

Tampereen ammattikorkeakoulu  
Tietojenkäsittelyn koulutusohjelma  
Mikko Jarva

Opinnäytetyö

## **Case: Javerdel Oy:n toimialue ja Exchange**

Työn ohjaaja      Tietoverkkopalveluiden suuntautumisvaihtoehdon vastaava, lehtori  
Harri Hakonen  
Työn teettäjä      Javerdel Oy, valvojana asiakaspalvelujohtaja Jussi Haverinen  
Tampere 11/2008

Tekijä(t)	Mikko Jarva
Työn nimi	Case: Javerdel Oy:n toimialue ja Exchange
Sivumäärä	32
Valmistumisaika	Marraskuu 2008
Työn ohjaaja	Harri Hakonen
Työn teettäjä	Javerdel Oy

---

## TIIVISTELMÄ

Javerdel Oy:ssä oli käytössä Microsoft Windows Server 2003:lla toteutettu toimialue ja Exchange Server 2003 -sähköpostijärjestelmä. Nämä palvelut toimivat vanhalla palvelimella, jonka päivittäminen tuli ajankohtaiseksi. Samalla haluttiin ottaa käyttöön sähköpostipalvelimeksi uusi Exchange Server 2007 -ohjelmisto. Tehtävänä oli suunnitella, asentaa, testata ja käyttöönottaa uusi palvelin. Työ liittyi Javerdelin omien palveluiden kehittämiseen ja Exchange Server 2007:n osalta yleiseen tuotekehitykseen, sillä uudesta sähköpostijärjestelmästä haluttiin kokemuksia asiakastoteutuksia varten.

Työn aloitusvaiheessa tutustuttiin olemassa olevaan ympäristöön ja sen konfiguraatioihin sekä uusien palveluiden asennusohjeisiin. Lisäksi selvitettiin palveluiden rakennetta alan kirjallisuuteen tukeutuen. Asennus toteutettiin Microsoftin ohjeiden avulla.

Toimialuepalvelut toteutettiin Microsoftin Active Directorylla. Toimialuepalvelut tarjoavat autentikointipalvelut ja mahdollisuuden hallita keskitetysti toimialueen koneita. Toimialuepalvelut muodostavat yrityksen ylläpidolle erittäin keskeinen kokonaisuuden.

Exchange Server 2007 on Microsoftin sähköposti- ja yhteistyöpalvelu. Se tarjoaa käyttäjille sähköpostien lisäksi jaettavat kalenterit ja yhteystiedot. Exchange Server 2007:n tarkoitus on helpottaa kommunikointia ja tiedon jakamista. Exchange on palvelinkeskeinen järjestelmä, jossa kaikki tiedot säilytetään palvelimella.

Ensimmäisessä työvaiheessa asennettiin palvelimen käyttöjärjestelmä ja toimialuepalvelut. Seuraavassa vaiheessa asennettiin Exchange Server 2007, testattiin sen toimivuus, ja siirrettiin vaiheittain käyttäjien postilaatikot uuteen järjestelmään.

Työ aloitettiin syksyllä 2007 ja päätettiin kesällä 2008. Aikataulu oli huomattavasti pidempi kuin tehtävä olisi vaatinut, mutta se toteutettiin muun työn ohessa. Lisäksi käytettiin testaukseen runsaasti aikaa. Työn tuloksena saatiin otettua käyttöön uusi palvelin, joka palvelee tehokkaasti Javerdelin toimialuetta ja sähköpostin käyttäjiä.

Author(s)	Mikko Jarva
Thesis	Case: Javerdel Active Directory Services and Exchange
Pages	32
Graduation time	November 2008
Thesis Supervisor	Harri Hakonen
Co-operating Company	Javerdel

---

## ABSTRACT

The thesis focused around Javerdel, an information technology company that used Active Directory services and Exchange Server 2003 on an old Windows Server 2003. It was time to upgrade the server and at the same time the decision was made to upgrade to the new Exchange Server 2007. The task was to design, install, test and take the new server into use. The project was related to the development of Javerdel's own services, and also to general product development of the Exchange server, as knowledge and experience were needed for future customer implementations.

First I familiarized myself with the production environment and its configurations, and read installation instructions for the new platforms. I also studied the structure of programs from literature. Installations were done according to Microsoft's instructions.

Microsoft Active Directory is used to serve Javerdel's domain. The domain controllers provide authentication and the possibility to manage all the computers within the domain. Active Directory services are very important tools for administrators.

Exchange Server 2007 is Microsoft's e-mail and collaboration software. It provides e-mail services, shared calendars and contact information for the users. Exchange Server is built to ease communication and sharing information. All the data is located within the Exchange Server machine.

In the first stage, the server and domain services were installed. In the second phase Exchange Server 2007 was installed, tested and taken into use. The transition from the old server was implemented in several phases.

The project started in the autumn 2007 and finished in the summer 2008. The schedule was remarkably longer than the task required, but it was done at the same time with other projects. The testing was also executed without haste. The project's result was a new server that efficiently provides services to Javerdel's domain and e-mail users.

## Sisällysluettelo

1 Johdanto .....	5
2 Toimeksiantaja .....	7
3 Aktiivihakemistopalvelut .....	8
3.1 Yleisesti .....	8
3.2 Toimialuepalvelimien roolit .....	10
4 Microsoft Exchange Server .....	13
4.1 Yleisestä .....	13
4.2 Rakenne .....	13
4.3 Ylläpito .....	16
4.4 Käyttö .....	17
5 Palvelimen asentaminen .....	20
5.1 Valmistelu .....	20
5.2 Windowsin asennus .....	22
5.3 Toimialuepalveluiden asennus .....	23
6 Exchange Server 2007:n asennus .....	25
6.2 Testaus .....	26
6.3 Käyttöönotto .....	27
7 Kehitettävää .....	29
Lähteet .....	31

# 1 Johdanto

Aktiivihakemistopalvelut ja sähköpostit muodostavat monessa yrityksessä tietojenkäsittelyn selkärangan. Aktiivihakemistopalvelut tarjoavat tehokkaan keinon käyttäjätilien ja oikeuksien hallintaan sekä asetusten ja ohjelmistojen jakamiseen. Sähköposti on monille yrityksille elintärkeä toiminto, sillä sen avulla tehdään runsaasti liiketoimintaa. Työ käsittelee Microsoftin Active Directory -palvelua ja Microsoft Exchange Server 2007 -palvelinta.

Microsoftin aktiivihakemistopalvelut ovat laajasti käytössä, sillä niiden käyttöönotto on mahdollista kaikenkokoisissa organisaatioissa. Käyttöönottoon tarvitaan tietoverkko ja Microsoftin palvelinkäyttöjärjestelmä, esimerkiksi Windows Server 2003. Järjestelmä skaalautuu alle kymmenestä käyttäjästä kymmeneen tuhansiin käyttäjiin.

Exchange Server 2007 on Microsoftin sähköposti- ja yhteystyöpalvelin. Siinä on pyritty luomaan edellytykset tehokkaalle tiedon jakamiselle. Sähköpostitoimintojen lisäksi sillä voidaan toteuttaa jaettuja kalentereita, yhteystietoja ja julkisia kansioita.

Sain opinnäytetyön aiheen Javerdel Oy:stä (jäljempänä Javerdel), jossa suoritin harjoitteluni. Javerdelilla oli käytössä Windows Server 2003 -käyttöjärjestelmällä toteutetut toimialuepalvelut ja Exchange Server 2003:lla toimiva sähköpostiratkaisu. Nämä palvelut toimivat yhdellä palvelimella, joka toimi resurssiensa ääri rajoilla. Palvelin oli yli 5 vuotta vanha, joten päivittäminen oli hyvin ajankohtaista.

Oman toimialueen palveluiden saatavuutta ja sähköpostin toimivuutta päätettiin parantaa asentamalla toimialueelle uusi palvelin, joka toimii toisena toimialuepalvelimena ja ensisijaisena sähköpostipalvelimena. Sähköpostijärjestelmä haluttiin päivittää uuteen versioon. Exchange Server 2007:stä oli tarkoitus saada tämän projektin avulla kokemuksia myös asiakastoteutuksiin.

