active Directory ja Exchange pienyrityksen IT-palveluiden tukena

Metropolia Ammattikorkeakoulu
Insinööri (AMK)
Tietotekniikan koulutusohjelma
Insinöörityö
21.11.2011

Metropolia

Tiivistelmä

Tekijä Otsikko Sivumäärä Aika	Antti Koivisto Active Directory ja Exchange pienyrityksen IT-palveluiden tukena 66 sivua 21.11.2011
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Tietoverkot
Ohjaaja	Yliopettaja Kari Järvi

Insinöörityössä rakennettiin IT-yhtiö General Media Carnac Oy:lle pienyrityskäyttöön soveltuva verkonhallintajärjestelmä käyttäen Microsoftin Active Directory -aktiivihakemistojärjestelmää sekä postinvälityspalveluna Microsoftin Exchange Server 2010 -ohjelmistoa.

Järjestelmän rakentamisen tavoitteena oli uudistettujen ja joidenkin uusien palveluiden tarjoaminen yhtiön asiakkaille, joista monet olivat näitä toivoneet. Myös yhtiö itse hyötyi keskitetystä verkkoratkaisusta, joka vähensi ulkopuolisten palveluntarjoajien käytön tarvetta. Uusi järjestelmä korvasi vanhentuneen Linux-pohjaisen sähköpostijärjestelmän.

Järjestelmä rakennettiin tyhjennetylle HP ProLiant G5 -palvelimelle Microsoft Windows Server 2008 R2 -käyttöjärjestelmän päälle käyttäen myöhemmässä vaiheessa apuna samanlaista palvelinta palveluiden tukena. Projekti koostui kolmesta vaiheesta, jossa ensimmäisessä ja toisessa käsiteltiin Active Directoryn ja Exchange Server 2010:n ominaisuuksia ja käyttömahdollisuuksia, minkä jälkeen palvelut asennettiin ja konfiguroitiin. Kolmannessa vaiheessa testattiin järjestelmän toimintaa ja palvelinten resurssien käyttöä.

Järjestelmä osoittautui toimivaksi ja sopivaksi IT-pienyritykselle, soveltuen hyvin myös sen asiakaskunnan palvelemiseksi. Uudesta järjestelmästä riippuvainen laitteiden kirjautumismekanismi toimi viiveettömästi ja luotettavasti. Sähköpostin välitys toimi sujuvasti testattaessa monella erilaisella asiakasohjelmalla.

Avainsanat	Active Directory, Exchange 2010, Windows Server 2008 R2, pienyritys

Metropolia

Abstract

Author(s) Title Number of Pages Date	Antti Koivisto Active Directory and Exchange supporting small business IT-services 66 pages 21 November 2011
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Networking
Instructor & supervisor	Kari Järvi, Principal Lecturer

This thesis focused on the project of utilizing the centralized network management software Active Directory and the mail exchanger software Exchange Server 2010, both developed by Microsoft Corporation, to be used in a small business environment at the IT-company General Media Carnac Inc.

The goal of the project was to rebuild outdated services and build new ones for the company's clients many of whom had previously requested these changes. The company itself also benefited from a centralized network service solution since it brought down the need for external commercial services. The new system also replaced the outdated Linux-based mail exchanger system.

The new system was built on an empty HP ProLiant G5 server which had the Microsoft Windows Server 2008 R2 as its operating system. Another similar server was later used as a supporting server. The project consisted of three phases where the first and second dealt with the features, possibilities, installation and configuration of Active Directory and Exchange Server 2010. In the third phase the system was tested and the servers' use of resources was monitored.

The new system turned out to be working and appropriate for a small IT business serving its clients as well. The log-on method depending on the new system works reliably and without latency. Mails are delivered as expected even when using several different mail clients.

Keywords	Active Directory, Exchange 2010, Windows Server 2008 R2, small business

Sisällys

Tiivistelmä
Abstract
Lyhenteet ja termit

1 Johdanto 1

2 Suunnitelma 2

2.1 Esittely 2
2.2 Laitteisto ja verkko 3
2.3 Toimintasuunnitelma 4

3 Active Directory 5

3.1 Esittely 5
3.2 Käyttötarkoitus 6
3.3 Logiikka 7
3.4 Toiminta 7
3.4.1 Domain Services 7
3.4.2 Rights Management Services 8
3.4.3 Lightweight Directory Services 8
3.4.4 Certificate Services 8
3.4.5 Federation Services 9
3.4.6 Read-only Domain Controller 9
3.5 Replikointi 10
3.6 Asennuksen valmistelu 10
3.7 Asennus 11
3.8 Konfigurointi 18
3.8.1 Laitteet ja käyttäjät 19
3.8.2 DNS 24
3.8.3 Toissijainen Domain Controller 25

4 Exchange 31

4.1 Esittely 31
4.1.1 Yhtiölle tarpeelliset ominaisuudet 32
4.1.2 Roolit 33

4.1.3 Send-Connector 35
4.1.4 Forefront Security 36
4.1.5 Autodiscover 36
4.2 Asennuksen valmistelu 37
4.3 Asennus 40
4.3.1 Lisenssitiedot 40
4.3.2 Virheiden raportointi 41
4.3.3 Asennustyyppi 42
4.3.4 Palvelimen roolien valinta 42
4.3.5 Exchange-organisaation määritys 43
4.3.6 Asiakasasetukset 44
4.3.7 Asiakkaan yhteydenottokäytännöt 44
4.3.8 Käyttöraporttien lähetys Microsoftille 45
4.3.9 Valmiuden tarkistus 46
4.3.10 Asennuksen valmistuminen 46
4.4 Asennuksen jälkeiset toimenpiteet 47
4.4.1 Service Pack 1 47
4.4.2 Exchange Management Console 48
4.4.3 Best Practices Analyzer 49
4.5 Konfigurointi 51
4.5.1 Lähtevä posti 52
4.5.2 Saapuva posti 53
4.5.3 Sallitut domainit 55
4.5.4 Postilaatikot 56
4.5.5 Sertifikaatti 58
5 Käyttöönotto, käyttö ja suorituskyky 59
5.1 Laitteiston liittäminen domainiin 59
5.2 Sähköpostin käyttö 60
5.2.1 Outlook 2010 60
5.2.2 Outlook Web App 61
5.2.3 Kolmannen osapuolen asiakasohjelmat 61
5.2.4 Mobiililaitteet 62
5.3 Palvelinten suorituskyky ja resurssien käyttö 63
6 Yhteenveto 64
Lähteet 65

Lyhenteet ja termit

DMZ	Demilitarized Zone, aliverkko, joka on avoin Internetiin päin.
DHCP	Dynamic Host Configuration Protocol, verkkoprotokolla, joka jakaa IP-osoitteita niitä pyytäville lähiverkon laitteille.
DNS	Domain Name System, nimipalvelu, jonka tehtävä on muuntaa IP-osoite nimeksi ja välittää sähköpostia.
Domain	Toimialue, kuten carnac.fi. Alue, joka sisältää verkkotunnukselle nimetyt palvelut.
Ethernet	Yleisesti käytetty pakettipohjainen lähiverkkotekniikka.
Forest	Metsä, looginen ryhmä kaikille Active Directory -palvelun alaisille puille (tree).
FQDN	Fully qualified domain name, eli absoluuttinen polku tietylle palvelulle. Esimerkiksi osoitteessa mail.carnac.fi mail on postipalvelu, carnac on yhtiön domain ja fi on suomalaisten domainien juuri. Eri osat eritellään pisteellä.
HTTPS	Hypertext Transfer Protocol Secure, webin tiedonsiirtoprotokolla, joka on salattu SSL/TLS-menetelmällä.
IIS	Internet Information Service, Windowsin sisäänrakennettu web-palvelinohjelmisto
IMAP4	Internet Message Access Protocol, sähköpostinsiirtoprotokolla, joka lukee reaaliajassa posteja palvelimelta. Mahdollistaa helpon synkronoinnin.
Kerberos	Autentikointiprotokolla Internetin yli tapahtuviin käyttöoikeuden todentamisiin. Ei salaa liikennettä.

LDAP	Lightweight Directory Access Protocol, kevennetty protokolla X.500:sta. Useimmiten käytetään käyttäjän tunnistukseen.
MAPI	Messaging Application Programming Interface, Microsoftin kehittämä protokolla, joka tarjoaa sovelluksille mahdollisuuden kommunikointiin muiden sovellusten kanssa.
NSPI	Name Service Provider Interface, Microsoftin kehittämä kommunikaatioprotokolla nimipalvelujen ja käyttäjän yhdistämiseen.
Policy	Käytäntö, jolla jokin asia tehdään samalla tavalla, kuten salasanan formaatti.
POP3	Post Office Protocol versio 3, yksinkertainen sähköpostinsiirtoprotokolla. Hakee viestit palvelimelta ja poistaa ne.
RAID	Redundant Array of Independent Disks, kiintolevyjen vikasietoisuutta parantava tekniikka, jolla yhdistetään useita levyjä yhdeksi loogiseksi levyksi.
RPC	Remote Procedure Call, protokolla, joka antaa sovellukselle mahdollisuuden käynnistää toimintoja muissa sovelluksissa.
Schema	Tietokannan rakenteen kuvausmenetelmä.
Sertifikaatti	Varmenne, virtuaalinen asiakirja, jolla palvelun salaus varmennetaan. Varmentaja on yleensä ulkopuolinen taho, mutta myös palvelun itse kirjoittamia sertifikaatteja käytetään.
Site	Verkkoalue, Active Directory -palvelun maantieteellinen sijainti.
SMB	Server Message Block, tiedostonjakoprotokolla Windowsille.
SMTP	Simple Mail Transfer Protocol, liikenneprotokolla sähköpostin välittämiseen palvelinten välillä.

TLS/SSL	Transport Layer Security tai Secure Sockets Layer, salausprotokolla, jolla voidaan salata IP-verkkojen yli liikkuvaa dataa. Käytetään webissä ja sähköposteissa.
Tree	Puu, ryhmä, joka sisältää tietyn organisaation domainit.
UPS	Uninterruptible Power Supply, varavirtajärjestelmä, joka suojaa laitteita sähkökatkoilta ja jännitteen vaihtelulta.
Velho	Ohjattu asennusikkunoiden sarja, jolla voidaan määritellä asetuksia yksi kerrallaan olennaisessa järjestyksessä.
VLAN	Virtual Local Area Network, tekniikka, jolla jaetaan fyysinen lähiverkko pienempiin osiin.
VoIP	Voice over IP, sateenvarjoprotokolla äänensiirrolle IP-verkkojen yli. Sisältää yleisiä protokollia kuten SIP ja H.323.
X.500	Täydellinen hakemistopalvelu, jonka haittapuolena on liiallinen monimutkaisuus.

1 Johdanto

Tämän insinöörityön aiheena on osakeyhtiö General Media Carnac Oy:n verkkoinfrastruktuurin nykyaikaistaminen eli vanhentuneiden palvelinten ja palvelukomponenttien korvaaminen keskitetyllä Microsoftin Active Directory -palvelinratkaisulla asennettuna kirjoitushetkellä uusimman Windows Server 2008 R2 -alustan päälle. Tässä yhtiössä ei ole aikaisemmin ollut käytössä minkäänlaista keskitettyä käyttäjätilien tai laitteistojen valvontaa. Tämän alustan päälle asennetaan samoin kirjoitushetkellä uusin Microsoftin Exchange Server 2010 -postipalvelujärjestelmä. Kokonaan asennetun ja koko verkkoon ulotetun järjestelmän toimintakykyä testataan erilaisilla työkaluilla ja niistä muodostetaan suppea tilasto.

General Media Carnac Oy on tiedeviestintäyhtiö, jonka liiketoiminnan ytimenä ovat tietokantapohjaiset julkaisujärjestelmät. Julkaisujärjestelmiä toteutetaan pääosin FileMaker-tietokantaohjelmalla ja useissa projekteissa yhtiön omilta tietokantapalvelimilta haetaan tietoja erilaisiin web-sovelluksiin. Sovelluksien yhteydessä käytetään projektista riippuen erilaisia postitustoimintoja, joissain suuria joukkopostituksia. Carnacin laajalla asiakaskunnalla on myös suuri määrä asiakas-domaineja, eli toimialueita, ja niihin sidottuja postilaatikoita.

Tähän mennessä postitus on hoidettu Linux-pohjaisella (Trustix) postipalvelimella, jonka elinikä lähentelee loppuaan. Postitussovelluksena käytetään SquirrelMailin vanhaa versiota, joka ei tue nykyaikaisia salausjärjestelmiä. Palvelimen suorituskyky ei myöskään enää vastaa asiakkaidemme vaatimuksia. Sama palvelin hoitaa myös ensisijaisen DNS- eli nimihakupalvelun.

Palveluratkaisun tarkoituksena on tarjota yhtiölle keskitetty postitusjärjestelmä, joka palvelee myös asiakkaitamme huomattavasti paremmin kuin vanha järjestelmä. Yhtiön palveluihin sisältyy ohjelmistoja, kuten FileMaker, jotka ovat suoraan Active Directory -integroitavissa. Tämä mahdollistaa valtavan parannuksen yhtiön valtavan sähköpostiarkiston varastoinnissa ja järjestämisessä. Yhtiön omistuksessa on myös henkilökuntaan suhteutettuna suuri määrä työasemia, kannettavia tietokoneita ja mobiililaitteita, joiden käyttö helpottuu huomattavasti keskitetyn käyttäjähallinnan ja sähköpostipalvelun myötä. Uuden Active Directory -järjestelmän avulla voimme myös

tarjota asiakkaillemme keskitettyjä informaationjakotapoja julkisten ja henkilökohtaisten hakemistojen avulla.

Tämä insinöörityö ei ole syvällinen katsaus Active Directoryn tai Exchange Serverin toimintaan ja ominaisuuksiin, vaan käytännöllinen selvitys siitä, miten pienyrityksissä näitä palveluita otetaan käyttöön ja mitä arvoa niistä näille yhtiöille voi olla. Lähtökohtana näitä palveluita asennetaan ja otetaan käyttöön siinä määrin, missä yhtiö niitä oikeasti tarvitsee. Internetistä löytyy runsaasti erilaisia ohjeita ja artikkeleita Active Directoryn ja Exchangen hienommista toteutustavoista, mitä voittoa tavoitteleva, aikatauluja noudattava pienyritys harvoin tarvitsee.

Kaikki ohjelmistot tässä projektissa ovat englanninkielisiä, joten väärinymmärrysten välttämiseksi kaikki raportissa käytetyt ohjelmistoihin liittyvät termit esiintyvät alkuperäiskielisinä. Esimerkiksi Active Directoryn ja Exchangen käyttämät domainien juuret eli metsät kirjoitetaan muodossa forest. Erilaiset toiminnot tai selvästi ohjelmaan liittyvät termit kirjoitetaan alkuperäisen kirjoitustavan mukaisesti isolla alkukirjaimella. Carnacin asiakasyhtiöt pysyvät nimettöminä, ja niihin viitataan projektissa ainoastaan asiakkaina.

2 Suunnitelma

2.1 Esittely

Tämän insinöörityön tarkoituksena on perustaa yhtiön palvelimille keskitetty tilinhallintajärjestelmä, eli Active Directory (AD, Aktiivihakemisto). Sen tarkoituksena on helpottaa tietokoneiden ja verkon käyttöä muuttamalla käyttäjähallintaa siten, että käytettävästä tietokoneesta riippumatta käyttäjä voi aina kirjautua sisään omilla tunnuksillaan. Näin käyttäjällä ovat aina saatavilla omiin yksityisiin kansioihin tallennetut dokumentit ja tiedostot. Toinen tärkeä tehtävä on hallita yksittäisten tilien ja ryhmien käyttöoikeuksia. Esimerkiksi myyntiosaston henkilökunnalla olisi aivan erilaiset käyttöoikeudet kuin verkonvalvontaosastolla. Ilman Active Directorya tilinhallinta on perinteistä, eli jokaisella tietokoneella on omat tilinsä ja omat dokumenttinsa, jotka eivät siirry automaattisesti minnekään muualle. Suurissa organisaatioissa hallinta ei olisi mahdollista ilman Active Directoryn kaltaista tilinhallintaa.

Active Directoryn luoman alustan päälle asennetaan Exchange Server 2010, joka on Active Directoryn kanssa idealtaan samantyyppinen järjestelmä. Exchange on sähköpostinhallintaohjelmisto, joka toimii ikään kuin puhelinkeskuksena vastaanottaen ja välittäen viestejä. Tämän järjestelmän avulla käyttäjä voi mistä tahansa kirjautua palveluun Active Directoryn avustuksella ja operoida sähköpostejaan. Tätä avustavat vielä erilaiset etälukumahdollisuudet, kuten puhelinviestintä ja selaimessa toimiva sähköposti.

2.2 Laitteisto ja verkko

Yhtiön laitteisto koostuu viidestä palvelimesta, kahdesta verkkolevyasemasta, kuitukytkimestä, ethernet-kytkimestä, reitittimestä, wlan-tukiasemasta, kahdesta UPS-laitteesta, kahdesta tulostimesta ja kolmesta työasemasta. Kaikki verkkoon kytketyt osoitteelliset laitteet kytketään Active Directoryyn. Alla on taulukoituna (taulukot 1-5) jokaisen laitteen projektin kannalta olennaiset tiedot.

Taulukko 1. Yhtiön verkot ja niiden tarkoitukset

Verkon IP-osoite	**Verkon tarkoitus**
84.239.231.80/30	Liitäntäverkko
84.239.231.64/28	Palvelinverkko
84.239.230.240/28	Työasema-/asiakasverkko

Taulukko 2. Yhtiön palvelimet

Palvelimen nimi	**Rooli**	**Käyttöjärjestelmä**	**IP-osoite**
AD-Exchange	Tyhjä kone projektin alustaksi	Server 2008 R2	84.239.231.67
Web	Web-palvelin, IIS, php, toissijainen DNS	Server 2003 R2	84.239.231.66
Filemaker	Tietokantapalvelin	Server 2003 R2	84.239.231.68
Filemaker2	Tietokantapalvelin, varalla	Server 2008	84.239.231.69
Mail	Ensisijainen DNS, Mail Exchanger (sähköpostin välittäjä)	Linux Trustix	84.239.231.70

Taulukko 3. Yhtiön verkkolevyt

Laitteen malli	IP-osoite
Buffalo linkstation	84.239.231.78
Iomega MHNDHD	84.239.231.77

Taulukko 4. Yhtiön työasemat

Työaseman nimi	IP-osoite
Juha	DHCP 84.239.230.248-252
Antti	DHCP 84.239.230.248-252
Varasto	DHCP 84.239.230.248-252

Taulukko 5. Yhtiön muut laitteet

Laite tai malli	Rooli	IP-osoite
HP ProCurve J9019B	Valokuitukytkin	84.239.231.82
Cisco SA520	Reititys, DHCP, VLAN	84.239.231.65, 84.239.230.241
Dlink DGS 1016D	Kytkin	
Dlink Wlan	Langaton verkko	
Kaksi tulostinta	Jaettu työasemilta	

Tulostimien liittäminen Active Directoryyn on mahdollista myöhemmin. Tämän etuna on se, että verkkoyhteyttä ei tarvitse erikseen muodostaa verkkotulostimeen ennen tulostusta.

2.3 Toimintasuunnitelma

Verkonuudistusprojektille on varattu kaksi palvelinta, AD-Exchange ja Filemaker2. AD-Exchange-palvelin toimii pääpalvelimena, johon asennetaan kaikki palvelut, eli Active Directory, Exchange ja DNS. Palvelin on täysin tyhjennetty ja käyttöjärjestelmäksi on asennettu tuore Windows Server 2008 R2. Palvelin on HP ProLiant ML 350 G5 -neliydinprosessorilla, neljällä gigatavulla muistia sekä RAID-5-varmistusjärjestelmä neljällä kiintolevyllä. Lisää kiintolevytilaa saa tarvittaessa Filemaker2-palvelimelta sekä verkkolevyiltä.

Filemaker2 toimii toissijaisena palvelimena, johon voidaan replikoida, eli kahdentaa Active Directoryn ja DNS:n varapalvelut. Exchangesta ei tehdä toissijaista instanssia ohjelmiston kevyehkön käytön ja lisenssikulujen vuoksi, mutta se varmuuskopioidaan säännöllisesti vikojen varalta. Filemaker2 nimetään myöhemmin Ad2:ksi.

Palveluista asennetaan ensin Active Directory, joka tulee asennuspakettina Windowsin mukana. Sen asennus aloitetaan samalla tavalla kuten muutkin Windowsin komponentit. Tämän jälkeen asennetaan DNS-palvelu ja tuodaan päivitetyt vanhat DNS-tietueet vanhalta palvelimelta uuteen. Active Directory -alustan ollessa kunnossa asennetaan ja konfiguroidaan Exchange Server 2010. Asennusjärjestys täytyy olla tämä, sillä Exchange käyttää Active Directorya suoraan tilienhallintaan. Kaikkien uusien ohjelmistojen ja palveluiden asennusten jälkeen kaikki liitettävissä olevat verkkolaitteet ja käyttäjät lisätään Active Directoryn tietokantaan. Palveluiden toiminta testataan ja niistä kerätään tilastoa rasitustestien aikana. Kaiken toimiessa tarkoituksellisesti vanhat palvelimet ja palvelut ajetaan alas ja otetaan uudet yhtiön käyttöön.

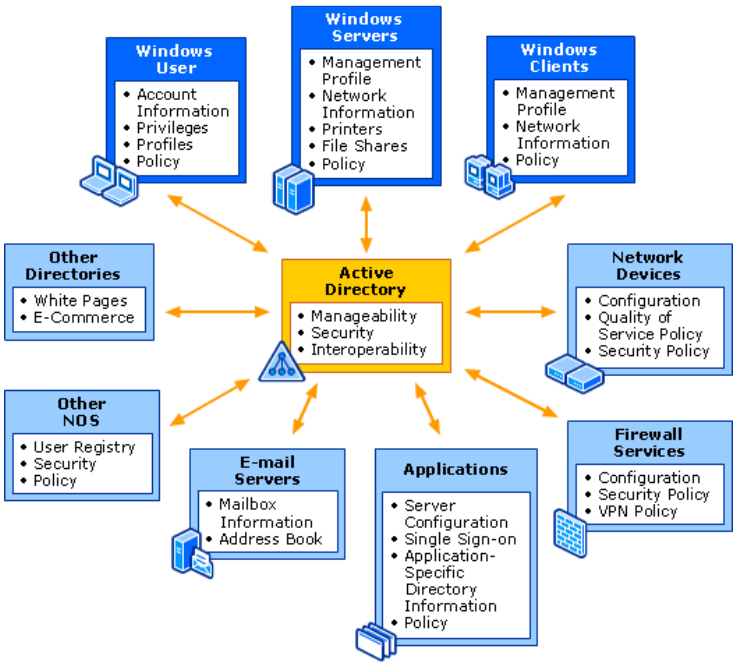
3 Active Directory

3.1 Esittely

Active Directory on Microsoftin vuodesta 1999 lähtien kehittämä domaininhallintapalvelu, jonka tarkoituksena on domainiin liitetyn verkon resurssien keskitetty hallinta. Ohjelmisto on ollut Windows Serverien, eli Windowsin palvelinversioiden mukana erikseen asennettavana komponenttina jo versiosta Windows 2000 Server. Uusin versio on Windows Server 2008 R2, jota käytetään myös tässä projektissa. Active Directory toimii vain Windows-alustalla, mutta muille käyttöjärjestelmille on olemassa vastaavanlaisia ohjelmistoja, kuten Linuxille avoimen lähdekoodin Samba, joka on suoraan Active Directory -yhteensopiva. Muita samanlaisia ohjelmistoja ovat kehittäneet Novell ja Oracle. Macintoshille on oma natiivi palvelunsa Open Directory. Kaikille näille on yhteistä liian monimutkaisesta X.500-standardista johdettu kevytversio LDAP:n käyttö, jolla ne voivat myös jossain määrin keskustella keskenään.

