MICROSOFT EXCHANGE SERVER 2010 -PALVELINPROJEKTI

LAHDEN AMMATTIKORKEAKOULU
Tekniikan ala
Tietotekniikan koulutusohjelma
Tietoliikennetekniikka
Opinnäytetyö
Kevät 2011
Niklas Loise

Lahden ammattikorkeakoulu
Tietotekniikan koulutusohjelma

LOISE, NIKLAS: Microsoft Exchange Server 2010 -palvelinprojekti

Tietoliikennetekniikan opinnäytetyö, 61 sivua

Kevät 2011

TIIVISTELMÄ

Tämän opinnäytetyön tavoitteena on tutkia kuinka, hyvin Exchange Server 2010 -sähköpostijärjestelmä pystyy vastaamaan Päijät-Hämeen koulutuskonsernin työntekijöiden asettamiin vaatimuksiin ja korvaamaan vanhan Novell GroupWise 8 -järjestelmän. Työssä selvitetään Exchange 2010:n uudet ominaisuudet ja tärkeimmät toiminnot.

Exchange Server 2010 on Microsoftin viimeisin viestintäpalvelinratkaisu, joka sisältää sähköposti-, kalenteri-, yhteystieto- ja vastaajaratkaisut. Exchange 2010 toimii Windows Server 2008 -käyttöjärjestelmässä ja tarvitsee organisaatiossa AD- ja DNS-palvelut toimiakseen. Exchange 2010 koostuu viidestä palvelinroolista, joilla luodaan tarpeisiin sopiva viestintäjärjestelmä. Exchange-järjestelmästä on helppo saada vikasietoinen ottamalla käyttöön useampia saman roolin palvelimia.

Exchangen etuna on hyvä skaalautuvuus, jolloin se sopii erikokoisiin organisaatioihin. Se tarjoaa monipuolisia palveluja ja monia tapoja niiden käyttämiseksi. Palveluita voidaan käyttää asiakasohjelmalla, selaimella tai puhelimella. Palveluiden käyttö ei myöskään ole sidottu yhteen paikkaan.

Työssä luotiin virtuaalikoneiden avulla testijärjestelmä, jossa testattiin Exchangen perustoimintoja sekä käyttäjien ja ylläpitäjien antamia tavoitteita järjestelmälle. Exchange vastasi kaikkiin asetettuihin tavoitteisiin. Lopuksi työssä esitetään yksi mahdollinen arkkitehtuuri PHKK:n sähköpostijärjestelmälle.

Avainsanat: Exchange 2010, sähköposti, palvelin, viestintäratkaisu

Lahti University of Applied Sciences
Degree Programme in Information Technology

LOISE, NIKLAS: Microsoft Exchange Server 2010 project

Bachelor's Thesis in telecommunications, 61 pages

Spring 2011

ABSTRACT

The aim of this thesis was to study how well the Exchange Server 2010 email system can respond to the demands set by employees from the Lahti Region Educational Consortium and replace the existing Novell GroupWise 8 system. In this work, new features and the most important functions of Exchange 2010 were studied.

Exchange Server 2010 is the latest release of the messaging system from Microsoft, which includes email, calendaring, address book and voicemail solutions. Exchange 2010 runs on the Windows Server 2008 operating system and requires AD and DNS services in the organization. Exchange 2010 consists of five server roles, which are used to create a suitable messaging system. The Exchange system is easy to make redundant by deploying multiple servers which have the same role.

Exchange has the advantage of good scalability, making it suitable for organizations different sizes. It offers a wide range of services and many ways to use them. Services can be used with a client application, web browser or mobile phone. Also, the use of services is not tied to one location.

In this work, a test environment was made with the help of virtual machines in order to test basic functions of Exchange 2010 and the demands of users and administrators. Exchange 2010 met all the objectives set. Lastly, the work provides a possible architecture for the e-mail system of Lahti Region Educational Consortium.

Key words: Exchange 2010, email, server, communications solution

LYHENNELUETTELO

AD	Active Directory on Microsoftin keskitetty käyttäjätietokanta sekä hakemistopalvelu.
CAS	Client Access Server on Exchange-palvelimen rooli, joka yhdistää käyttäjän ja sähköpostilaatikon.
DAG	Database Availability Group on Exchange Mailbox -palvelimien muodostama vikasietoinen klusteri.
DHCP	Dynamic Host Configuration Protocol on verkkoprotokolla, joka jakaa lähiverkkoon kytkeytyville laitteille IP-osoitteita ja muita asetustietoja.
DNS	Domain Name System on nimipalvelujärjestelmä, joka muuntaa verkkonimet IP-osoitteiksi ja päinvastoin.
FQDN	Fully qualified domain name on täydellinen DNS-toimialuenimi, joka ilmaisee tarkan sijainnin toimialueen nimialueen puurakenteessa.
HTTP	Hypertext Transfer Protocol on protokolla, jota selaimet ja WWW-palvelimet käyttävät tiedonsiirtoon.
IMAP	Internet Message Access Protocol on sähköpostiviestien lukemiseen tarkoitettu protokolla.
IP	Internet Protocol on Internet-kerroksen protokolla, joka pakettikytkentäisessä Internet-verkossa huolehtii IP-pakettien toimittamisesta perille.
LAN	Local Area Network on tietoliikenneverkko, joka toimii rajoitetulla maantieteellisellä alueella.
MAPI	Messaging Application Program Interface on Microsoftin sovellusrajapinta, joka mahdollistaa sähköpostien lähettämisen Windows-ohjelmalla.
PBX	Private Branch Exchange on yrityksen puhelinvaihde.
POP	Post Office Protocol on sähköpostien noutamiseen tarkoitettu protokolla.
RAID	Redundant Array of Independent Disks on tekniikka, jolla voidaan yhdistää useita kiintolevyjä yhdeksi loogiseksi levyksi.
RAM	Random access memory on nopeaa tietokoneohjelmien käyt-

	töön tarkoitettua luku- ja kirjoitusmuistia.
RBAC	Role Based Access Control on Exchange Server 2010:n käyttämä roolipohjainen oikeusmalli.
RPC	Remote Procedure Call mahdollistaa ohjelmien suorittaa toimintoja toisessa osoiteavaruudessa, esimerkiksi jaetussa verkossa toisilla tietokoneilla.
STNEF	Summary Transport Neutral Encapsulation Format on SMTP-viestiformaatti, jota Exchange-palvelimet käyttävät sähköpostiviestien välittämiseen samassa reititysryhmässä.
UNC	Universal Naming Convention määrittelee syntaksin, joka kertoo verkkoresurssin sijainnin.
WAN	Wide Area Network on tietoliikenneverkko, joka toimii laajalla maantieteellisellä alueella.

SISÄLLYS

1 JOHDANTO

Opinnäytetyön tavoitteena on perehtyä Microsoft Exchange Server 2010 -sähköpostijärjestelmään ja tutkia, kuinka hyvin se soveltuu korvaamaan Päijät-Hämeen koulutuskonsernissa nykyisin toimivan Novell Groupwise 8 -järjestelmän. Opinnäytetyö perustuu PHKK:n koulutuskonsernin työntekijöiden toiveisiin uudistaa ja parantaa tämän hetkistä järjestelmää. Uuteen järjestelmään on kiinnitettävä huomiota myös ylläpidon näkökulmasta.

PHKK:n vanhassa sähköpostijärjestelmässä on sähköpostitilejä lähes 2500 ja suurimmassa osassa niistä on vain 250 Mt tilaa käytettävissä. Tämä on ollut suurin ongelma käyttäjille. Uuteen järjestelmään on ajateltu 1000 Mt:n postilaatikoita. Nykyisessä järjestelmässä F-Secure-ohjelmisto hoitaa virustarkistuksen ja SpamAssassin-ohjelmisto hoitaa roskapostinsuodatuksen. Nämä ohjelmat ja niiden palvelimet on tarkoitus säilyttää eikä ottaa käyttöön Microsoftin vastaavia toimintoja.

Tavoitteina oli käyttäjien näkökulmasta, että uudessa järjestelmässä olisi suuremmat sähköpostilaatikot, tuki mobiililaitteille ActiveSync-toiminnon avulla, jakelulistat, henkilöstön yhteystiedot, kalenteri ja mahdollisuus siirtää vanhat kalenteritiedot uuteen järjestelmään. POP- ja IMAP-protokollia ei aiota ottaa käyttöön.

Ylläpitäjien näkökulmasta tavoitteena oli, että uudessa järjestelmässä voitaisiin luoda sähköpostilaatikot AD:n käyttäjätilien perusteella, olisi kasvumahdollisuus tulevaisuutta varten, olisi mahdollisuus antaa ja muokata käyttöoikeuksia monipuolisesti eri ryhmille, voitaisiin antaa oikeuksia muihinkin kuin vain käyttäjien omiin sähköpostilaatikoihin, järjestelmä olisi vikasietoinen ja siinä olisi luotettavat ja yksinkertaiset tilien varmistus- ja palautusmahdollisuudet.

Työn tutkimusongelmana on siis selvittää, kuinka Exchange Server 2010 pystyy toteuttamaan PHKK:n käyttäjien ja ylläpitäjien asettamat tavoitteet ja testata testiympäristössä, kuinka ne voidaan ottaa käyttöön.

2 MICROSOFT EXCHANGE SERVER

2.1 Exchangen historia

Microsoft Exchange Server 2010 on seitsemäs ja viimeisin Microsoftin julkaisema viestintä- ja kommunikointijärjestelmä pienille ja suurille organisaatioille. Ohjelmistolla on 15-vuotias historia. Exchange Server 2010 on toiminnoiltaan pääasiassa sähköposti-, kalenteri- ja osoitekirjajärjestelmä. Exchangessa käyttäjien tiedot tallennetaan palvelimelle, jolloin ne eivät ole työpistesidonnaisia ja työaseman rikkoutuessa, käyttäjä ei menetä tietojaan. Exchange Serverin kehityksessä on tehty merkittäviä muutoksia, jotka parantavat tietoturvaa, luotettavuutta, skaalautuvuutta, mobiilitoimintoja ja yhtenäisyyttä eri kommunikointimenetelmien välillä. (Morimoto, Noel, Amaris, Abbate & Weinhardt 2010, 5; Jarva 2008, 13.)

Käyttäjät pääsevät käsiksi Exchangen sähköpostilaatikoihin sähköpostiohjelmalla, mobiililaitteella tai selaimella. Kattavimman tuen Exchangelle sähköpostiohjelmista tarjoaa Microsoft Outlook, jonka kanssa Exchange on ensisijaisesti suunniteltu toimimaan. Outlook on ainoa, jolla on täysi MAPI-tuki. MAPI on rajapinta, joka mahdollistaa kommunikoinnin asiakasohjelman ja palvelimen välillä. Sillä voidaan käsitellä palvelimen tietovarastoja ja niiden asetuksia. (Jarva 2008, 17.)

Ensimmäinen julkaistu versio Exchange-sähköpostijärjestelmästä oli Exchange Server 4.0, joka julkaistiin 1996. Versionumero 4.0 johtuu aikaisemmista Microsoftin MS-Mail-sähköpostijärjestelmistä, jotka kuitenkin erosivat Exchange-järjestelmästä. Käyttöjärjestelmänä Exchange 4.0:lle toimi ”Microsoft Windows NT Server 3.51”. Exchange Server 4.0 oli suuri läpimurto ja organisaatiot aloittivat migraatiot MS-Mail-järjestelmistä. Suurin syy tähän oli, että Exchange Server 4.0 oli ensimmäisiä järjestelmiä, joilla voitiin lähettää helposti sähköpostia Internetin yli. (Morimoto ym. 2010, 6.)

Exchange Server 5.0 julkaistiin 1997, ja se oli suunniteltu toimimaan Windows NT 4.0 -käyttöjärjestelmässä, joka toi vakautta toimintaan. Exchange Server 5.0

tuki ensimmäistä Outlook-sähköpostiohjelmaa. Exchange Server 5.0 toi mukanaan sähköpostin, kalenterin ja osoitekirjan yhteenliittymän sekä Web-käyttöliittymän. Järjestelmä tuki aikaisempaa paremmin kolmansien osapuolten fax-järjestelmiä, ääniviestiohjelmistoja, tiedostojenjakotyökaluja ja jaettuja julkisia kansioita. (Morimoto ym. 2010, 7.)

Exchange Server 5.5 tuli markkinoille 1998. Siinä oli korjattu joitain aikaisemman version virheitä. Lisäksi sähköposti, kalenteri ja kontaktit olivat paremmin integroitu yhteen. Exchange 5.5 tuki aikaisempaa suurempaa sähköpostiviestien tietokantaa, jolloin se sopi paremmin suurille yrityksille. (Morimoto ym. 2010, 7.)

Exchange 2000 Server julkaistiin vuonna 2000, ja se vaati Windows 2000 Server -käyttöjärjestelmän alustakseen. Tämän version suurin muutos oli, että se käytti AD:ta sähköpostiosoitteiden säilyttämiseen ja yhdisti AD:ssa verkko- ja sähköpostitunnuksen yhdeksi tunnukseksi. Web-käyttöliittymää oli myös parannettu ja se oli muutettu pelkästä HTML-versiosta monipuolisemmaksi ActiveX-versioksi. Samaan aikaan Novell GroupWise -sähköpostijärjestelmän suosio laski dramaattisesti ja monet yritykset vaihtoivat Exchange 2000 -järjestelmään. (Morimoto ym. 2010, 8.)

Exchange Server 2003 -versio oli yhdistetty tiiviimmin AD:n kanssa, ja toimivuutta näiden välillä oli parannettu. Tämä tarjosi luotettavamman järjestelmän ja paremman suorituskyvyn. Exchange Server 2003 toi mukanaan tuen mobiililaitteille ja Web-käyttöliittymä oli muutettu muistuttamaan Outlook-näkymää. Lisäksi nyt voitiin Windows 2003 Server -alustalla tehdä neljän solmun klustereita aikaisemman kahden sijaan. Vuonna 2005 julkaistu Service Pack 1 toi Exchange Server 2003:lle tietokantojen virheentarkistuksen. (Morimoto ym. 2010, 9.)