Sain tehtäväksi suunnitella ja toteuttaa palvelimen ja ohjelmistojen asennuksen, testauksen ja käyttöönoton. Työn ensisijainen tavoite oli päivittää Javerdelin sähköpostijärjestelmä Exchange Server 2007 -ohjelmistoon. Toisena tavoitteena oli parantaa Javerdelin toimialueen aktiivihakemiston palveluiden saatavuutta asentamalla toinen toimialuepalvelin.

## 2 Toimeksiantaja

Javerdel Oy on tietotekniikka-alan yritys, joka tarjoaa asiakkailleen kaikenlaista tietotekniikkaan liittyvää ylläpitoa. Javerdelilla työskentelee 30 henkilöä ja se toimii kahdella paikkakunnalla: pääkonttori ja konesali Helsingissä sekä sivukonttori Kajaanissa. Javerdel on perustettu 1998. (Javerdel - Yritys 2008.)

Javerdelin liikeidea on tuottaa asiakkaille IT-palveluiden ulkoistusta ja suunnittelua. Tuotevalikoimaan kuuluvat muun muassa asiakkaan tietojärjestelmien dokumentointi ja kehittäminen, laitteiden asennukset ja ylläpito, Internet-yhteyksien hankinta ja vikatilanteiden selvitys operaattoreiden kanssa, sähköpostipalvelut sekä Internet-sivujen ylläpito. Tuotevalikoimaa päivitetään jatkuvasti uusimmilla tekniikoilla. Exchange Server 2007 on tässäkin mielessä merkittävä kehityskohde.

Tavoitteena on saada täysi vastuu asiakkaan järjestelmistä, mutta myös osatoteutuksia tehdään. Perusajatuksena on antaa asiakkaalle enemmän aikaa keskittyä omaan liiketoimintaansa, kun IT-järjestelmistä ei tarvitse huolehtia. Javerdel keskittyy 50-250 työaseman ympäristöihin.

## 3 Aktiivihakemistopalvelut

### 3.1 Yleisesti

Active Directory -palvelu on Microsoftin aktiivihakemistopalvelu, joka varastoi tietoa tietoverkon objekteista. Tieto on järjestetty hierarkiseen malliin. (Active Directory Overview: 2008.) Aktiivihakemistopalvelut tarjoavat toimialueelle muun muassa autentikointipalvelut sekä mahdollisuuden määrittellä koneiden asetuksia ja jakaa ohjelmistoja Group Policy -työkalun avulla.

Microsoft toteutti toimialuepalvelut nykymallin mukaan Windows Server 2000 -palvelinversiossa. Sitä ennen Windows NT 4.0:ssa oli tehty toimialuepalvelu, johon saattoi tallentaa vain perustiedot käyttäjästä, kuten nimen, käyttäjätunnuksen ja salasanan. Kaikki tiedot sijaitsivat samassa tassa; hierarkiaa ei ollut käytettävissä. Tämä toimialuemalli oli vain turvallisuuslaajennus työryhmäympäristöihin. (Morimoto, Gardinier, Noel & Droubi 2004: 102.)

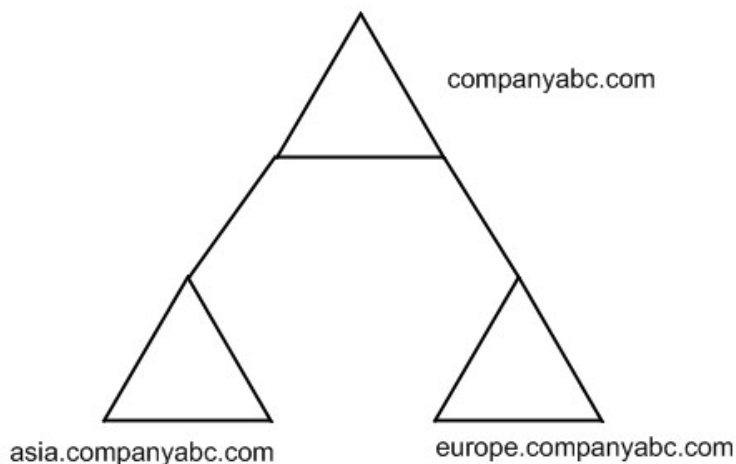
Microsoftin aktiivihakemistopalvelut perustuvat LDAP-protokollaan (Lightweight Directory Access Protocol). LDAP on IETF-järjestön (Internet Engineering Task Force) hyväksymä protokolla, joka on määritelty artikkelissa RFC-1777 (1995) (Request For Comments). Tämän protokollan mukaan tietoa voidaan lisätä ja hakea aktiivihakemistopalvelun tietokannasta.

Toimialuepalveluihin liittyen on tärkeää tuntea seuraavat käsitteet: toimialue, toimialuepuu ja metsä. Toimialue on looginen kokoelma objekteja, joita voidaan hallita keskitetysti. Objekteja ovat esimerkiksi käyttäjätunnukset, ryhmät ja toimialueeseen liitetyt tietokoneet. Toimialue luo loogisen tietoturvarajan objektiensa ympärille.

Toimialuepuu koostuu toimialueista, joilla on jaettu nimiavaruus (kuva 1). Samassa toimialuepuussa toimialueiden välillä on kaksisuuntainen luotta-



mussuhde. Luottamussuhteiden avulla toimialueen resursseja voidaan jakaa muiden toimialueiden käyttöön (Tulloch & Tulloch 2002: 1136).



Kuva 1: Toimialuepuu (Morimoto ym. 2004: 104)

Metsäksi kutsutaan loogista kokoelmaa toimialueista, jossa toimialuepuiden ylimpien tasojen välille luodaan luottamussuhde. Metsän eri toimialuepuiden nimiavaruuksien välillä ei tarvitse olla jatkuvuutta.

Group Policy on myös erittäin tärkeä toimialueen osa. Group Policyillä voidaan jakaa ohjelmistoja ja tehdä asetusten muutoksia kaikille toimialueen objekteille. Näin voidaan helposti vakioda ympäristöä ja saada säästöjä ylläpitokustannuksissa. Jokaiseen toimialueeseen tulee asennuksessa valmiiksi Default Group Policy. Tämä on merkittävä Group Policy, sillä se ajetaan aina kaikille toimialueen koneille ja sitä ei voi ottaa pois käytöstä. Onkin suositeltavaa, että Default Group Policyllä tehdään mahdollisimman vähän asetuksia.

Group Policyja voi tehdä itse lisää ja niitä voi osoittaa eri toimialueen organisaatioyksikkö-säiliöille (Organisation Unit Container). Näin eri yksiköille voidaan laittaa helposti eri asetuksia. Oletuksena Group Policyt periytyvät hierarkiassa alaspäin, mutta tämän voi organisaatioyksikkökohtaisesti estää. Jotta toimialueen tuomista eduista saisi mahdollisimman paljon irti, Group Policyjen tuntemus on välttämätöntä.

Group Policyjen kanssa tulee olla varovainen juuri samoista syistä, jotka tekevät niistä tehokkaita. Huolimattomilla asetuksilla voidaan saada merkittävää haittaa aikaan: saatetaan esimerkiksi kieltää kaikkia tunnuksia kirjautumasta toimialuepalvelimille. Tämä tarkoittaa sitä, ettei palvelimia voi ylläpitää lainkaan. Onkin tärkeää ymmärtää, mitä muutoksia on tekemässä, ja testata niitä etukäteen. Group Policyjen suunnittelu kannattaa tehdä huolella. On tärkeää huomata myös se, että kaikki Group Policyilla tehtävät muutokset hidastavat hieman koneille sisäänkirjautumista, sillä kaikki määritellyt asetukset käydään siinä vaiheessa läpi.

Toinen tärkeä seikka on se, että edestakaisia muutoksia tulee välttää. Jos esimerkiksi ensimmäisellä Group Policyllä määritellään "Tietokoneet"-organisaatioyksikön koneille Windowsin palomuri pois päältä, ja toisella Group Policyllä sen alla olevalle "Tehotyöasemat"-organisaatioyksikölle palomuri takaisin päälle, voidaan törmätä ongelmiin asetusten voimaan tulemisessa. Aina tällaista ei voi järkevästi välttää, mutta pääsääntöisesti on syytä suunnitella Group Policyt mahdollisimman yksinkertaisiksi ja suoraviivaisiksi.