3.2 Käyttötarkoitus

Active Directory toimii verkon runkopalveluna, jota lähes kaikki muut palvelut hyödyntävät tavalla tai toisella (kuvio 1). Active Directoryn käyttötarkoitus on koko domainin kaikkien luetteloitavissa olevien objektien tarkka hallinta. Jokaisesta verkon käyttäjästä on oma profiili, johon voidaan määritellä suuri määrä erilaista tietoa, kuten käyttäjätunnus, nimi, osoite, sähköpostiosoite, jne. Jokainen käyttäjä sidotaan yhteen tai useampaan käyttöoikeusryhmään, jotka taas ovat tarkkaan määriteltyjä listoja oikeuksista ja käytettävistä resursseista. Käyttäjien oletustyöpöydät voidaan vaikka tarvittaessa muokata samanlaisiksi tai asennusoikeuden voi poistaa. Käyttöoikeusryhmille löytyy runsaasti käyttötarkoituksia. Käyttäjien lisäksi Active Directory pitää kirjaa domainiin kytketyistä laitteista, joille jokaiselle annetaan oma verkkonimi sekä valinnaisesti ryhmä ja suuri määrä muuta informaatiota. Näin mahdollistetaan verkossa liikkuminen ilman erillistä uudelleenautentikointia jokaisen laitteen kohdalla. Koko luettelon nitoo kokoon schema, joka on tietokantaa kuvaava malli. Malli määrittää, minkälaisia objekteja tietokannassa voi olla ja mitä attribuutteja niille voi määrittää. Active Directory on kuin kontrolloitu puhelinluettelo, josta nähdään vain ne tiedot, joihin itsellä on käyttöoikeus.



Kuvio 1. Havainnollistava kaavio Active Directoryn roolista organisaatiossa.

3.3 Logiikka

Active Directoryn toimii kolmella loogisella tasolla. Ylin on **forest**, eli metsä, joka pitää kaiken organisaatioon liitetyn koossa. Sen hallinnassa on global catalog, eli eräänlainen suppea ja nopeasti etsittävä luettelo kaikesta, mitä kyseisessä Active Directory organisaatiossa on. Myös schema, rakenne ja kaikki asetukset löytyvät tältä tasolta. Forestin alla on **tree**, eli puu, joka määrittää domainien nimien ja alinimien hierarkian. Alimpana on **domain**, jonka tietokantaan on kaikki siihen liitetyt objektit, eli resurssit ja käyttäjät, sidottu. Jokainen domain on oma tietokantansa, jonka voi monistaa toissijaisille palvelimille tai varmuuskopioksi. Domainien alle on mahdollista vielä perustaa organisaatioyksiköitä (Organizational Unit, OU). **Organizational Unit** on abstrakti järjestelmänvalvojien työtä helpottamaan tarkoitettu hallintaryhmä, ei siis varsinainen taso. Looginen puumalli mahdollistaa suurten domainmäärien hallinnan periaatteessa samalla järjestelmällä kuin yhden. Ainoastaan laitevaatimukset nousevat hallinnoitavan määrän noustessa, mutta ohjelmisto ja logiikka pysyy samana. Maantieteellistä aluetta määrittää **site**, eli verkkoalue, joka käytännössä tarkoittaa yksittäistä Exchange-organisaation verkkoa. Exchangen asennuksen yhteydessä luodaan automaattisesti oletus-site, joka tarkoittaa pääkonttorin verkkoa. [1, s. 42.]

3.4 Toiminta

Active Directory sisältää kuusi palvelua, joista osa on pakollisia ydinpalveluita ja osa lisäpalveluita laajennettua toimintaa varten. Jokainen palvelu on asennettavissa Windowsin komponenteista tai asennusmedialta. Tässä projektissa käytetään ainoastaan Active Directory Domain Serviceä, sillä muut palvelut on tarkoitettu vaativampiin rooleihin suuremmissa organisaatioissa, eikä niitä yleisimpiin käyttötarkoituksiin tarvita.

3.4.1 Domain Services

Domain Services -palvelu (DS) tarjoaa Active Directoryn pääasiallisen käyttötarkoituksen, eli tietokannan (global catalog) verkkoon liitetyistä resursseista ja käyttäjistä, sekä alustan erilaisille Active Directory -yhteensopiville ohjelmille, kuten Exchangelle. Domain Servicen kautta muodostetaan saatavilla olevista resursseista hierarkkinen puu, eli kerrosmalli, jossa forest, puut ja domainit ovat. Palvelu pitää

sisällään myös käyttäjäntunnistuksen, scheman, etsintä- ja luettelointimekanismin sekä replikaation. Palvelin, johon Domain Services on asennettu, toimii Domain Controllerina (ohjauskone), eli Active Directory -organisaation juurena. [1, s. 50.]

3.4.2 Rights Management Services

Tämän lisäpalvelun tarkoituksena on parantaa tietoturvaa lisäämällä pysyviä käyttökäytäntöjä, eli policyja, sekä sertifikaatteja ja lisenssitietoja. Rights Management (RMS) -palvelua käytetään Windowsiin integroidulla RMS-asiakasohjelmalla, joka on ollut erikseen asennettavana komponenttina Vistasta lähtien. Palvelu suojaa käytännössä dokumentteja, sähköpostia ja erilaisia sovelluksia siten, että omistava käyttäjä voi määrittää, kuka tiettyä dokumenttia voi käyttää ja millä tavalla. [1, s. 704.]

3.4.3 Lightweight Directory Services

Aikaisemmalta nimeltään tunnettu Active Directory Application Mode, Lightweight Directory Services (LDS) on Domain Servicen kevytversio, joka tarjoaa suurimman osan täysversion ominaisuuksista Active Directory -yhteensopiville ohjelmille, mutta ilman Domain Servicen domain-toiminnallisuuksia. LDS:n tarkoitus on varastoida verkon AD-yhteensopivien palveluiden tietoja keskitettyyn verkkolevyvarastoon, joka on käytössä muille sovelluksille tai sovellukselle itselleen. LDS on suunniteltu toimimaan itsenäisenä palveluna puhtaassa palvelinympäristössä, mutta LDS ja DS voivat olla toiminnassa samaan aikaan, sillä LDS käyttää omia tietokantojaan tietojen varastointiin. Tällaisessa tilanteessa se voi käyttää DS:n tarjoamaa käyttäjätiliautentikointia. [1, s. 620.]

3.4.4 Certificate Services

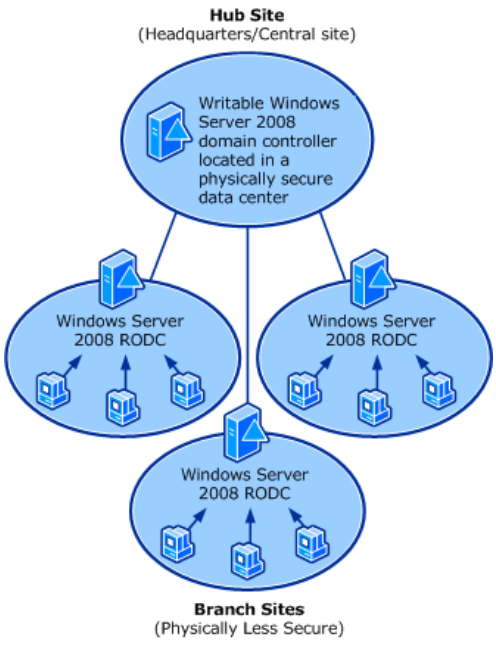
Certificate Services (CS) tarjoaa julkisen avaimen periaatteella toimivia sertifikaattipalveluita, joita käytetään muun muassa web-sivuilla, kirjautumisissa, sähköposteissa, VPN-palveluissa yms. Active Directory -ympäristössä sertifikaatteja käytetään myös yksittäisten käyttäjien ja koneiden autentikointiin. Sertifikaattien varmennus organisaation omalla palvelulla vähentää huomattavasti kuluja ja mahdollistaa niiden käytön myös sellaisissa palveluissa, joihin ei tavallisesti käytettäisi kaupallista sertifikaattia. Tämä parhaimmassa tapauksessa lisää huomattavasti organisaation tietoturvaa. [1, s. 661.]

3.4.5 Federation Services

Federation Servicen käyttötarkoitus on palveluun sidottujen web-sovellusten käyttäjäkohtaisten kirjautumistietojen keskittäminen siten, että käyttäjän täytyy kirjautua vain kerran, jolloin kaikki sovellukset ovat käytössä session ajan. Palvelu myös ottaa vastaan väliaikaisia käyttäjäprofiileja muista organisaatioista, joilla on pääsyoikeus johonkin tiettyyn palveluun. Käyttäjät voivat olla organisaatiosta riippumattomia, mikä mahdollistaa suuren julkisen yksittäisistä palveluista koostuvan kokonaisuuden. Yleinen käyttötarkoitus on kahden tai useamman organisaation välinen kommunikaatiokanava, eli niin sanottu business-to-business-malli. [1, s. 745.]

3.4.6 Read-only Domain Controller

Read-only Domain Controller (RODC) ei ole varsinainen lisäpalvelu, mutta kuuluu ominaisuuksiensa vuoksi tähän kategoriaan. RODC:n tarkoitus on tarjota vain lukutilassa toimiva Domain Controller, joka replikoi omat tietonsa yleensä turvallisessa verkon osassa olevalta pääpalvelimelta. Yleinen käyttötarkoitus on domain-palveluiden ulottaminen verkon turvattomampiin osiin tai muihin maantieteellisiin sijainteihin, kuten haarakonttoreihin, joista yhdistäminen pääkonttoriin saattaa olla hidasta, turvatonta tai reaaliajassa mahdotonta (kuvio 2). [1, s. 120.]



Kuvio 2. RODC käytettynä sivukonttoreissa.

3.5 Replikointi

Active Directoryn replikointi, eli palvelun reaaliaikainen kopioituminen varapalvelimelle on tärkeä toimenpide mille tahansa organisaatiolle koosta riippumatta. Jos ensisijainen Domain Controller vikaantuu, siirtyy verkko käyttämään toissijaista palvelinta. Muuten vikatilanteessa koko verkko käytännössä jumiutuisi ilman varapalvelua. Toissijainen Domain Controller voi olla myös kuormaa jakava palvelin, jolloin osa domaineista siirretään tänne. Replikaation toiminta perustuu domain-kohtaisen tietokannan, global catalogin ja scheman päivittämiseen varapalvelimelle reaaliajassa sitä mukaa, kun muutoksia Domain Controllerille tehdään. Replikointi tapahtuu siten, että Domain Controller lähettää tiedon tapahtuneesta päivityksestä replikoivalle palvelimelle, joka hakee tiedot Domain Controllerilta. Tietoja ei siis anneta suoraan.

Kuten monissa muissakin Active Directoryyn liittyvissä yhteyskäytännöissä, replikointi käyttää yhteyden muodostamiseen FQDN-nimiä, joten asiaankuuluvat DNS-palvelun tietueet täytyy päivittää varmistavan palvelimen osoitteella. Myös mahdolliset palomuurit täytyy ottaa huomioon, jolloin replikoinnin käyttämä RPC (Remote Procedure Call, tietojen hallinta palvelussa verkon avulla), LDAP, SMB (Server Message Block, tiedostonjakoprotokolla Windowsille) ja Kerberos sallitaan. Replikointi onnistuu myös Internetin yli SMTP:n avulla, mutta silloin itse domainin tietokanta ei päivity. [17.]

3.6 Asennuksen valmistelu

Active Directoryn asennus poikkeaa jonkin verran aikaisempien Windows Server -versioiden asennustavoista, erityisesti Windows Server 2003:sta. Vähintään seuraavien asioiden täytyy olla huomioituna asennusta aloittaessa:

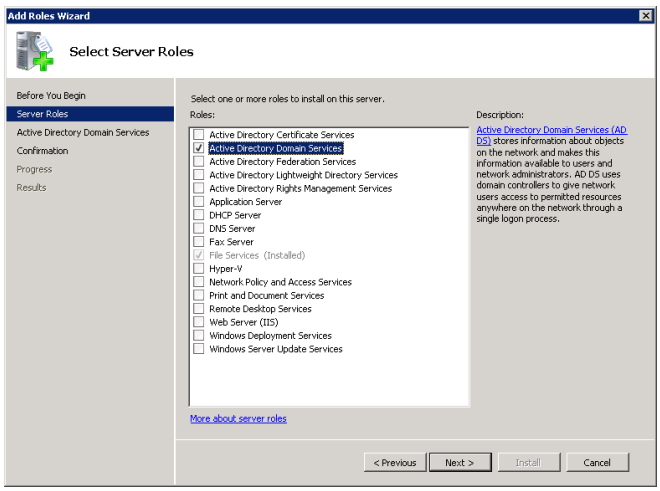
- kohdelevyn on oltava NTFS-muodossa
- käyttöjärjestelmä asennettu ja päivitetty, mielellään tyhjä, vain tätä tarkoitusta varten
- ol oltava kirjautuneena järjestelmänvalvojana
- domainin nimi ja mahdolliset subdomainit, eli alidomainit mietitty

- domainiin liitettävien koneiden ja laitteiden nimet dokumentoitu
- IP-avaruus määritelty
- DHCP-alueet suunniteltu
- käyttäjätunnusten oikeusperiaatteet suunniteltu.

Itse Active Directoryn asentaminen ei ole monimutkainen operaatio. Ensimmäinen askel on määritellä Active Directory -palvelimen rooliksi. Tämän jälkeen palvelu vasta asennetaan. Vaivattomin tapa aloittaa asennus on Server Managerin kautta. Yleensä tämä palvelu käynnistyy uuden palvelinasennuksen mukana jokaisella käynnistyskerralla, kunnes automaattinen käynnistys otetaan pois päältä. Toinen tapa on käyttää komentorivin komentoa dcpromo. Tämä kuitenkin on suunniteltu skriptikäyttöön, eikä tarjoa normaalitilanteisiin lisäarvoa.

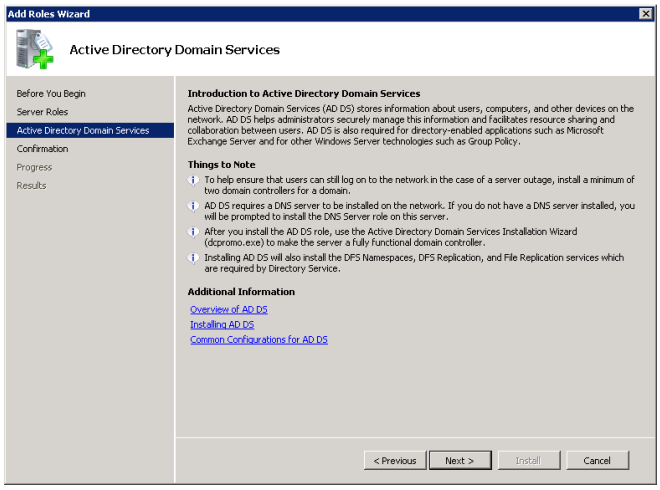
3.7 Asennus

Kätevin tapa aloittaa AD:n asennus on avata Server Manager, joka on tuoreen Windowsin asennuksen jälkeen käynnistä-valikon oikealla puolella quickstart-paneelissa. Manageri löytyy myös Administrative Toolsista. Klikataan Server Managerin pääikkunassa Roles Summary -kohdasta Add Roles. Tässä kohdassa asennusohjelma kertoo vielä asioista, joiden täytyy olla selvillä asennusta jatkettaessa. Valitaan listalta vain Active Directory Domain Services, sillä tässä vaiheessa asennetaan vain tämä peruspalvelu (kuvio 3). AD-palveluita on muitakin, mutta tämä on varsinainen juuripalvelu, jonka päällä muut palvelut toimivat. ADDS tarvitsee toimiakseen. Net Framework -version 3.5.1, jonka asennus varmistetaan ponnahdusikkunassa. Vaikka versio 3 tai sitä uudempi olisikin jo asennettu, paikkaa asennus mahdolliset puutteet tai ohittaa kokonaan tämän kohdan, jos mitään ei tarvitse asentaa. Versio 4 on jo julkaistu, mutta sitä käytetään vasta tulevissa AD-versioissa.



Kuvio 3. Active Directory Domain Services -palvelun esiasennus.

Seuraava ikkuna kertoo ADDS:n tarkoituksen, sekä ohjeita, miten palvelu konfiguroidaan asennuksen jälkeen (kuvio 4). Yleinen suositus on asentaa ensisijainen DNS ADDS:n kanssa samalle palvelimelle helpon ja vakaan synkronoinnin vuoksi, mutta on täysin mahdollista käyttää DNS:lle tarkoitettuja omia palvelimia.

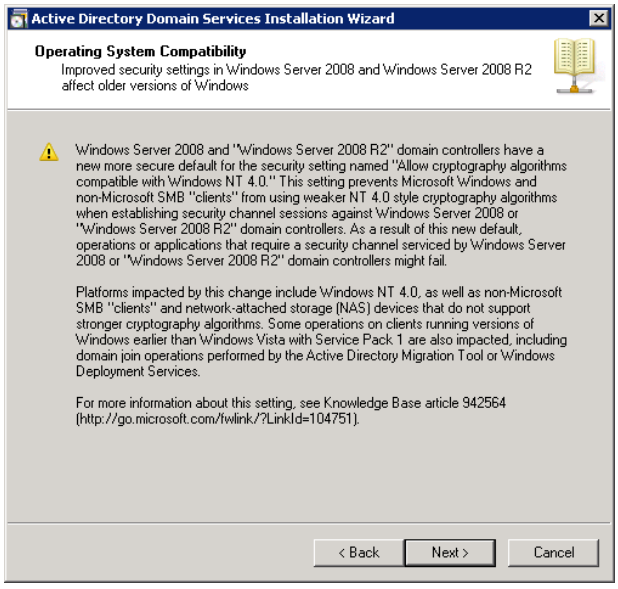


Kuvio 4. Active Directoryn esittely.

Tämän jälkeen esiasennus on valmis. Asennuksen voi aloittaa suoraan klikkaamalla sinistä linkkiä (Close this wizard and launch... dcpromo.exe). Dcpromon auetessa on mahdollisuus valita Advanced Mode, joka mahdollistaa muutamia lisäasetuksia, kuten NetBios, ylimääräisiä foresteja sekä mahdollisuus liittää ADDS vain lukutilassa toimivaan AD:een (kuvio 5). Advanced Moden voi myös käynnistää suoraan komentoriviltä komennolla dcpromo /adv. Perusasennuksessa Advanced Modea ei tarvita.

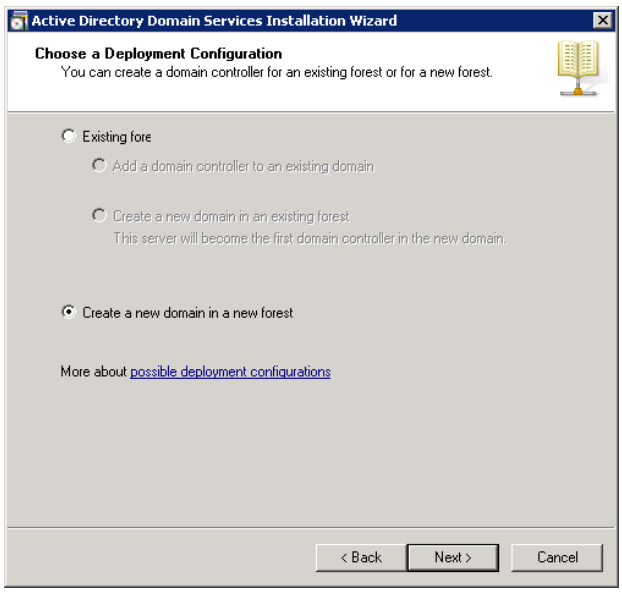
Kuvio 5. Active Directoryn asennuksen aloitusikkuna.

Seuraava ikkuna kertoo uuden AD:n tehokkaammasta salausmenetelmästä (kuvio 6). Toisin sanoen tämä tarkoittaa, etteivät Windows Vista Service Pack 1:tä aiemmat versiot voi kommunikoida uuden AD:n kanssa oikein. Windows XP toimii rajoitetusti, mutta aikaisemmat versiot eivät ollenkaan.



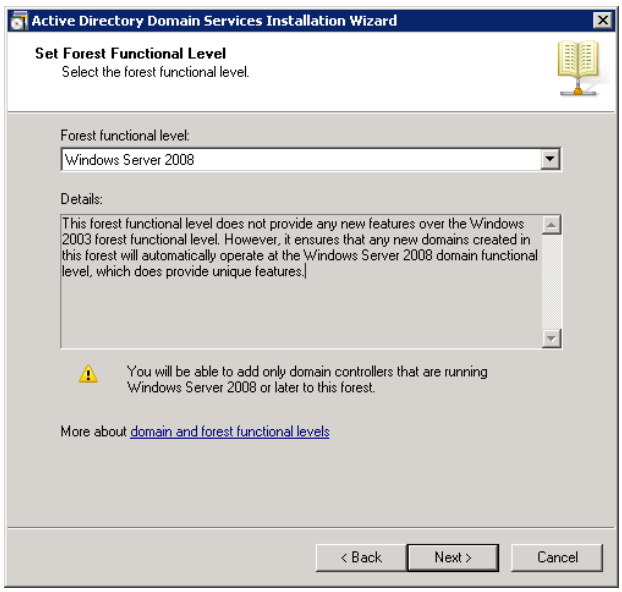
Kuvio 6. Maininta käyttöjärjestelmien yhteensopivuuksista.

Nyt valitaan uuden domainin määritykset. Koska tästä asennuksesta tulee ensisijainen AD-palvelin, valitaan Create a new domain in a new forest (kuvio 7). Jos asennus liitettäisiin olemassa olevaan domainiin, valittaisiin ylempi vaihtoehto.