Exchange Server 2007:ssä reititysryhmät katsottiin AD:n toimipaikkatiedoista. Aikaisemmin nämä tiedot olivat olleet erillään. Tässä versiossa Exchangen ”bridgehead”-palvelin oli korvattu Hub Transport -palvelimella, jonka kautta kaikki uloslähtevät ja sisääntulevat viestit kulkivat. Tämä mahdollisti viestien suodatuksen viesteille, joiden lähettäjä ja vastaanottaja sijaitsevat samalla palvelimella. Web-käyttöliittymää ja mobiilitukea oli parannettu aikaisemmasta versi-

osta. Lisäksi Exchange 2007:ssä tuli jatkuva replikointi, jolloin käyttäjien sähköpostitileistä oli aktiivinen ja passiivinen kopio. Kun aktiivisen kopion palvelin lakkaa vastaamasta, muuttuu passiivinen kopio aktiiviseksi ja sähköpostitiedot voidaan hakea sieltä. (Morimoto ym. 2010, 10.)

Uusin Exchange Server 2010 julkaistiin lokakuussa 2009. Sen tärkeimpiä uudistuksia olivat muun muassa tietokantatason klusterointi, palvelun korkea saatavuus, parempi suorituskyky, arkistointi, tuki tekstiviesteille ja parannettu virus- ja roskapostisuojaus. (Microsoft 2010.)

Erona aikaisempiin Exchange-versioihin on, että Exchange Server 2007- ja Exchange Server 2010 -sähköpostijärjestelmät koostuvat palvelimille asennettavista rooleista. Jokaisella näistä rooleista on oma tehtävänsä. Roolit voidaan asentaa sähköpostijärjestelmässä eri palvelimille, jolloin eri palvelimet erikoistuvat omaan tehtäväänsä. Näitä rooleja on Exchange 2010:ssä viisi: ”Edge Transport”, ”Hub Transport”, ”Client Access”, ”Mailbox” ja ”Unified Messaging”. (Morimoto ym. 2010, 26 - 27.)

2.2 Exchange 2010 -laitteistovaatimukset

Exchange Server 2010 toimii vain 64-bittisellä laitteistolla. Prosessoreina voidaan käyttää Intelin tai AMD:n x64-perheen prosessoreja, mukaan lukien AMD64 ja Intelin EM64T. Tärkein etu 64-bittisellä prosessorilla verrattuna 32-bittiseen on sen mahdollisuus osoittaa yli 4 Gt keskusmuistiin ilman osoitelaajennuksia. Tällöin keskusmuistiin voidaan tallentaa suurempi määrä dataa ja saada nopeampi datan käsittely. Lisäksi 64-bittinen prosessori voi käsitellä dataa ja suorittaa käskykantoja, jotka ovat kaksi kertaa suurempia verrattuna 32-bittiseen. Suurin hyöty näistä saadaan laskutoimituksissa, jotka vaativat suurta tarkkuutta. Suuria suorituskyvyn lisäyksiä saadaan suurella prosessorin välimuistilla, joten prosessorin L1-, L2- ja L3-muisteihin kannattaa kiinnittää huomiota. Mitä nopeampi ”Front side bus” -dataväylä prosessorin ja emolevyn välillä on, sitä nopeammin prosessori voi käyttää keskusmuistia. (Stanek 2010, 3 - 4.)

Sähköpostilaatikoiden kokojen kasvaessa on keskusmuistin tarve Exchange-palvelimilla lisääntynyt. Exchange Server 2010:n Mailbox-roolin omaava palvelin tukee maksimissaan 64 Gt:n keskusmuistia. Muiden roolien palvelimissa voi keskusmuistia olla enintään 16 Gt, ja jos samassa palvelimessa on useita rooleja, voi keskusmuistia olla 64 Gt. Kaikissa palvelimissa keskusmuistia tulee olla vähintään 2 Gt, mutta suorituskyvyn takia suositeltavaa olisi kuitenkin vähintään 4 Gt. Mailbox-palvelimella tulisi olla minimi 2 Gt:n lisäksi 5 Mt keskusmuistia jokaista sähköpostilaatikkoa kohden. Sivutustiedoston (Page file) koon tulisi olla vähintään yhtä suuri kuin palvelimen keskusmuistin. (Stanek 2010, 3; Jarva 2008, 13.)

Exchange Server 2010 tukee useampia identtisiä prosessoreja, mikä mahdollistaa huomattavan suorituskyvyn lisäyksen. Microsoft on kehittänyt Exchange Server 2010:n toimimaan tuplaydin- ja moniydinprosessoreilla. Prosessorien tai ytimien minimimäärä riippuu Exchange-palvelimen rooleista. Kuitenkin pienessä organisaatiossa yhden moniytimisen prosessorin pitäisi riittää. Keskisuuressa tai suuressa organisaatiossa, jossa on useampia toimialueita, on hyvä harkita useampia prosessoreja. Hinnan ja suorituskyvyn takia kaksi neljän ytimen prosessoria on suositeltavampi kuin yksi kahdeksan ytimen prosessori. Vaihtoehtoisesti työ voidaan jakaa myös eri palvelimille. (Stanek 2010, 4.)

Tiedontallennuskapasiteetti riippuu täysin datan määrästä, joka kulkee sähköpostijärjestelmän läpi, jää lokitiedostoihin tai tallentuu Exchange-palvelimille. Tilaa tarvitaan lokitiedostoille, työtilalle, järjestelmätiedostoille ja virtuaalimuistille. Kirjoitus- ja lukunopeus on yhtä tärkeää kuin tallennuskapasiteetti. Yhden suuren levyn sijasta on parempi käyttää useita levyjä, jolloin saadaan vikasietoisuutta RAID:n käyttöönotolla. Tietokoneen käynnistys- ja järjestelmälevyillä on hyvä käyttää RAID 1 -asetusta. Tällöin levyt peilataan ja yhden levyn vikaantuessa palvelin jatkaa toimintaansa. Kuitenkaan uusien korkean saatavuuden ominaisuuksien ansioista ei ole välttämätöntä käyttää RAID:a Exchange-datalle ja lokitiedostoille, koska nämä tiedot voivat sijaita usealla palvelimella. Myöskään kalliita tallennusjärjestelmiä ei välttämättä tarvitse käyttää, vaan voidaan sijoittaa useampia Exchange-palvelimia jokaiselle Exchange-roolille. Jos kuitenkin halutaan käyttää RAID:a, on datalle hyvä käyttää RAID 0- tai RAID 5

-konfiguraatiota ja lokitiedostoille RAID 1 -konfiguraatiota. RAID 0 -asetus antaa parhaimman suorituskyvyn, mutta on riskialtein. RAID 5 -asetus antaa hyvän suojan yhden levyn vikaantumisille, mutta kirjoitusnopeus heikkenee siinä. Kaikki levypartitiot, joita Exchange käyttää tulee formatoida käyttäen NTFS-tiedostojärjestelmää. (Stanek 2010, 4, 7.)

Exchange Server 2010 on suunniteltu säilyttämään aina tietokannan eheys, ja se voi palauttaa tietoja käyttäen tapahtumalokeja, vaikka virta katkeaisi ja palvelin sammuisi. Kuitenkin on tärkeää käyttää palvelimissa varavirtajärjestelmää, joka takaa virransyötön sähkön katketessa, koska virran katkeaminen voi vahingoittaa laitteistoa. (Stanek 2010, 5.)

2.3 Exchange 2010 -versiot ja ohjelmistovaatimukset

Exchange Server 2010 voidaan asentaa palvelimelle, joka käyttää Windows Server 2008 -palvelinkäyttöjärjestelmää ja johon on asennettu Service Pack 2, tai se voidaan asentaa palvelimelle, joka käyttää Windows Server 2008 Release 2 -versiota. Release 2 -versio on suositellumpi, koska se on näistä uudempi. (McBee & Elfassy 2010, 32.)

Exchange 2010 -sähköpostijärjestelmästä on saatavissa Standard- ja Enterprise-versiot. Nämä versiot tukevat samoja ydinominaisuuksia ja hallintatyökaluja. Standard-versio on suunniteltu tarjoamaan oleelliset viestipalvelut pienelle tai keskisuurelle organisaatiolle ja sivutoimistoille. Se tukee kuitenkin vain rajoitettua määrää tietokantoja. Enterprise-versio on suunniteltu tarjoamaan oleelliset viestipalvelut, paremman palvelunsaatavuuden, luotettavuuden ja hallittavuuden organisaatiolle. Enterprise-versio tukee sataa tietokantaa kyseisellä palvelimella, johon se asennetaan. Samaa ohjelmakooditiedostoa käytetään kummassakin versiossa, mutta lisenssikoodi määrittää, kumpi versio tulee voimaan. Standard-versio voidaan päivittää Enterprise-versioon vaihtamalla lisenssikoodi. Mailbox-palvelimessa lisenssikoodin vaihdon jälkeen tulee kuitenkin käynnistää ”Microsoft Exchange Information Store-palvelu” uudestaan, jotta muutokset tulevat voimaan. (Stanek 2010, 6.)

Exchange Server 2010 vaatii, että palvelimelle on asennettu versio 3.0 tai uudempi ”Microsoft Management Console” -hallintakonsolista. Lisäksi palvelimelle tulee olla asennettuna ”Microsoft .NET Framework” -ohjelmistokomponenttikirjastosta versio 3.5.1. ”Exchange Management Shell” -hallintakonsoli ja Exchangen etähallinta tarvitsevat ”Windows PowerShell” -komentotulkista version 2.0. Jos halutaan hallita Exchange-palvelinta työpisteiltä, tarvitaan ”Windows Management Framework” -komponenttikirjasto, joka sisältää ”WinRM 2.0”- ja ”PowerShell 2.0” -palvelut. Komentoja varten PowerShell tulee ajaa Windows pääkäyttäjä -tilassa riittävien oikeuksien saamiseksi. (Stanek 2010, 7.)

2.4 Exchange 2010 ja Windows-ympäristö

Exchange Server 2010 ja Forefront Protection -suojaohjelmisto tekevät laajoja muutoksia palvelinkäyttöjärjestelmän ympäristöön, kun ne asennetaan. Nämä muutokset sisältävät uusia järjestelmäpalveluja, integroidun autentikoinnin ja uusia turvaryhmiä. (Stanek 2010, 11.)

Exchange Server 2010 tallentaa sähköpostiosoitteet, jakeluryhmät ja muut hakemistoresurssit hakemistotietokantaan AD:ssa. Kun käytössä on useita toimialueen ohjauspalvelimia, ne automaattisesti replikoivat hakemistotiedot keskenään käyttäen ”multimaster replication” -mallia. Tällöin Exchangen tiedot tallennetaan kaikille AD-palvelimille. (Stanek 2010, 14.)

Kun Exchange Server 2010 asennetaan Windows-toimialueelle, asennus tekee päivityksiä ja laajennuksia AD:hen, jotka sisältävät objekteja ja attribuutteja, joita Exchange käyttää. Toisin kuin Exchange Server 2003 -versiossa, tämä prosessi ei tee muutoksia ”Active Directory Users & Computers” -työkaluun eikä sitä käytetä sähköpostilaatikoiden hallintaan, sähköpostiosoitteisiin eikä viestienlähetysominaisuuksiin tai asetuksiin. Nämä tehtävät tehdään käyttäen ”Exchange Management” -työkalua. (Stanek 2010, 15.)

Exchange Server 2010 tukee täysin Windows Server -turvamallia ja luottaa tähän turvamekanismiin kontrolloidessaan pääsyä hakemistoresursseihin. Tämä tarkoit-

taa, että standardi Windows Server -oikeuksien kautta voidaan kontrolloida pääsyä sähköpostilaatikoihin, jäsenyyttä jakeluryhmissä ja suorittaa muita Exchange turvaan liittyviä ylläpitotehtäviä. Esimerkiksi käyttäjän lisääminen jakeluryhmään tapahtuu lisäämällä käyttäjä jäseneksi jakeluryhmän objektiin AD:ssa ”Active Directory Users & Computers” -työkalulla. (Stanek 2010, 15.)

Koska Exchange palvelin käyttää Windows Server -turvatoimia, ei sähköpostilaatikoita voida luoda ilman, että ensin luodaan käyttäjä, joka käyttää sähköpostilaatikkoa. Jokainen sähköpostilaatikko tulee liittää verkkotunnukseen, jopa ne joita Exchange käyttää yleisiin viestitehtäviin. ”Exchange Management” -hallintakonsolissa voidaan kuitenkin luoda uusi käyttäjä osana uuden sähköpostilaatikon luontia. (Stanek 2010, 15.)

2.5 Exchange 2010 ja Active Directory

Active Directory on Microsoftin toteutus hakemistopalveluista. AD sisältää tietokannan ja tarjoaa palvelut, joilla käyttäjät ja ohjelmat pääsevät tietokantaan käsiksi. AD:n tehtävänä on vähentää ylläpidettävien hakemistojen määrää, koska yhtenäisillä rajapinnoilla ja työkaluilla voidaan suorittaa esimerkiksi käyttäjätilien, tietokonetilien ja jaettujen resurssien hallinta. (Kivimäki 2005, 1.)

Exchange Server 2010 on kiinteästi integroitu AD:hen ja tarvitsee toimiakseen luotettavat ja oikein konfiguroidut AD-palvelut. Exchange 2010 ei ainoastaan käytä AD:ta tiedon tallentamiseen ja katso käyttäjien sähköpostiosoitteita sieltä, vaan se käyttää myös sen reititystopologiaa päättämään, kuinka viestit reititetään organisaatiossa. AD tarjoaa Exchangelle myös autentikointipalveluja. Kun viesti saapuu Internetistä, tarkastetaan AD:sta, löytyykö vastaanottajaa organisaatiosta. Jos sitä ei löydy, viesti eristetään tai poistetaan eikä sitä jouduta käsittelemään. (Stanek 2010, 17 - 18; Morimoto ym. 2010, 80, 150.)

AD ja Exchange Server ovat riippuvaisia DNS-palvelusta, joka muuttaa verkkonimet IP-osoitteiksi ja päinvastoin. Suositeltuna tapana on asentaa DNS-nimipalvelu AD-palvelimelle. Tämä mahdollistaa DNS-tietojen tallentamisen

AD:hen useina kopioina. Muitakin kuin Microsoftin DNS-palvelua voidaan käyttää, mutta se ei ole suositeltua. (Morimoto ym. 2010, 91.)