### **3.2 Toimialuepalvelimien roolit**

Toimialuepalvelimilla on useita eri rooleja. Kaikki roolit asentuvat aluksi (tehtävänsä mukaan) metsän tai toimialueen ensimmäiselle toimialuepalvelimelle. Ne voidaan kuitenkin siirtää siltä pois.

Ensimmäinen rooli on Global Catalog -indeksi. Toimialueen sisällä jokaisella toimialuepalvelimella on kaikki toimialueen objektit. Jos palvelimella on Global Catalog -rooli, sillä on oman toimialueensa tietojen lisäksi suppea, vain luettavissa oleva tietokanta kaikista saman metsän toimialueiden objekteista. Objekteista on tallennettu kantaan hauissa useimmin tarvittavat objektit, jotka on määritelty schemassa (skeema, malli). Schemaa muokkaamalla voidaan Global Catalogin sisältöön lisätä tai poistaa haettavia attribuutteja. Global Catalog -palvelimia voi olla useita. (Domain Controller Roles: 2008.)

Schema on malli, joka määrittelee kaikkien aktiivihakemistopalvelun objektien ja attribuuttien muodon. Tätä mallia hoitaa Schema Master -rooli. Schema Master -rooli huolehtii siitä, että objekteihin tehdyt muutokset replikoidaan kaikille toimialuepalvelimille. (Corbin 2004: 94, 359.) Metsässä voi olla vain yksi Schema Master -palvelin, jotta vältetään replikoinnin päällekkäisyydet (Morimoto ym. 2004: 111).

Kun metsään tehdään uusi toimialue, Domain Naming Master -palvelin varmistaa, ettei toimialueelle annettava nimi ole vielä käytössä. Domain Naming Master -roolin pitää olla Global Catalog -palvelimella, sillä se tarvitsee tarkistuksiin tiedon kaikista metsän objekteista. Yhdessä metsässä voi olla vain yksi Domain Naming Master. (Corbin 2004: 94.)

PDC Emulator -rooli tarjoaa vanhemmille käyttöjärjestelmille, kuten Windows NT 4.0, -95 ja -98, mahdollisuuden käyttää toimialueen palveluita. Tämä rooli on käytössä vain, jos toimialueen toiminnallisuustaso on Windows 2000 Mixed, eli uusissa toimialueissa rooli on hyvin harvoin käytössä. PDC Emulator -rooleja voi olla yksi toimialuetta kohden. (Corbin 2004: 92.)

RID master jakaa kaikille toimialuepalvelimille joukon RID-tunnuksia (Relative ID, uniikki tunnus objekteille). Toimialuepalvelimet jakavat näitä tunnuksia uusille objekteille. RID master siis huolehtii, että kaikilla toimialueen objekteilla on oma uniikki tunnus. Jos roolin sisältävä palvelin ei ole käytettävissä, voidaan joutua tilanteeseen, jossa toimialueelle ei voida lisätä objekteja. RID master -rooleja on yksi jokaisella toimialueella. (Morimoto ym. 2004: 111.)

Infrastructure master pitää tietokantaa kaikista metsän toimialueiden objekteista. Sillä ei ole kopioita objekteista, vaan pelkät viittaukset niihin. Metsän Infrastructure masterit tiedottavat toisilleen muutoksista objekteihin. Jokaisella toimialueella voi olla yksi Infrastructure master. Tämä rooli ei voi olla samalla palvelimella kuin Global Catalog, sillä ne käyttävät samaa tietokantaa, ja se sekoittaisi Infrastructure Masterin toiminnan. Jos

kaikki toimialueen toimialuepalvelimet ovat Global Catalog -palvelimia, ei tätä roolia tarvita, sillä toimialuepalvelimilla on jo täydelliset tietokannat metsän objekteista. Infrastructure master -roolia ei tarvita myöskään silloin, kun on kyseessä yhden toimialueen ympäristö. (Cobin 2004. 92; Morimoto ym. 2004: 111-112.)

Pienissä organisaatioissa, joissa on yksi toimialuepalvelin tai yksi toimialue, näitä FSMO-rooleja (Flexible Single-Master Operation) täytyy harvoin pohtia. Roolien ymmärtäminen on tärkeää silloin, kun toimialue jakaantuu useampaan toimipaikkaan, tai kun hallinnoidaan metsää, jossa on useita toimialueita. Suurissa ympäristöissä sijoittelu ja saatavuuden varmistaminen täytyy suunnitella hyvin.

## 4 Microsoft Exchange Server

### 4.1 Yleisestä

Microsoft Exchange Server on järjestelmä, joka tarjoaa käyttäjille sähköposti- ja yhteistyöpalvelut. Exchangen palveluita ovat sähköpostit, jaetut kalenterit ja osoitekirjat sekä julkiset kansiot. Exchangessa kaikki tiedot säilytetään palvelimella. (Exchange Server 2007 Product Overview: 2008; Exchange Server 2007 Data Sheet: 2008.) Näin käyttäjät eivät menetä tietojaan työaseman rikkoutuessa tai kadotessa. Tämä helpottaa runsaasti tiedon hallintaa ja varmistusta, sillä sähköpostien, yhteystietojen ja kalentereiden osalta täytyy varmistaa vain yksi palvelin kymmenien tai satojen työasemien sijaan. Exchange Server 2007 on Microsoftin Exchange-palvelimen kuudes myyntiversio. Se julkaistiin 30. marraskuuta 2006 (Steve Ballmer ... 2008). Ohjelmistoon on tullut runsaasti uudistuksia Exchange Server 2003:een verrattuna. Suuri osa uudistuksista koskee Exchangen rakennetta ja ylläpitotoimia.

### 4.2 Rakenne

Exchange 2007 on rakennettu 64-bittisen arkkitehtuurin päälle. Tähän on päädytty, jotta saadaan entistä enemmän suorituskykyä erityisesti keskusmuistin kanssa. Muistin tarve on kasvanut postilaatikkojen kokojen kasvun takia. 32-bittisellä osoiteavaruudella voidaan käyttää 4 gigatavua keskusmuistia. 64-bittisellä osoiteavaruudella muistia voidaan käyttää 16 exatavua (exatavu = miljardi gigatavua). (Microsoft Exchange ... 2008: 4.) Ohjelmistosta on myös 32-bittinen versio, mutta se on tarkoitettu ainoastaan testaukseen eikä ole tuettu tuotantoympäristöissä (Gerber & McBee 2007: 14).

Exchangen perusrakenteessa on myös alettu käyttää uutta mallia. Aikaisemmissa Exchange Serverin versioissa asennettiin ensin Exchange-palvelu, ja sen jälkeen se mukautettiin vastaamaan haluttua tehtävää. Tehtävien vaihtoehtoja olivat back-end -palvelin, jossa sijaitsee sähköpostilaatikat, tai front-end -palvelin, johon käyttäjät ottavat yhteyttä. Exchange

Server 2007:ssä nämä asetukset on jaettu rooleihin, jotka valitaan asennusvaiheessa. Tämä selkeyttää asennusta, sillä vain tarvittavat Exchangen osat tulevat automaattisesti palvelimille. Se myös nopeuttaa käyttöönottoa vähentämällä konfigurointivirheiden määrää. Rooleja on 7 kappaletta:

- Mailbox
- Client Access
- Hub Transport
- Unified Messaging
- Edge Transport
- Active Clustered Mailbox
- Passive Clustered Mailbox

Sähköpostilaatikot sijaitsevat palvelimella, jolla on Mailbox -rooli.

Client Access -roolin kautta käyttäjät ottavat yhteyttä sähköpostilaatikoihin. Tämä rooli hoitaa kaikki protokollat, joilla käyttäjä ottaa yhteyttä järjestelmään. Client Access -roolin sisältävällä palvelimella täytyy olla IIS (Internet Information Services, Microsoftin WWW-sovelluspalvelu) Outlook Web Accessia (OWA) varten.