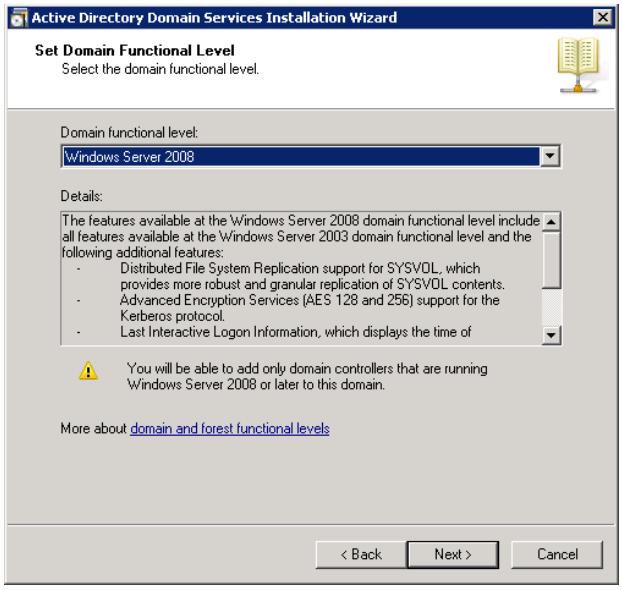
Kuvio 7. Uuden tai olemassaolevan forestin valinta.

Seuraavaksi törmätään mielenkiintoiseen ja tärkeään määritykseen, AD:n forestin toiminnalliseen tasoon. Koska asennettava AD-versio on 2008 R2, olisi luontevaa valita AD:lle suurin mahdollinen toiminnallinen taso. Tämä ei kuitenkaan ole välttämättä järkevää, sillä R2:lla uusia ominaisuuksia on hyvin vähän ja ylimmän tason valitseminen rajoittaa toissijaisten AD-palvelinten asennuksen ainoastaan Windowsin versiolle R2. Jos muut yhtiön palvelimet ovat versioita 2008 ja 2003 R2, on erittäin kallista päivittää koneet uusimmalla Windowsilla ainoastaan parin lisäominaisuuden takia. Uudet domain-ominaisuudet ovat merkintä kirjautumisen tavasta (kirjautuminen vai älykortti) ja uusi hallintaluokka palveluille (kuten Exchange, IIS ja SQL). Forestin ominaisuuksiin lisättiin vain yksi: roskakori, joka kykenee palauttamaan tuhottuja objekteja koko domainin alueelta. Ennen tähän tarvittiin järjestelmän palautus varmuuskopiolta. Tässä kokoonpanossa valitaan huomattavasti suuremman yhteensopivuuden turvaamiseksi toiminnallinen taso 2008 (kuvio 8).



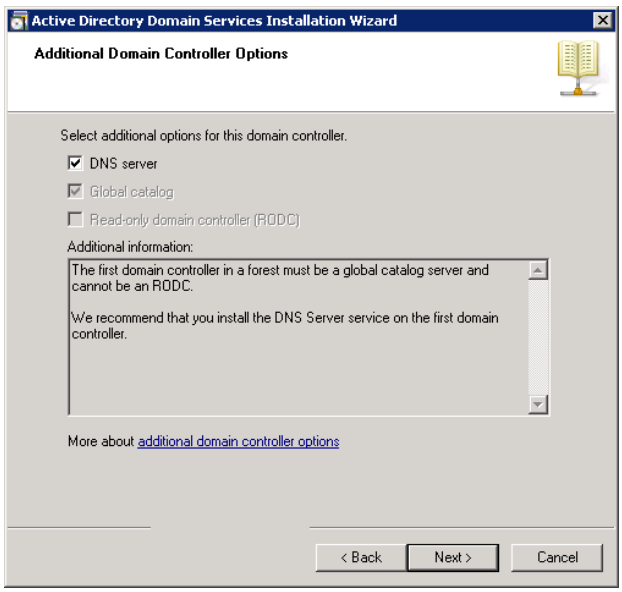
Kuvio 8. Forestin toiminnallisen tason valinta.

Kuten myös edellisessä ikkunassa, valitaan domainin toiminnalliseksi tasoksi 2008 (kuvio 9).



Kuvio 9. Domainin toiminnallisen tason valinta.

Tässä kohdassa dcpromo tarkistaa DNS:n olemassaolon ja suosittelee sitä asennettavaksi ensisijaiselle AD-palvelimelle (kuvio 10). Tässä projektissa on nimenomaan tarkoitus siirtyä käyttämään AD:ta myös DNS:n tarpeisiin, valitaan DNS asennettavaksi.

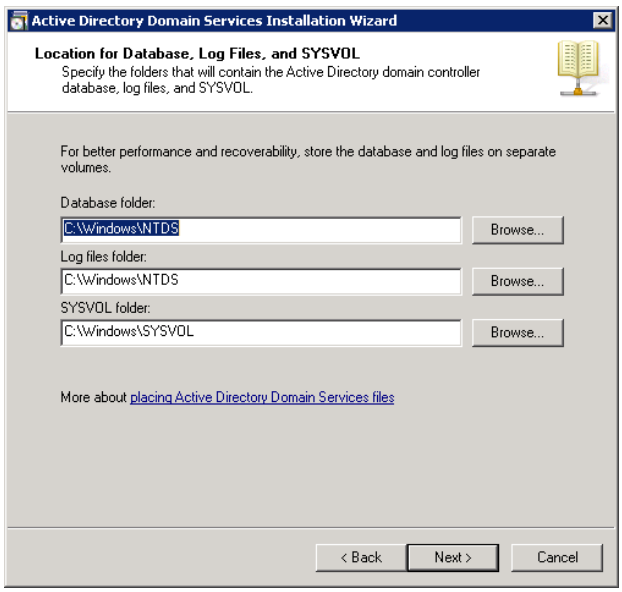


Kuvio 10. DNS-palvelun asennus.

Seuraavaksi aukeaa varoitusikkuna, joka kertoo, ettei DNS-palvelua voi asentaa, sillä ensisijaista DNS-palvelinta ei löydy (kuvio 11). Virheilmoitus ei haittaa tässä tapauksessa, sillä uuden forest-juuren asennusvaiheessa DNS-palvelinta ei vielä ole. Virheilmoituksen voi ohittaa, ellei ole asentamassa juuri-domainiin toissijaista DNS-palvelinta.

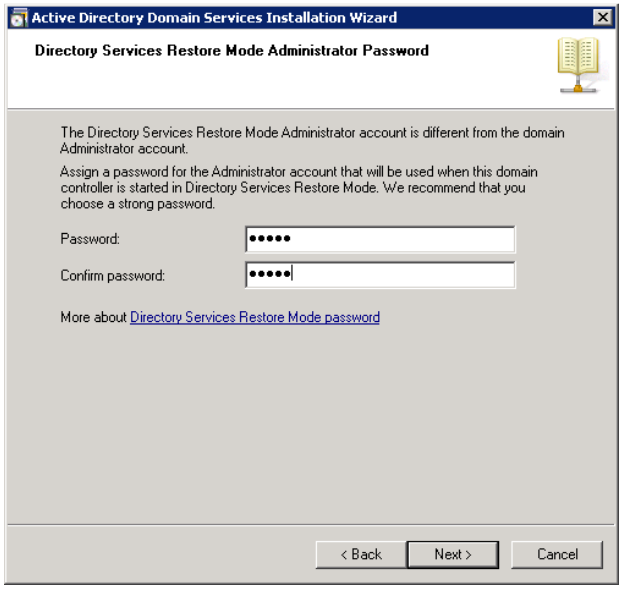
Kuvio 11. Varoitus DNS-palvelun puuttumisesta.

Seuraava ikkuna suosittelee eri tiedostojen (tietokanta, loki ja SYSVOL) asentamista eri levyille (kuvio 12). Tässä palvelimessa on kuitenkin neljän levyn RAID-5 yhtenä loogisena levynä, joten nopeuden tai vikasietoisuuden puutetta ei tarvitse pelätä. Asetukset jätetään oletuksiksi.



Kuvio 12. Tietokantojen ja lokitiedostojen asennuspolkujen määrittely.

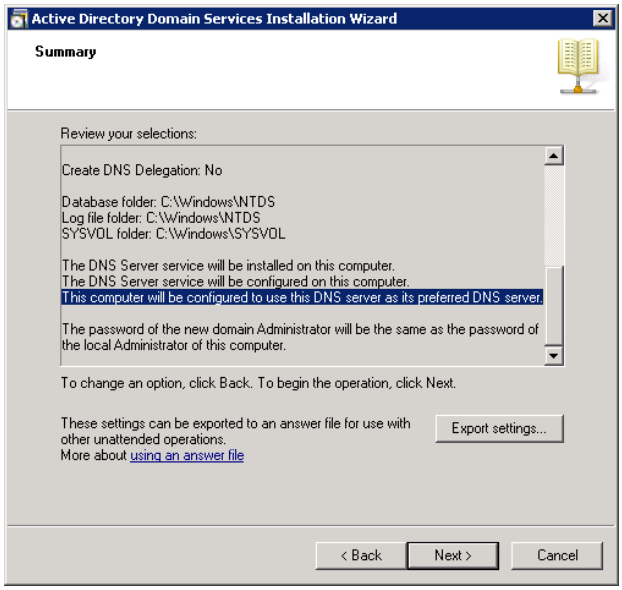
Tässä kohdassa määritetään salasana palautusoperaatioita varten (kuvio 13).



Kuvio 13. Järjestelmän pelastusoperaation aloitukseen tarvittavan salasanan määrittely.

Seuraavaksi asennus näyttää yhteenvedon asennuksen keräämistä tiedoista asennusta varten. Tässä on syytä huomata maalattu rivi, jossa kerrotaan palvelimen siirtyvän automaattisesti käyttämään itseään DNS-palvelimena (kuvio 14). Näin juuri luotu DNS-palvelin on tyhjä, ei sen käyttöönottoon tässä vaiheessa ole tarvetta. Asennuksen jälkeen täytyy muistaa sammuttaa DNS palvelunhallinnasta ja määrittää verkkokortin käyttämä DNS-osoite, mikäli aikoo jatkaa entisen DNS:n käyttöä. Tämän jälkeen

varsinainen asennus alkaa. Kun ohjelma ilmoittaa valmistuneensa, klikataan finish. Palvelin pitää vielä käynnistää uudelleen. Uudelleenkäynnistyksen jälkeen on hyvä hetki tarkistaa DNS-asetukset. [4.]



Kuvio 14. Asennuksen asetusten yhteenveto.

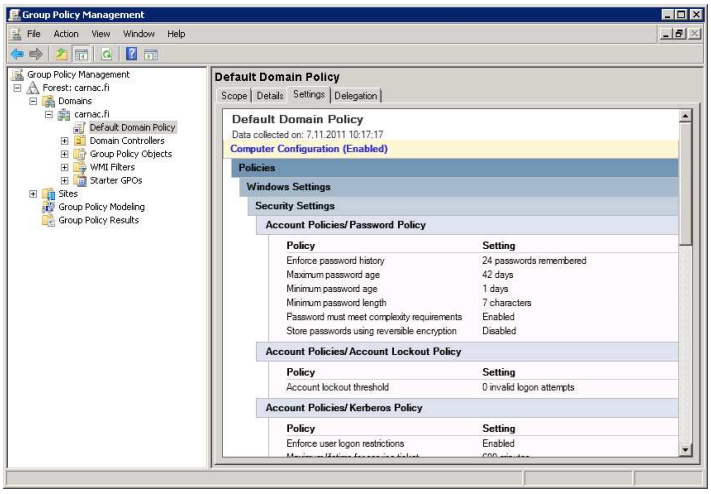
3.8 Konfigurointi

Asennuksen valmistuttua ennen muiden asetusten muokkausta kannattaa määrittää turvallisuusasetukset, jotka ovat oletuksena tavalliseen käyttöön liian tiukat. Muun muassa salasanan monimuotoisuus ja pituus yhdistettynä nopeaan vanhenemiseen johtavat usein siihen, ettei kukaan muista salasanaansa, kun se on muutettava kuuden viikon välein ja vieläpä muotoon, jossa täytyy olla isoja ja pieniä kirjaimia numeroihin yhdistettynä. Samankaltaistakaan salasanaa ei saa määrittää uudelleen. Yleisessä skenaariossa ihmiset kulkevat käytävillä keltainen muistilappu kourassa, johon sen hetkinen salasana on kirjoitettu. Tämä ei liene kovinkaan turvallista.

Klikataan Start-valikkoa, Administrative Tools ja Group Policy Management. Laajennetaan uusi forest, Domains, domainin nimi ja valitaan Default Domain Policy. Tässä näkymässä on yhteenveto useimmin käytetyistä asetuksista. Asetuksia pääsee muokkaamaan klikkaamalla domainin nimeä oikealla hiiren napilla ja valitsemalla edit.

Avautuneessa Group Policy Management Editorissa avataan puu Policies, Windows Settings, Security Settings, Account Policies, Password Policy (kuvio 15). Näillä asetuksilla

saadaan salasanan hallinnoinnin perusasetukset kuntoon. Huomionarvoinen asia on asetusten määrittäminen tilaan ”Not Defined”. Esimerkiksi ”Maximum password age” arvolla 0 (ei vanhene) ei ole sama asia kuin arvon jättäminen tyhjäksi. Tyhjä arvo on mahdollista ohittaa jostain muualta, jopa käyttäjän toimesta, mutta määritelty arvo on aina ensisijainen. [1, s. 399.]

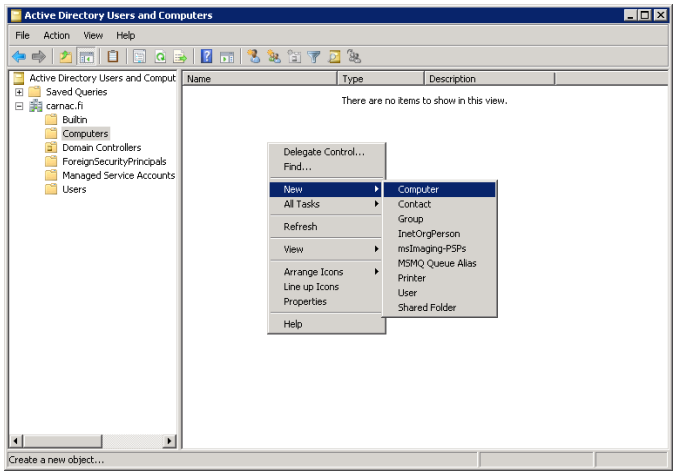


Kuvio 15. Yleiset turvallisuusasetukset.

3.8.1 Laitteet ja käyttäjät

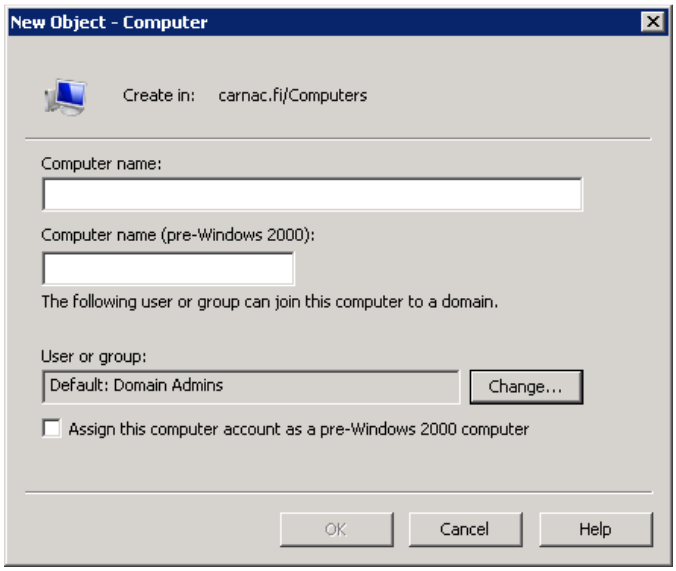
Seuraava vaihe Active Directoryn käyttöönotossa on käyttäjien ja laitteiden määritteleminen. AD ei millään tavoin tunnista laitteita automaattisesti, joten niiden syöttäminen tietokantaan on järjestelmänvalvojan tehtävä. Suurissa järjestelmissä automaattisen tunnistuksen voi järjestää Visual Basic -skriptillä, eli sarjan komentoja sisältävällä listalla käyttäen AD:n alla toimivaa LDAP:ta.

Käyttäjänhallinnan saa auki Start-valikosta, Administrative Tools, Active Directory Users and Computers. Kuten AD:ssä useimmiten kaikki muukin toiminta, uuden laitteen saa määritellyksi klikkaamalla Computers-osiossa hiiren oikeaa nappia ja valitsemalla New, Computer (kuvio 16).



Kuvio 16. Active Directoryyn kytkettyjen laitteiden hallinta.

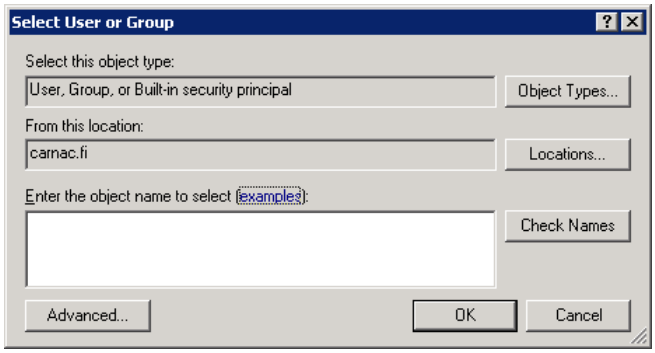
Käyttöoikeusryhmän määrittäminen objektille on AD:ssa hieman erikoisempi toimenpide, sillä seuraavissa kuvankaappauksissa esiintyvät varsin moniselitteiset nappulat eivät tavallisesti selviä käyttäjälle ihan noin vain. Käyttöliittymä on näennäisesti sekava historiallisista syistä, mutta mahdollistaa nopean toiminnan harjautuneen käyttäjän käsissä.



Kuvio 17. Luodun laitteen tiedot ja käyttöoikeusryhmä.

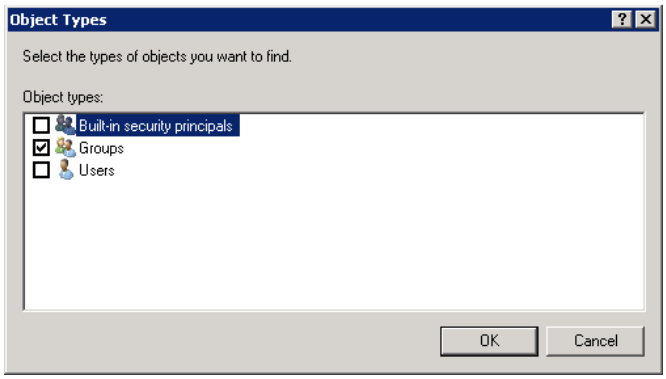
Change-nappulalla avautuva ikkuna on itse asiassa hakukone, jolla etsitään tiettyjä objekteja, eikä lista käyttöoikeusryhmistä, mitä voisi kuvitella nappulan takaa avautuvan (kuvio 17). Käyttöoikeusryhmän voi kirjoittaa suoraan hakukenttään ja painamalla Check Names kone löytää sitä vastaavan ryhmän. Tämä lähestymistapa on

suunniteltu enemmän erittäin suuria järjestelmiä silmälläpitäen. Kuitenkin tässä järjestelmässä kannatta käyttää suoraviivaisempia keinoja. Klikataan Advanced (kuvio 18).



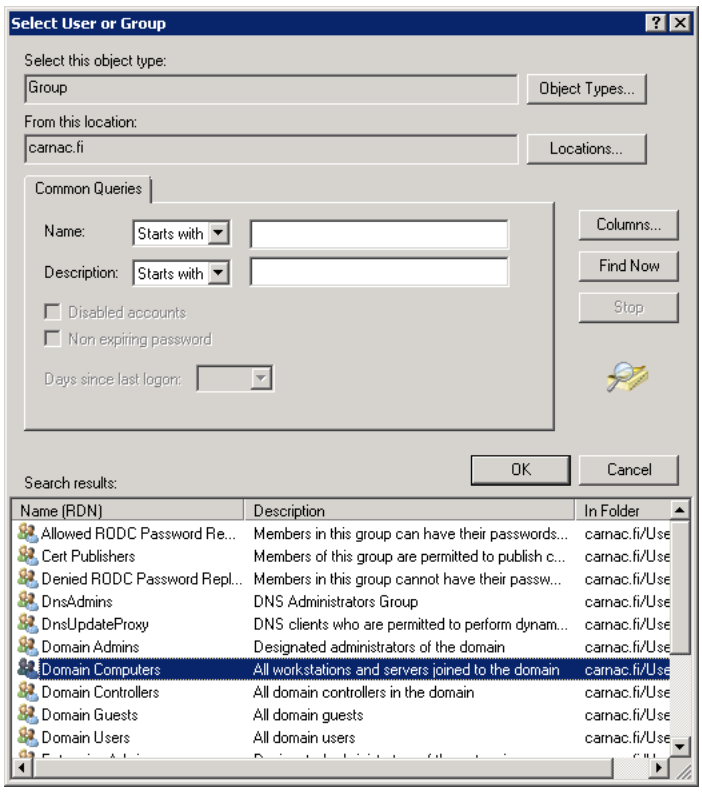
Kuvio 18. Hakukone käyttöoikeusryhmän määrittämiseen.

Nappulan takaa avautuva vielä sekavampi ikkuna listaa varsinaiset ryhmät. Klikkaamalla Object Types voidaan suodattaa kaikki muut paitsi ryhmät pois hausta (kuvio 19).



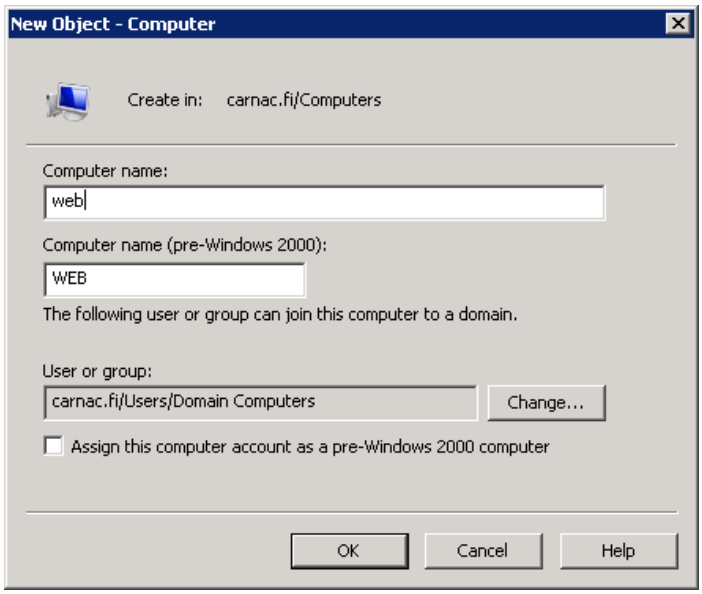
Kuvio 19. Hakukoneen suodatin, jolla karsitaan listalta epäoleelliset kohteet.

Klikkaamalla Find Now saadaan lista kaikista ryhmistä (kuvio 20). Koska ollaan lisäämässä AD:n tietokantaan palvelinta, valitaan Domain Computers, jonka kuvauksessa suositellaan tämän valintaa työasemien lisäksi myös palvelimille.