AD-metsässä, johon Exchange 2010 asennetaan, tulee ohjauspalvelimen (Schema Master) käyttää Windows Server 2003 -käyttöjärjestelmää tai uudempaa. Tämä ohjauspalvelin ylläpitää metsän laajuisesti AD:n skeemaa (Schema) eli mallia, joka määrittelee objektien ja attribuuttien muodon. Metsäksi kutsutaan useamman toimialueen muodostamaa ryhmää. AD:n tulee olla vähintään Windows Server 2003 -metsä toimintatilassa ja AD-toimipaikalla tulee olla vähintään yksi ”Global Catalog” -palvelin, joka käyttää Windows Server 2003 -versiota tai myöhempää. ”Global Catalog” -palvelimella on tietokanta kaikista metsän toimialueiden objekteista oman toimialueensa tietojen lisäksi. AD-metsien välillä, joihin Exchange on asennettu, pitää olla luottosuhde. Tällöin voidaan Exchange-resursseja jakaa toimialueiden kesken. Verkkotunnuksen tulisi olla konfiguroitu käyttämään usean nimen (multiple-label) DNS-nimiä. (Morimoto ym. 2010, 26 - 27; Stanek 2010, 7; Kivimäki 2005, 6,71; Jarva 2008, 10.)

Exchange tallentaa neljän tyyppistä dataa AD:hen. Näitä ovat skeemadata, konfiguraatiotiedot, toimialuetiedot ja ohjelmistotiedot. Jokainen näistä tallennetaan omaan tiettyyn osioonsa. Skeemasäännöt päättävät, minkä tyyppisiä objekteja on saatavilla ja mitä arvoja niillä on. Kun Exchange asennetaan AD-metsään, AD:n valmisteluprosessi lisää monia Exchange-objektiluokkia ja attribuutteja skeemaosioon. Tämä mahdollistaa Exchange-objektien kuten välittäjien (agent) ja liittimien (connector) luonnin. Se myös mahdollistaa aikaisempien objektien kuten käyttäjien ja ryhmien laajentamisen uusilla attribuuteilla, jotka voivat esimerkiksi sallia olemassa olevan käyttäjän lähettää ja vastaanottaa sähköpostia. Jokaisella ohjauspalvelimella ja Global Catalog -palvelimella on täydellinen kopio skeemasta. (Stanek 2010, 17 - 18.)

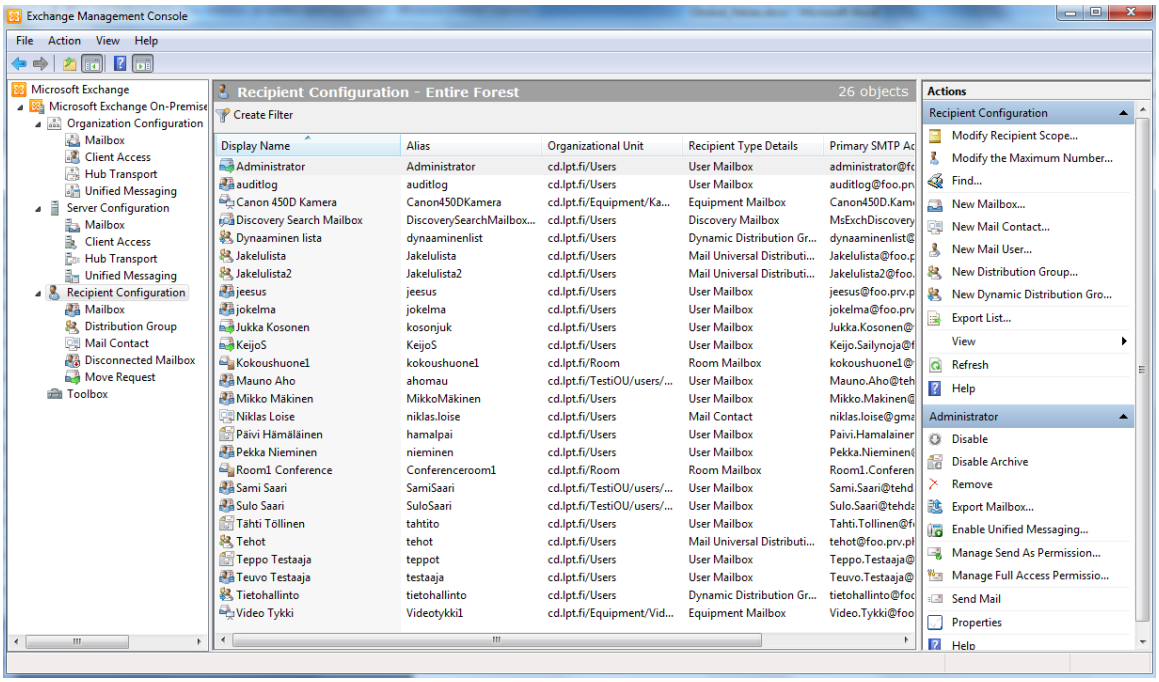
Ensimmäisen Exchange-palvelimen asennuksessa AD-metsään Exchangen konfigurointitiedot luodaan ja tallennetaan AD:n konfiguraatio-osioon. Nämä tiedot kuvaavat hakemiston rakennetta. Konfigurointisäilö (container) sisältää kaikki toimialueet, puut, metsät, ohjauspalvelimet ja Global Catalog -palvelimet.

Exchangelle nämä konfigurointitiedot kuvaavat organisaation rakennetta. Konfigurointisäilö pitää sisällään listan malleja (template), sääntöjä ja muita organisaatiotason tietoja. (Stanek 2010, 18.)

2.6 Exchange 2010 -palvelimien hallinta

Exchange Server 2010 tarjoaa erityyppisiä hallintatyökaluja. Näistä tärkeimpiä ovat graafinen hallintatyökalu ”Exchange Management Console” ja komentotulkki ”Exchange Management Shell”. Exchange Server 2010:n graafinen hallintakonsoli on uusittu ja hallinta on aikaisempaa yksinkertaisempaa. Ominaisuudet löytyvät konsolista lisäksi aiempaa helpommin. Exchange Server 2010:n komentotulkki tarjoaa tehokkaan vaihtoehdon hallintaan ja sillä voidaan tehdä monimutkaisempia toimintoja kuin graafisella hallintatyökalulla. Se myös helpottaa ylläpitäjän työtä mahdollistamalla toimintojen automatisoinnin. (McBee & Elfassy 2010, 31.)

Hallintatyökaluihin pääsee valitsemalla Windowsin käynnistysvalikosta Microsoft Exchange Server 2010 -valikon. Kuviossa 1 on näkymä Exchangen graafisesta hallintatyökalusta, jolla voidaan tehdä muun muassa sähköpostilaatikoiden hallinta. (Stanek 2010, 19.)



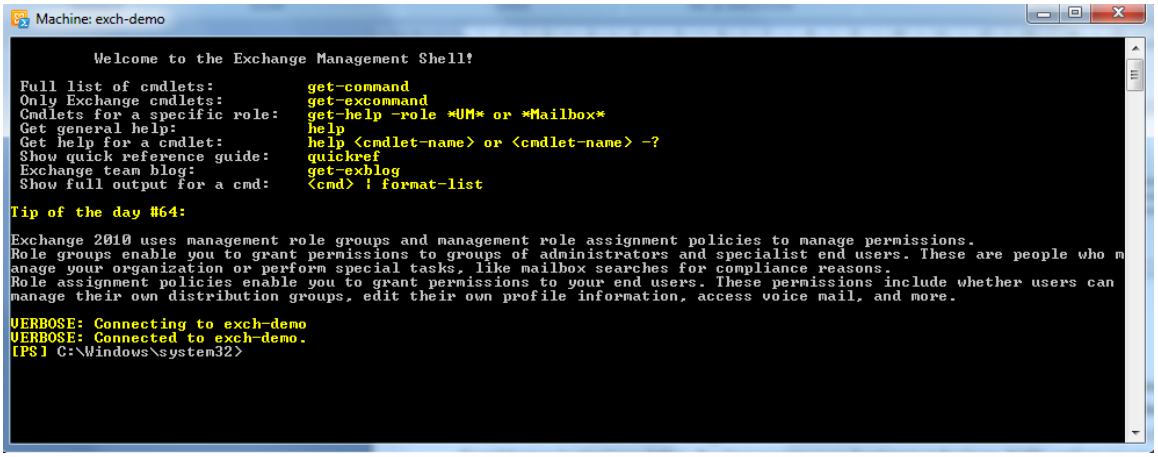
KUVIO 1. Exchange Management -hallintakonsolin näkymä

Exchange Management -konsolin työkaluvalikosta löytyy seuraavat hallintatyökalut:

- Best Practices Analyzer
- Details Templates Editor
- Mail Flow Troubleshooter
- Message Tracking
- Performance Monitor
- Performance Troubleshooter
- Public Folder Management Console
- Queue Viewer
- Remote Connectivity Analyzer
- Role-Based Access Control User Editor
- Routing Log Viewer
- Tracking Log Explorer.

Hallintatyökaluilla voidaan muun muassa tutkia viestijonoja, reititystopologiaa, viestien kulkua, tutkia suorituskykyongelmia, testata yhteyksiä ja tarkastaa Exchange-organisaation kunto (Stanek 2010, 20 - 21).

Komentoriviltä voidaan automatisoida asennuksia, hallintaa tai ylläpitoa komentosarjoilla. Kuviossa 2 näkyvä ”Exchange Management Shell” on laajennus ”Windows PowerShell” -komentorivityökaluun ja tarjoaa laajan määrän sisäänrakennettuja komentoja Exchange-palvelimien kanssa työskentelemiseksi. (Stanek 2010, 22.)



KUVIO 2. Näkymä Exchange Management Shell komentorivistä

Esimerkiksi komennolla ”get-command” nähdään lista kaikista käytössä olevista komennoista ja komennolla ”get-excommand” nähdään kaikki Exchange-komennot. Antamalla komennon alkuun ”help” saadaan tietoja kyseisestä komennosta. (Stanek 2010, 23.)

2.7 Roskapostinsuodatus ja virustentorjunta

Exchange Server 2010 sisältää erilaisia roskapostinsuodatus- ja viruksentorjunta-ominaisuuksia. Näitä ovat yhteydensuodatus, joka mahdollistaa IP-listat, joilla voidaan estää tai sallia yhteydet. Sisällönsuodatus käyttää älykkäitä suodattimia viestien sisällön tarkistamiseen ja roskapostin tunnistamiseen. Roskaposti voidaan automaattisesti poistaa, eristää tai kansioida roskapostiksi. ”IP reputation” -palvelu tarjoaa Exchange-asiakkaille Microsoftin toimittaman IP-estolistan, jonka avulla ei-toivotut lähettäjät karsitaan. Outlook-roskapostisuodatuslistojen yhdistäminen mahdollistaa käyttäjien omien roskapostisuodatuslistojen levittämisen Exchange-palvelimille. Vastaanottajasuodatus mahdollistaa ylläpitäjien monistaa vastaanottajien tiedot ”Edge Transport” -palvelimelle. Tämä palvelin voi sitten

verrata näitä tietoja vastaanotettavien viestien tietoihin ja estää viestit, jotka ovat käyttäjille, joita ei ole olemassa. Tämä estää tietyn tyyppiset hyökkäykset ja vihamieliset tiedonkalastelut. Lähettäjän henkilöllisyyden varmistaminen tarkastaa, että tulevat sähköpostiviestit ovat Internet-toimialueelta, josta väittävät tulevansa. Exchange tarkistaa tämän tutkimalla lähettäjän IP-osoitteen ja vertaamalla sitä lähettäjän julkisiin DNS-tietoihin. Lähettäjien pisteyttäminen auttaa päättämään tuntemattoman lähettäjän luotettavuuden käyttämällä lähettäjän henkilöllisyyden tarkistusta, tutkimalla viestin sisällön ja tutkimalla lähettäjän aikaisemman käyttäytymishistorian. Lähettäjä voidaan näiden tulosten perusteella tarvittaessa lisätä väliaikaisesti estolistalle. (Stanek 2010, 10.)

Vaikka nämä haittaohjelma- ja roskapostinsuodatusominaisuudet ovat laajat, tulee kattavan virustorjuntasuojan saamiseksi asentaa ”Forefront Protection for Exchange Server”. Se auttaa suojautumaan viruksilta, madoilta ja muilta haittaohjelmilta käyttäen sähköpostiviesteihin useita skannaustekniikoita ja tiedostosuodatusta. Forefront tarjoaa suojan Exchange-palvelimille, joilla on Mailbox-, Hub Transport- tai Edge Transport -rooli. Client Access- ja Unified Messaging -palvelimille sitä ei tarvita, koska suodatus suoritetaan muilla palvelimilla. (Stanek 2010, 10 - 11.)

3 EXCHANGE SERVER 2010 -PALVELINROOLIT

3.1 Arkkitehtuuri ja palvelinroolit

Ennen Exchange Server 2010:n hankkimista tulisi huolellisesti suunnitella organisaation viestitysarkkitehtuuri. Jokaisella Exchange-toteutuksella on arkkitehtuurissaan kolme kerrosta. Näitä ovat verkkokerros, hakemistokerros ja viestikerros. Toteutuksen suunnittelussa pitää tarkastella, mitä rooleja palvelimille annetaan ja valita laitteisto tämän mukaan. (Stanek 2010, 25 - 26.)

Verkkokerros tarjoaa pohjan tietokoneiden väliselle kommunikoinnille ja oleelliset nimenselvitys ominaisuudet. Verkkokerroksella on sekä fyysisiä että loogisia komponentteja. Fyysiset komponentit pitävät sisällään IP-osoitteen, IP-aliverkon, palomuurit sekä LAN- tai WAN-linkit, joita viestitysjärjestelmä ja reitittimet käyttävät. Loogiset komponentit ovat DNS-alueita, jotka määrittävät nimeämisrajat ja sisältävät oleelliset tiedot nimenselvitykselle. (Stanek 2010, 25.)