Hub Transport -rooli hoitaa sähköpostien kuljettamisen oman Exchange -organisaation sisällä sekä välittää viestit mahdollisesti käytettävälle SMTP Smart Hostille (Simple Mail Transfer Protocol, sähköpostien lähettämiseen käytettävä protokolla), joka hoitaa sähköpostien välittämisen.

Unified Messaging -rooli mahdollistaa äänipostin ja faksien vastaanottamisen sähköpostitileille.

Edge Transport -roolilla voidaan Exchange -palvelimesta tehdä SMTP Smart host -välityspalvelin. Edge Transport -palvelimen kautta voidaan reitittää kaikki oma liikenne sekä sisään- että ulospäin. Tällä pyritään minimoimaan sähköpostipalvelimia vastaan kohdistuvien hyökkäysten pinta-ala. Edge Transport -palvelimeen voidaan liittää roskaposti- ja virussuodatusominaisuudet. Lisäksi voidaan tehdä runsaasti erilaisia Edge Transport

-sääntöjä. Säännöillä voidaan valvoa sekä lähetettyjen että vastaanotettujen viestien sisältöä sanojen tai tekstin rakenteen perusteella. Sääntöihin osuvaa viestiä voidaan käsitellä halutusti: esimerkiksi poistaa viesti, laittaa viesti karanteeniin, lisätä vastaanottajia tai merkitä logiin. Edge Transport -rooli asennetaan erilliselle itsenäiselle palvelimelle. (Edge Transport Role: 2007; Gerber & McBee 2007: 17.)

Active Clustered Mailbox - ja Passive Clustered Mailbox -rooleja käytetään Exchange-palvelimen klusterointiin. Exchange-rooleista ainoastaan Mailbox Server -rooli voidaan klusteroida. Jos klusterointi toteutetaan, kannattaa Mailbox Server -roolit sijoittaa omille palvelimilleen ja muut tarvittavat roolit muualle. Tällöin Mailbox Server -palvelimen hajotessa muita rooleja ei poisteta käytöstä. Klusterointi voidaan toteuttaa kahdella tavalla: Single Copy -klusterilla (SCC) tai jatkuvalla replikoinnilla (Clustered Continuous Replication, CCR). (Gerber & McBee 2007: 17.)

SCC on malli, jossa sähköpostitilit sijaitsevat jaetussa tietovarastossa. Tähän tietovarastoon täytyy kaikilla klusterin palvelimilla olla pääsy. Palvelimia voi olla 2-8 kappaletta, joista useampi voi olla yhtä aikaa aktiivisena. Perustilassa yksi palvelin on passiivisena (Passive Clustered Mailbox -rooli) valmiina ottamaan aktiivisen roolin jonkun muun palvelimen pettäessä. (Gerber & McBee: 515.)

CCR on aina kahden palvelimen klusteri, joista toinen on aktiivinen ja toinen passiivinen. Sähköpostitilien muutokset tehdään aktiiviselle palvelimelle ja kopioidaan sieltä passiiviselle palvelimelle. Kun aktiivinen palvelin hajoaa, passiivinen ottaa Mailbox Server -roolin aktiiviseksi. (Gerber & McBee 2007: 516.)

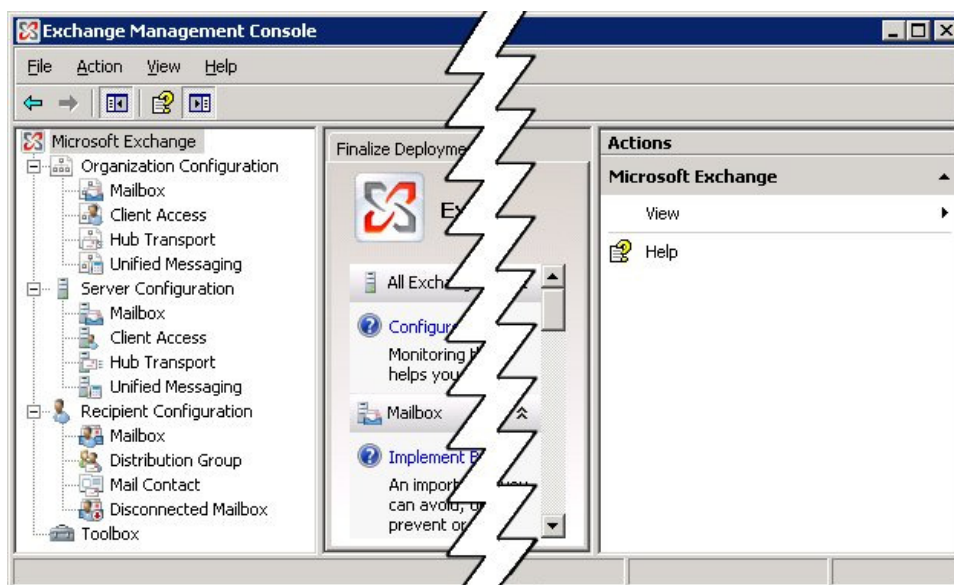
Klusterointi monimutkaistaa huomattavasti Exchange-järjestelmää ja lisäksi lisenssit, palvelimet ja ylläpito lisäävät kustannuksia. Tämä tulee siis kysymykseen ympäristöissä, joissa sähköposti on liiketoiminnalle niin kriittinen järjestelmä, ettei siihen saa tulla varmistusten palautuksista johtuvaa taukoa.

Roolien tunteminen helpottaa huomattavasti Exchange Server 2007:n toiminnan ymmärtämistä. Tämän lisäksi selkeä roolijako helpottaa suurempien ympäristöjen suunnittelua ja madaltaa kynnystä haastavampien toteutuksien tekemiseen.

### 4.3 Ylläpito

Ylläpidon suurin muutos on PowerShell-komentorivympäristön käyttöönotto. PowerShell on Microsoftin uusi komentorivympäristö. Se käyttää .NET Framework -ohjelmistokomponenttikirjastoa. PowerShell on suunniteltu helpottamaan ylläpitäjien työtä tarjoamalla mahdollisuuden ylläpito toimintojen automatisointiin. (Windows PowerShell Getting Started Guide: 2007.) Toinen etu on se, ettei graafista, paikoitellen hankalaa käyttöliittymää hallintaan ole välttämätöntä käyttää hallintaan.

Myös graafista käyttöliittymää on pyritty parantamaan. Kaikki toiminnot on kerätty samaan MMC-ikkunaan (Microsoft Management Console, graafinen hallintatyökalu). Ikkunasta löytyy kaikki yhdellä palvelimella olevat Exchangen asetukset jaoteltuna rooleittain sekä valitun objektin kaikki mahdolliset toiminnot (kuva 2).



Kuva 2. Exchange Management Console



Graafisen käyttöliittymän huono puoli on siinä, että sillä voi hallita vain kyseisellä palvelimella olevia rooleja. Jos siis Exchange-järjestelmässä on käytössä useita palvelimia, joutuu hallintaa tekemään monesta paikasta. Organisaatiota koskevat yleisasetukset saa tehtyä miltä tahansa järjestelmän palvelimelta.

Jos Exchange-järjestelmässä on yhtä aikaa käytössä useampia Exchangen versioita esimerkiksi siirtovaiheen takia, Exchange Server 2007:llä oleviin postilaatikoihin ei voi tehdä muutoksia vanhemmilta versioilta, vaikka laatikot näkyvätkin siellä. Exchange Server 2007 estää näiden muutosten tekemisen, joten vahingossa tällaista virhettä ei voi tehdä.