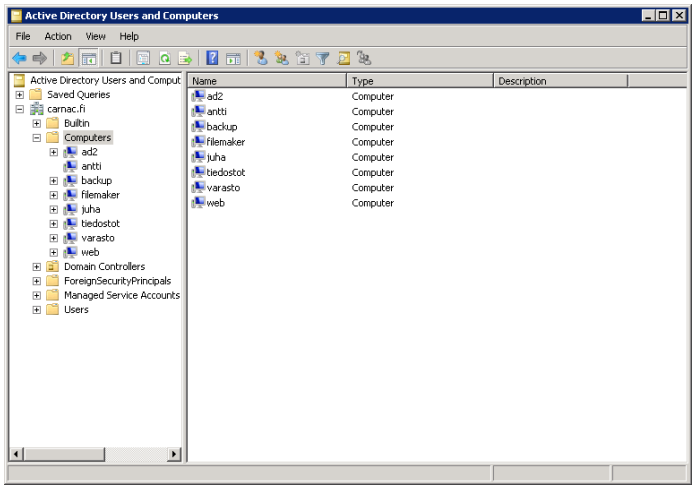
Kuvio 20. Haun tuloksena löydetyt käyttöoikeusryhmät.

Kun kaikki kohdat dialogissa ovat oikein, klikataan Ok. Tällä tavalla määritellään kaikki yhtiössä käytettävät laitteet (kuvio 21). Kaikki palvelimet ja työasemat kuuluvat oletuksena käyttöoikeusryhmään Domain Computers, paitsi Domain Controllerit, jotka kuuluvat vastaavaan ryhmäänsä.



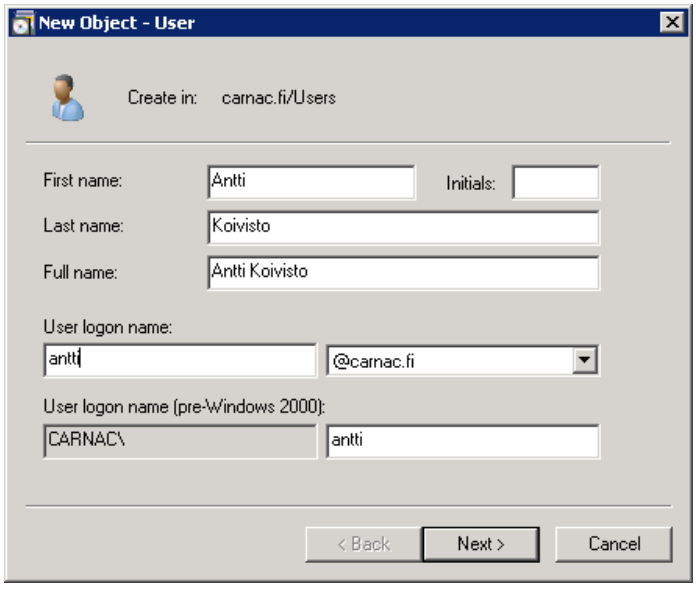
Kuvio 21. Valmiiksi määritelty web-palvelin.

Valmis lista näyttää kaikki lisätyt laitteet (kuvio 22). Itse Domain Controlleria ei voi lisätä laitelistaan. Listan hyötyä voi lisätä muokkaamalla tietosarakkeita ja asettamalla haluttuja tietoja, kuten käyttöoikeusryhmät.



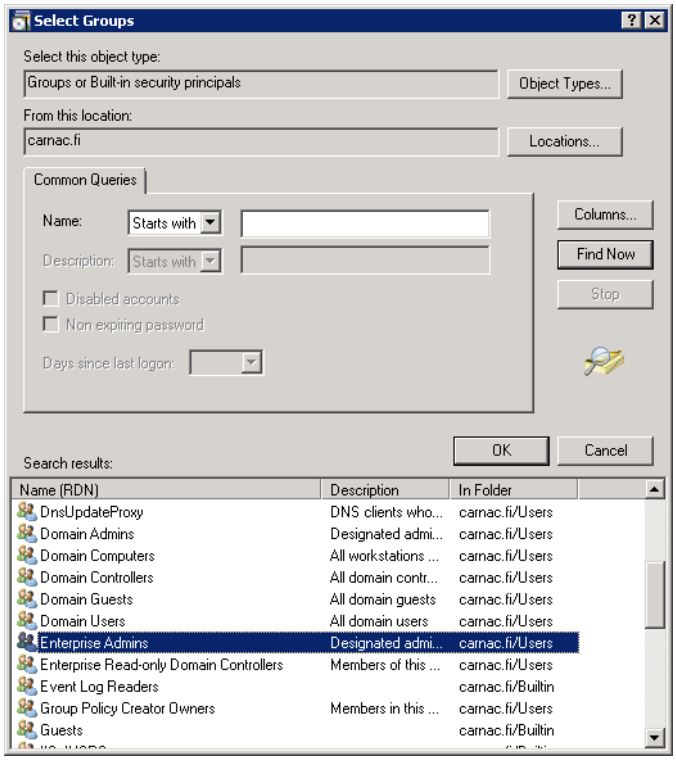
Kuvio 22. Lista verkkoon kuuluvista laitteista.

Seuraavaksi lisätään käyttäjät Users-paneeliin lähes samalla tavalla kuin koneetkin (kuvio 23). Käyttäjätietojen jälkeen seuraa salasanan määritys. Koska määritetään ennalta tiedossaolevat salasanat, poistetaan rasti salasanan pakollisesta muuttamisesta ja merkitään Password never expires. Klikataan next. Yhteenvetoikkunassa klikataan finish.



Kuvio 23. Käyttäjän lisäys.

Lisätään käyttäjäkantaan sopiva määrä testikäyttäjiä, eli Antti Koivisto ja Juha Kirkkala. Koska haluan pitää itselläni käyttöoikeudet koko AD-puuhun, valitsen itseni ja klikkaan oikealla hiiren napilla Properties. Välilehdeltä Member of lisään itseni Enterprise Adminiksi, asetan ensisijaiseksi ryhmäksi nappulalla Set Primary Group ja poistan Domain Usereista (kuvio 24).



Kuvio 24. Käyttäjän käyttöoikeusryhmän määrittäminen tapahtuu samalla työkalulla kuin laitteiden.

3.8.2 DNS

Ensisijainen DNS-palvelu oli aikaisemmin Linux-palvelimella ja toissijainen web-palvelimen yhteydessä. Nyt on tarkoitus tehdä ensisijaisesta Active Directory-palvelimesta myös ensisijainen DNS-palvelin. Näin nimihaku nopeutuu oleellisesti ja tekee siitä vakaampaa, sillä AD:n ei tarvitse turvautua muihin palvelimiin. DNS-tietueiden tuonti sellaisenaan Linuxin Named-palvelusta ei onnistu kovinkaan helposti ilman erikoistyökaluja. Tietueiden luominen käsin kaikille domaineille on hidasta ja saattaa aiheuttaa kirjoitusvirheitä.

Paras tapa on kopioida DNS-tietueet vanhalta toissijaiselta Windows-pohjaiselta DNS-palvelimelta, sillä tietueet ovat jo valmiiksi siirrettävässä muodossa. Kopioidaan polusta

c:\windows\system32\dns\ kaikki siirrettävät tietueet uudelle koneelle samaan kansioon. Samalla tarkistetaan, että jokaisen tietueen MX-rivillä, eli sähköpostipalvelimen osoittavalla tietueella, osoite on mail.carnac.fi, sillä tämä tulee olemaan käytettävän postipalvelimen osoite. Tämän jälkeen avataan rekisterieditori regedit, josta polusta HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\DNS Server\Zones viedään tiedostoksi kaikki DNS-viitteet. Tämä rekisteritiedosto siirretään uudelle koneelle ja ajetaan se. Kun DNS-palvelu sammutetaan ja käynnistetään uudelleen, uudet domainit ovat ilmestyneet DNS-manageriin. Tässä vaiheessa muutetaan palvelimen verkkoasetuksista DNS-osoitteeksi palvelin itse. Tämä on hyvä olla tehtynä viimeistään Exchange Serverin asennuksen alkaessa. [5, 10.]

3.8.3 Toissijainen Domain Controller

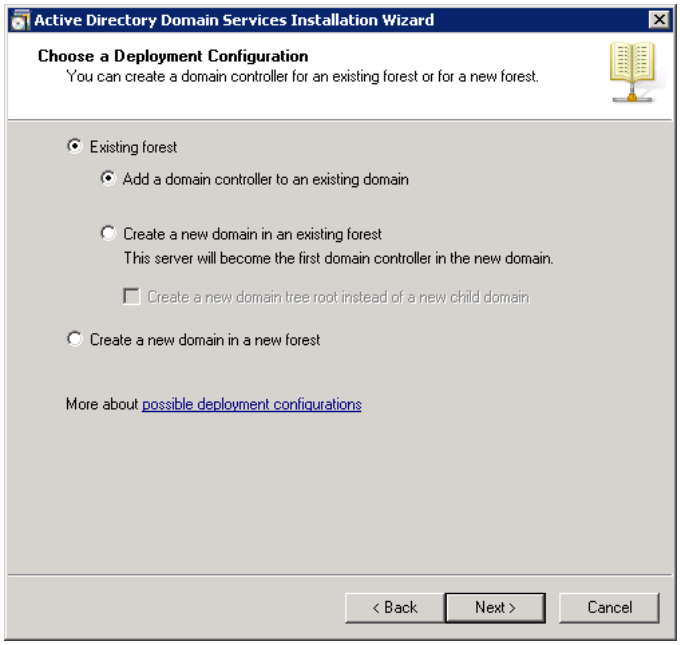
Verkon tärkeimmän elementin, eli Domain Controllerin varmistaminen on erittäin tärkeää. Tämän vuoksi Active Directory Domain Services (AD DS) asennetaan myös toissijaiselle palvelimelle, eli Ad2:lle. Itse peruspalvelu asennetaan tarkalleen samalla tavalla kuin ensisijaiselle Domain Controllerille, paitsi tiedostojen kopioinnin jälkeen palvelu täytyy määrittää toissijaiseksi Domain Controlleriksi Active Directoryn kehittyneiden ominaisuuksien asennusvelholla. Tämä tapahtuu kirjoittamalla komentokehotteeseen komento dcpromo /adv (kuvio 25).

Kuvio 25. Komentokehotteen komento, jolla kehittyneiden ominaisuuksien asennus aloitetaan.

Komento avaa Active Directory Domain Services -asennusvelhon, jolla asennettiin ensisijainen Domain Controller, mutta tällä kertaa kehittyneessä tilassa, jolla toissijaiset DC:t asennetaan (kuvio 26).

Kuvio 26. Kehittyneen tilan asennuksen aloitus.

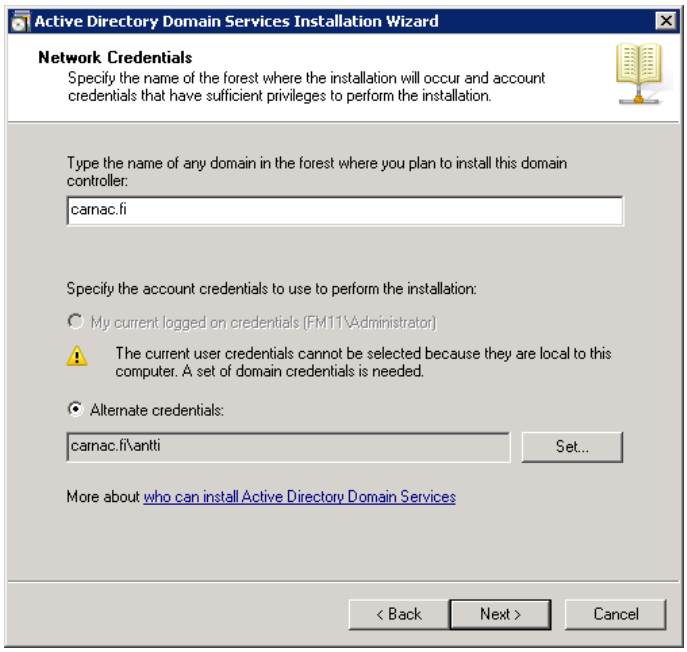
Tällä menetelmällä asennetaan kaikki toissijaiset palvelimet, uudet domainit olemassa oleviin foresteihin sekä kokonaan uudet forestit. Nyt valitaan olemassa olevaan forestiin uusi Domain Controller (kuvio 27).



Kuvio 27. Määrittely toissijaiseksi palvelimeksi.

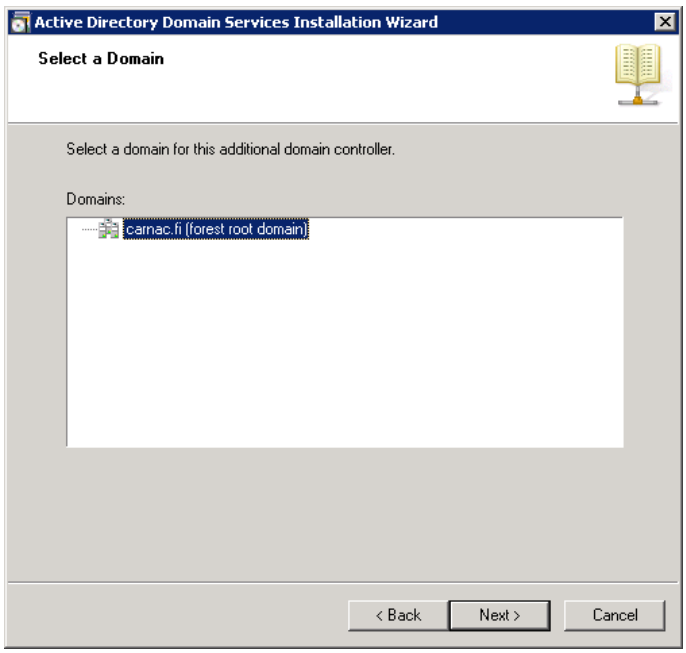
Seuraavassa ikkunassa valitaan domain, johon uusi Domain Controller liitetään (kuvio 28). Samalla syötetään riittävillä oikeuksilla varustettu tunnus, jolla voidaan

kommunikoida ensisijaisen palvelimen kanssa. Tilitietojen hakeminen ei ole mahdollista, sillä palvelin ei ole vielä domainissa.



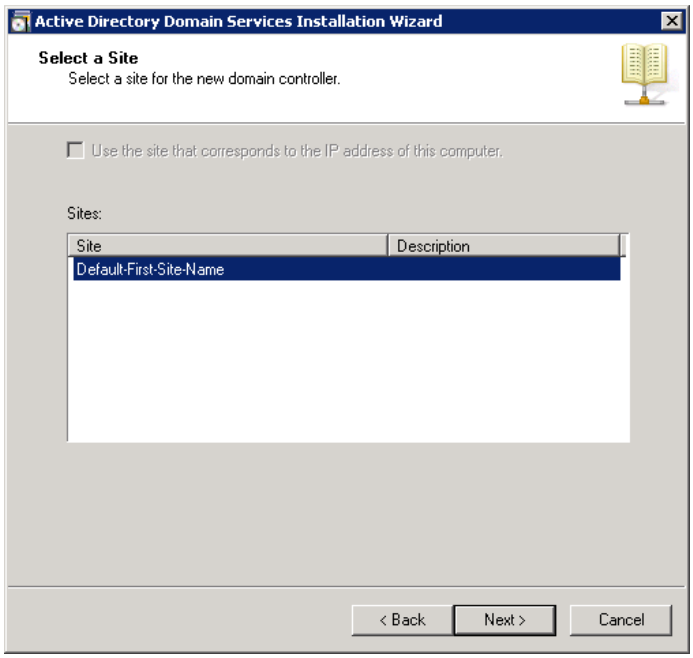
Kuvio 28. Domain- ja käyttäjätietojen tarkistus.

Seuraavaksi asennusohjelma löytää annetun käyttäjätunnuksen ja domainin avulla varsinaisen ensisijaiselta palvelimelta löydetyn domainin, joka valitaan (kuvio 29). Tässä kohdassa olisi mahdollista valita jokin muukin domain, jos niitä olisi tarjolla. Näin saataisiin toissijainen palvelin varmistamaan vain tiettyä domainia.



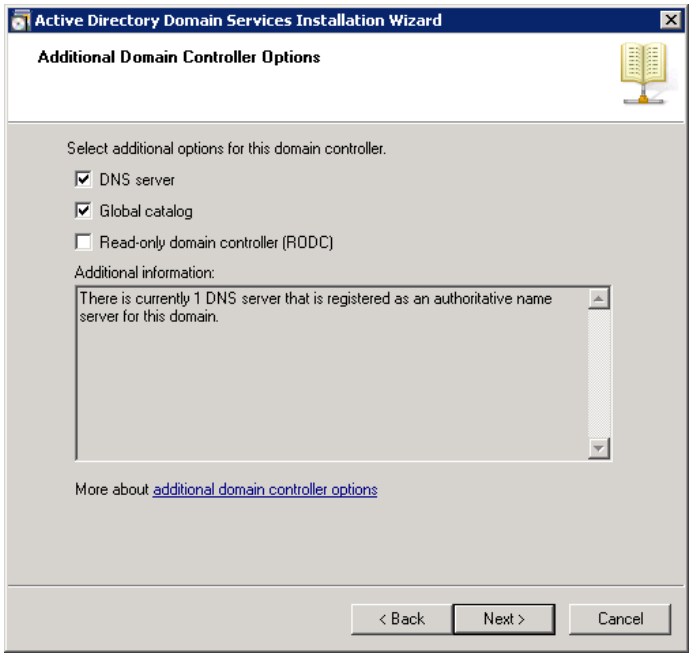
Kuvio 29. Domainin valinta.

Domainin löydyttyä valitaan vielä Site, joita on tässä asennuksessa vain yksi (kuvio 30). Mahdollisten sivukonttoreiden tapauksessa Sitejä löytyisi lisää, jolloin asennettava palvelin voisi toimia jonkin muun Siten valvojana.



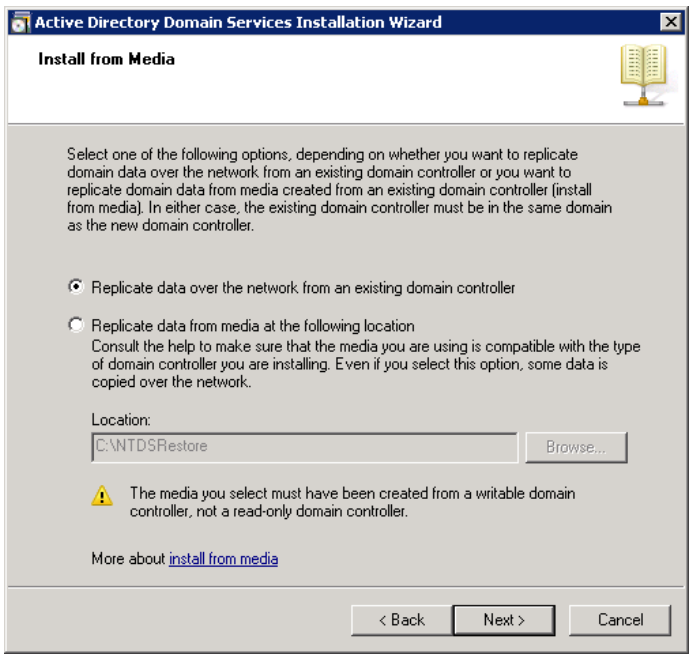
Kuvio 30. AD-alueen valinta.

Lisäpalveluvalinnassa valitaan vielä tavalliset palvelut, joita Active Directory hyödyntää, kuten toissijainen DNS ja Global Catalog (kuvio 31). DNS täytyy vielä erikseen määrittää toissijaiseksi ja tarpeelliset domainit määritellä.



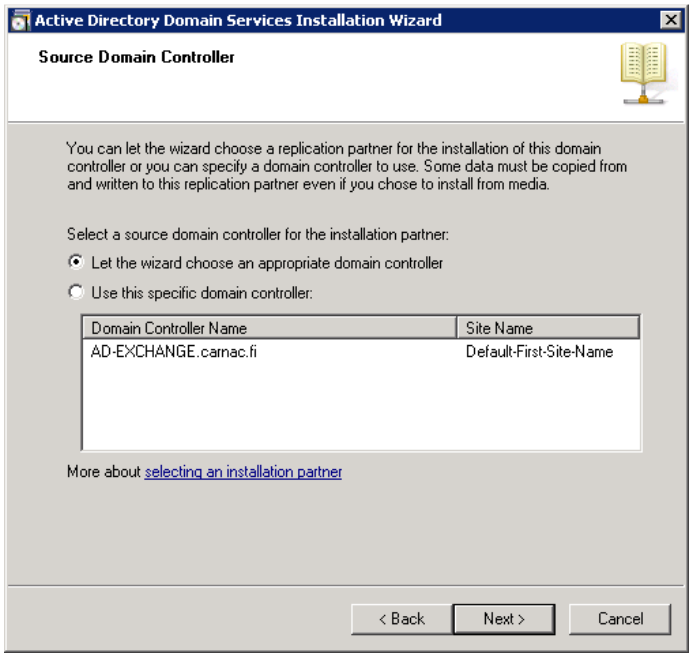
Kuvio 31. Lisäpalveluiden valinta.

Replikaatio valitaan toimimaan suorana hakuna ensisijaiselta palvelimelta, jolloin ei tarvita välivaiheita (kuvio 32). Toinen mahdollisuus on käyttää väliaikaisvarastoa, johon ensisijainen palvelin kopioi tietonsa. Tästä varastosta tiedot haetaan väliajoin. Tällaisesta menettelystä on hyötyä, jos toissijaisia palvelimia on monta, jolloin liikenteen määrä vähenee. Toinen voi olla palvelinten vaikeus yhdistää toisiinsa.



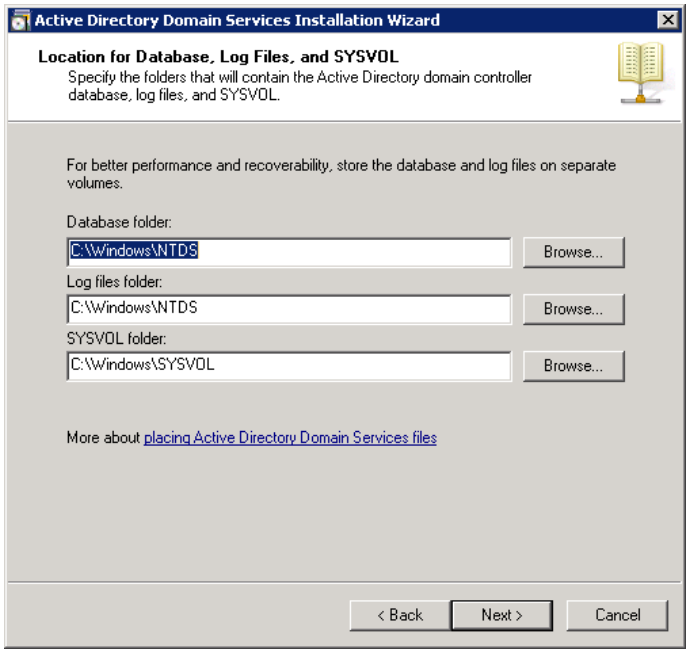
Kuvio 32. Replikaation toimintatavan valinta.

Seuraavaksi valitaan replikoitava kumppanipalvelin. Velho ehdottaa yhdistettävän palvelimen, mutta on myös mahdollista valita jokin muu kuin ensisijainen palvelin (kuvio 33).



Kuvio 33. Replikoitavan palvelimen valinta.