Hakemistokerros tarjoaa tarpeellisen perustan autentikoinnille, valtuuttamiselle ja replikoinnille. Hakemistokerros on rakennettu AD-hakemistopalvelulle ja sillä on fyysisiä ja loogisia komponentteja. Fyysiset komponentit pitävät sisällään ohjauspalvelimet, Global Catalog -palvelimet ja toimipaikkalinkit. Näitä käytetään autentikointiin, valtuutuksiin ja replikointiin. Loogiset komponentit pitävät sisällään AD-metsät, toimipaikat, toimialueet ja organisaatioyksiköt. Näitä käytetään ryhmittelemään objektit resurssien jakamiseksi, hallinnan keskittämiseksi ja replikoinnin kontrolloimiseksi. Loogiset komponentit pitävät sisällään myös käyttäjät ja ryhmät, jotka ovat osana AD-rakennetta. (Stanek 2010, 25.)

Viestikerros tarjoaa perustan viestitykselle ja yhteistyölle. Sillä on fyysisiä ja loogisia komponentteja. Fyysiset komponentit pitävät sisällään yksilölliset Exchange-palvelimet, jotka päättävät miten viestit toimitetaan. Lisäksi ne pitävät sisällään viestiyhdistimet (mail connectors), jotka päättävät kuinka viestit reititetään Exchange-palvelimien rajojen ulkopuolelle. Loogiset komponentit määrittelevät organisaation rajat viestien lähettämiselle, sähköpostilaatikoille, julkisille kansi-

oille ja jakelulistoille. Sähköpostilaatikoissa säilytetään sähköpostiviestit ja julkisessa kansiossa säilytetään dataa sekä jakelulistoja, joita käytetään viestien välittämiseen usealle käyttäjälle. (Stanek 2010, 26.)

Viestikerroksessa määritellään ja asetetaan Exchange-palvelinroolit. Rooleja voivat olla ”Mailbox Server”, ”Client Access Server”, ”Unified Messaging Server”, ”Hub Transport Server” ja ”Edge Transport Server”. Mailbox Server on järjestelmän perällä oleva palvelin ja on isäntänä sähköpostilaatikoille, julkisille kansioille ja niihin liittyvälle viestidatalle, kuten sähköpostilistoille, resurssien aikatauluille ja tapaamisille. Korkean saatavuuden saavuttamiseksi voidaan Exchange-järjestelmässä käyttää useita Mailbox-palvelimia, jotka on liitetty DAG-tietokantaryhmään. (Stanek 2010, 27.)

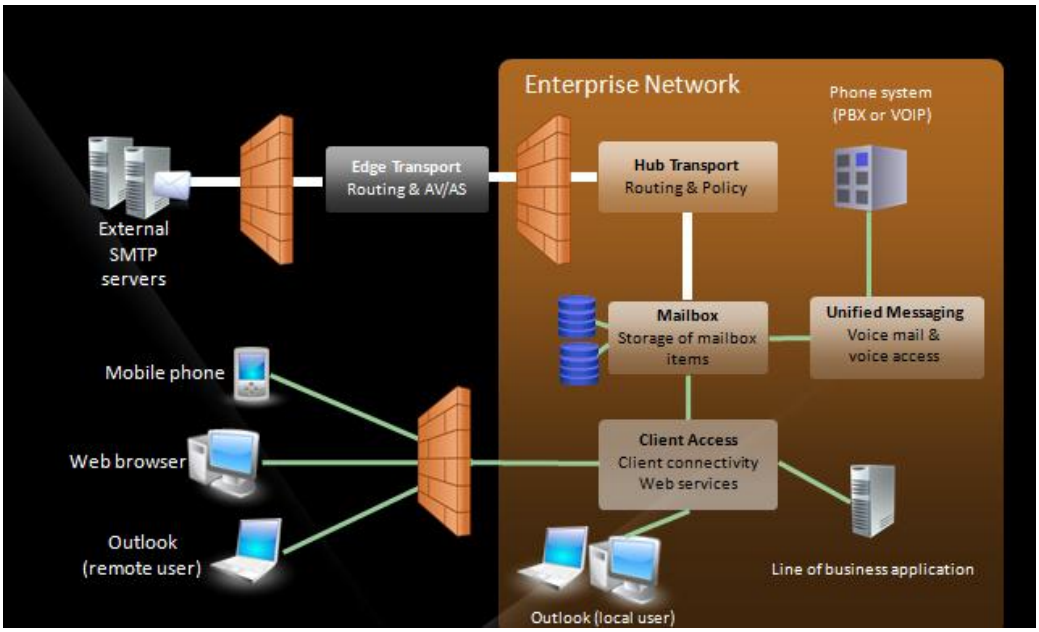
Client Access -palvelin sijaitsee tietokannan ja käyttäjän välissä ja vastaanottaa yhteyksiä Exchange-järjestelmään käyttäjiltä (KUVIO 3). Se on isäntänä protokollille, joita käyttäjät käyttävät viestien vastaanottamiseen ja lähettämiseen. Lähiverkossa Outlook MAPI -käyttäjät ottavat yhteyttä suoraan Client Access -palvelimeen. Etäkäyttäjät voivat tarkistaa viestinsä Internetin yli käyttämällä ”Outlook Anywhere”-, ”Outlook Web App”-, ”Exchange ActiveSync”-, POP3- tai IMAP4-palveluja. (Stanek 2010, 27.)

Unified Messaging -palvelin sijaitsee PBX-järjestelmän ja tietokannan välissä ja integroi PBX-järjestelmän Exchange-järjestelmään (KUVIO 3). Unified Messaging mahdollistaa ääniviestien, faksien ja sähköpostitoimintojen integroimisen niin, että data voidaan tallentaa käyttäjien sähköpostilaatikoihin. Jotta Unified Messaging -rooli voidaan ottaa käyttöön, organisaatiossa tulee olla PBX-järjestelmä, joka on yhdistetty lähiverkkoon. Unified Messaging -palvelin vastaa puheluihin vastaamisesta, faksien vastaanottamisesta ja puhelinpalveluihin pääsystä. (Stanek 2010, 27, 36.)

Hub Transport Server on reitityspalvelin, joka hoitaa viestien liikkumisen, reitityksen ja välittämisen Exchange-organisaatiossa. Se käsittelee kaikki viestit, jotka lähetetään organisaation sisällä ennen kuin viesti välitetään sähköpostilaatikkoon organisaatiossa tai reititetään ulos organisaatiosta. Käsittely varmistaa, että lähet-

täjät ja vastaanottajat selvitetään ja suodatetaan, viesti suodatetaan, viestin muoto tarvittaessa muutetaan ja liitetiedostot tarkastetaan. Hub Transport -palvelin voi myös tallentaa tai lokikirjata viestit ja lisätä niihin vastuunvapautuslausekkeen. (Stanek 2010, 27.)

Edge Transport Server on lisäreitityspalvelin, joka reitittää viestit organisaatioon ja sieltä ulos. Se on suunniteltu sijoitettavaksi organisaation eteisverkkoon ja sitä käytetään luomaan turvallinen raja organisaation ja Internetin välille (KUVIO 3). Palvelin vastaanottaa viestejä Internetistä ja luotetuilta palvelimilta ulkopuolisilta organisaatioilta. Tämän jälkeen se käsittelee viestit ruoskapostien ja virusten varalta ja reitittää hyväksytyt viestit organisaation sisällä olevalle Hub Transport -palvelimelle (KUVIO 3). (Stanek 2010, 27.)



KUVIO 3. Exchange 2010 -arkkitehtuuri (Microsoft TechNet 2009)

Nämä viisi roolia ovat Exchange-organisaation rakennuspalikoita. Taulukko 1 näyttää tuettujen prosessoriytimien määrän palvelimille rooleittain. Käytettävät prosessorit voivat olla yksi- tai moniytimisiä. (Stanek 2010, 27.)

TAULUKKO 1. Prosessoriytimien määrät Exchange Server 2010 -palvelimille rooleittain

Palvelinrooli	Minimi	Suositus	Maksimi suositus
Edge Transport	1	4	12
Hub Transport	1	4	12
Client Access	2	8	12
Unified Messaging	2	4	12
Mailbox	2	8	12
Useita palvelinrooleja	2	8	16

Kaikki roolit paitsi Edge Transport -palvelinrooli voidaan asentaa yhdelle palvelimelle. Yksinkertaisin pienen yrityksen Exchange-organisaatio voi muodostua yhdestä palvelimesta, jolla on Mailbox-, Client Access- ja Hub Transport -roolit. Lisätietoturvan saamiseksi voidaan lisätä Edge Transport -palvelin. Käyttämällä kuitenkin useampia palvelimia pienessäkin yrityksessä saadaan korkeampi saatavuus palveluille. (Stanek 2010, 28.)

Exchange Server 2010:n ominaisuudet ja toiminnot sopivat kaiken kokoisiin yrityksiin. Exchange 2010 skaalautuu pienistä yrityksistä suuriin, tuhansien käyttäjien ja useiden palvelimien järjestelmiin. Suuressa Exchange-organisaatiossa yksittäinen palvelin tai palvelinklusteri omistetaan yleensä vain yhdelle roolille. Pienissä ja keskisuurissa yrityksessä eri rooleja voi olla samalla palvelimella ja vain Edge Transport -roolin tulee olla omalla palvelimellaan. Yhden Exchange-palvelimen järjestelmä voi helposti palvella jopa satoja käyttäjiä. (Morimoto ym. 2010, 94. 100.)

Laitteistokonfiguraatiot voivat vaihdella hyvin paljon riippuen palvelinrooleista ja järjestelmän käyttömäärästä. Järjestelmän suunnittelussa olisi hyvä käyttää Microsoftin suosituksia ja suunnitella järjestelmä maksimikäyttömäärälle ja varata tilaa myös kasvulle. Käytettävien prosessorien kellotaajuuden tulisi olla vähintään 1,6 GHz. Neljä prosessoriydintä riittää Hub Transport -palvelimelle, jolla siirretään noin 1000 viestiä tunnissa. Kaksi prosessoriydintä Client Access -palvelimella riittää palvelemaan muutamaa sataa käyttäjää. Yksi prosessoriydin riittää Mailbox-palvelimella aina noin 1000 postilaatikolle. Exchange-palvelimien

verkkoyhteyksien tulisi olla nopeudeltaan vähintään 1 Gb/s. (McBee & Elfassy 2010, 319 - 326.)

Mailbox-palvelimille voidaan konfiguroida automaattinen vikaantumissuoja asettamalla Mailbox-palvelimet samaan DAG-ryhmään. Client Access -palvelimille voidaan laittaa kuormantasaus ja vikaantumissuoja asettamalla Client Access -palvelimet jäseniksi samaan Client Access -tauluun (Client Access Array). Jokainen jäsen pystyy tarjoamaan Outlook MAPI-, POP3-, IMAP4-, Outlook Anywhere-, Outlook Web App- ja Exchange ActiveSync -palveluja. Client Access -taululla voidaan luoda jopa 32 palvelimen kuormatasattuja ryhmiä. Palvelimet, jotka kuuluvat ryhmään, eivät voi pitää samanaikaisesti Mailbox-roolia. Yli kahdeksaa Client Access -palvelinta ei suositella, jos käytetään ”Network Load Balancing” -palvelua. (Stanek 2010, 28.)

Exchange Server 2010 -asennusohjelmaa voidaan käyttää roolien ja Exchange Management -työkalujen asentamiseen, niiden poistamiseen sekä komponenttien ylläpitoon. Organisaation AD- ja DNS-asetukset tulee olla konfiguroituna ennen Exchange-asennusta. Jotta asiakkaiden pääsy järjestelmään onnistuu, tulee jokaisessa AD-toimipaikassa, jossa on Mailbox-palvelin, olla vähintään yksi Client Access -palvelin. (Stanek 2010, 50 - 51.)

3.2 Mailbox-palvelin

Mailbox-palvelimen toiminta muistuttaa tietokantapalvelimien toimintaa. Jokaisella käyttäjällä on sähköpostilaatikko, jota käytetään viestitysdatan tallentamiseen. Toisiinsa liittyvät sähköpostilaatikot organisoidaan käyttäen tietokantoja, ja jokaisella tietokannalla voi olla yksi tai useampi kopio. Korkean saatavuuden saamiseksi ei tarvita erillistä klusterointilaitteistoa, vaan siihen riittää DAG-ryhmän luominen. Koska Exchange Server 2010 -tietokannat ovat organisaatiotasolla, ne voidaan helposti siirtää palvelimelta toiselle. Tietokantojen nimien tulee olla organisaatiossa yksilöllisiä. Mailbox-palvelimien, jotka sijaitsevat samassa DAG-ryhmässä, ei tarvitse eivätkä ne saa jakaa samaa tallennustilaa. Kuitenkin täyden hakemistopolun tulee olla identtinen kaikilla tietokantakopioilla. Julkisia

kansioita voidaan pitää Mailbox-palvelimilla, jotka kuuluvat DAG-ryhmään, mutta nämä kansiot eivät voi olla osana ryhmää. Niistä ei voida myöskään tehdä kopioita. (Stanek 2010, 29 - 30.)

Mailbox-palvelimen tarvitsema tallennuskapasiteetti riippuu sähköpostilaatikoiden määrästä ja koosta, joita palvelimen pitää isännöidä. Esimerkiksi palvelimelle joka ylläpitää 2500 sähköpostilaatikkoa joiden kokorajoitus on 2 Gt, tulee sähköpostilaatikoille varata vähintään 5 Tt tilaa käyttöjärjestelmän ja Exchangen tarvitseman tilan lisäksi. Mitä enemmän sähköpostilaatikoita on tallennettu levylle tai levyryhmälle sitä enemmän luku- ja kirjoitusoperaatioita suoritetaan ja mahdollinen viive kasvaa. Jokaisella tietokannalla on omat tapahtumalokitiedostonsa. Suorituskyvyn parantamiseksi voidaan sähköpostilaatikoille käyttää useampia tietokantoja. On myös kannattavaa tallentaa eri tietokannat yhdessä niiden tapahtumalokien kanssa eri levyille. Joissain tilanteissa voidaan myös haluta tallentaa tietokannat ja tapahtumalokit eri levyille. (Stanek 2010, 31 - 32.)