#### 4.4 Käyttö

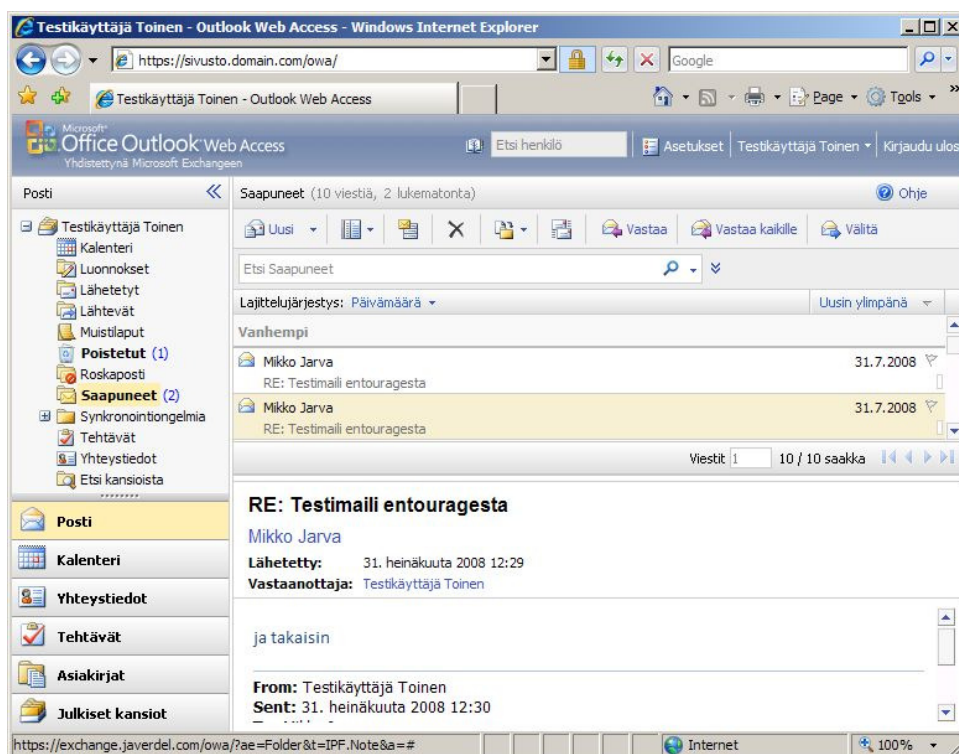
Exchangen sähköpostilaatikoita käytetään sähköpostiohjelmalla, selaimella tai mobiililaitteella. Sähköpostiohjelmista kattavin tuki eri toiminnoille on Microsoft Outlookissa. Exchange Server on ensisijaisesti suunniteltu toimimaan sen kanssa, ja se on ainoa sähköpostiohjelma, jossa on täysi MAPI-tuki (Gerber & McBee 2007: 114). Messaging Application Programmin Interface (MAPI) on rajapinta, jolla voidaan käsitellä palvelimella sijaitsevia tietovarastoja ja niiden asetuksia (Messaging Application Programmin Interface: 2008). Outlook käyttää MAPI Remote Procedure Calls -protokollaa kommunikointiin. Remote Procedure Call (RPC) on protokolla, jolla voidaan lähettää palvelukutsuja verkon yli toisille koneille (Bott 2004: 326).

Outlook voi kommunikoida Exchange-palvelimen kanssa myös RPC over HTTP -protokollaa käyttäen. Tässä RPC-kutsut kuljetetaan HTTP-yhteyden (Hypertext Transfer Protocol) avulla palvelimelle. Yhteyden muodostamiseen voidaan käyttää HTTPS-protokollaa (Hypertext Transfer Protocol Secure), jolloin liikenne on salattua. Tämän toimimiseksi palvelimella täytyy olla sertifikaatti. RPC over HTTP mahdollistaa Outlook-ohjelman käytön mistä tahansa ilman VPN-yhteyden (Virtual Private Network) muodostamista yrityksen verkkoon. RPC over HTTP on saanut

Exchange 2007:ssä uuden nimen: Outlook Anywhere. (Gerber & McBee 2007: 647.)

Muita sähköpostiohjelmia, kuten Outlook Expressiä tai Mozilla Thunderbirdiä voi käyttää Exchangen kanssa IMAP- (Internet Message Access Protocol) tai POP3-protokollia (Post Office Protocol version 3) käyttäen. Tällöin voi käyttää vain Exchangen sähköpostitoimintoja.

Selaimella pääsee käyttämään Exchange-sähköpostilaatikkaa Outlook Web Accessilla (OWA). Se on Exchangen Client Access -roolin sisältäville palvelimelle automaattisesti asentuva sivusto. OWA:an on tehty runsaasti käytettävyyteen liittyviä uudistuksia edelliseen versioon verrattuna. Nyt OWA antaa lähes samanlaisen käyttökokemuksen kuin Outlook (kuva 3). Jaettujen kalentereiden käyttäminen vaatii kuitenkin kolmannen osapuolen ohjelmiston palvelimelle. OWA on suunniteltu käytettäväksi Internet Explorer -selaimella. Muilla selaimilla tulee käyttöön Outlook Web Access Light, jossa on vähemmän toimintoja. Sillä pääsee käsittelemään sähköposteja, kalenteria ja yhteystietoja. OWA toimii HTTP- tai HTTPS-protokollalla. Ei ole kuitenkaan syytä käyttää HTTP:ta, sillä tietoliikenne on tällöin salaamatonta. Outlook Web Accessin uudistukset ovatkin merkittävin käyttäjälle näkyvä uudistus.



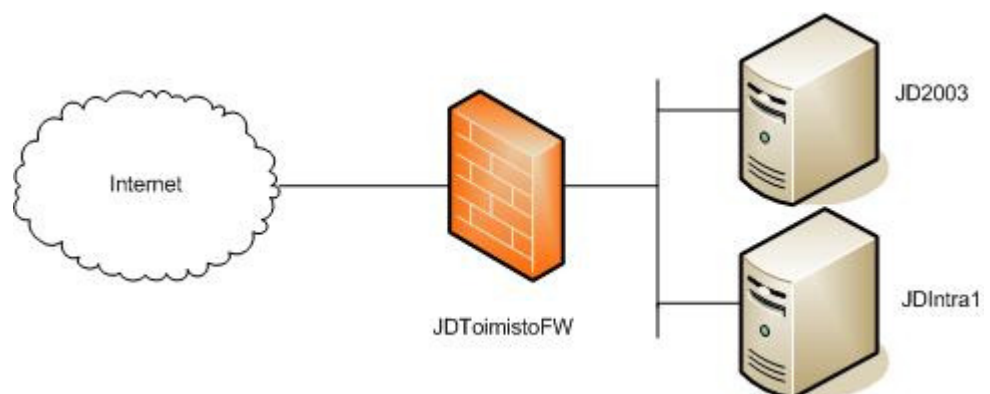
Kuva 3: Outlook Web Access

Mobiiliohjelmistot ottavat palvelimeen yhteyden Exchange ActiveSync -protokollalla, joka toimii HTTP- tai HTTPS-protokollan päällä. Microsoft Windows Mobile -laitteiden ActiveSync-ohjelmalla saa haettua kaikki sähköpostilaatikon kansiot, kalenterin ja yhteystiedot. Muut ohjelmistot, kuten Nokian Mail For Exchange, hakevat vain Saapuneet-laatikon, kalenterin ja yhteystiedot (Mail For Exchange: 2007). Tämä rajoittaa merkittävästi sähköpostien käyttöä, koska Exhangen postien lajittelusääntöjä ei voi käyttää mobiiliratkaisun kanssa. Jos mobiilipäätteellä käyttää paljon sähköpostia, kannattaa harkita Windows Mobile -laitetta.

## 5 Palvelimen asentaminen

### 5.1 Valmistelu

Alkutilanteessa Javerdelin oma verkko rakentui työtä koskevin osin seuraavasti: kahdesta toimialuepalvelimesta (JD2003 ja JDIntra1), Exchange-palvelimesta (JD2003) ja palomuurista (JDToimistoFW) (kuva 4). Työn aloitushetkellä toimialueella oli kaksi toimialuepalvelinta: korvattava JD2003 ja uudempi JDIntra1. Tehtävänä oli asentaa uusi toimialuepalvelin JDIntra2, ja myöhemmin poistaa JD2003:lta toimialuepalvelimen rooli. Näin toimialueelle jää kaksi toimialuepalvelinta, ja niiden toimialueeseen liittyvät palvelut ovat saatavilla, vaikka toinen palvelimista olisi pois käytöstä esimerkiksi huoltokatkon takia.