Viimeinen ikkuna varmistaa tallennettavien tietokantojen ja lokitiedostojen kansioiden polun (kuvio 34). Nämä voivat olla periaatteessa missä vain, mutta oletuskansiot palvelimen omalla levyllä ovat yleensä nopein ja varmin paikka.



Kuvio 34. Tietokantojen varastointi.

Asennuksen jälkeen palvelin täytyy vielä käynnistää uudelleen, jolloin kone liittyy domainiin ja ottaa käyttöön toissijaisen Domain Controllerin roolin. Palvelin on nyt asennettu, eikä lisäkonfiguraatioita tarvita. Uusi palvelin replikoi tiedot tästä lähtien automaattisesti, mikäli verkkovirheitä ei esiinny. [18.]

4 Exchange

4.1 Esittely

Exchange Server 2010 on Microsoftin viestintäratkaisun peruskomponentti, jonka päätehtävänä on keskitetty sähköpostipalveluiden ja kalenteriominaisuuksien tarjoaminen yritystason vakaudella ja saatavuudella. Usein pienyritys turvautuu ulkopuolisen palveluntarjoajan sähköpostiratkaisuihin, mutta tässä tapauksessa yhtiöllä on useita asiakkaita, jotka haluavat ostaa sähköpostipalvelunsa meiltä, jolloin Exchange on siihen kaikin puolin paras ratkaisu. Muitakin samankaltaisia kehittyneitä sähköpostipalveluratkaisuita olisi, mutta Exchange tarjoaa saumattoman

yhteensopivuuden Outlookin kanssa, joka on yrityskäytössä hyvin yleinen sähköpostiasiakasohjelma.

Exchange Server 2010:n alustan käyttöjärjestelmävaatimukset ovat kiitettävän väljät:

- forestin toiminnallinen taso vähintään Windows Server 2003
- schemalle vähintään Windows Server 2003 SP1
- itse asennus vähintään Windows Server 2008.

Tämä siis mahdollistaa toissijaisen varmistavan Exchange-palvelun asentamisen suoraan olemassaolevaan varapalvelimeen ilman käyttöjärjestelmän päivitystä (nykyinen versio on Windows Server 2008). [3, luku 1, s. 3.]

4.1.1 Yhtiölle tarpeelliset ominaisuudet

Palvelimelle keskitetyt sähköpostilaatikot. Ennen Exchange-projektia yhtiön työntekijät ovat joutuneet pitämään jokaisella työasemalla, kannettavalla tietokoneella ja mobiililaitteella erillistä sähköpostilaatikkoa, johon postit imuroitiin yhtiön POP3-sähköpostipalvelimelta. Jos lähetetystä sähköpostista täytyi saada kopio muualle, täytyi se lähettää kopiona itselleen. Myös arkistointi täytyi hoitaa jokaiselta työasemalta erikseen. Näin syntyi hirvittävä määrä ylimääräistä työtä. Exchangen myötä postilaatikot synkronoidaan samaan tilaan, jolloin mistä tahansa omaa tiliä katsottaessa näkee saman tilanteen.

Kalenteri. Vaikka yhtiöllä on käytössään itse valmistamat kalenterisovellukset, on todennäköistä, että Exchange mahdollistaa vielä helpomman tavan jakaa kalenterimerkintöjä yhtiön sisällä ja asiakkailleen. Vaikka edellinen kalenterisovellus on täysin toimiva asiakastöiden ja tapaamisten organisointiin, siirtyminen Exchangeen vähentäisi erilaisten palveluiden määrää ja toisi toiminnot yhteen paikkaan.

Postien arkistointi. Yhtiössä on jokainen sähköposti arkistoitu yhtiön perustamisesta saakka, eli vuodesta 1996. Arkistosta luonnollisestikin paisuu mittava järkäle, jota ei ole mitenkään järkevää säilyttää työasemilla. Exchangen avulla postit voidaan jatkossa arkistoida erillisille arkistopalvelimille ja tietokantoihin ilman manuaalisia toimenpiteitä.

Asiakaspostit. Yhtiö ylläpitää useiden organisaatioiden työhön tai projekteihin tarkoitettuja sähköpostilaatikoita. Sähköpostin vastaanotto on ollut suhteellisen hidasta ja turvatonta, eikä lähettäminen ole onnistunut salattuna, joten uuden järjestelmän tuomat mahdollisuudet ovat tähän verrattuna mittavat.

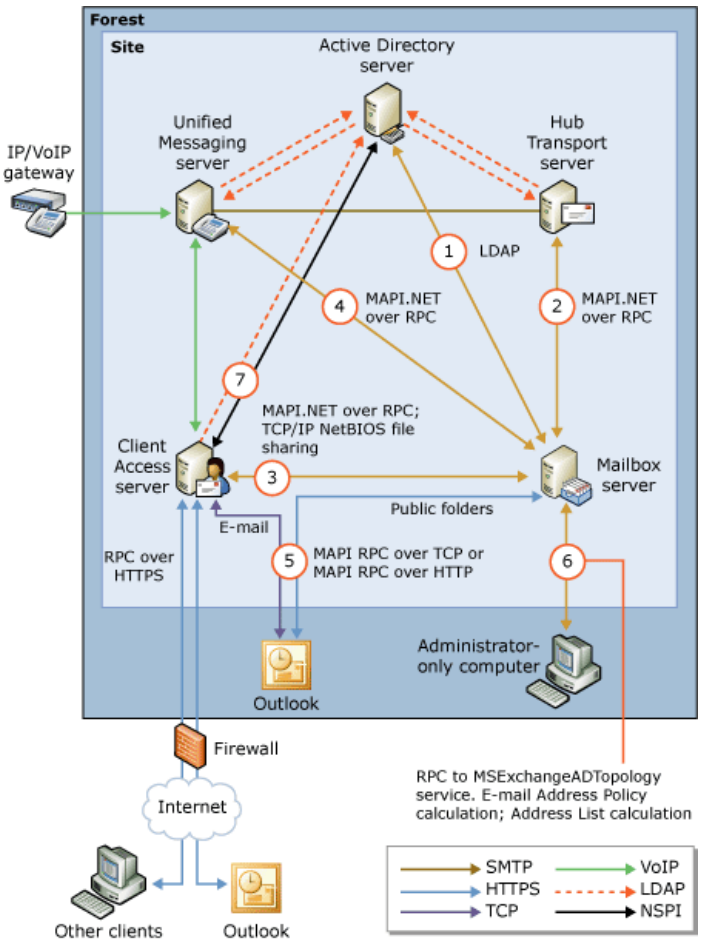
Suodattimet. Vaikka entisessäkin järjestelmässä oli roskapostisuodattimia, ne piti päivittää käsin, eikä sähköpostitietojaan levittäville asiakkaille voitu tarjota tarpeeksi hyviä keinoja kontrolloida roskapostia. Uudessa järjestelmässä tämä käy automaattisesti ja suodattimien muokkaus käy helposti ja yksilöllisesti.

Internet-selaintuki. Webmailin käyttö on aina ollut suosittua ja Exchangen avulla saadaan käyttöön entistä laajemmat toiminnot ja lisää yhteensopivuutta entistä monimutkaisemmille selaintoiminnoille. Yhtiöllä on myös runsaasti Mac-käyttäjiä asiakkaina.

Automaattiset varoitukset. Exchange voi hälyttää esiintyvistä ongelmista, kuten sähköpostilaatikon täyttymisestä, vuotavasta roskapostisuodattimesta, väärin menneestä lähetyksestä tai systeemin virheistä. Tämä helpottaa huomattavasti asiakkaiden ilmoittamien vikojen paikantamisessa.

4.1.2 Roolit

Exchange Server on hajautettu useisiin rooleihin, jotka tarjoavat tietyn osa-alueen sähköpostipalveluja. Hajautetun mallin tarkoitus on tarjota organisaatiolle mahdollisuus lisätä tiettyä roolia edustavia palvelimia tarpeen mukaan lähes rajoituksetta (kuvio 35). Runsaasti asiakaspostilaatikoita tarjoava yritys voisi tarvita usean Mailbox- ja Edge Transport -palvelimen, mutta vain yhden Hub Transport- ja yhden Client Access -palvelimen. [6, 2, s.22-25.]



Kuvio 35. Kaaviokuva Exchange-roolien välisistä suhteista ja protokollista, joilla ne keskustelevat keskenään.

Mailbox-roolin tehtävä on tarjota kiintolevytila käyttäjien postilaatikoille ja julkisesti jaetuille kansioille. Muita tälle roolille kuuluvia tehtäviä ovat sähköpostin arkistointi, sähköpostiosoitteiden sallitun kirjoitustavan laskeminen, käyttäjien osoiteluetteloiden ylläpito ja sähköpostien haku. [15.]

Client Access -rooli tarjoaa sähköpostin hakuprotokollat POP3 ja IMAP4, Outlook Web App:n, eli Internet-selaimen kautta käytettävän sähköpostipalvelun, sekä Exchange ActiveSync:n, eli mobiililaitteen synkronoinnin. Outlookin asiakasohjelmille tarjotaan kaksi palvelua: Availability, eli palveluiden automaattisen paikantamisen, sekä Autodiscovery, joka noutaa palvelimelta profiiliasetukset. Jälkimmäinen toimii myös joillain mobiililaitteilla.

Hub Transport hoitaa sähköpostin kuljetuksen organisaation sisällä, sekä huolehtii säädettyjen kuljetussääntöjen toteutumisesta. Tämä palvelu myös lähettää Internetiin

tarkoitetun sähköpostin palvelulle, joka hoitaa varsinaisen kommunikaation organisaation ja Internetin välillä. Välittäjäpalvelu voi olla SMTP-palvelin, Internet-palveluntarjoajan välityspalvelin tai Exchange-organisaatioon asennettu Edge Transport -palvelin.

Unified Messaging -rooli tuo mahdollisuuden liittää Exchange-palvelu organisaation olemassaolevaan Unified Messaging -palveluun, eli IP-verkon päällä toimivaan puhelinverkkoon. Tämä mahdollistaa postilaatikkotyypin, johon soittamalla voi kuunnella sähköpostit ja ääniviestit.

Edge Transport on niin sanottu ulkopuolinen rooli, joka ei suoraan kuulu Exchangen palvelinorganisaatioon, vaan on organisaation verkon ulkoreunalla tai DMZ-verkossa toimiva välityspalvelin. Sen tarkoituksena on välittää liikennettä Internetin ja organisaation välillä tarjoten mahdollisuuden pitää varsinainen Exchange-verkko kokonaan piilossa Internetistä. Tämä vähentää huomattavasti mahdollisuuksia Internetistä tuleviin hyökkäyksiin. Palvelun muihin ominaisuuksiin kuuluu sähköpostisuodattimia ja virustorjuntaohjelmia, sekä sähköpostin välityssääntöjen kontrollointi. Rooli on myös ainoa, jolla ei ole yhteyttä Active Directoryyn.

Tämän projektin Exchange-organisaatioon otetaan mukaan Mailbox, Hub Transport ja Client Access. Unified Messaging on yhtiölle turha, sillä minkäänlaista IP-verkon yli tapahtuvaa puhelinpalvelua ei ennestään ole. Harvoin pienyrityksissä muutenkaan tarvitaan tämäntyyppisiä palveluita. Myös Edge Transport -rooli jää pois, sillä se asennettaisiin oikeaoppisesti erilliseen DMZ-verkkoon, jollaista ei yhtiössä ole tarjolla. Muutenkin palvelun käyttöaste ei ole laaja tai raskas, joten erillinen välityspalvelin saattaisi helposti osoittautua turhaksi. Viestien välityksen ulkomaailmaan hoitaa tässä tapauksessa Client Access -rooli.

4.1.3 Send-Connector

Sähköpostien välitys onnistuu mainiosti domainin sisällä ilman erillisiä säätöjä, mutta Internetiin päin välitettävä sähköposti täytyy ohjata SMTP-palvelun kautta. Send Connectorilla, eli sähköpostin lähetyskomponentilla, on kaksi mahdollista käyttötapaa. Ensimmäinen on välitystietojen haku DNS:n MX-tietueesta, jolloin järjestelmä tietää, minne lähettää postia. Toinen tapa on käyttää ns. smart hostia, eli ulkopuolisen

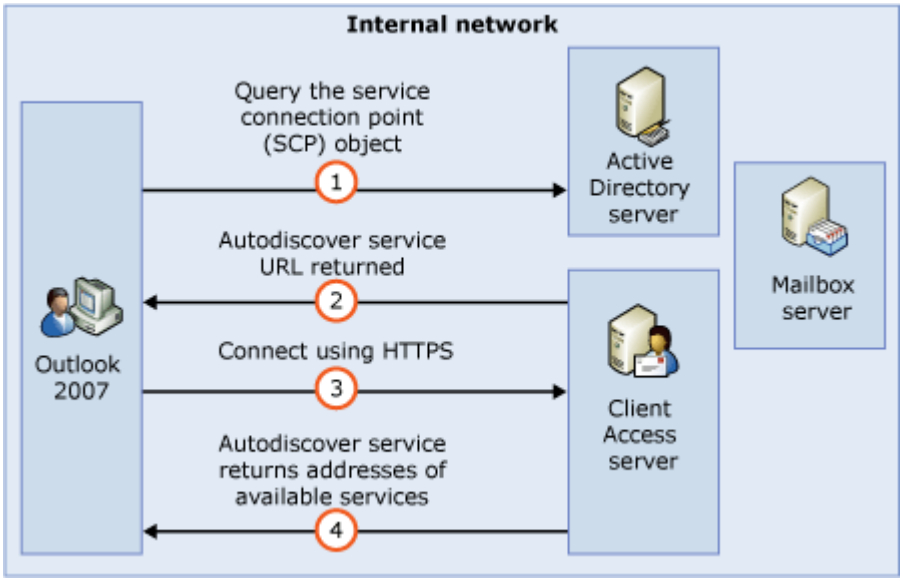
palveluntarjoajan SMTP-palvelinta, joka hoitaa välityksen. Tässä projektissa käytetään ensimmäistä käyttötapaa, sillä yhtiöllä on kaksi hyvin toimivaa DNS-palvelinta. Send Connector asennetaan alempana Exchangen asennuskappaleessa. [3, luku 5, s. 227.]

4.1.4 Forefront Security

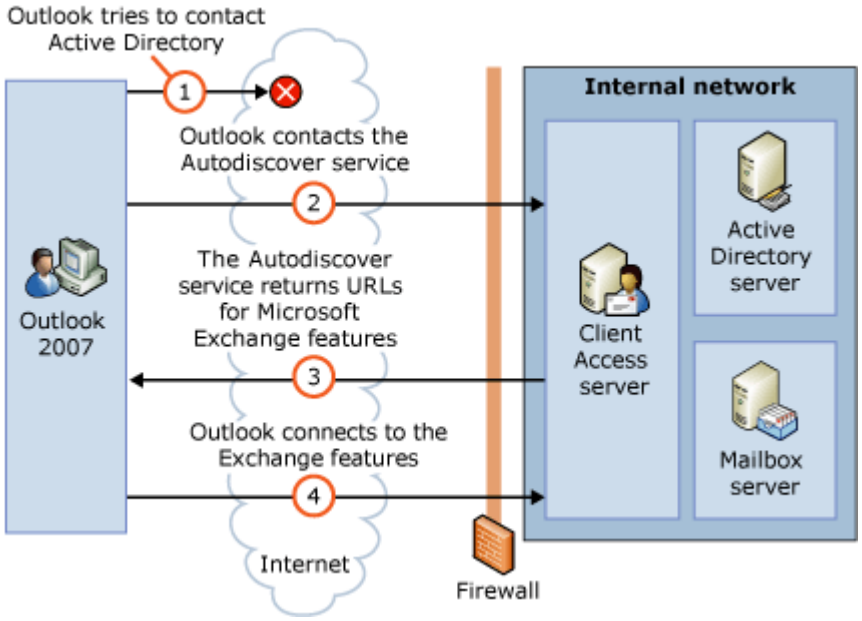
Forefront Security on Exchangeen integroitavissa oleva virustorjuntaohjelmisto. Se ei varsinaisesti ole Microsoftin oma virustorjuntasovellus vaan käyttää rinnakkain useita eri valmistajien moottoreita. Forefront Security osaa myös roskapostisuodatuksen ja siihen voidaan määrittää runsaasti erilaisia avainsana- ja tiedostosuodattimia. Forefront Securityn lisenssin voi ostaa monella eri tavalla, kuten monien eri Exchangen lisenssityyppien mukana. Monet näistä ovat Enterprise-lisenssejä, jotka ovat saatavilla vain erillisen sopimuksen kautta. Tähän projektiin Forefront Securitya ei oteta tässä vaiheessa mukaan juuri lisensoinnin vuoksi. Ohjelmisto saattaa myös kuormittaa systeemiä turhan paljon. Jos tulevaisuudessa roskapostia tulee läpi liikaa tai Forefront Security vaikuttaisi järkevältä lisäykseltä, voidaan se hankkia. [3, luku 7, s. 316.]

4.1.5 Autodiscover

Exchangen Autodiscover-palvelu helpottaa huomattavasti Outlook-sähköpostiohjelman käyttöönottoa hakemalla sähköpostitili- ja palvelintiedot automaattisesti Exchange-palvelimelta pelkän sähköpostiosoitteen ja salasanan avulla. Palvelu toimii Outlook 2007:stä eteenpäin, ja tuki on lisätty myös Windows Mobileen 6.1:stä alkaen. Hakutilanteessa Autodiscover ottaa ensin yhteyden Active Directory -palveluun ja etsii oikean henkilön, jonka jälkeen käyttäjäkysely toimitetaan Exchangeen, josta IIS:n (Internet Information Service, web-sivupalvelu) virtuaalikansiona toimiva Autodiscovery lähettää tiedot takaisin käyttäjälle (kuviot 36-37). Outlook päivittää tiedot automaattisesti tasaisin väliajoin, jotta ne myös pysyvät ajan tasalla. Autodiscover käyttää liikennöintiin DNS-palvelua, joten siellä täytyy tässä tapauksessa olla A-tietue autodiscover.carnac.fi. [3, luku10, s.457.]



Kuvio 36. Autodiscoveryn yhteystapa sisäverkossa



Kuvio 37. Autodiscoveryn yhteystapa ulkoverkosta sisäverkkoon

4.2 Asennuksen valmistelu

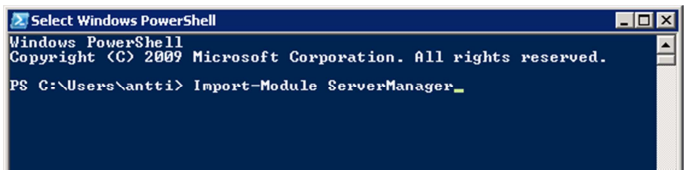
Ennen asennusta täytyy tarkastella erilaisia komponentteja ja päivityksiä, joita Exchange tarvitsee toimiakseen täydellisesti. Kaikkia paketteja ei siis toimiteta asennuslevyn mukana. Exchange on myös huono raportoimaan tarkasti havaituista virheistä, kuten perinteisesti muutkin Microsoftin ohjelmistot. Nämä toimenpiteet auttavat ehkäisemään tulevia ongelmia.

Ensimmäinen tehtävä on asentaa pakolliset käyttöjärjestelmän päivitykset. Nämä toimitetaan Windows Updaten kautta, mutta eivät asennu yleensä automaattisesti. Tarvittavien päivitysten Microsoft Knowledge Base -koodit ovat:

- 979099, Active Directory Rights Management Services -päivitys joka vähentää kaatuilua
- 979744, .NET Framework 2.0 -pohjaiset sovellukset kaatuilevat ilman tätä
- 983440, ASP.NET -koneita varten
- 977020, Web-palvelun vakauspäivitys.

Palvelimelle, johon asennetaan Hub Transport- tai Mailbox-roolit, tarvitaan Microsoft Filter Pack, jonka tehtävä on mahdollistaa tiettyjen Exchangen käyttämien tiedostoformaattien sisältöjä. Koska tässä työssä asennetaan kaikki roolit samaan palvelimeen, tulee tämä vaihe myös tehdä nyt. [7.]

Windowsin ominaisuuksia voidaan tavallisesti lisätä ja poistaa ohjauspaneelista, mutta kaikkia, varsinkaan palvelinominaisuuksia ei sieltä löydä. Myös suuren ominaisuusmäärän asentaminen käsin on työlästä ja hidasta. Tässä auttaa Windowsin PowerShell, eli skriptiajoihin tarkoitettu komentotulkki. PowerShell löytyy oletuksena pikakäynnistyspalkista. Se täytyy käynnistää ylennetyssä moodissa, eli järjestelmänvalvojan oikeuksilla, jotta komponenttien asennus onnistuisi. Jokaisella ominaisuuksien asennuskerralla täytyy siihen ensin tuoda ServerManager -moduuli komennolla Import-Module ServerManager (kuvio 38). [9.]



Kuvio 38. PowerShell-komento, jolla komponenttien asennukseen tarvittavat komennot aktivoidaan.

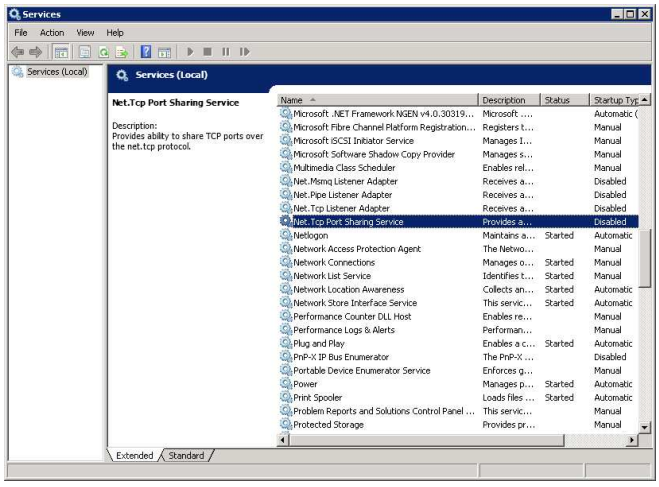
Komennon jälkeen järjestelmä vastaanottaa asennuskäskyjä komennolla Add-WindowsFeature. Microsoftin Technetin sivulta löytyvät valmiit komennot jokaista

roolikombinaatiota varten. Palvelimeen asennetaan peruskokoonpano, (Client Access, Hub Transport ja Mailbox) jolloin käytetään komentorivinä ensimmäistä vaihtoehtoa:

```
Add-WindowsFeature NET-Framework,RSAT-ADDS,Web-Server,Web-Basic-
Auth,Web-Windows-Auth,Web-Metabase,Web-Net-Ext,Web-Lgcy-Mgmt-
Console,WAS-Process-Model,RSAT-Web-Server,Web-ISAPI-Ext,Web-Digest-
Auth,Web-Dyn-Compression,NET-HTTP-Activation,RPC-Over-HTTP-Proxy -Restart
```

Tämä komento asentaa joukon erilaisia palveluita, joista osa on kuitenkin jo asennettu. Asennuksien päätteeksi palvelin käynnistetään automaattisesti uudelleen. Käynnistyksen jälkeen voi tarkistaa esiasennuksen onnistumisen Server Managerista, jonka Features-listaan on ilmestynyt suuri joukko erilaisia komponentteja. [8.]