64-bittinen arkkitehtuuri mahdollistaa tietokantojen välimuistin olevan jopa 90 % RAM-muistista. Suuri keskusmuisti lisää mahdollisuutta, että käyttäjän hakema tieto tarjotaan nopeasta keskusmuistista hitaamman levyjärjestelmän sijaan. Exchange 2010 voi suorittaa 1024 kt:n kokoisia luku- ja kirjoitusoperaatioita Exchange 2003:n 64 kt:n sijaan. Tämä lisää mahdollisuutta lukea ja kirjoittaa suuremmilla yksittäisillä luku- tai kirjoitusoperaatioilla, jolloin operaatioita tarvitaan vähemmän. Exchangen tietokantojen sivutustiedoston koko on nostettu aikaisemmista versioista 32 kilotavuun, joka vähentää luku- ja kirjoitusoperaatioita. (Stanek 2010, 31 - 32.)

Ennen Exchange 2010 Mailbox-roolin asentamista tulee palvelinkäyttöjärjestelmään asentaa ”Active Directory remote management” -työkalu. Tämä voidaan tehdä PowerShell -komennolla ”Add-WindowsFeature -name RSAT-ADDS -restart”. Lisäksi tulee asentaa ”Microsoft. NET Framework 3.5.1”, ”Windows PowerShell 2.0”, ”WINRM 2.0”, ”IIS Web Server, Basic Authentication”, ”Windows Authentication”, ”IIS 6 Metabase Compatibility” ja ”IIS 6 Management Console”. Microsoft Office dokumenttien indeksoimiseksi tulee asentaa ”2007 Office System Converter: Microsoft Filter Pack”. (Stanek 2010, 31 - 32.)

3.3 Client Access -palvelin

Client Access -palvelimet hoitavat kaikki käyttäjiin liittyvät viestitehtävät. Niiden toiminta on samankaltaista kuin ohjelmistopalvelimilla, jotka käyttävät laajasti Web-palveluja. Koska paikalliset ja etäkäyttäjät ottavat yhteyden Client Access -palvelimiin tekevät ne paljon luku- ja kirjoitusoperaatioita. Tämä tarkoittaa, että prosessointikyky, muisti, verkkoyhteys ja tallennuslevy ovat potentiaalisia pullonkauloja. Client Access -palvelimet suorittavat sisällön muuttamista käyttäjille muodosta toiseen TMP-kansiossa. Suorituskykyä saadaan lisää asettamalla tämä kansio eri fyysiselle levylle kuin käyttöjärjestelmä ja sivumuisti. (Stanek 2010, 33.)

Client Access -palvelimet tarjoavat pääsyn Outlook MAPI-, IMAP4-, POP3- ja HTTP-verkkoprotokollilla. Ne voivat vastaanottaa pyyntöjä lähiverkosta tai Internetistä. Paikallinen pääsy voidaan suorittaa käyttäen Outlook MAPI -rajapintaa. Etäkäyttö voidaan suorittaa käyttäen Outlook Anywhere-, Outlook Web App- tai Exchange ActiveSync -palveluja. IMAP4 ja POP3 ovat vaihtoehtoina standardi protokollille. Client Access -palvelimet tarjoavat vapaa/varattu-tiedot käyttäen Availability-palvelua. Ne mahdollistavat myös käyttäjien ladata automaattisesti Outlookin konfiguraatiot Autodiscover-palvelulla. (Stanek 2010, 33 - 34.)

Exchange 2010:ssä Outlook MAPI -käyttäjien verkon yli tehtävät yhteydet eli RPC-proseduurikutsut tehdään suoraan Client Access -palvelimen MAPI RPC -rajapintaan. HTTP-yhteydet tehdään Client Access -palvelimen RPC Proxy -komponenttiin. Client Access -palvelin kommunikoi tämän jälkeen sopivan Mailbox-palvelimen kanssa. (Stanek 2010, 33.)

Client Access -taulu tarjoaa kuormantasauksen ja vikatilanteista toipumisen ominaisuuksille, jotka liittyvät käyttäjien pääsyyn palveluun. Palvelimet, jotka ovat taulussa, eivät voi samalla pitää Mailbox-roolia. Jokaisella taululla on oma verkkotunnuksensa. Kun jokin palvelin pettää, ottavat muut palvelimet sen tehtävät muutamissa sekunneissa. Palvelimen pystyessä taas toimimaan, liittyy se automaattisesti tauluun mukaan. Kun taulu on käytössä, tulisi ulkoisten URL-osoitteiden viitata taulun yhteiseen verkkotunnukseen, jotta ominaisuudet toimisi-

vat. Kuormanjako käyttää ”Windows Load Balancing” -palvelua. Kuormantasauksessa voidaan käyttää myös laitteistoratkaisua. (Stanek 2010, 34.)

3.4 Hub Transport- ja Edge Transport -palvelimet

Hub Transport- ja Edge Transport -roolit ovat samankaltaisia. Kumpaakin käytetään viestin reitittämiseen, ja molemmilla on samantyylisiä suodattimia organisaation suojaamiseksi viruksilta ja roskapostilta. Tärkeimpänä erona näillä rooleilla on niiden sijoitus. Hub Transport -palvelin asetetaan sisäverkkoon ja se konfiguroidaan organisaation toimialueen jäseneksi. Edge Transport -palvelin taas sijoitetaan organisaation reunaverkkoon eikä sitä konfiguroida toimialueen jäseneksi. Palvelimelle, jolle asennetaan jompikumpi näistä rooleista, ei saa asentaa SMTP- tai NNTP-palveluja, koska Exchange ei tue NNTP-palveluja ja Exchangen asennuksessa asennetaan oma parannettu SMTP-palvelu. Vaikka Edge Transport -palvelin sijoitetaan AD-metsän ulkopuolelle, tulee sillä olla toimialueen pääte ja sen tulee kyetä selvittämään kaikkien Hub Transport -palvelimien IP-osoitteet niiden verkkotunnuksista. (Stanek 2010, 37; Posey 2007.)

Transport-palvelimet säilyttävät kaikki vastaanotetut viestit tietokannassa, kunnes kaikki hypyt viestille on suoritettu. Hub Transport- ja Edge Transport -roolit suorittavat protokollan lokikirjaamista ja viestien seurantaa. Protokollaan lokit kertovat sen toiminnasta ja sen tarvitaanko toimintaan puuttumista. Näistä rooleista vain Hub Transport voi suorittaa sisällön muutoksen. Siinä Internetistä vastaanotetut viestit muutetaan Exchange 2010 -palvelimien käyttämään ”Summary Transport Neutral Encapsulation Format” -viestiformaattiin. (Stanek 2010, 37 - 38.)

3.5 Exchange-roolit ja AD

Exchange 2010 käyttää AD:ta laajasti ja jokaisella roolilla tulee olla pääsy sinne hakemaan tietoja vastaanottajista ja muista Exchange-palvelimista. Jokainen rooli käyttää AD:ta myös omilla yksilöllisillä tavoillaan. (Stanek 2010, 39.)

Exchange Server 2010:n fyysiset rajat ja aliverkot määräytyvät AD:n mukaan johon se asennetaan. Kun ensimmäinen Exchange-palvelin asennetaan toimialueeseen, tulee Exchange-organisaation nimeksi tämä verkkotunnus. Tämän jälkeen toimialueeseen lisättävät Exchange-palvelimet liittyvät automaattisesti organisaatioon. Exchange tiedustelee AD:ta reitityksien tekemiseen. Mailbox- ja Unified Messaging -palvelimet näkevät AD:lta, mitkä Hub Transport -palvelimet kuuluvat niiden kanssa samaan toimipaikkaan. (Stanek 2010, 41.)

Hub Transport -palvelimet käyttävät AD:n toimipaikkatietoja päättämään, kuinka viestit reititetään organisaatiossa, ja ne voivat reitittää viestejä toimialueen toimipaikkalinkkien yli toisiin toimipaikkoihin. Viestin saapuessa Hub Transport -palvelin selvittää tiedon vastaanottajasta ja selvittää AD:lta mikä käyttäjätunnus kuuluu vastaanottajaosoitteeseen. AD:n vastauksessa on mukana Mailbox-palvelimen FQDN-nimi, jossa käyttäjän sähköpostitili sijaitsee. Tästä FQDN:sta päätellään Mailbox-palvelimen toimipaikka. Mikäli postilaatikko on samassa toimipaikassa kuin Hub Transport -palvelin, välittää se viestin suoraan käyttäjän postilaatikkoon Mailbox-palvelimelle. Postilaatikon ollessa eri toimipaikassa kuin Hub Transport -palvelin välittää se viestin sen toimipaikkaan Hub Transport -palvelimelle, jossa postilaatikko sijaitsee. AD:sta saatavien tietojen takia lisäkonfiguraatiota ei tarvita reitityksen käyttöönottamiseksi AD-metsässä. Lisäkonfiguraatiota tarvitaan, kun organisaatioon, jossa on Exchange 2003 -järjestelmä, lisätään Exchange Server 2010 -järjestelmä. Lisäkonfiguraatiota tarvitaan myös, kun organisaatiossa on useampi metsä tai kun halutaan suora viestien kulku eri metsissä olevien Exchange-palvelimien välillä. (Stanek 2010, 18 - 19, 40; Morimoto ym. 2010, 178.)

Hub Transport -palvelimet säilyttävät kaiken asetusinformaation AD:ssa. Tämä asetusinformaatio pitää sisällään tiedon kuljetus- ja lokikirjaamissäännöistä sekä liittimistä (connectors). (Stanek 2010, 40.)

Client Access -palvelimet vastaanottavat yhteyksiä sekä paikallisilta että etäasiakkailta. Kun käyttäjäyhteys on vastaanotettu, Client Access -palvelin ottaa yhteyden AD:hen käyttäjän autentikoimiseksi ja tämän postilaatikon sijainnin selvittämiseksi. Jos postilaatikko on samassa AD-toimipaikassa kuin Client Access

-palvelin, käyttäjä yhdistetään hänen postilaatikkoonsa. Jos taas postilaatikko on eri AD-toimipaikassa, yhteys ohjataan sen toimipaikan Client Access -palvelimelle. (Stanek 2010, 40.)

Client Access -palvelin kommunikoi Mailbox-palvelimien kanssa käyttäen RPC:tä. Jokaisessa AD-toimipaikassa, jossa on Mailbox-palvelin, tulee olla yksi Client Access -palvelin. Vähintään yhden Client Access -palvelimen tulee olla suunnattu myös Internetiin. Tämä palvelin välittää yhteyksiä Outlook Web App:sta, ActiveSync:stä ja Exchange Web -palveluista käyttäjän postilaatikon lähimmälle Client Access -palvelimelle. Välitystä ei käytetä POP3- tai IMAP4-yhteyksille, joten käyttäjän tulee yhdistää sille Client Access -palvelimelle, jonka AD-toimipaikassa käyttäjän sähköpostilaatikko sijaitsee. (Stanek 2010, 40.)

Kun käytetään kuormantasausta Client Access -palvelimilla, CAS-taulu rekisteröidään AD:ssa tähän liittyvien objektien luomiseksi ja jokaisen taulun liittämiseksi tiettyyn AD-toimipaikkaan. Jokaiselle CAS-taululla voi olla vain yksi AD-toimipaikka. Aivan kuin itsenäisillä Client Access -palvelimilla, toimipaikkatiedot päättävät, kuinka yhteydet ohjataan. (Stanek 2010, 40.)

Unified Messaging -palvelimet yhdistävät AD:hen hakeakseen tietoja globaaleista asetuksista, kuten IP-välityspalvelimista. Kun Unified Messaging -palvelin saa viestin, se etsii AD:sta vastaanottajia, joiden puhelinnumero vastaa vastaanottajan osoitetta. Vastaanottajan löydyttyä se lähettää viestit paikalliselle Hub Transport -palvelimelle kuljetettavaksi oikeaan sähköpostilaatikkoon. (Stanek 2010, 41; Morimoto ym. 2010, 178.)

Mailbox-palvelimet käyttävät AD:ta selvittääkseen tietoja paikallisista Hub Transport -palvelimista. Tämän tiedon avulla ne voivat välittää viestejä paikalliselle Hub Transport -palvelimelle eteenpäin reititettäviksi. Mailbox-palvelimet säilyttävät tietoja AD:ssa sähköpostilaatikoiden käyttäjistä, sähköpostilaatikoiden tallennuspaikoista, osoitelistoista ja säännöistä. (Stanek 2010, 41; Morimoto ym. 2010, 178.)

4 VIESTIEN VÄLITYS JA KÄYTTÖOIKEUDET

4.1 Viestien välittäminen

Organisaation Mail Transport -palvelimet hoitavat viestien välityksen ulos organisaatiosta ja vastaanottavat viestejä sen ulkopuolelta. Tähän voidaan käyttää joko Hub Transport- tai Edge Transport -palvelimia. Nämä palvelimet sijoitetaan organisaation sisälle tai Edge Transport -palvelin voidaan vaihtoehtoisesti sijoittaa eteisverkkoon lisäturvan saamiseksi. Eteisverkko on turvattu verkko organisaation yksityisen sisäverkon ulkopuolella. (Stanek 2010, 19.)

Microsoft Exchange Server 2010 -organisaatio voidaan konfiguroida käyttämään vain Hub Transport -palvelinta viestien välittämiseen ja reitittämiseen. Tällöin Se vastaa viestien reitittämisestä ja välittämisestä organisaatiossa, viestien vastaanottamisesta organisaation ulkopuolelta ja niiden kuljettamisesta Mailbox-palvelimelle. Se vastaa myös viestien vastaanottamisesta Mailbox-palvelimelta ja välittämisestä organisaation ulkopuolelle. Edge Transport -palvelimella voidaan optimoida viestien reititys ja toimittaminen, konfiguroimalla yksisuuntainen synkronointi sisäisiltä Hub Transport -palvelimilta eteisverkon Edge Transport -palvelimille. Kun organisaatiossa on Edge Transport -palvelin, hoitaa se liikennöinnin organisaation ulkopuolelle ja Hub Transport -palvelin hoitaa liikennöinnin organisaation sisällä. (Stanek 2010, 381.)