Kuva 4: Javerdelin oma verkko

Uudelle palvelimelle oli tarkoitus asentaa toimialuepalvelut, Exchange Server ja näiden lisäksi DHCP-palvelin (Dynamic Host Configuration Protocol, verkkoasetusten dynaamisen konfiguroinnin protokolla). Palvelimen kokoonpano mitoitettiin kattamaan Exchange 2007:n tarpeet (taulukot 1, 2 ja 3). Laitteistoksi asennettiin Intelin SR2400 -palvelinrunko, joka on kahden yksikön (2U) kokoinen rakkipalvelin. Runkoon asennettiin kaksi tuplaydinprosessoria ja 8 gigatavua muistia. Tämä on toteutettu suositeltujen maksimiarvojen mukaan.

Taulukko 1: Processor Recommendations Based on Server Role  
(Gerber & McBee 2007: 36.)

Exchange 2007 Server Role	Minimum	Recommended	Recommended Maximum
Edge Transport	1 x processor core	2 x processor core	4 x processor core
Hub Transport	1 x processor core	4 x processor core	4 x processor core
Client Access	1 x processor core	4 x processor core	4 x processor core
Unified Messaging	1 x processor core	4 x processor core	4 x processor core
Mailbox	1 x processor core	4 x processor core	8 x processor core
Multiple server roles (combination of Hub Transport, Client Access, Unified Messaging, and Mailbox server roles)	1 x processor core	4 x processor core	4 x processor core

Taulukko 2: Minimum and Recommended RAM for Exchange Server 2007 Roles

(Gerber & McBee 2007: 37.)

Server Role	Minimum	Recommendation	Maximum
Mailbox	2GB	2GB base memory plus per mailbox calculation	32GB
Hub Transport	1GB	1GB per CPU core	16GB
Client Access	1GB	1GB per CPU core	4GB
Unified Messaging	1GB	1GB minimum plus 512MB for each additional CPU core	4GB
Edge Transport	1GB	1GB per CPU core	16GB
Multiple roles	2GB	4GB for combination Hub Transport, Client Access, and Unified Messaging plus the per-mailbox calculation	8GB

Taulukko 3. Additional Memory Factor for Mailbox Servers

(Gerber & McBee 2007: 37.)

User Profile	Mailbox Memory Recommendation
Light	Add 2MB per mailbox
Average	Add 3,5MB per mailbox
Heavy	Add 5MB per mailbox

Uusi palvelin sijoitettiin samaan verkkoon kuin työasemat. Palomuurille määriteltiin NAT-muunnos (Network Address Translation, osoitteenmuunnos) omaan julkiseen IP-osoitteeseen. Tämä tarvitaan sähköpostien

kulkuun ja niiden käyttöön työpaikan ulkopuolelta. Palomuurisäännöt määriteltiin siten, että palvelimelle päästetään Internetistä HTTP- ja HTTPS-liikenne sähköpostien lukemista varten sekä omalta sähköpostien suodatuspalvelimelta SMTP. Palvelimelta Internetiin käytetään samaa sääntöä kuin koko toimiston verkkoon: kaikki liikenne sisältä ulos sallitaan.

## 5.2 Windowsin asennus

Palvelimen asennus alkoi Windows Server 2003:n perusasennuksesta. Käyttöjärjestelmäversio oli 64-bittinen Windows Server 2003 R2 Standard Edition. Asennus olisi voitu tehdä myös Windows Server 2008:lle, mutta projektia aloitettaessa syksyllä 2007 se oli vasta beta-asteella. Kun Windows Server 2008 varsinaisesti julkaistiin helmikuussa 2008 (Windows Server ... 2008), olisi periaatteessa ollut mahdollista tehdä asennukset uudelleen. Uuteen palvelinversioon ei kuitenkaan ollut ehditty kattavasti tutustua eikä testata sitä. Oman sähköpostipalvelimen toimivuusvaatimukset ovat korkeat, joten päätettiin pysyä vanhemmassa mutta tutussa ja varmasti toimivassa versiossa.

Perusasennus sisältää käyttöjärjestelmän asennuksen ja Javerdelin sisäisen ohjeen määrittelemiä konfiguraatioita tietoturva- ja päivitysasetuksiin sekä varmistuksiin. Paikallisesti varmistetaan Windowsin System State, joka sisältää muun muassa käyttöjärjestelmän rekisterin, käynnistystiedostot sekä toimialuepalvelimelta aktiivihakemistojen tiedostopalvelut (Active Directory directory service) ja SYSVOL-kansion. Aktiivihakemistojen tiedostopalvelut sisältävät aktiivihakemistopalveluiden tietokannan, jossa on kaikki toimialueen objektit. SYSVOL-kansiossa on muun muassa Group Policyt ja kirjautumisissa ja käynnistyksissä mahdollisesti käytettävät komentosarjat (Morimoto ym. 2004: 1067). Nämä kaksi ovat erityisen oleellisia, jos toimialuepalvelinta joudutaan laite- tai käyttöjärjestelmärikon takia palauttamaan varmistuksista. Tiedot replikoituvat myös toisille toimialuepalvelimille, joten Javerdelin ympäristössä aktiivihakemistopalveluiden tietoa ei katoa ongelmatilanteessa. Käyttöjärjestelmän asennuksen lopuksi palvelin liitettiin Javerdelin toimialueeseen.

Oman verkon DHCP-palvelu oli hajautettu kahdelle toimialuepalvelimelle siten, että työasemille käytössä olevasta alueesta ensimmäinen jakoi noin 66% ja toinen 34%. Näin työasemat saavat osoitteen myös toisen toimialuepalvelimen ollessa pois käytöstä.

DHCP-palvelun siirtoa JD2003:lta yritettiin toteuttaa tietokannan siirrolla. Uudelle palvelimelle asennettiin DHCP-palvelu ja se pysäytettiin. Tämän jälkeen JD2003:lta pysäytettiin DHCP-palvelu ja kopioitiin %System-Root%\System32\dhcp -kansion sisältö uudelle palvelimelle vastaavaan kansioon. (Kivimäki, 2005: 1342.) Siirto ei toiminut, ja syyksi epäiltiin käyttäjärjestelmäversion vaihtumista 32-bittisestä 64-bittiseen. Ongelmaa ei selvitetty, koska DHCP:n konfiguraatio oli yksinkertainen, ja oli nopeampaa konfiguroida uusi järjestelmä manuaalisesti.

DHCP:n asetuksissa määriteltiin työasemille jaettavat osoitteet ja kaksi kiinteää varausta tulostimille. DNS-palvelimiksi asetuksissa merkittiin toimialuepalvelimet ja oletusyhdykäytäväksi verkon palomuri. Toimialueella pitää DNS-palvelimiksi antaa toimialuepalvelimet, jotta toimialueeseen liittyvät palvelut toimivat oikein.

Aktiivihakemistopalvelut vaativat palvelimelta DNS-palvelimen (Domain Name System, järjestelmä jolla palvelinten nimet muutetaan IP-osoitteiksi) roolin. Tästä suoritettiin perusasennus. Varsinaiset DNS-palvelimen konfiguroinnit tekee aktiivihakemistojen asennusprosessi. Itse lisättiin vain Forwarders-määrittelyt, joissa kerrotaan, miltä palvelimilta toimialuepalvelin kysyy ne DNS-kyselyt, jotka eivät koske sen omaa toimialuetta.

### 5.3 Toimialuepalveluiden asennus

Aktiivihakemistopalvelut asennetaan Microsoftin DCPromo.exe -ohjelmalla. Se on ohjattu asennustoiminto, joka asentaa palvelimelle toimialuepalveluiden komponentit. Ensin määritellään, asennetaanko uusi toimialuepalvelin uudelle toimialueelle vai toimialuepalvelin olemassa

olevalle toimialueelle. Näistä valittiin jälkimmäinen. Tämän jälkeen annetaan ylläpitokäyttäjätunnukset ja kirjoitetaan toimialueen nimi, johon palvelin liitetään. Seuraavaksi valitaan asennuspolut toimialueen tietokannalle, loki-tiedoille ja SYSVOL-kansiolle.