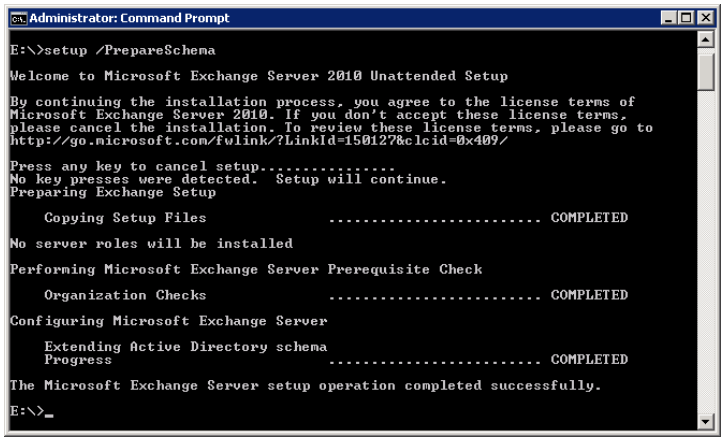
Seuraavaksi täytyy käynnistää Exchangen käyttämä käyttöjärjestelmän sisäänrakennettu palvelu Net. Tcp Port Sharing Service (kuvio 39). Avataan Start-valikon Administrative tools, jossa Services -paneelista kyseinen palvelu löytyy. Palvelu on oletuksena disabled-tilassa, joten se täytyy käynnistää ja muuttaa käynnistyväksi automaattisesti palvelimen käynnistyksen yhteydessä. [3, luku 3, s. 142.]



Kuvio 39. Net. TCP Port Sharing Servicen määrittäminen käynnistettäväksi automaattisesti Windowsin mukana.

Käynnistyksen jälkeen täytyy varmistua siitä, että käyttäjätiliin, jolla on kirjauduttu sisään Windowsiin, on määritetty oikeusryhmä Schema Admins tai Enterprise Admins. Ilman tätä Exchangen asennusohjelmalla ei ole oikeutta tehdä tarvittavia muutoksia Active Directoryn schemaan. Ohje, jolla oikeuksia muutetaan, löytyy tämän työn Active Directory -osasta. Oikeuksien muutosten jälkeen täytyy kirjautua ulos, jotta muutokset tulisivat voimaan.

Viimeinen tarvittava asia on Active Directoryn scheman valmistelu. Schema on tietokanta asetuksista ja niiden arvoluetteloista. Scheman valmistelu ei ole nimestään huolimatta iso operaatio, sillä tässä työssä tarvitaan ainoastaan asennuslevyltä asennettava oletus-schema. Scheman asennus aloitetaan ylennetyn komentokehotteen asennuslevyn kansiosta komennolla setup /PrepareSchema (kuvio 40). Tämän valmistuttua voidaan siirtyä varsinaiseen asennukseen. [11.]



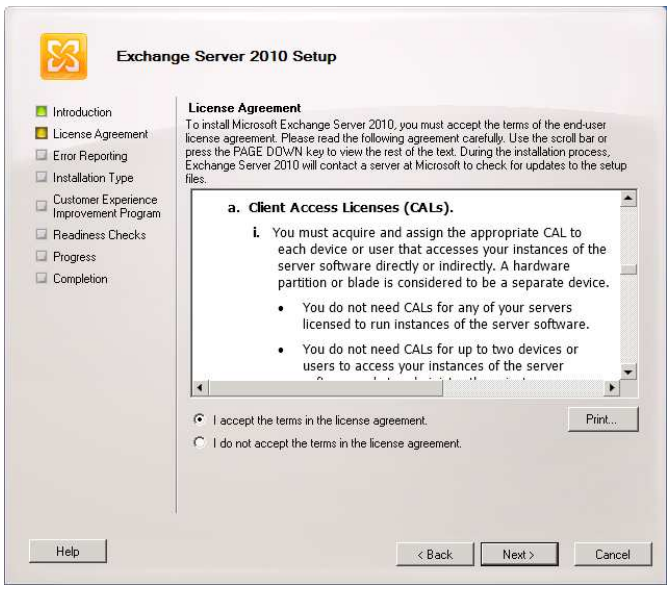
Kuvio 40. Scheman valmistelu komentokehotteessa järjestelmänvalvojan käyttöoikeuksilla.

4.3 Asennus

Kun esiasennus on kokonaisuudessaan tehty, voi varsinaisen Exchangen asennuksen aloittaa asennuslevyn Setup-sovelluksella. Kuten asennusikkuna ilmoittaa, kaksi ensimmäistä vaihetta on jo tehty. Siirrytään vaiheeseen 3, kielen valinta. Vaihtoehtoina on asentaa kaikki tuetut kielet erillisestä kielipaketista, mutta sellaisen puutteessa valitaan oletuskieli asennuslevyltä. Vaiheessa 4 asennusohjelma kopioi kaiken tarvittavan ohjelmiston koneelle. Kun kopiointi on valmis, aukeaa asennusvelho.

4.3.1 Lisenssitiedot

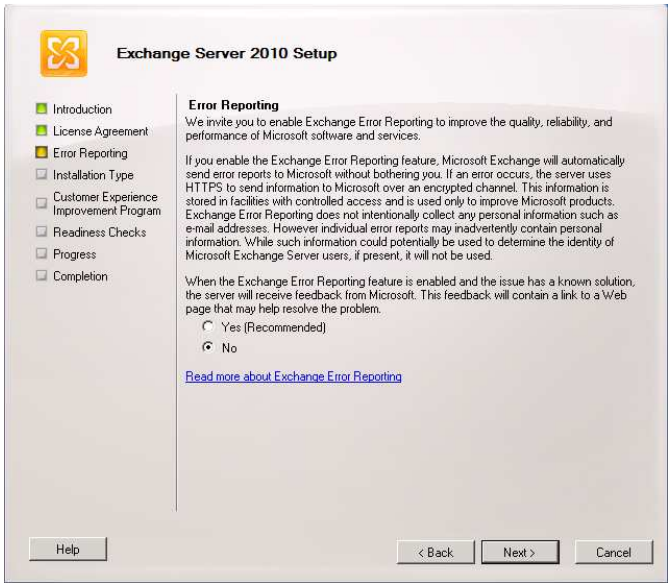
Lisenssitietojen lukeminen voi olla puuduttavaa, mutta varsinkin tässä tapauksessa aukeaa hyvin tärkeää tietoa esimerkiksi myöhemmin kaupallisessa käytössä olevan Exchange-palvelimen laillisista käyttötavoista Microsoftin Client Access License -järjestelmän puitteissa (kuvio 41). On hyvä tietää seikkoja, kuten asiakaskäyttäjät eivät tarvitse lisenssejä, jos Active Directoryn ei tarvitse autentikoida heitä.



Kuvio 41. Lisenssiehtojen selvitys.

4.3.2 Virheiden raportointi

Mikäli asetus laitetaan päälle, annetaan Microsoftille lupa saada automaattisesti tiedot sattuneesta virheestä. Tässä kokoonpanossa ominaisuus jätetään aktivoimatta (kuvio 42).



Kuvio 42. Virheiden raportoinnin määritys.

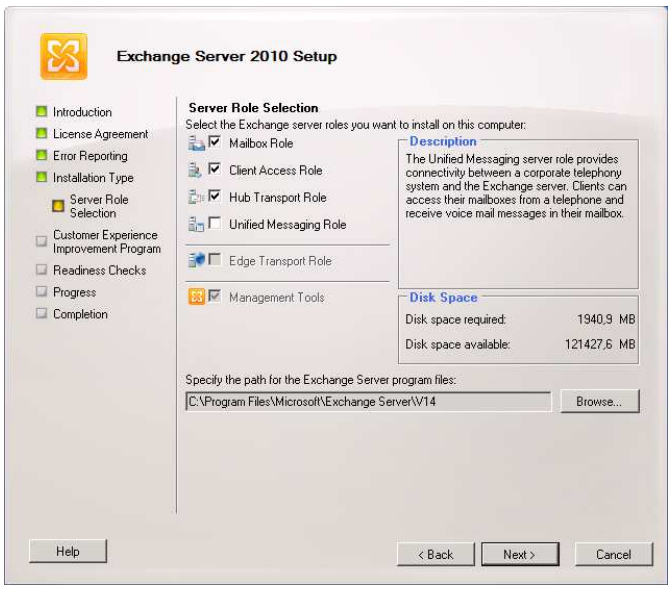
4.3.3 Asennustyyppi

Exchangen voi asentaa oletuskokoonpanona tai erikseen määriteltävänä pakettina. Harvoin mitään ohjelmistoa asennetaan palvelinkäyttöön edes tarkistamatta asennettavia komponentteja, joten tässäkin tapauksessa valitaan Custom Exchange Server Installation (kuvio 43). Asennuspolun perässä on kummallinen kansio V14, minkä voi poistaa, jos arvostaa selkeyttä hakemistopuissa. Joskus harvoin keskeneräisissä ohjelmistoissa tai niihin liitettävillä komponenteilla voi olla ongelmia, jos asennus ei olekaan sen oletetussa polussa. Kaiken varalta pidetään tässä asennuksessa polku oletuksena.

Kuvio 43. Asennustyypin valinta itsemääriteltäväksi asennukseksi.

4.3.4 Palvelimen roolien valinta

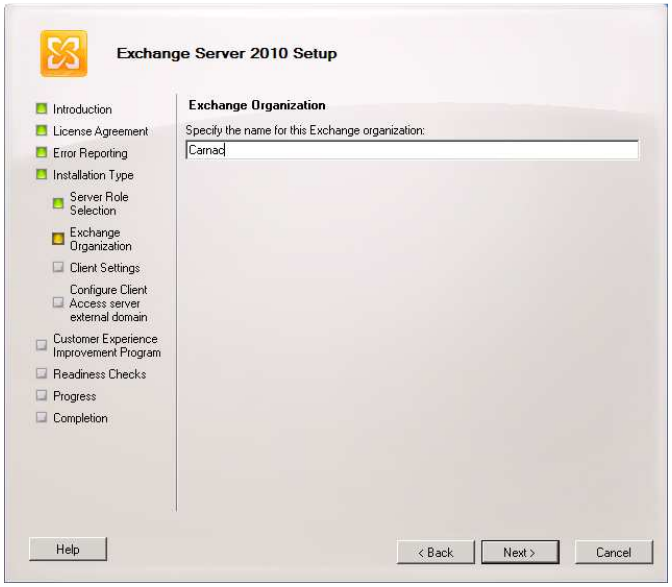
Tarkennetun asennuksen valinnoissa voi itse valita asennettavat komponentit (kuvio 44). Mailbox ja Client Access ovat itsestäänselvyyksiä jo nimensä perusteella. Hub Transport tarjoaa viestien reititystä Active Directory -alueen sisällä ja mahdollisesti roskaposti- ja virussuodattimia, joten se valitaan myös. Unified Messaging jää valitsematta, sillä yhtiö ei käytä IP-puhelimia tai muitakaan yhteensopivia järjestelmiä.



Kuvio 44. Roolien valinta.

4.3.5 Exchange-organisaation määritys

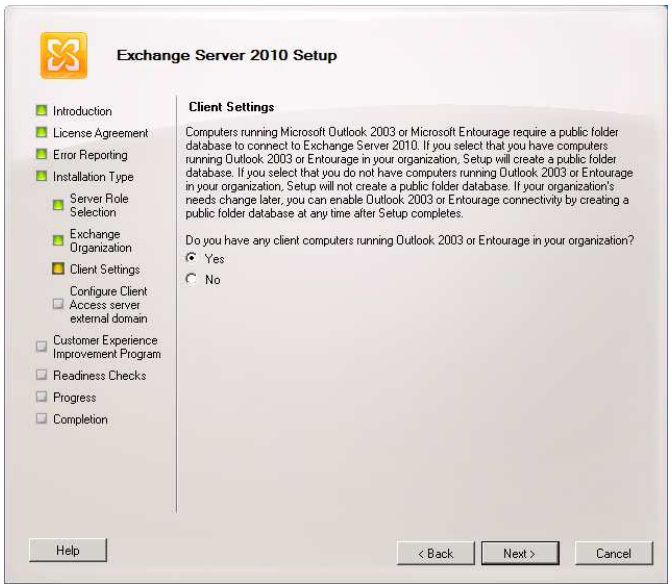
Organisaation nimeksi tulee Carnac (kuvio 45). Isommissa yrityksissä tähän saattaisi tulla osaston nimikin, jos Exchange-palvelimia on useita.



Kuvio 45. Exchange-organisaation nimen määritys.

4.3.6 Asiakasasetukset

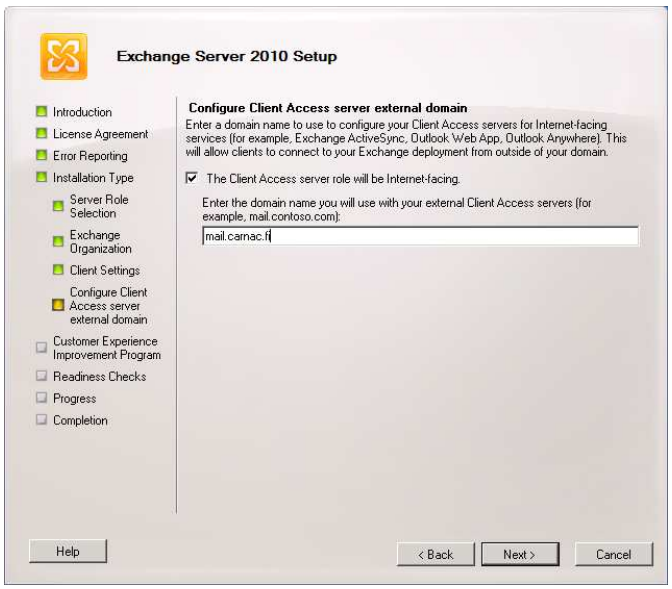
Yhtiön sisällä käytetään Outlook-versiota 2007, mutta asiakkaillamme saattaa olla vanhempia versioita. Myöhemmän konfiguroinnin vähentämiseksi valitaan Outlook 2003 -yhteensopivuustila jo nyt (kuvio 46).



Kuvio 46. Outlook 2003 -yhteensopivuustilan määritys.

4.3.7 Asiakkaan yhteydenottokäytännöt

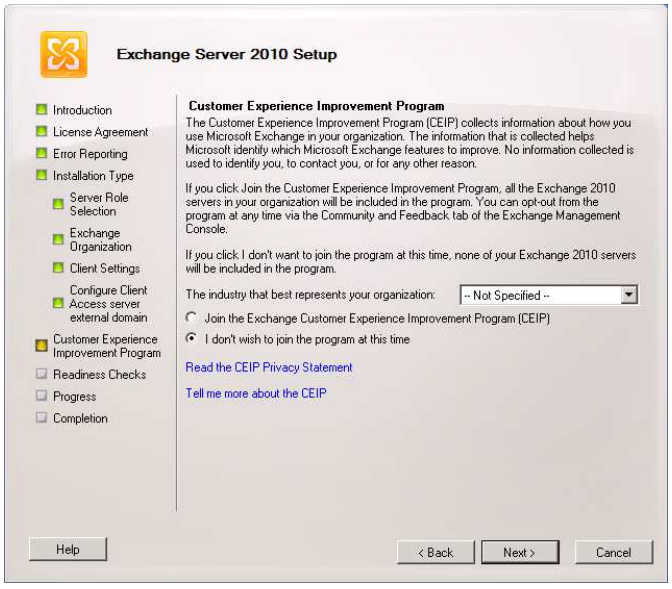
Jos Exchange-palvelimeen tulee voida yhdistää organisaation ulkopuolelta erilaisilla palveluilla, kuten Outlook Web App:lla, täytyy tämä kohta täyttää. Koska asiakaspostilaatikoiden ylläpito on oleellinen osa tätä projektia, tämä ominaisuus otetaan käyttöön. Aladomainin nimeksi tulee mail.carnac.fi, jolloin varsinainen palvelu on nimeltään mail (kuvio 47). Tämä tieto täytyy myöhemmin huomioida DNS-palvelussa.



Kuvio 47. Asiakasyhteyksille varattu Internetiin päin näkyvä osoite.

4.3.8 Käyttöraporttien lähetys Microsoftille

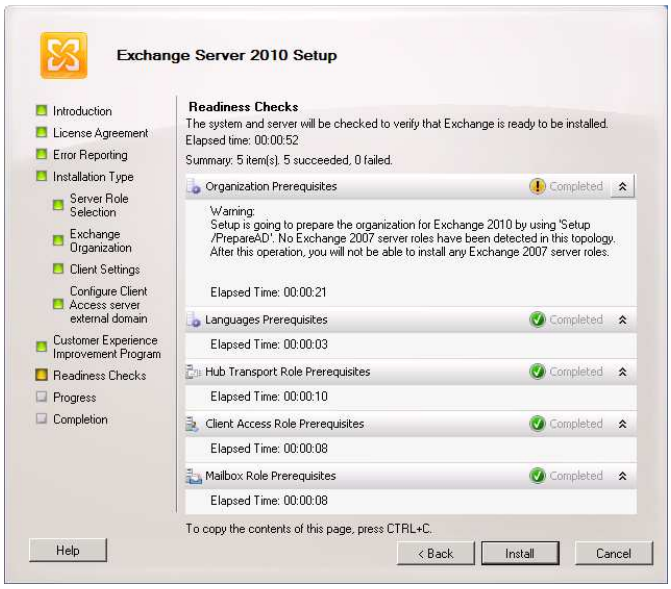
Henkilökohtaisesti en pidä ajatuksesta liittyä minkäänlaisiin tiedonkeruuohjelmiin, jotka keräävät ainakin väitetysti tunnistamatonta tilastotietoa ja lähettävät tiedot kehittäjäyhtiöön ellei syy ole jollain tavalla erityisen tärkeä. Tässä projektissa ei liitytä tähän ohjelmaan (kuvio 48).



Kuvio 48. Microsoftin seurantaohjelmaan liittyminen.

4.3.9 Valmiuden tarkistus

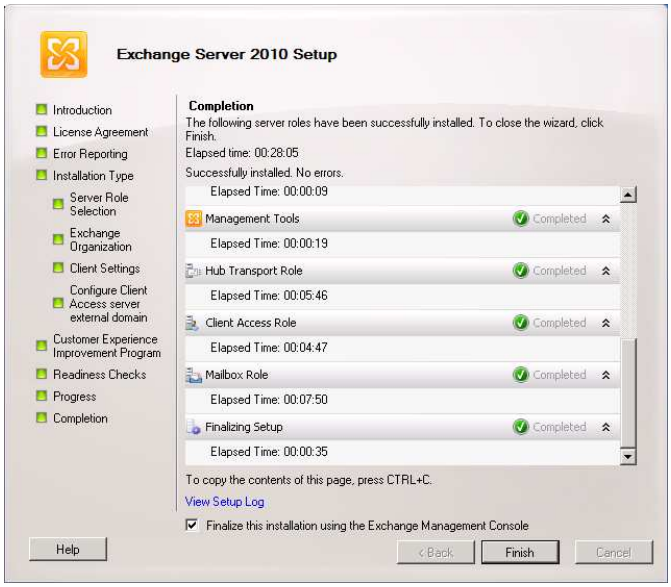
Tämä vaihe tarkistaa järjestelmän, jotta kaikki tarvittavat esiasennuksen toimenpiteet on tehty (kuvio 49). Tässä vaiheessa viimeistään ilmoitetaan, jos jotain on unohtunut. Kuvassa näkyvä virheilmoitus kertoo asennuksen suorittavan seuraavaksi komennon Setup /PrepareAD. Komennon voisi syöttää myös käsin ennen asennusta, mutta asennusohjelma tekee sen kätevästi, joten siitä ei ole erityistä hyötyä.



Kuvio 49. Asennusvalmiuden tarkistus.

4.3.10 Asennuksen valmistuminen

Asennus kesti tässä tapauksessa noin puoli tuntia ajan painottuen lähinnä roolien asennukseen. Yhteenvetoikkunasta nähdään mahdollisesti tapahtuneet virheet, joita ei tässä tullut (kuvio 50). Rastimalla kohdan Finalize this installation using the Exchange Management Console päästään heti katsomaan, mitä asennus sai aikaan. [16.]

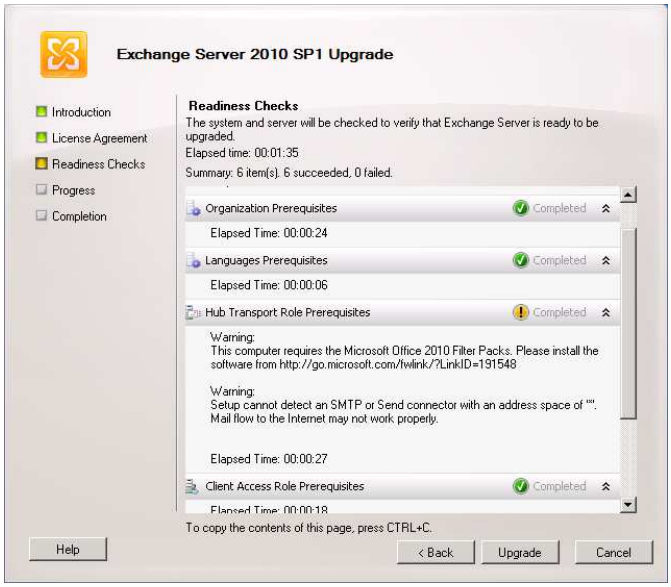


Kuvio 50. Raportti asennuksen valmistumisesta.

4.4 Asennuksen jälkeiset toimenpiteet

4.4.1 Service Pack 1

Exchange Serverille on julkaistu Service Pack 1, joka kannattaa ladata ja asentaa. Päivitys tarjoaa korjauksia ja muutaman uuden ominaisuuden mukaan lukien selainpohjaisen kommunikaation uudistuksia. Service Packin asennuksen kohdassa Readiness Checks käy ilmi, että päivitys tarvitsee uuden Office 2010 filter packin sekä SMTP-liitännäisen. Vaikka puutteet eivät estä päivityksen asennusta, kannattaa tällaiset yleensä asentaa kuitenkin etukäteen, jotta toiminta olisi mahdollisimman sujuvaa jälkeenpäin. Send Connector, eli sähköpostin lähetin, konfiguroidaan myöhemmin Exchangen muun konfiguroinnin yhteydessä.

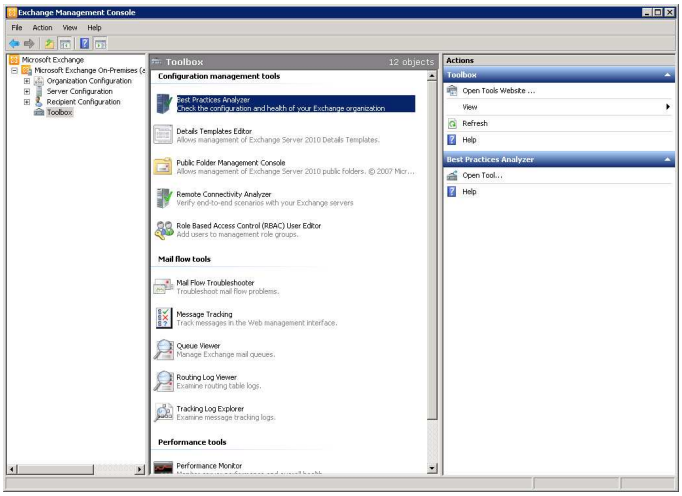


Kuvio 51. Exchangen päivityspaketin asennus.