Exchange käyttää sähköpostiosoitteita viestien reitittämiseen organisaation sisä- ja ulkopuolella. Kun viestit reititetään sisäisesti, Hub Transport -palvelin käyttää ”mail connector” -liittimiä viestien reitittämiseksi toisille Exchange-palvelimille. Koska jokainen liitin edustaa yksisuuntaista yhteyttä, käyttää Exchange sekä lähetys- ja vastaanottoliittimiä. Ne käyttävät kuljetuksissa oletuksena SMTP-protokollaa ja tarjoavat suoran yhteyden Transport-palvelimien välillä. Hub Transport- ja Edge Transport -palvelimet voivat kommunikoida myös muiden sähköpostipalvelimien kanssa. Silloin kun nämä palvelimet kommunikoivat yrityksen ulkopuolelle, käyttävät ne välitysyhdyskäytäviä viestien välittämiseen.

Exchange 2010 käyttää hakemistopohjaista vastaanottajan selvittämistä kaikille viesteille, jotka lähetetään ja vastaanotetaan organisaatiossa. Kategorisoija yhdistää saapuvassa viestissä olevan vastaanottajan oikeaan objektiin eli käyttäjätiliin AD:ssa. (Stanek 2010, 119, 382.)

Lähetysliitin on looginen yhdyskäytävä, joka kuljettaa kaikkia Transport-palvelimelta ulospäin lähteviä viestejä. Kun lähetysliitin luodaan, se tallentaa AD:hen liitinobjektin. Useat palvelimet voivat käyttää tätä viestien lähettämiseen. Lähetysliitin lähettää viestejä etsimällä DNS-palvelimelta MX-tietueen ja katsomalla sen IP-osoitteen. (Stanek 2010, 382 - 383.)

Hub Transport -palvelin sisältää oletuksena lähetysliittimen, jota käytetään viestin kuljettamiseen organisaatiossa eikä sitä tarvitse erikseen konfiguroida. Lähetysliitin tulee kuitenkin luoda, jotta organisaatiosta voidaan lähettää viestejä ulos. (Redmond 2010, 845.)

Vastaanottoliitin on looginen yhdyskäytävä, jonka kautta kaikki viestit vastaanotetaan. Myös sillä on objekti AD:ssa. Toisin kuin lähetysliitin, vastaanottoliitin palvelee vain yhtä palvelinta ja se määrittelee kuinka palvelin kuuntelee tulevia yhteyksiä. Se määrittelee myös mistä liitin sallii yhteydet. Autentikointimekanismi joka yhdistimelle konfiguroidaan, määrittelee sallitaanko anonyymit yhteydet ja minkä tyyppiset autentikointitavat ovat sallittuja. (Stanek 2010, 383.)

Oletuksena Hub Transport -palvelimet käyttävät AD:n kustannuksia, jotka on määritelty sen IP-protokollan linkkeihin. Näitä tietoja se käyttää valitessaan kustannuksiltaan pienimmän reitti muille Hub Transport -palvelimille organisaatiossa. (Stanek 2010, 383.)

Hyväksytty verkkotunnus on SMTP-nimiavaruus, johon Exchange-organisaatio vastaanottaa ja josta se lähettää sähköpostiviestejä. Organisaatiolla voi olla useampia SMTP-verkkotunnuksia. Kun ensimmäinen Hub Transport -palvelin asennetaan, yksi hyväksytty verkkotunnus asetetaan organisaation viralliseksi verkkotunnukseksi. Tämän verkkotunnus pohjautuu FQDN-nimeen. (Stanek 2010, 436.)

4.2 MAPI, POP3, IMAP4 ja mobiilipalvelut

MAPI on Microsoftin kehittämä ohjelmointirajapinta, joka mahdollistaa kehittäjien kirjoittaa helpommin ohjelmia, joilla päästään käsiksi sähköposti- tai kansiotoimintoihin ja palveluihin. Outlook käyttää MAPI:a päästäkseen Exchange-palvelimien ja AD:n. tietoihin. Kun käytössä on Exchange Server 2010, Outlook MAPI ottaa yhteyden Client Access -palvelimeen. Tällä saavutetaan parempi pääsyn hallinta ja suorituskyky. (McBee 2009, 29; Morimoto ym. 2010, 526.)

Exchange Server 2010 tukee myös IMAP4- ja POP3-protokollia. IMAP4 on protokolla viestien lukemiseen ja se mahdollistaa pääsyn julkisiin ja yksityisiin kansioihin palvelimella. Asiakkaat voivat kirjautua Exchange-palvelimelle ja käyttää IMAP4:ää viestien otsikoiden lataamiseksi ja lukea viestit yksitellen. IMAP4 säilyttää viestit palvelimella. POP3-protokolla on tarkoitettu viestien lataamiseksi palvelimelta yhteydettömään käyttöön. Outlook Web -käyttöliittymä, ActiveSync ja Outlook Anywhere tarjoavat kuitenkin enemmän palveluita ja ovat suositellumpi tapa käyttää Exchangea. POP ja IMAP eivät ole oletuksena päällä. Ne voidaan kuitenkin aktivoida Client Access -palvelimelta käynnistämällä nämä palvelut Windows -palvelimen ”Services”-valikosta. (Stanek 2010, 488 - 489.)

Etäkäyttäjät voivat tarkistaa viestinsä käyttämällä ”Outlook Anywhere”-, ”Outlook Web App”-, ”Exchange ActiveSync”-, POP3- tai IMAP4-palveluja. Mobiilipääsy Exchange-palvelimelle käyttäen ActiveSync-palvelua on tuettu kaikilla Windows Mobile -ohjelmistoilla. Exchange ActiveSync on synkronointiprotokolla, joka on optimoitu toimimaan korkean latenssin ja matalan kaistan verkoissa. Se mahdollistaa mobiililaitteiden käyttäjien pääsyn sähköposteihin, kalenteriin, kontakteihin ja tehtäviin. (Stanek 2010, 503; Microsoft TechNet 2010.)

4.3 Exchange 2010 -tietojenkäsittely

AD:n tietovarasto sisältää suurimman osan hakemistotiedoista, kuten Exchange 2010:n konfiguraatiot ja Exchange-vastaanottajat. Ohjauspalvelin ylläpitää dataa, ja tämän tiedon sijainti on asetettu AD:hen. (Stanek 2010, 74.)

Exchange 2010 Mailbox-palvelimella on yksi tietokantatiedosto jokaiselle postilaatikko- tai julkinentietokannalle. Tiedot tietokannoissa on tallennettu objektipohjaisesti. Exchange käyttää tapahtumia kontrolloidakseen muutoksia tietokannoissa. Tapahtumat on kirjattu muutoslokeihin, ja Exchange suorittaa tai peruuttaa muutokset riippuen tapahtuman onnistumisesta. (Stanek 2010, 75 - 77.)

Exchange-palvelimien viestijonot ovat väliaikaisia sijoituspaikkoja viesteille, jotka odottavat käsittelyä. Kun lähetetty viesti on replikoitu kaikkiin tietokantoihin, johon vastaanottajan postilaatikko kuuluu, viesti poistetaan viestijonosta. (Stanek 2010, 75 - 77.)

”Shadow redundancy” -ominaisuutta voidaan käyttää Exchange 2010:ssä. Se estää kuljetuksessa olevien viestien katoamisen palvelimen vikaantuessa tallentamalla jonossa olevat viestit siksi aikaa, kunnes seuraava palvelin on saanut viestin välitettyä. (Stanek 2010, 80.)

4.4 Roolipohjaiset käyttöoikeudet

AD:ssa ja Exchangessa voidaan hallita tietoturvaa käyttämällä oikeuksia. Käyttäjillä, kontakteilla ja turvaryhmillä on kaikilla niille määrätyt oikeudet. Nämä oikeudet kontrolloivat, mihin resursseihin käyttäjät, kontaktit ja ryhmät pääsevät ja mitä toimenpiteitä ne voivat suorittaa. Tarkkailulla (auditing) voidaan seurata näiden oikeuksien käyttöä, kuten myös sisään- ja uloskirjautumisia. Exchange-oikeuksia voidaan hallita joko AD-työkaluilla tai ”Exchange Management” -työkaluilla. (Stanek 2010, 233.)

Exchange 2010 sisältää uuden oikeusmallin ”Role Based Access Control”. Tämä malli toteutetaan yhdessä standardin Windows-oikeusmallin kanssa ja kumpaakin voidaan käyttää Exchange-organisaation hallintaan. Kun Exchange 2010 tuodaan Exchange 2003- tai Exchange 2007 -ympäristöön, aikaisemmat oikeusmallit toimivat yhdessä 2010:nen käyttämien standardien ja uuden oikeusmallin kanssa. Suurin osa Exchangen tiedoista on tallennettu AD:hen. AD:n ominaisuuksia voidaan käyttää standardioikeuksien hallintaan Exchange-organisaatiossa. (Stanek 2010, 233.)

RBAC-oikeudet mahdollistavat helpon tavan kontrolloida, mihin tietoihin ylläpitäjät ja käyttäjät pääsevät käsiksi. Rooliksi kutsutaan kokoelmaa oikeuksia. RBAC-oikeusmallissa oikeudet annetaan rooleille eikä suoraan käyttäjätunnuksille. Jäsenet lisätään tiettyyn rooliryhmään, kun ne tarvitsevat sen tason oikeuksia. Lisäksi rooleja voidaan rajata (scope) sisältämään vain tietyt resurssit organisaatiossa. (Morimoto ym. 2010, 186.)

Roolipohjainen käytönvalvonta on oikeusmalli, jossa käytetään roolimäärittelyä määräämään, mitä hallintatehtäviä käyttäjä tai ryhmä voi suorittaa Exchange-organisaatiossa. Exchange sisältää monia sisäänrakennettuja hallintarooleja, joita voidaan käyttää Exchange-organisaation hallinnassa. Jokainen sisäänrakennettu rooli toimii ryhmänä oikeuksia, jotka määräävät, mitä hallintatoimia ne, joilla rooli on, voivat suorittaa. Rooleja voidaan luoda myös itse. (Stanek 2010, 244.)

Rooleja voidaan määrätä ryhmille tai käyttäjille. Rooleja voidaan antaa mille tahansa sähköpostilaatikon sisältävälle käyttäjätunnukselle. Niitä voidaan antaa myös mille tahansa turvaryhmälle, mutta niitä ei voida antaa verkkotunnuksen laajuudella eikä jakeluryhmille. Kun rooli lisätään ryhmälle, rajaus (scope) päättää, missä AD:n resursseissa tätä objektia voidaan käyttää roolin omaavan käyttäjän toimesta. Rajaus määrätään joko ryhmän oletuksen mukaan tai muuttamalla sitä. (Stanek 2010, 245.)

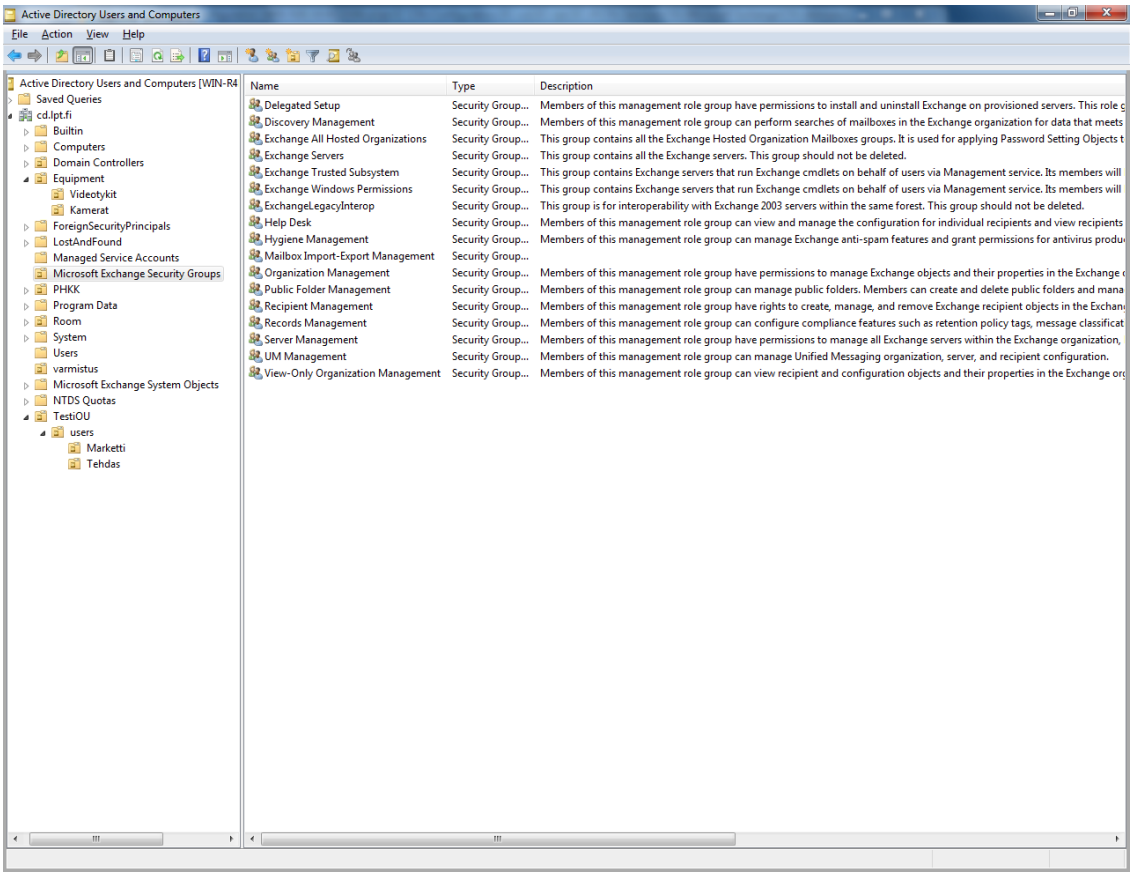
Roolin tuomat oikeudet antavat käyttäjille esimerkiksi mahdollisuuden muokata heidän ”Outlook Web App” -asetuksiaan ja suorittaa rajoitettuja hallintatoimia. Kun Exchange-palvelin asennetaan, asennus luo ”Default Role Assignment

Policy” -säännön ja asettaa tämän oletuksena kaikille uusille sähköpostilaatikoille. Tämä sääntö antaa käyttäjille oletuksena ”MyBaseOptions”-, ”MyContactInformation”-, ”MyDistributionGroupMembership”- ja ”MyVoiceMail”-roolit, mutta ei ”MyDistributionGroups”- ja ”MyProfileInformation”-rooleja. Nämä roolit mahdollistavat peruskäyttäjien muuttaa omia kontaktitietoja, oman sähköpostilaatikon perusasetuksia, omia jäsenyyksiään jakeluryhmissä ja muokata omia ääniviesti asetuksia. Peruskäyttäjät eivät kuitenkaan oletuksena voi muuttaa heidän nimeään, eivätkä he voi luoda tai muokata jakeluryhmiä. (Stanek 2010, 249.)