Viimeisenä asetuksena annetaan aktiivihakemistojen palautustilan salasana. Tämä salasana on tärkeää säilyttää, sillä jos aktiivihakemistopalveluiden tietokantaa joudutaan palauttamaan varmistuksesta, sitä tarvitaan. Se on salasana, jota ei ole liitetty mihinkään aktiivihakemistopalvelussa näkyvään käyttäjätiliin, vaan ainoastaan palautustilan käyttöön. Asennukseen käytettiin Microsoftin ohjetta toisen toimialuepalvelimen asentamisesta. (Installing a domain controller: 2007.) Aktiivihakemistopalveluiden asennuksen päätteeksi palvelimelle aktivoitiin Global Catalog -rooli.



## 6 Exchange Server 2007:n asennus

Exchange Server 2007:n asennus toteutettiin yhden palvelimen mallilla: kaikki tarvittavat roolit sijoitettiin samalle palvelimelle. Exchange Server 2007:n asentaminen vaatii, että koneella on .NET Framework 2.0, Microsoft Management Console 3.0 -hallintatyökalu ja Microsoft Windows PowerShell 1.0 -komentoriviyö-ympäristö. (Gerber & McBee 2007: 124-125.) Näiden lisäksi Client Access -roolin sisältävälle palvelimelle tarvitaan IIS.

Prosessissa asentuu Exchange Management Shell -laajennus (EMS) PowerShell-ympäristöön. EMS sisältää komentoja Exchangen hallintaan ja sillä saa tehtyä kaikki Exchangen ylläpitotoiminnot. (Gerber & McBee 2007: 234.) On myös toimintoja, joita ei voi helposti tehdä graafisesta käyttöliittymästä. Tällainen toimenpide on esimerkiksi sähköpostilaatikoiden kokojen listaus. Komentoriviltä listaus onnistuu, mutta graafisessa ympäristössä tiedot joutuu hakemaan jokaiselta laatikolta erikseen. Exchange 2003:n graafisen käyttöliittymässä listaus oli helposti saatavilla.

Asennus tapahtuu ohjatulla toiminnolla, jossa valitaan asennettavat roolit. Tämän lisäksi voidaan valita Exchange-järjestelmä, johon palvelin liitetään. Palvelimelle asennettiin Mailbox-, Client Access -, Hub Transport - ja Unified Messaging -roolit. Tämän lisäksi palvelin liitettiin olemassa olevaan Exchange-ympäristöön. Tuotteeseen ei enää asennusvaiheessa syötetä tuoteavainta, vaan se annetaan hallintaikkunan kautta jälkikäteen.

Seuraavaksi asennettiin Exchange Server 2007 Service Pack 1, joka sisälsi päivityksiä järjestelmään, muun muassa julkisten kansioiden graafisen hallintatyökalun. Service Packin asennuksessa on otettava huomioon, että se aiheuttaa palvelimen kokoonpanosta riippuen noin 40 minuutin käyttökatkon. Päivityksen asentaminen ei vaadi uudelleenkäynnistystä.

OWA:n käytön helpottamiseksi tehtiin sivustolle uudelleenohjaus. Kun selaimen osoiteriville kirjoittaa sivusto.domain.com, selain ottaa yhteyttä

HTTP-protokollalla osoitteeseen `http://sivusto.domain.com`. OWA vastaa kuitenkin vain osoitteesta `https://sivusto.domain.com`. Jotta käyttäjän ei tarvitse kirjoittaa jokaisella käyttökerralla osoitteen alkuun ”https://”, on sivustolle tehty uudelleenohjaus osoitteesta HTTP:stä HTTPS:ään.

## 6.2 Testaus

Käyttöönottovaihetta alustettiin testauksella. Aluksi luotiin testilaatikoita Exchange Server 2003:lle ja generoitiin laatikoihin jonkin verran sisältöä. Tämän jälkeen laatikot siirrettiin Exchange Server 2007:lle ja niiden toimintaa testattiin eri menetelmin. Ensimmäisenä kokeiltiin Outlookin käyttöä omasta verkosta ja Internetin yli. Outlook Web Accessia testattiin myös eri verkoista sekä eri selaimilla. Mobiiliohjelmista testattiin Nokian MailForExchange -ohjelmaa ja Microsoft Windows Mobile 5 -käyttöjärjestelmän Exchangea tukevaa sähköpostiohjelmaa. Molemmat mobiiliohjelmat kommunikoivat palvelimen kanssa HTTPS-protokollalla. Windows Mobile 5 -version kanssa tuli sertifikaattiongelma.

Ongelma johtui siitä, että Javerdelille oli hankittu web-sivustoja varten niin sanottu wildcard-sertifikaatti. Se on sertifikaatti, joka on muodossa \*.domain.com. Samalla sertifikaatilla voidaan todentaa monta alasivua, esimerkiksi tuotanto.domain.com ja testi.domain.com. Tällä saadaan säästää sertifikaattien hankintakuluissa.

Eri sertifikaattien myöntäjät tarjoavat sertifikaatteja hieman erilaisin käyttöehdoin. Esimerkiksi Thawten wild card -sertifikaatin saa laittaa monelle fyysiselle palvelimelle, mutta ensimmäisen asennuksen jälkeen muille palvelimille tarvitaan lisäksi maksullinen lisenssi (Thawte - Frequently ... 2007). Otimme sertifikaatin tarjoajalta, joka ei rajoittanut laitteiden määrää, joihin sertifikaatin saa asentaa.

Wild card -sertifikaattien ongelma on siinä, ettei niiden käytöstä ole vielä varsinaisia standardeja. Esimerkiksi selaimet käsittelevät niitä eri tavoin. Jos sivustolla x.y.domain.com on sertifikaatti on \*.domain.com, Firefox hyväksyy sertifikaatin, mutta Internet Explorer ei. Wild card -sertifikaatti

toimi Outlook Web Accessin kanssa hyvin, mutta Windows Mobile -laitteet muodostuivat ongelmaksi. Windows Mobile 5 -käyttöjärjestelmässä ei ole tukea wild card -sertifikaateille. Tällaisia puhelimia on käytössä noin kymmenen, eikä niistä haluttu luopua. Tämän takia tilattiin erillinen sertifikaatti Exchangelle ja se ratkaisi mobiililaitteiden ongelmat.

### 6.3 Käyttöönotto

Exchange Server 2007:n julkaisuversiossa ei ollut MMC-työkalua julkisten kansioiden (Public Folders) hallintaan. Javerdelilla on käytössä julkisia kansioita, eikä uutta Exchangea voitu ottaa heti käyttöön, sillä PowerShell -ympäristöstä ei ollut tarpeeksi osaamista. Tämä työkalu toteutettiin ensimmäisessä Services Packissa, joka asennettiin tammikuussa. Tämä viivästytti jonkin verran käyttöönottovaihetta.

Sähköpostilaatikoiden siirto toteutettiin useammassa osassa. Ensin kirjoitettiin ohje OWA:n käyttöön sekä mobiililaitteisiin ja Outlook-ohjelmaan tehtävistä muutoksista. OWA:ssa ja mobiililaitteissa muuttui palvelimen osoite. Outlook sai asetukset automaattisesti lukuun ottamatta välityspalvelimen osoitetta, joka piti vaihtaa manuaalisesti. Ohjeistuksen jälkeen postilaatikot siirrettiin tiimi kerrallaan, ja työntekijöitä informoitiin siirrosta tekstiviestillä.

Sähköpostilaatikoiden siirrossa on otettava huomioon siirtämiseen käytettävän store.exe -prosessin toimintatapa. Siirto toimii siten, että valitaan siirrettävät laatikot ja kohdepalvelin, johon laatikot siirretään. Sen jälkeen store.exe aloittaa siirron lataamalla laatikot muistiin. Tässä törmättiin erikoiseen ongelmaan. Store.exe ei toimi siten, että se lataisi yhden laatikon muistiin, siirtäisi sen ja tyhjentäisi muistin, vaan se lataa kaikki laatikot muistiin, ja tyhjentää muistin vasta kun tehtävä on valmis. Tämä aiheutti palvelimen kaatumisen, kun yöksi oli laitettu siirtymään suuria laatikoita ja palvelimelta loppui sekä muisti että virtuaalimuisti.