Haetaan Filter Pack osoitteesta http://go.microsoft.com/fwlink/?LinkID=191548 ja asennetaan se. Asennuksen jälkeen suoritetaan Service Packin asennus uudelleen. Tällä kertaa ainoastaan Send Connectorista tulee varoitus (kuvio 51).

4.4.2 Exchange Management Console

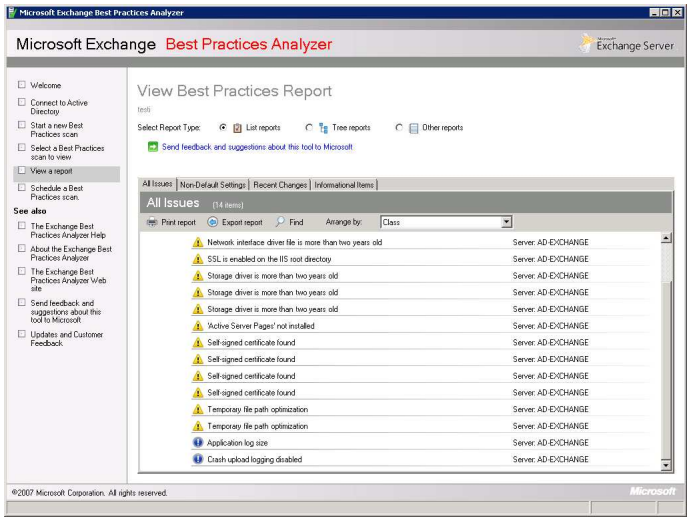
Exchangen konfigurointi aloitetaan Exchange Management Consolesta, jonka kuvake on automaattisesti sijoitettu Start-valikkoon. Management Consolen ainoan luodun Forestin puun alimman valinnan Toolboxin sisältä löytyy Best Practices Analyzer (kuvio 52). Tämä työkalu tarkistaa järjestelmän ja Exchangen asennuksen tietoja ja kertoo mahdollisista virheistä ja parannusehdotuksista.



Kuvio 52. Best Practices Analyzer, eli työkalu Exchangen optimaalisen toiminnan varmistamiseen.

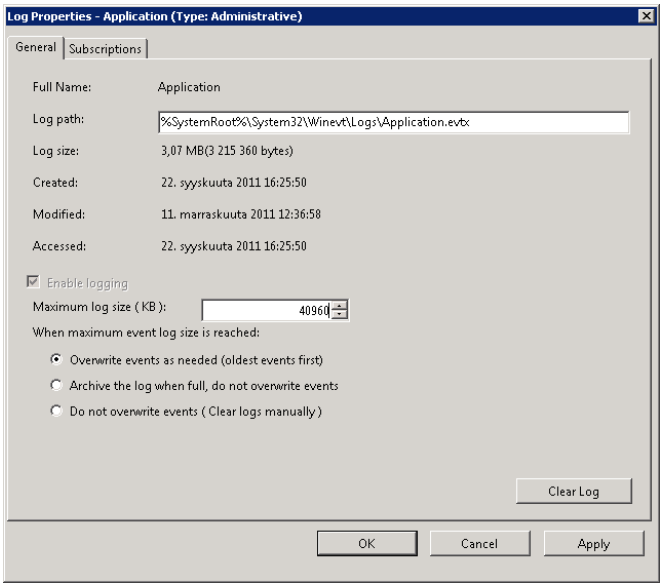
4.4.3 Best Practices Analyzer

Työkalun Health Scanin jälkeen löytyi kuvan osoittamat virheet ja huomautukset (kuvio 53). Monet huomautukset koskevat vanhoja ajureita, jotka kuitenkin ovat valmistajan mukaan viimeisimmät. Varoitus SSL:n löytymisestä IIS:n juuresta tarkoittaa sitä, että mahdolliset muut Client Access Serverit eivät toimi tämän kokoonpanon kanssa. Tälle virheelle ei tarvitse tehdä mitään, sillä juuri konfiguroitava palvelin pysyy toistaiseksi ainoana asiakaspalvelimena. Toinen huomattava varoitus on, että Active Server Pages eli ASP puuttuu järjestelmästä. Ainoa ongelma tähän liittyen on käyttäjän mahdollisuus vaihtaa oma salasanansa ennen web-liittymään pääsyä, eli jos salasana on vanhentunut tai se halutaan vaihtaa ennen kirjautumista. Tämä tulee olemaan tärkeä ominaisuus, joten ASP täytyy asentaa, vaikkei yhtiö sitä muuhun käytäkään. Ohje ASP:n asentamiseen löytyy lähdeluettelosta. [13.]



Kuvio 53. Best Practices Analyzerin ajon tulos. Monet laiteajurit ovat vanhentuneet.

Seuraavat neljä virheilmoitusta liittyvät palvelimen käyttämään itse kirjoitettuun sertifikaattiin. Minkäänlaista oikeaa sertifikaattia ei ole tässä vaiheessa asennettu. Yhtiö omistaa oikeita sertifikaatteja, joita voitaisiin ennen pitkää käyttää, mutta tähän projektiin niitä ei vielä oteta käyttöön. Väliaikaistiedostojen polku on tällä hetkellä samalla levyosiolla kuin varsinainen Exchange-palvelu, joten systeemi varoittaa mahdollisista hitauksista käytössä tämän takia. Tätä ei kannata tässä vaiheessa muuttaa, sillä järjestelmän keskimääräinen kuormitus tuskin tulee olemaan kovin suuri ajoittaisia mahdollisia piikkejä lukuun ottamatta. Tämä varmistetaan vielä lopuksi testausosiossa. Viimeinen muutettava asia on lokin koko, joka on oletuksena 20 Mt, mutta Exchangea käyttävässä palvelimessa sen suositellaan olevan 40 Mt tai enemmän. Muutetaan koko siis 40 Mt:uun Event Viewerin asetuksista (kuvio 54). Koska kaikki oleellinen on korjattu, voidaan siirtyä seuraavaan kohtaan.



Kuvio 54. Lokin enimmäiskoon muuttaminen.

4.5 Konfigurointi

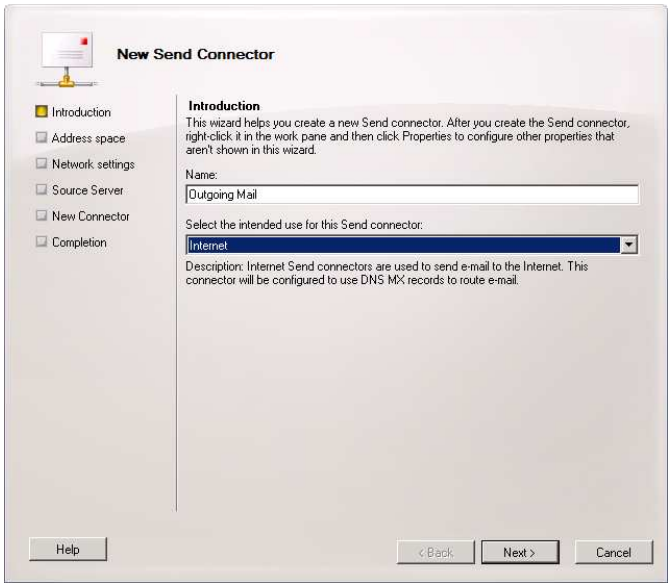
Perusasetuksia on runsaasti, kuten lähtevä posti (Send Connector), saapuva posti, sallitut domainit, sähköpostilaatikot ja niiden yhdistäminen Active Directoryyn. Komponentit voi käydä läpi missä järjestyksessä tahansa, mutta tässä noudatetaan edellä mainittua listaa.

Päätyökaluna Exchangen konfiguroinnissa toimii Exchange Management Console, jonka kuvake lisätään käynnistä-valikkoon automaattisesti asennuksen jälkeen. Konsolin logiikka toimii listaamalla alkunäkymään kaikki havaitut Exchange-palvelimet, joihin otetaan yhteys ennen säätöjen muokkausta. Jokaisella palvelinnäkymällä on neljä asetuspuuta: Organization Configuration, josta määritellään Exchange-organisaatioon, eli päädomainin hallitseman Exchange-palvelukokonaisuuteen, liittyvät asetukset. Server Configurationista määritellään palvelimen toimintaan liittyvät asetukset. Recipient Configurationin alta löytyy vastaanottajien tiedot, kuten postilaatikot ja jakelulistat. Toolboxista löytyy monenlaisia diagnosointi-, virheenkorjaus ja tilastotyökaluja. [14.]

4.5.1 Lähtevä posti

Send Connector tai SMTP-connector on välityskomponentti, jolla ohjataan verkon ulkopuolelle tarkoitettu posti seuraavaan reitittävään postipalvelimeen. Ilman Send Connectoria posti ei reitity organisaation ulkopuolelle. Vanhemmissa Exchange Serverin versioissa täytyi asentaa erillinen SMTP-palvelin tätä toimintoa varten, mutta uusimmassa versiossa roolin hoitaa Hub Transport.

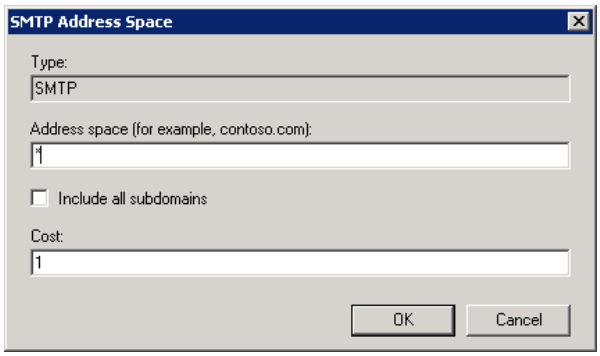
Yhdistetään Send Connector paikalliseen palvelimeen klikkaamalla Exchange Management Consolessa Microsoft Exchange On-Premises -juurta. Jonkin aikaa kestävän latauksen jälkeen avataan Organization Configurationin alta löytyvä Hub Transport. Send Connectors -välilehden alta löytyy tyhjä lista, johon lisätään lähetyskomponentti oikeanpuoleisen paneelin New Send Connector -nappulalla. Aukeava dialogi kysyy kuvaavaa nimeä ja käyttötarkoitusta sekä ilmoittaa, että tästä asennusvelhosta ei löydy kaikkia asetuksia, vaan osa säädetään vasta asennuksen jälkeen (kuvio 55). [12.]



Kuvio 55. Uuden Send Connectorin luonti.

Address spacen nappula Add lisää verkkoalueen, johon tämä Send Connector lähettää postia. Tarkoitus on käyttää tätä connectoria kaikkeen postiin. Siksi kirjoitetaan kenttään tähti, eli mikä tahansa osoite (kuvio 56). Seuraavalla sivulla valitaan lähetystapa, tässä tapauksessa käytetään oman DNS:n MX-tietueita osoitteiden löytämiseksi. Toinen vaihtoehto olisi välityspalvelin, mutta sellaiselle ei ole tarvetta.

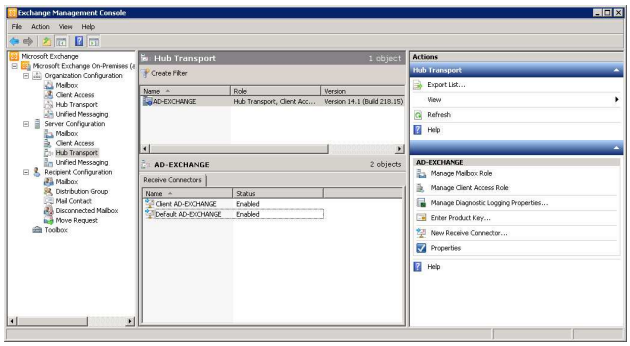
Seuraavan sivun Source Serveriksi valitaan ainoa listalla oleva, eli juuri asennettu Hub Transport -komponentti. Enää tarvitsee vain hyväksyä uusi lähetin, jolloin se luodaan.



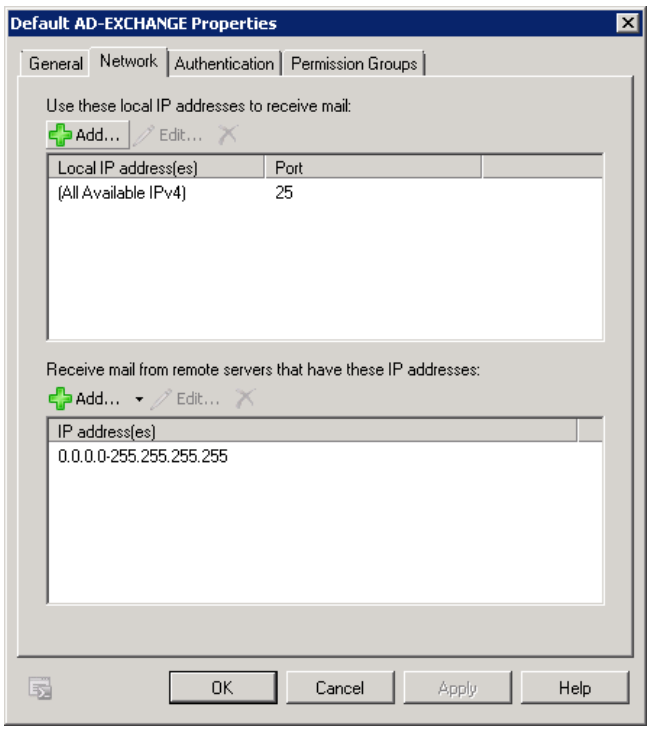
Kuvio 56. Lähetysosoiteavaruudeksi määritetään tähti, jolloin tämä komponentti reitittää kaiken ulkomaailmaan lähtevän postin.

4.5.2 Saapuva posti

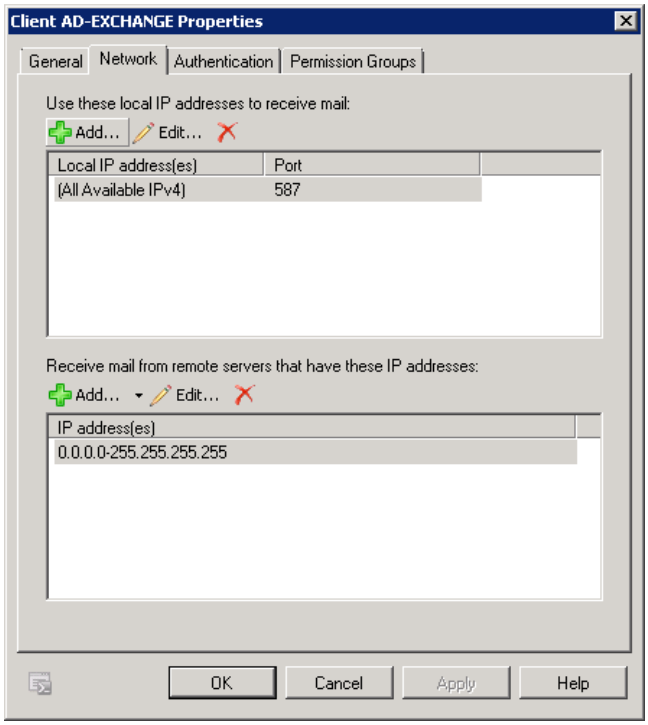
Internetistä saapuva posti torjutaan oletuksena, joten se täytyy sallia. Exchange Management Consolen Server Configurationin Hub Transport -ikkunassa näkyy alemmassa listassa kaksi Receive Connectoria, eli sähköpostia vastaanottavaa komponenttia (kuvio 57). Näiden ero on se, että Default on Exchangen sisäinen välitysyhteys, joka vastaanottaa postia ja lähettää sen Exchange Serverille porttiin 25, joka on salaamaton (kuvio 58). Client taas on käyttäjille tarkoitettu yhteys, joka lähettää postit porttiin 587, joka on salattu TLS:lla (kuvio 59). Kumpikaan välittäjä ei hyväksy postia anonyymeistä lähteistä eli Internetistä. Emme halua ollenkaan salaamatonta postia, joten konfiguroidaan Client Connector, eli salatun yhteyden välittäjä, hyväksymään Internetistä tulleet postit. [3, luku 14, s. 650.]



Kuvio 57. Receive Connectorien listaus Exchange Management Consolessa.



Kuvio 58. Default Connectorin verkkoasetukset.

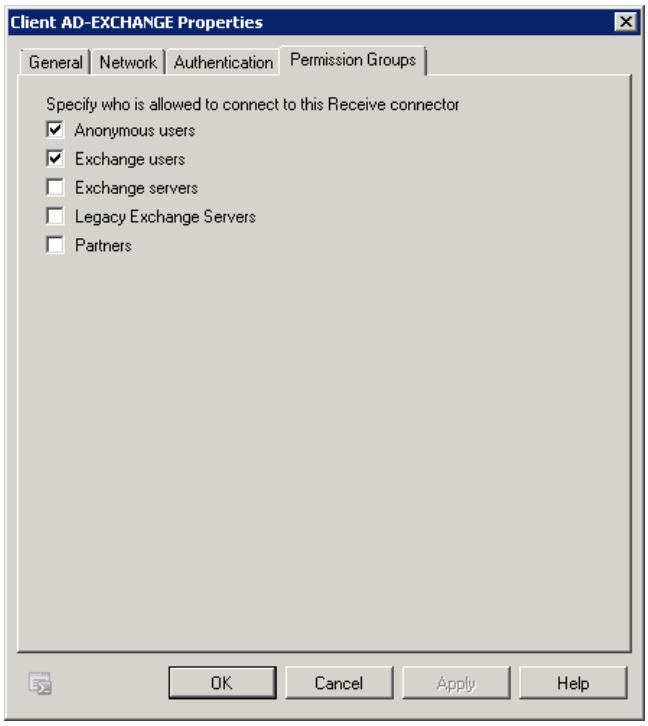


Kuvio 59. Client Connectorin verkkoasetukset.

Default Connectorin osoite on ad-exchange.carnac.fi, eli postipalvelimen NetBios-osoite. Tällä osoitteella Exchange kommunikoi eri komponenttien välillä. Client Connectorille asennuksessa määritelty osoite on mail.carnac.fi, joka on tarkoitettu

asiakkaita varten. Tähän osoitteeseen otetaan yhteys, kun halutaan lähettää tai vastaanottaa sähköpostia tämän Exchange-palvelun avulla.

Client Connectorin asetuksia pääsee muuttamaan klikkaamalla oikealla hiiren napilla valintaa Properties. Välilehdellä Permission Groups on käyttöoikeudet tälle connectorille. Valituiksi jäävät Anonymous users ja Exchange users (kuvio 60). Nyt postin jakelun pitäisi toimia salattuna.



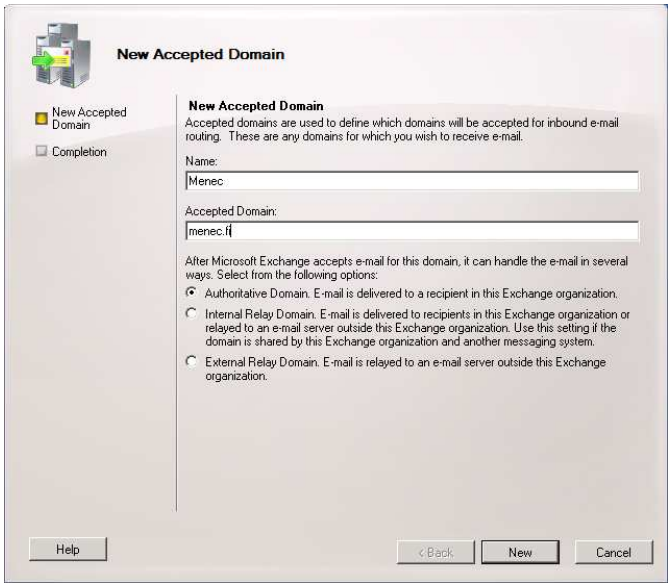
Kuvio 60. Client Connectorin käyttöoikeusasetukset.

POP3- ja IMAP -palvelut eivät ole automaattisesti päällä vaan ne täytyy erikseen aktivoida. MAPI-liikenne Outlookilla ja OWA:lla toimivat ilman näitäkin, mutta kolmannen osapuolen sähköpostiohjelmat eivät MAPIa tue. POP3 ja IMAP aktivoidaan Windowsin Service- eli palveluvalikosta nimellä Microsoft Exchange POP3 ja IMAP. Palvelut ovat manuaalisessa tilassa, eli ne eivät käynnisty Windowsin mukana, vaan ne täytyy erikseen käynnistää. On siis tarpeellista määrittää ne automaattiseen tilaan.

4.5.3 Sallitut domainit

Exchangen täytyy tietää, mihin domaineihin voi ottaa vastaan postia. Tämä asetus määritellään Exchange Management Consolen Organization Configurationin Hub

Transport -valinnasta, eli samasta paikasta kuin Send Connector. Nappulalla New Accepted Domain aukeaa ikkuna, johon voi määrittää domainin kuvaavan nimen ja varsinaisen domainin nimen (kuvio 61). Päädomain, eli carnac.fi, on jo olemassa, joten voidaan jatkaa lisäämään kaikki asiakasdomainit. Esimerkkikuvan domain on menec.fi, eli Carnacin omistama aputoiminimi. Muita domaineja ei esitellä, vaikkakin ne luodaan. Kaikista domaineista tehdään Authoritative Domaineja, sillä tämä palvelin, tai Exchange-organisaatio, ohjaa kaikkia domaineja. [3, luku 15, s. 696.]

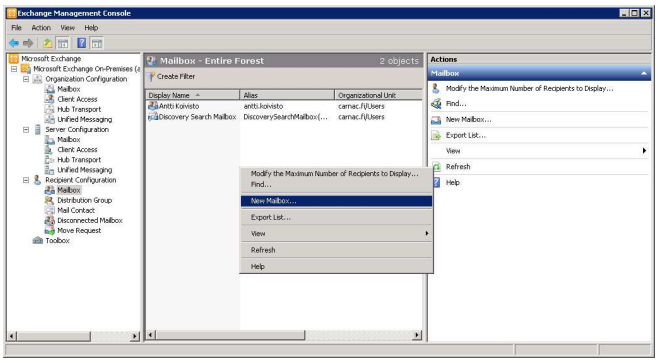


Kuvio 61. Sallitun domainin määrittäminen.