4.5 Standardi-hallintaryhmät

Käyttäjät, kontaktit ja ryhmät on esitetty AD:ssa objekteina. Näillä objekteilla on useita ominaisuuksia, jotka määrittelevät, kuinka niitä käytetään. Tärkeimmät ominaisuudet ovat objekteille määrätyt oikeudet. Objektille määrätyt oikeudet voivat tulla suoraan objektilta tai ne voivat periytyä toiselta objektilta. Yleisesti objektit perivät oikeuksia ”parent”-objekteilta, jotka ovat hierarkiassa ylempänä. Periytyminen voidaan kuitenkin ohittaa. (Stanek 2010, 234.)

Exchangen tietojen ja palvelimien hallintaan Exchange Server 2010 käyttää monia esimääriteltyjä ryhmiä. Näillä turvaryhmillä on oikeuksia hallita Exchange-organisaatiota, Exchange-palvelimia ja vastaanottajien tietoja. ”Active Directory Users & Computers” -työkalulla voidaan nähdä Exchangeen liittyvät ryhmät ja työskennellä niiden kanssa. Nämä ryhmät löytyvät ”Microsoft Exchange Security Groups” -haarasta. Kuviossa 4 on näkymä tästä työkalusta ja Exchange-hallintaryhmien haarasta. (Stanek 2010, 234.)



KUVIO 4. ”Active Directory Users and Computers” -työkalun näkymä Exchange-hallintaryhmistä

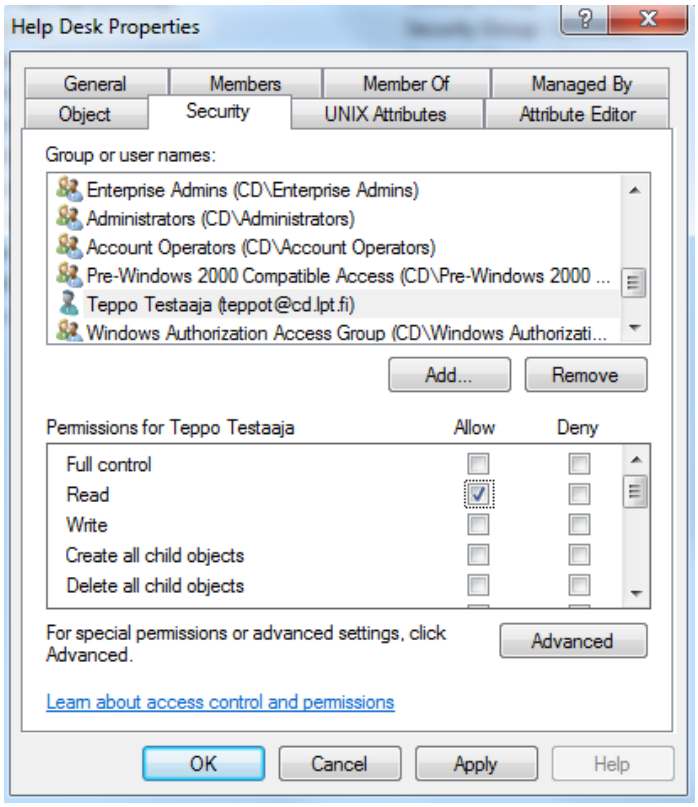
Oikeuksien antaminen käyttäjille tai ryhmille tapahtuu lisäämällä ne jäseniksi sopivaan Exchange-hallintaryhmään. Käyttäjien hallintaan sopiva työkalu on ”Active Directory Users & Computers”. Siellä hallintaryhmään lisääminen tapahtuu seuraavasti: Avataan ”Microsoft Exchange Security Groups” -puu ja valitaan tarkoitukseen sopiva hallintaryhmä. Avataan sen asetusikkuna valitsemalla ”Properties” ja valitaan sieltä ”Members”-välilehti, jossa voidaan käyttäjiä lisätä ryhmään. Taulukossa 2. on esitetty käytössä olevat valmiit hallintaryhmät. (Stanek 2010, 239.)

TAULUKKO 2. Hallintaryhmät, joilla määritellään hallintaoikeuksia käyttäjille

Hallintaryhmä	Kuvaus ryhmästä
Organization Management	Ryhmän jäsenillä on oikeus hallita Exchangen objekteja ja niiden asetuksia Exchange-organisaatiossa. Jäsenet voivat myös delegoida rooliryhmiä ja hallinta rooleja organisaatiossa. Antaa eniten oikeuksia Exchange-hallintaan.
Public Folder Management	Ryhmän jäsenet voivat luoda ja poistaa julkisia kansioita sekä hallita niiden asetuksia.
Recipient Management	Ryhmän jäsenillä on oikeus muuttaa, hallita ja poistaa Exchange-vastaanottajia Exchange-organisaatiossa.
View-Only Organizational Management	Ryhmän jäsen voi nähdä vastaanottaja- ja konfigurointiobjektit heidän asetuksissaan Exchange-organisaatiossa.
UM Management	Ryhmän jäsen voi hallita Unified Messaging:n organisaatio-, palvelin- ja vastaanottaja-asetuksia.
Help Desk	Ryhmän jäsen voi nähdä ja hallita yksittäisten vastaanottajien asetuksia ja nähdä vastaanottajat Exchange-organisaatiossa. Ryhmän jäsen voi hallita käyttäjien asetuksia, mutta vain kuten käyttäjä itse voisi.s
Records Management	Ryhmän jäsenet voivat konfiguroida määräysominaisuuksia, kuten säilytyssääntöjä, viestin luokittelua, kuljetussääntöjä yms.
Discovery Management	Ryhmän jäsenet voivat suorittaa sähköpostilaatikoiden hakuja Exchange-organisaatiossa datalle, joka täyttää tietyt kriteerit.
Server Management	Ryhmän jäsenillä on oikeus hallita kaikkia Exchange-palvelimia

	Exchange-organisaatiossa, mutta heillä ei ole oikeuksia suorittaa operaatioita, joilla on globaali vaikutus Exchange-organisaatioon.
Delegated Setup	Ryhmän jäsenillä on oikeus asentaa ja poistaa Exchange-palvelimia.
Hygiene Management	Ryhmän jäsenet voivat hallita roska-postinsuodatuksen asetuksia ja sallia oikeuksia viruksentorjuntaohjelmille, jotta ne voivat integroitua Exchangen kanssa.
Mailbox Import-Export Management	Ryhmän jäsenet voivat tuoda ja vielä sähköpostilaatikoiden sisältöä ja poistaa ei-haluttua sisältöä sähköpostilaatikoista.

Käyttäjän lisääminen hallintaryhmään tapahtuu valitsemalla ”Add”. Tämän jälkeen ilmestyy ”Select Users, Contacts, Computers, Service Accounts, Or Groups” -ikkuna. Annetaan tekstikenttään käyttäjän tunnus ja valintaan ”Check Names”. ”Advanced”-kohdasta voidaan tarkemmin etsiä käyttäjiä. Käyttäjiä voidaan poistaa hallintaryhmästä valitsemalla käyttäjä ”Members”-välilehdeltä ja valitsemalla ”Remove”. ”Security”-välilehdeltä voidaan tehdä yksityiskohtaisempia muutoksia käyttäjien ja ryhmien oikeuksiin. Kuviossa 5 on näkymä näistä edistyneemmistä asetuksista, joissa voidaan oikeudet yksityiskohtaisemmin sallia tai evätä. Microsoft kuitenkin suosittelee roolipohjaista hallintaa näiden objektien hallinnan sijasta. (Stanek 2010, 240 - 243.)



KUVIO 5. Näkymä ”Help Desk”-ryhmän ”Security”-välilehden asetuksista

Jäsenyyksien hallintaa voidaan tehdä myös selaimen kautta ottamalla yhteys Exchangen hallintapaneeliin, jonka oletusosoite on mallia ”https://palvelin.domain.fi/ecp”. Kirjaudutaan palveluun tunnuksilla, joilla on riittävät oikeudet hallintaan ja valitaan ”Administrator Roles”. Tuplaklikkaamalla ryhmää nähdään sen jäsenet ja päästään hallitsemaan ryhmää. (Stanek 2010, 240.)

Itse rooliryhmiä ja sitä kautta käyttäjien oikeuksia voidaan muokata käyttämällä ”Exchange Control Panel” -työkalua. Kun sillä hallitaan organisaatiota ja ”User & Groups” on valittuna, voidaan valita ”User Roles”-välilehti olemassa olevien roolien oikeuksien hallintaan. Tuplaklikkaamalla haluttua ryhmää päästään asetuksiin. Muokattaessa roolin oikeuksia valitaan halutut valintaruudut ja poistettaessa oikeuksia poistetaan valinnat. Oletuksena ”Organization Management” -ryhmän jäsenet voivat hallita kaikkia rooliryhmiä Exchange-organisaatiossa. Rooliryhmiä voidaan muokata myös Exchange-komentokehotteella. Sillä voidaan myös poistaa ja luoda rooleja. (Stanek 2010, 249 - 250.)

5 EXCHANGEN 2010:N VIKASIETOISUUS

5.1 Vikasietoisuuden toteuttaminen

Sähköpostipalvelin on kriittinen tekijä organisaatiossa. Jos sähköpostipalvelin vikaantuu eikä siihen ole varauduttu, saattaa jokainen käyttäjä tällä palvelimella menettää päivien, viikkojen tai kuukausien työt. Jos ensisijainen Client Access -palvelin kaatuu eikä vaihtoehtoista ole, eivät käyttäjät pääse käsiksi viesteihin, kalenteriin ja osoitelistoihin. Jos ensisijainen Transport-palvelin kaatuu eikä vaihtoehtoista ole, viestit eivät reitity ja välity oikein. Jotta voidaan varmistaa pääsy Exchange-palvelimelle ja suojata käyttäjien tiedot, tarvitaan palautumissuunnitelma. (Stanek 2010, 569.)

Exchange-organisaation suunnittelu korkealle saatavuudelle ja palautusskenaariolle voi antaa suojan tietokantojen korruptoitumista, laitevikoja, vahinkoja joissa käyttäjien viestejä poistuu ja luonnonkatastrofeja vastaan. Korkean saatavuuden ratkaisu saadaan yksinkertaisesti ottamalla käyttöön useita Hub Transport, Edge Transport ja Client Access -palvelimia ja sijoittamalla lisäpalvelimet AD:hen. Tällä voidaan varmistaa palveluiden saatavuus kun avainasemassa oleva viestipalvelu esimerkiksi ensisijainen Hub Transport-, Edge Transport- tai Client Access -palvelin vikaantuu. (Stanek 2010, 569 - 570.)

5.2 Database Availability Group

Database Availability Group on ryhmä Mailbox-roolin omaavia Exchange Server 2010 -palvelimia. DAG-ryhmä tarjoaa sähköpostilaatikoille automaattisen tietokantatason elpymisen vikatiloissa. Näitä vikoja voivat olla laitteistovika, vika tallennusjärjestelmässä tai vika tietoverkossa. DAG-ryhmän jäsenet käyttävät ”Windows 2008:n Failover Clustering” -ominaisuutta tarkkaillakseen toistensa toiminnan tilaa. Mailbox-palvelimia pitää olla ryhmässä vähintään kaksi, jotta vikatiloista voidaan toipua. Yhdessä ryhmässä voi olla enintään 16 palvelinta. (Morimoto ym. 2010, 1028 - 1030.)

DAG-ryhmää luotaessa sille annetaan IP-osoite. Kun ensimmäinen palvelin lisätään ryhmään, DAG-ryhmän nimi ja IP-osoite rekisteröidään DNS-järjestelmään käyttämällä ”Host(A)”-tietuetta. Ryhmän nimen tulee olla yksilöllinen AD-metsässä. DAG-ryhmällä voi olla useampia IP-osoitteita ja tällöin vai yksi, joka tulee toimintaan rekisteröidään DNS-palveluun. (Stanek 2010, 288.)

Jokaisella DAG-ryhmällä tulee olla vähintään kaksi verkkoa: yksi replikointiverkko replikointitiedoille ja yksi viestintäverkko MAPI-liikenteelle ja muulle viestinnälle. DAG-ryhmää asennettaessa valitaan, mitkä verkot ovat replikointiliikenteelle ja mitkä MAPI-liikenteelle. Jos kaikki replikointiverkot ovat poissa käytöstä, Exchange käyttää muita verkkoja replikointiin, kunnes replikointiverkko on taas käytettävissä. Jokaisella DAG-verkolla tulee olla yksilöllinen nimi ja sillä voi olla valinnainen kuvaus. (Stanek 2010, 295 - 296.)

Luotaessa DAG-ryhmää voidaan määritellä todistajapalvelin (witness server) tai antaa Exchangen valita se automaattisesti. Todistajapalvelin auttaa ryhmää ylläpitämään sen tilaa ja päätösvaltaa muutoksiin silloin, kun ryhmässä on parillinen määrä jäseniä. Se siis auttaa ryhmää päättämään mitkä tietokantakopiot ovat aktiivisia ja mitkä passiivisia. Todistajapalvelimella voidaan valita kansio, jota DAG-ryhmä pääsee käyttämään tai Exchange voi automaattisesti luoda kansion. Kansiota ei tulisi käyttää mihinkään muuhun. Todistajapalvelin ei voi olla DAG-ryhmän jäsen, sen tulee sijaita samassa AD-metsässä ja sen pitää käyttää Windows Server 2003 tai Windows Server 2008 -käyttöjärjestelmää. (Stanek 2010, 287 - 288.)