Käyttöönottoa ei voitu toteuttaa vielä lopullisesti. Javerdelissa on käytössä mukautettu Microsoft Dynamic CRM (Customer Relationship Manage-

ment, asiakkuudenhallintajärjestelmä). Siinä käytetään JD2003-palvelimella sijaitsevia Exchange-sähköpostilaatikoita. CRM-projektin johtaja ilmoitti, ettei näitä laatikoita voida siirtää ennen uuden CRM:n version testausta ja käyttöönottoa. Tämän takia JD2003:lta ei voida vielä poistaa Exchangea.

## 7 Loppupäätelmät

Työssä päästiin päätavoitteisiin. Uusi Exchange saatiin otettua käyttöön, ja siitä on saatu kokemusta. Uusi palvelin toimii myös toimialuepalvelimen roolissa. Exchangen osalta työ jäi hieman kesken JD2003:lla olevien CRM-sähköpostilaatikoiden takia. Exchange Server 2003:a ei vielä saatu poistettua käytöstä, vaikka tämä oli alkuperäinen tavoite.

Koska JD2003:lla toimii vielä Exchange, siitä ei ole myöskään poistettu toimialuepalveluita. Se on toimialueen ensimmäinen toimialuepalvelin, joten sillä on kaikki FSMO-roolit. Nämä roolit täytyy siirtää toisille toimialuepalvelimille ennen tuotannosta poistamista. Aktiivihakemistopalveluiden poistaminen onnistuu DCPromo-työkalulla. (Demote a Domain Controller: 2008.) Sovimme, että roolien siirto tehdään palvelimen tuotannosta poistamisen yhteydessä.

Omalle toimialueelle jäi vielä kehitettävää. Yksi tällainen asia liittyy Exchangen ja aktiivihakemistopalveluiden sijoittamiseen. Aktiivihakemistopalveluiden ja Exchange-palvelimen Client Access-roolin sijoittamista samalle palvelimelle ei suositella. Yksi syy tähän on aktiivihakemiston käyttäjätilit ja Client Access-roolin yhteistyö: Exchange käyttää toiminnassaan aktiivihakemistopalveluiden käyttäjätunnuksia. Periaatteessa Client Access-roolin sisältämä palvelin on alttein hyökkäyksille, koska sille täytyy avata palomuurista portteja sähköposteihin käsiksi pääsyä varten. Jos hyökkääjä saa tämän palvelimen haltuunsa, ja siellä sijaitsevat toimialueen käyttäjätunnukset, vahingot voivat olla mittavat. Tämä tarkoittaa sitä, että hyökkääjä voisi esimerkiksi vaihtaa kaikkien käyttäjätilien salasanat haluamikseen ja pääsisi käsiksi käyttäjien sähköposteihin.

Toinen mahdollinen syy palveluiden erottamiseen liittyy suorituskykyyn. Aktiivihakemistopalvelut vaativat huomattavasti resursseja, jos objekteja on paljon. Tällöin on varmempaa sijoittaa palvelut eri palvelimille, jotta taataan kaikille riittävät resurssit. Tämä tulee kuitenkin vastaan vasta siten, kun aktiivihakemistopalvelussa on kymmeniä tuhansia objekteja.

Javerdelin ympäristössä on riittävän perusteltua laittaa aktiivihakemisto-palvelut ja Exchange-palvelut samalle palvelimelle. Omien palvelimien määrä halutaan pitää mahdollisimman pienenä ylläpidon tarpeen ja lisenssimaksujen takia, eikä järjestelmän koko aiheuta suorituskykyongelmia.

Exchange-palvelimen klusterointi olisi mielenkiintoista toteuttaa. Tällöin päästäisiin eroon palvelinriippuvuudesta, eikä huoltokatkojen aikataulutusta tuottaisi ongelmia. Tämä olisi kuitenkin kohtuutonta ylimitoittamista omaan ympäristöön.

## Lähteet

Active Directory Overview [online] [viitattu 3.10.2008]

<http://technet.microsoft.com/en-us/library/cc758436.aspx>

Bott, Greg 2004. Implementing, Managing and Maintaining a Microsoft Windows Server 2003 Network Infrastructure (70-291).

Washington: Microsoft Press.

Corbin, Wendy 2004. Planning, Implementing, and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure (70-294).

Washington: Microsoft Press.

Demote a Domain Controller [online] [viitattu 11.10.2008]

<http://technet.microsoft.com/en-us/library/cc740017.aspx>

Domain Controller Roles [online] [viitattu 3.10.2008]

<http://technet.microsoft.com/en-us/library/cc786438.aspx>

Gerber, Barry & McBee, Jim 2007. Mastering Microsoft Exchange Server 2007.

Indianapolis: Wiley Publishing, Inc.

Edge Transport Server Role: Overview [online] [viitattu 24.9.2008]

[http://technet.microsoft.com/en-us/library/bb124701\(EXCHG.80\).aspx](http://technet.microsoft.com/en-us/library/bb124701(EXCHG.80).aspx)

Exchange Server 2007 Data Sheet [online] [viitattu 27.9.2008]

[http://download.microsoft.com/download/f/c/c/fccf22eb-30df-4471-92ce-452abfd4e565/Exchange\\_Server\\_2007\\_Data\\_Sheet.pdf](http://download.microsoft.com/download/f/c/c/fccf22eb-30df-4471-92ce-452abfd4e565/Exchange_Server_2007_Data_Sheet.pdf)

Exchange Server 2007 Product Overview [online] [viitattu 27.9.2008]

<http://www.microsoft.com/exchange/evaluation/overview/default.mspx>

Installing a domain controller [online] [viitattu 3.10.2008]

<http://technet.microsoft.com/en-us/library/cc759011.aspx>

Javerdel - Yritys [online] [viitattu 15.9.2008]

<http://www.javerdel.fi/default.aspx?id=620>

Kivimäki, Jyrki 2005. Windows Server 2003 - Tehokas hallinta. Jyväskylä,

Gummerus Kirjapaino Oy.

Mail For Exchange [online] [viitattu 28.9.2008]

<http://business.nokia.fi/A4546322>

- Microsoft Exchange Server 2007 White Paper [online] [viitattu 11.10.2008]  
<http://download.microsoft.com/download/5/9/a/59a63f2c-602d-41db-afc4-552936f80534/Microsoft%20Exchange%20Server%202007%20White%20Paper.doc>
- Morimoto, Rand, Gardeinier, Kenton, Noel, Michael & Droubi, Omar 2004.  
Microsoft Windows Server 2003 Unleashed. Indianapolis, Sams.
- Messaging Application Programming Interface [online] [viitattu 28.9.2008]  
<http://msdn.microsoft.com/en-us/library/aa142548.aspx>
- RFC-1777 [online] [viitattu 3.10.2008]  
<http://www.ietf.org/rfc/rfc1777.txt?number=1777>
- Steve Ballmer Kicks Off Most Significant Product Launch in Microsoft's History  
[online] [viitattu 3.10.2008]  
<http://www.microsoft.com/presspass/press/2006/nov06/11-30NewDayPR.mspx>
- Thawte - Frequently Asked Questions about the SSL Web Server Wildcard Certificate  
[online] [viitattu 11.10.2008]  
<https://search.thawte.com/support/ssl-digital-certificates/index?page=content&id=S:SO3923&actp=search&searchid=1223721561361>
- Tulloch, Mitch & Tulloch, Ingrid 2002. Microsoft Encyclopedia of Networking.  
Washington, Microsoft Press.
- Windows PowerShell Getting Started Guide [online] [viitattu 27.9.2008]  
[http://msdn.microsoft.com/en-us/library/aa973757\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/aa973757(VS.85).aspx)
- Windows Server 2008 markkinoille näyttävästi [online] [viitattu 16.10.2008]  
[http://www.tietokone.fi/uutta/uutinen.asp?news\\_id=32963](http://www.tietokone.fi/uutta/uutinen.asp?news_id=32963)