4.5.4 Postilaatikot

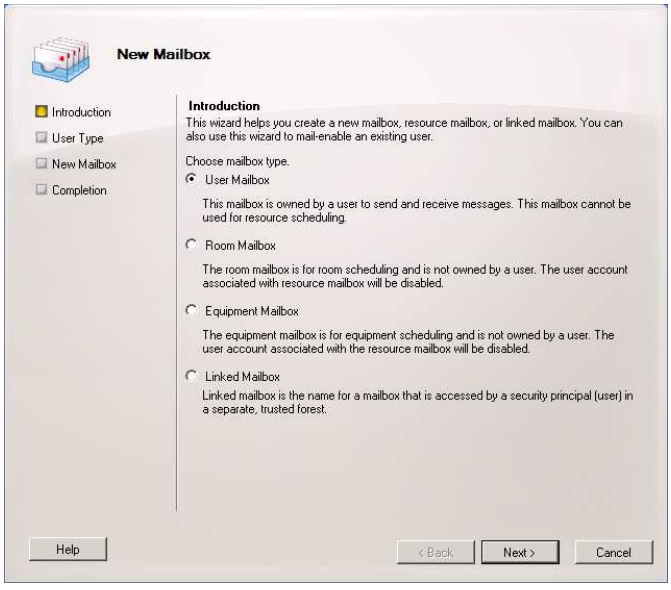
Viimeinen Exchange Management Consolella tehtävä konfiguraatio on sähköpostilaatikoiden teko. Postilaatikot on sidottu Active Directoryn käyttäjätileihin, joten jokaista postilaatikkoa varten tarvitaan käyttäjätili. Näissä tileissä määritelty tieto, kuten nimi, näkyy myös sähköpostia käyttäessä. Sähköpostilaatikoita voi muutella Recipient Configuration -puun Mailbox-ikkunalla. Oma sähköpostiosoitteeni on jo listalla, mutta osoite on väärin. AnttiKoivisto@carnac.fi, joka on luotu automaattisesti asennuksessa, täytyy muuttaa muotoon antti.koivisto@carnac.fi. Muutos onnistuu klikkaamalla objektia hiiren oikealla napilla ja valitsemalla Properties. Alias-kentässä oleva teksti on varsinainen osoite, johon lähettämällä viestit menevät oikealle käyttäjälle. Muutetaan tämä siis oikeaan muotoon. Listaan palattua klikataan tyhjään

listan alueeseen hiiren oikealla napilla ja klikataan New Mailbox. Sama valinta löytyy myös oikean paneelin Actions-listasta (kuvio 62).



Kuvio 62. Uuden sähköpostilaatikon luonti.

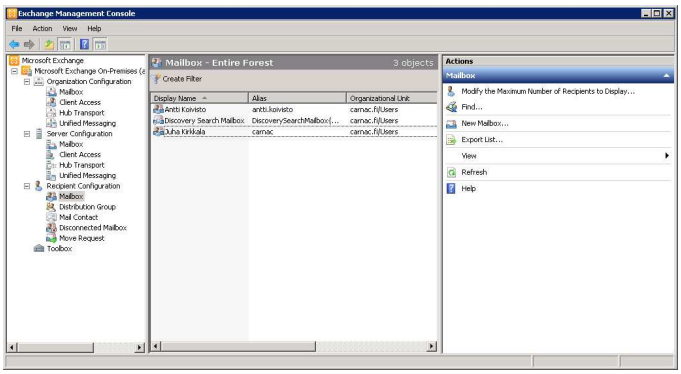
New Mailbox -velho aukeaa, ja ensimmäiseksi valitaan sähköpostilaatikon tyyppi (kuvio 63). Koska tuleva käyttäjä on ihminen, valitaan User Mailbox. Muita vaihtoehtoja ovat Room Mailbox, jolla voidaan tehdä huonevarauksia, Equipment Mailbox, jolla voidaan vastaavasti tehdä laitteistovarauksia. Näitä kahta sähköpostilaatikkotyyppiä ei sidota käyttäjiin. Nämä ovat käteviä esimerkiksi kouluissa, joihin tarvitaan tilanvarausjärjestelmä. Linked Mailbox on lähinnä järjestelmänvalvojille tarkoitettuja laatikoita, joita voi käyttää resursseille tarkoitetuissa domaineissa.



Kuvio 63. Uuden sähköpostilaatikon tyypin määritys.

Seuraavassa ikkunassa määritellään käyttäjä uudelle laatikolle. Käyttäjän voi tehdä tässä, jolloin se monistuu Active Directoryyn automaattisesti. Nyt valitaan Existing users, sillä lisättävä henkilö on jo olemassa Active Directoryssa. Velho etsii järjestelmästä käyttäjät, joista valitaan haluttu.

Sähköpostilaatikon nimeksi tulee carnac@carnac.fi, joten aliakseksi määritellään carnac. Mitään muita asetuksia ei tarvitse määrittää, sillä halutaan käyttää oletuksia. Sähköpostilaatikko on nyt luotu ja uusi laatikko on ilmestynyt listalle. Tulevaisuudessa tämä lista tulee olemaan täynnä asiakaspostilaatikoita, mutta testikäyttöön riittää vain kaksi (kuvio 64).



Kuvio 64. Luettelo olemassa olevista sähköpostilaatikoista.

4.5.5 Sertifikaatti

SSL-sertifikaatin asentaminen ei ole postipalvelun toiminnan kannalta oleellista, mutta se suojaa sähköpostiliikenteen, jolloin posteja on ulkopuolisen lähes mahdoton kaapata. Kirjautumisprosessi on oletuksena suojattu itsekirjoitetulla sertifikaatilla, joka antaa perusturvan. Tämänkin voi korvata kaupallisella sertifikaatilla, mutta se ei juuri paranna tietoturvaa.

Sertifikaatti rakennetaan omalla palvelimella, jonka jälkeen se lähetetään jollekin kaupalliselle palveluntarjoajalle hyväksyttäväksi. Palveluntarjoajan tarkastettua tiedot ja lisättyä sertifikaatin palvelimilleen se lähettää sen takaisin, jolloin oman palvelimen esiasennettu sertifikaatti täydennetään palveluntarjoajalta tulleella kopiolla. Tavalliset kaupalliset sertifikaatit ovat yleensä voimassa yhdestä viiteen vuoteen ja toimivat ainoastaan yhdellä palvelulla, kuten mail.carnac.fi. Palvelua ei voi lyhyen varmistusajan jälkeen muuttaa. Suurille yhtiöille tarkoitetut kalliit wildcard- eli domainkohtaiset

sertifikaatit käyvät mille tahansa palvelulle domainin sisällä. [2, s. 62-63. 3, luku 3, s. 111.]

Sertifikaatin asentaminen aloitetaan Exchange Management Consolen Server Configuration -puusta, jonka oikeassa työkalupaneelissa on nappula New Exchange Certificate. Sertifikaatille annetaan nimi, määritellään tavalliseksi sertifikaatiksi (ei wildcard, ellei sellaista erityisesti haluta), määritellään palvelut, joihin sertifikaattia käytetään (yksi palvelun nimi yhtä sertifikaattia kohden, tässä mail.carnac.fi on jokaisen palvelun nimi), sekä sertifikaattia käyttävän organisaation tiedot. Valmistumisvaiheessa tarkistetaan vielä yhteenvetoikkunasta, jotta nyt luotava sertifikaatti on tavallinen eikä Unified Communications -sertifikaatti.

Tässä vaiheessa tiedostoon tallennettu sertifikaatti lähetetään palveluntarjoajalle, joka päivän tai parin kuluttua lähettää tiedoston takaisin. Tämä päivitetty tiedosto syötetään samalla nappulalla kuin asennuksen aloitus, tällä kertaa nappulan nimi on Complete Pending Request. Sertifikaatin asennuksen jälkeen se määritellään palveluiden käyttöön klikkaamalla hiiren oikealla nappulalla alapaneelin sertifikaattilistasta uusinta kohdetta ja valitsemalla menusta Assign Services to Certificate. Asennusikkunassa määritellään palvelin, jonka käyttöön sertifikaatti asetetaan, sekä käytettävät palvelut. Valitaan palveluiksi IMAP, POP3, SMTP ja IIS. Unified Messaging ei ole käytössä. Asennuksen valmistuttua täytyy vielä vanha itsekirjoitettu sertifikaatti poistaa.

5 Käyttöönotto, käyttö ja suorituskyky

5.1 Laitteiston liittäminen domainiin

Käyttöönottovaiheessa yhtiöllä on vielä käytössä vanha Linux-palvelimella toimiva DNS-palvelu ohjaamassa palvelinliikennettä. Tätä palvelua ei myöskään pureta ennen kuin uusi järjestelmä toimii ehdottoman luotettavasti. Domainiin siirtyminen aloitetaan käyttötarkoitukseen sopivalla kannettavalla tietokoneella. Koneen DHCP:ltä saamat IP-tiedot ovat muuten oikein, mutta DNS-palvelimet osoittavat vanhaan järjestelmään. IP-tiedot täytyy siis käsin muuttaa vastaamaan uuden Active Directory -palvelimen osoitetta. Uuden järjestelmän toimiessa myös DHCP-palvelun tiedot päivitetään.

Työasema tai palvelin liitetään domainiin Windowsin ohjauspaneelista, jossa järjestelmäkuvake avaa järjestelmän perusnäkymän. Tietokoneen nimen ja domainin määrittävässä kohdassa näitä määrityksiä voi muuttaa. Tietokoneen nimi tulee olemaan jokin vastaava laite, jotka Active Directoryn asetusvaiheessa määriteltiin laiteluetteloon. Domain on Active Directoryn juuridomain, eli carnac.fi. Asetusten muuttamisen jälkeen tietokone täytyy käynnistää uudelleen, jonka käynnistyttyä kirjaudutaan sisään Active Directoryyn määriteltyjen käyttäjätunnusten mukaan. Domainiin kirjautumisen voi ohittaa kirjoittamalla tietokoneen paikalliset tunnukset ilman domainin nimeä. Tällä tavalla määritellään kaikki domainiin liitettävät Windows-laitteet. Muilla käyttöjärjestelmillä on omat menetelmänsä, kuitenkin säilyttäen peruslogiikan laitteen nimestä.

5.2 Sähköpostin käyttö

5.2.1 Outlook 2010

Outlook on luonnollisesti integroitavissa Exchangeen Microsoftin oman MAPI/RPC-protokollan avulla. Tämä on ylivoimaisesti helpoin tapa käyttää Exchangen tarjoamia palveluita (mikäli kallis ohjelmisto on saatavilla), sillä Outlook voi tilinluontivelhon avulla hakea kaikki asetukset Exchange-palvelimelta parilla hiiren naksautuksella tietämällä ainoastaan sähköpostiosoitteensa ja salasanansa. Palvelun huono puoli on MAPI-protokollan tietoliikenteen sitominen tietoliikenneporttiin TCP 135, joka on erityisen haavoittuvainen. Tämä käytännössä rajoittaa automaattisen asetusten haun vain VPN:n yli tapahtuviin hakuihin.

Velho aukeaa pääikkunan tiedosto-valikon tiedot-osion tiliasetukset-nappulalla. Tilitietojen kirjoittamisen jälkeen ohjelma aloittaa tietojen haun Exchange-palvelimelta. Tässä vaiheessa järjestelmä ei vielä käytä virallista sertifikaattia, joten tästä varoitetaan vielä erikseen. Tilin perustaminen tapahtuu alle minuutissa ilman teknistä osaamista. Sähköpostin vastaanottaminen ja lähettäminen onnistuu ongelmitta ja posti on perillä parissa sekunnissa.

5.2.2 Outlook Web App

Microsoft suosittelee pääasialliseen organisaation ulkopuoliseen sähköpostikäyttöön Outlook Web Appia, eli Internet-selaimelta käytettävää asiakasohjelmaa. Liikenne Web Appiin on oletuksena suojattu Exchangen omalla itsekirjoitetulla sertifikaatilla. Useimmat selaimet varoittavat tällaisista sertifikaateista väärentämisvaaran takia ennen sivulle astumista, joten käyttöliittymä ei näytä kovin ammattimaiselta. Näistä varoituksista pääsee eroon asentamalla virallisen varmentajan myöntämän sertifikaatin, joka tähän järjestelmään otetaan myöhemmin käyttöön yhtiön voimassaolevista sopimuksista.

Web App aukeaa ensimmäisellä kerralla hyvin hitaasti, johtuen ensimmäisen kirjautumisen aiheuttamista asetusmuutoksista. Sisäänpääsyn jälkeen toiminta nopeutuu huomattavasti. Käyttöliittymä on lähes sama kuin uusissa Outlookin versioissa, mikä onkin hyvä ohjelmaan tottuneille. Asetuksissa voi määritellä ja ottaa käyttöön runsaasti käteviä toimintoja, kuten poissaoloviesti, mobiiliyhdistäminen (vain Direct Push, eli Microsoftin oma teknologia Windows Mobile -puhelinten yhdistämiseksi Exchangeen), Outlookin tavallisen asiakasohjelman integrointi, palvelintietojen tarkastelu sekä järjestelmänvalvojille hallinnan lisäominaisuuksia. Järjestelmänvalvojan asetuksista voi hallita käyttäjätilejä ja ryhmiä, valvontaa, ohjauksia, lokeja, yms. Tämä mahdollistaa perusasetusten muuttamisen ilman palvelimelle kirjautumista.

5.2.3 Kolmannen osapuolen asiakasohjelmat

Testausohjelmana toimii ilmainen avoimen lähdekoodin Eudora OSE 1.0. Tarkoituksena on kokeilla sähköpostin lähetystä ja vastaanottoa ulkoverkosta salausprotokollia käyttäen, eli juuri siten, miten asiakas ohjelmaa käyttäisi. Varsinaisen sähköpostiliikenteen salaus onnistuu Exchangen itsekirjoitetulla sertifikaatilla, mutta virallisen sertifikaatin voi joko ostaa ulkopuoliselta palveluntarjoajalta tai sen voi luoda itse käyttämällä Active Directoryn Certificate Service -palvelua. Itsekirjoitettu sertifikaatti kuitenkin aiheuttaa virheilmoituksen asiakkaalle.

Uuden tilin luova velho osaa kokeilla yleisimmin käytettyjä sähköpostiasetuksia, joista se löytääkin oikeat asetukset (taulukko 6). Asetusten määrittämisen jälkeen muutama testiviesti latautuu vastaanotettujen postien kansioon osoittaen IMAP-protokollan

toimimisen. Myös testilähetys onnistuu osoittaen Exchangen Client Receive Connectorin toimimisen.

Taulukko 6. Sähköpostiohjelman tiliasetukset

Palvelimen osoite (saapuva ja lähtevä)	mail.carnac.fi
Saapuva protokolla Portti Käyttäjätietojen salaus Salattu liikenne	IMAP 993 Päällä Päällä
Lähtevä protokolla Portti Käyttäjätietojen salaus Salattu liikenne	SMTP 587 Päällä Päällä

5.2.4 Mobiililaitteet

Testattavana mobiililaitteena on Samsung Galaxy S 2 -matkapuhelin, jonka Android-alustalle löytyy muutamia ilmaisia ja maksullisia Exchange-asiakasohjelmia. Esimerkkiohjelmaksi sopii 30-päivän esittelyversiona toimiva NitroDesk Inc:n kehittämä Exchange for Android 2.x. Ohjelma tukee suoraa kommunikaatiota Exchangen kanssa ActiveSyncin, eli mobiililaitteille tarkoitetun synkronointimenetelmän avulla. Sähköpostiosoitteen ja salasanan syöttämisen jälkeen nappulalla ”try autodiscover” ohjelma löytää asetukset automaattisesti ja sähköposti on heti käyttövalmis. Ainoa haittapuoli ohjelmalla on jatkuva päälläoleminen, joka luonnollisesti kuluttaa akkua nopeammin.

5.3 Palvelinten suorituskyky ja resurssien käyttö

Palvelin, joka ajaa ensisijaista Domain Controlleria ja Exchange Serveriä, eli AD-Exchange, kuluttaa Windows Task Managerin mukaan noin 85 % kaikesta muistista. Käynnissä olevien prosessien määrä on kasvanut käyttöjärjestelmän asennuksen jälkeen kymmenillä. Active Directoryyn suoraan liittyviä palveluita on päällä vain kaksi vieden yhteensä kymmenen megatavua muistia, mutta todennäköisesti suuresta määrästä isäntäprosesseja (Host Process) ja apuprosesseja (Client Server Runtime Process, IIS Worker Process) muutama kuuluu Active Directorylle. Exchangella sen sijaan on suuri määrä prosesseja, yhteensä 25, kuluttaen noin gigatavun verran muistia. Prosessorin käyttö kuitenkin on hyvin matalaa, kiiveten välillä muutamaan prosenttiin liikenteen mukaan.

Toissijainen Domain Controller, eli Ad2, kuluttaa muistia huomattavasti vähemmän, noin 20 %. Suoraan Active Directoryyn liittyviä prosesseja ei Task Managerin listalta löydy, mutta apuprosesseja on runsaasti viitaten samanlaiseen toimintatapaan edellisen palvelimen kanssa. Tästä voidaan suoraan päätellä Exchange-palveluiden olevan erittäin muistiriippuvaisia verrattuna Active Directoryyn. Organisaation kasvaessa palvelintenkin vaatimukset kasvavat nopeasti.

Sähköpostin testilähetys samanaikaisesti kahteen eri sähköpostilaatikkoon nosti prosessorin käytön hetkeksi noin kahteenkymmeneen prosenttiin. Muistin käyttöaste ei muuttunut. Joukkopostin lähetys on toimenpide, joka todennäköisesti kuormittaa palvelinta erittäin paljon, mutta sitä tapahtuu vain harvoin. Tästä voi päätellä palvelinten resurssien riittävän hyvin pienyrityksen tarpeisiin.

6 Yhteenveto

Insinöörityön tavoitteena oli rakentaa työpaikalleni General Media Carnac Oy:lle, IT-alan pienyritykselle, kokonaisvaltainen verkonhallintaratkaisu hyödyntäen markkinoilla yleisesti käytettyjä ohjelmistoja ja standardeja. Lähtökohtana oli myös koko yhtiön asiakaskunnalle tarjottavat uudet ja monipuolisemmat yhteyskäytännöt ja sähköpostipalvelut, joiden monet tarvittavat ominaisuudet eivät ole ennen olleet mahdollisia. Näitä verkko- ja sähköpostipalveluita ovat monet asiakkaamme jo pitkän aikaa toivoneet.

Työni laajuus on hieman suurempi, mitä aluksi olin suunnitellut, mutta kaikki työssä mainitut asiat ovat joko insinöörityön tai yhtiölle jäävän dokumentaation kannalta oleellisia eikä niitä voi asiasisällön kärsimättä jättää pois. Työn suurimmaksi haasteeksi muodostuikin ehkä juuri sisällön rajoittaminen kuin sen luominen. Active Directory ja Exchange yhdessä sisältävät valtavan määrän toimintoja, joiden edes pinnallinen tarkastelu olisi ollut mahdotonta kasvattamatta työn laajuutta tuskallisen suureksi. Uskonkin, että tätä insinöörityötä voi käyttää suoraan vastaavanlaisen järjestelmän rakentamiseen hyvin suoraviivaisella tavalla harhautumatta epäoleellisiin asioihin. Myös tarkka dokumentaatio mahdollistaa järjestelmän vikatilanteiden nopeamman ratkaisemisen.

Ohjelmistojen asennusvaiheessa vaivalloisin osuus oli Exchangen yhteyspalvelujen, kuten erilaiset sähköpostin lähetys- ja vastaanottoyhdyskäytävien, konfigurointi. Myös sertifikaattien asennuksessa ongelmaksi muodostuivat palveluntarjoajan viiveet ja vanhojen sertifikaattien muutto uudelle palvelimelle. Oman haasteensa loi kahden päällekkäisen DNS-palvelun (toinen tuotantokäytössä, toinen uuden järjestelmän testaukseen) olemassaolo verkossa, sillä kumpaakaan ei voinut karsia pois eikä niitä voinut yhdistää. Selvisin työstä kuitenkin ilman tuotantokäytössä olevien palveluiden häirintää.

Olen erittäin tyytyväinen, että valitsin insinöörityöni aiheeksi juuri tämän, sillä vastaavat järjestelmät ovat niin yleisiä, että niiden hallinta on eduksi missä tahansa IT-työssä. Osa asiakkaistamme on myös ottanut samanlaisen järjestelmän käyttöön ja jotkut suunnittelevat sitä tulevaisuudessa. Asiantuntemus yhtiössä voi siis auttaa myös asiakkaidemme pyrkimyksiä.

Lähteet

1 Reimer Stan & Kezema Conan & Mulcare Mike & Wright Byron, Windows Server 2008 Active Directory Resource Kit. Microsoft Press, 2008.

2 Wesselius Jaap, Exchange 2010 A Practical Approach. Red Gate Books, 2009. ISBN 978-1-906434-31-1.

3 Stidley Joel & Jagott Siegfried, Exchange Server 2010 Best Practices. Microsoft Press, 2010.

4 Installing Active Directory on a Windows Server 2008R2. Verkkodokumentti. <http://akfash.wordpress.com/2010/01/29/installing-active-directory-on-a-windows-server-2008r2/>. Luettu 24.10.2011.

5 Active Directory Domain Services and DNS Server Migration Guide. Verkkodokumentti. <http://technet.microsoft.com/en-us/library/dd379558%28WS.10%29.aspx>. Luettu 24.10.2011.

6 Overview of Exchange 2010 Server Roles. Verkkodokumentti. <http://technet.microsoft.com/en-us/library/dd298026.aspx>. Luettu 9.11.2011.

7 2007 Office System Converter: Microsoft Filter Pack. Verkkodokumentti. <http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=20109>. Luettu 9.11.2011.

8 Use the Server Manager module for Windows PowerShell. Verkkodokumentti. <http://technet.microsoft.com/en-us/magazine/ff476071.aspx>. Luettu 9.11.2011.

9 Exchange 2010 Prerequisites. Verkkodokumentti. <http://technet.microsoft.com/en-us/library/bb691354%28EXCHG.140%29.aspx#WS08R2>. Luettu 12.9.2011.

10 How to import DNS records. Verkkodokumentti. <http://social.technet.microsoft.com/Forums/en/winserverNIS/thread/bd1c9d25-eb63-4140-b59f-0a50d1448359>. Luettu 2.11.2011.

11 Prepare Active Directory and Domains. Verkkodokumentti. <http://technet.microsoft.com/en-us/library/bb125224.aspx>. Luettu. 15.11.2011.

12 Understanding Send Connectors. Verkkodokumentti. <http://technet.microsoft.com/en-us/library/aa998662.aspx>. Luettu 17.11.2011.

13 Active Server Pages is not installed. Verkkodokumentti. <http://technet.microsoft.com/fi-fi/library/dd421840%28en-us,EXCHG.80%29.aspx>. Luettu 15.11.2011.

14 Exchange 2010 configuration. Verkkodokumentti. <http://www.servolutions.com/support/config_exchange_2010.htm>. Luettu 15.11.2011.

15 Overview of the Mailbox Server Role. Verkkodokumentti. <http://technet.microsoft.com/en-us/library/bb124699.aspx>. Luettu 16.11.2011.

16 Installing Exchange 2010 Step-by-Step. Verkkodokumentti. <http://www.enterprisenetworkingplanet.com/windows/article.php/3877601/Installing-Exchange-2010-StepbyStep.htm>. Luettu 14.11.2011.

17 Active Directory Replication Guide. Verkkodokumentti. <http://searchwindowsserver.techtarget.com/tutorial/Active-Directory-Replication-Guide>. Luettu .11.11.2011.

18 Create an additional domain controller. Verkkodokumentti. <http://technet.microsoft.com/en-us/library/cc781792%28WS.10%29.aspx>. Luettu 12.11.2011.