Microsoft suosittelee Exchange 2010 -palvelimen käyttöä todistajakansion isäntänä. Tämä varmistaa, että Exchangella on riittävät oikeudet käyttää todistajakansiota. Suositeltu todistajapalvelin on Hub Transport -palvelin, joka sijaitsee samassa AD:ssa kuin suurin osa DAG-ryhmän jäsenistä. Yksi palvelin voi toimia todistajapalvelimena usealle DAG-ryhmälle, mutta jokaisella ryhmällä tulee olla oma kansionsa. (Stanek 2010, 288.)

Jokaisella DAG-ryhmällä on resurssi, joka on vastuussa todistajalokin ylläpidosta. Tämä resurssi tallentaa tiedon kaikista klusterin tietokannanmuutoksista todistajalokiin varmistaen näin, että klusterin asetukset ja tilatiedot voidaan palauttaa.

DAG-ryhmää luodessa Exchange päättää automaattisesti sopivan päätösvalta-asetuksen klusterille. Asetus perustuu jäsenpalvelimien määrään. Jos palvelimia on pariton määrä, käytetään ”Node Majority” -tilaa, jossa palvelimilla on oma paikallinen ”quorum device”, joka varastoi klusterin tiedot. Jos taas palvelimia on parillinen määrä, käytetään ”Node and File Share Majority” -tilaa, jossa palvelin käyttää todistajapalvelinta ennemmin, kuin paikallista päätösvaltaa. (Stanek 2010, 289.)

Silloin kun DAG-ryhmässä on vain yksi Mailbox-palvelin, vikatilaklusteri käyttää ”Node Majority” -tilaa päätösvallassa. Kun toinen Mailbox-palvelin lisätään ryhmään, Exchange muuttaa päätösvallan ”Node and File Share Majority” -tilaan. Tällöin DAG-ryhmä alkaa käyttää todistajapalvelimen UNC-polkua ja kansiota klusterin päätösvaltaan. Jos todistajapalvelinta ei vielä tässä vaiheessa ole, yrittää Exchange luoda sen automaattisesti Hub Transport -palvelimelle, jolla ei ole Mailbox -roolia. Tämän jälkeen Exchange konfiguroi DAG-ryhmää varten paikalliselle ylläpitäjälle ja klusterin tietokonetilille täydet oikeudet todistajakansioon. (Stanek 2010, 289.)

Kun DAG-ryhmä luodaan, Exchange luo ”msExchMDB-AvailabilityGroup”-kansion ja siihen liittyvät objektit AD:hen. Nämä edustavat DAG-ryhmää, sen jäseniä, verkkoa ja attribuutteja. Tätä kansiota käytetään DAG-ryhmän tietojen, kuten jäsenyyksien säilyttämiseen. Tiedot sisällytetyistä tietokannoista säilytetään klusteritietokannassa (cluster database). (Stanek 2010, 288.)

Kun DAG-ryhmä on luotu, voidaan siihen lisätä tai siitä poistaa palvelimia. Lisättyt palvelimet lisätään AD:ssa ”msExchMDBAvailabilityGroup”-objektiin. Kun ensimmäinen Mailbox-palvelin lisätään DAG -ryhmään, ottaa Exchange automaattisesti ”Windows Failover Cluster” -ominaisuuden käyttöön DAG-ryhmälle. Tällöin jäsenten toiminnan tarkkailu käynnistyy. Vikatilaklusterin ”heartbeat”-mekanismia ja klusteritietokantaa käytetetään seuraamaan ja hallinnoimaan tietoa DAG-ryhmässä. Vikatilaklusteri toimii vain Exchange 2010 Enterprise Edition Mailbox -palvelimilla. Lisäksi Mailbox-palvelimissa tulee olla vähintään kaksi verkkosovitinta, jotta saadaan erilliset replikointi- ja viestintäverkot. Autentikoin-

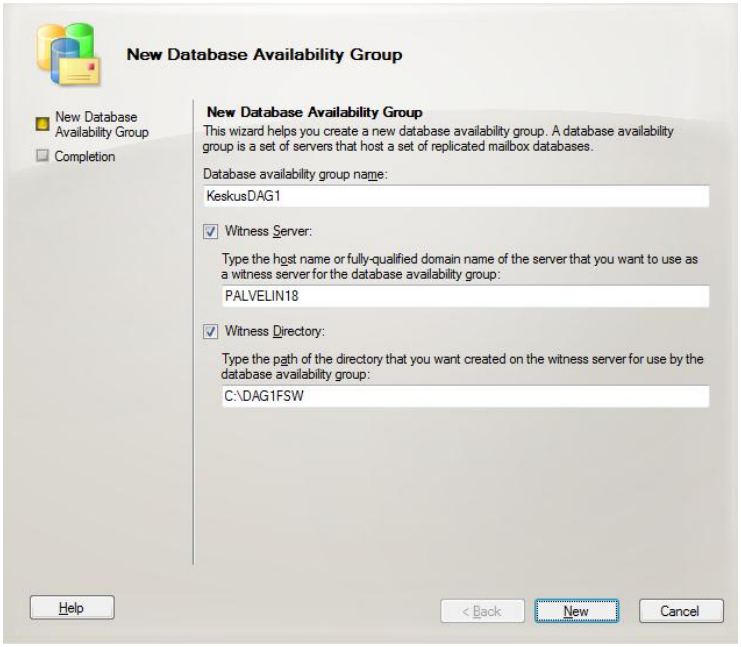
nin ja käyttöoikeuksien takia vikatilaklusteri esitetään AD:ssa tietokonetilinä. (Stanek 2010, 288.)

Klusterin tultua toimintaan, sen tietokanta päivittyy tiedoilla aktiivisista sähköpostitietokannoista. Tämän jälkeen Exchange tutkii tämänhetkiset klusterin verkkoasetukset. Jos palvelimella on asianmukaisesti konfiguroitu verkkosovitin, tätä käytetään luomaan replikointiverkko. Jos palvelimella on kaksi verkkosovitinta, toisella luodaan replikointiverkko ja toisella viestintäverkko. Todistajahakemisto ja todistajatiedostojenjako (witness file share) luodaan tämän jälkeen. Oikeudet asetetaan niin, että tili joka edustaa klusteria saa täydet oikeudet. (Stanek 2010, 288.)

Kun DAG-ryhmään lisätään myöhemmin uusia palvelimia, tulevat ne automaattisesti myös vikatilaklusteriin mukaan. Lisäksi ne tulevat ”msExchMDBAvailabilityGroup” -objektiin AD:ssa. Klusterin tietokanta päivittyy tämän jälkeen palvelimilla olevien tietokantojen tiedoilla. (Stanek 2010, 289.)

5.3 DAG-ryhmän luonti

Uuden DAG-ryhmän luonti onnistuu Exchange-hallintakonsolin kautta. Avataan Exchange-hallintakonsoli ja laajennetaan ”Organization Configuration”, josta valitaan ”Mailbox”. Seuraavaksi valitaan pikavalikosta ”New Database Availability Group”, jolloin ohjattu asennus käynnistyy ja käyttäjälle aukeaa kuvion 6 mukainen näkymä. ”Database Availability Group Name” -tekstikenttään annetaan halutu maksimissaan 15 merkkiä pitkä nimi ryhmälle. Nimen tulee olla AD-metsässä yksilöllinen, eikä se saa sisältää välejä tai erikoismerkkejä. (Stanek 2010, 289 - 290.)



KUVIO 6. Näkymä Exchange hallintakonsolista luotaessa uutta DAG-ryhmää

Valinnaisesti voidaan valita ”Witness Server” -valintaruutu ja antaa nimi palvelimelle, joka toimisi todistajapalvelimena. Palvelimen tulee olla samassa AD-metsässä. Huomioitavaa on, että tämä palvelin ei voi olla mukana tässä DAG-ryhmässä, mutta se voi olla mukana jossain toisessa ryhmässä. Jos valintaruutu jätetään tyhjäksi, Exchange yrittää automaattisesti valita AD:sta todistajapalvelimeksi Hub Transport -palvelimen, jolla ei ole Mailbox -roolia. (Stanek 2010, 289 - 290.)

Valitaan ”Witness Directory” -valintaruutu ja annetaan paikallinen polku hakemistolle, johon tallennetaan todistajadata. Jos hakemistoa ei ole tai sitä ei anneta, yrittää Exchange luoda sen todistajapalvelimelle DAG-ryhmän nimellä. (Stanek 2010, 289 - 290.)

Huomioitavaa on, että Exchangella tulee olla riittävät oikeudet palvelimelle, luodakseen ja jakaakseen todistajakansion. Vaikka paikallisen kansion polku voidaan antaa, on sen jakonimi automaattisesti myös muodossa ”DAGName .DomainName”. Jos todistajapalvelin ei ole Exchange-palvelin, täytyy sen paikalliselle ylläpitäjäryhmälle (Administrators) lisätä Exchange ”Trusted Subsystem” -ryhmä. (Stanek 2010, 289 - 290.)

Valitaan ”New” uuden ”Database Availability” -ryhmän luomiseksi. Loppusivulla nähdään operaation tiedot ja se oliko se onnistunut. Jos operaatio oli onnistunut, valitaan ”Finish”. Muussa tapauksessa voidaan palata takaisin korjaamaan asetuksia valitsemalla ”Back”. DAG-ryhmä voidaan luoda myös Exchange Management Shell -konsolin kautta. (Stanek 2010, 290 - 291.)

Jos ”Availability”-ryhmä on luotu käyttäen Exchange Management -konsolia ja halutaan lisätä sillä palvelimia ryhmään, tulee vähintään yksi palvelimen verkkosovittimista olla konfiguroitu käyttämään DHCP:tä. Kun ensimmäinen Mailbox-palvelin lisätään DAG-ryhmään, ryhmä saa IP-osoitteen. Oletuksena Exchange käyttää DHCP:tä saadakseen tämän IP-osoitteen. Vaitoehtoisesti voidaan määrätä käsin staattinen osoite konsolikomennolla ”-DatabaseAvailabilityGroupIp”. (Stanek 2010, 289.)

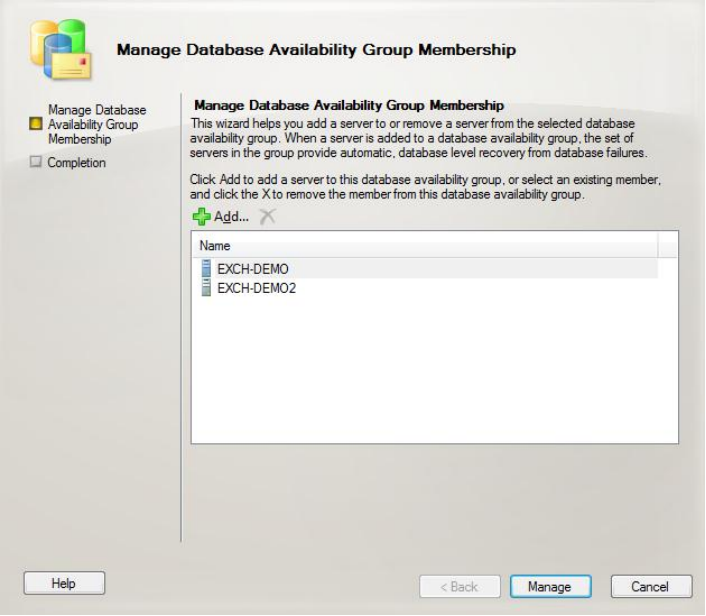
Esimerkiksi konsolissa tehtäisiin edellinen DAG-ryhmä IP-osoitteen lisämäärityksellä komennolla: ”New-DatabaseAvailabilityGroup -Name ”KeskusDAG1” -WitnessServer ”PALVELIN18” -WitnessDirectory ”C:\DAG1FSW” -DatabaseAvailabilityGroupIp 192.168.101.165, 192.168.101,166” (Stanek 2010, 289.)

5.4 DAG-ryhmän jäsenyydet

Kun ”Database Availability” -ryhmään lisätään uusi palvelin, se toimii muiden palvelimien kanssa ryhmässä tarjoten automaattisen tietokantatason palautuksen tietokanta-, palvelin- ja verkkovikaantumisissa. Jotta palvelin voidaan lisätä, tulee sen olla Windows 2008 SP2 tai R2 -palvelin ja siinä tulee olla vähintään kaksi verkkosovitinta eri aliverkoille. (Stanek 2010, 292.)

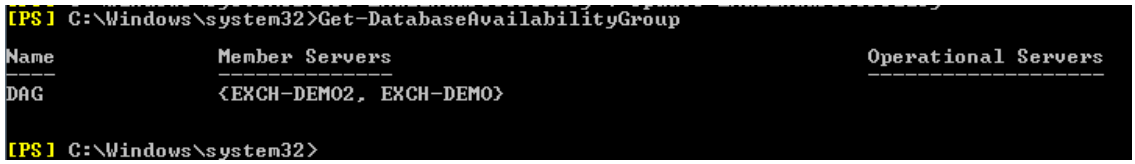
Jos palvelimen ei enää haluta olevan jäsen ”Availability”-ryhmässä, se voidaan poistaa siitä, jolloin se ei enää ole suojattu vikaantumisilta. Kaikki kopiot tietokannasta tulee poistaa palvelimelta ennen kuin tietokanta voidaan poistaa ryhmästä. (Stanek 2010, 293.)

Mailbox-palvelin lisätään DAG-ryhmään avaamalla Exchange-hallintakonsoli ja valitsemalla ”Organization Configuration” kohdasta ”Mailbox”. Seuraavaksi valitaan ”Database Availability Group” -välilehti, josta nähdään olemassa olevat ryhmät. Tämän jälkeen klikataan oikealla haluttua DAG-ryhmää ja valitaan ”Manage Database Availability Group Membership”. Tällä avautuvalla sivulla, joka näkyy kuviossa 7, voidaan lisätä uusi palvelin DAG-ryhmään. Tämä tapahtuu valitsemalla ”Add”. Palvelin voidaan poistaa ryhmästä valitsemalla se listasta ja painamalla punaista ruksia. Tiedot päivittyvät painamalla ”Manage”. Loppusivulla nähdään yhteenveto oliko operaatio onnistunut. (Stanek 2010, 293 - 294.)



KUVIO 7. Näkymä DAG -ryhmän jäsenten hallinnasta

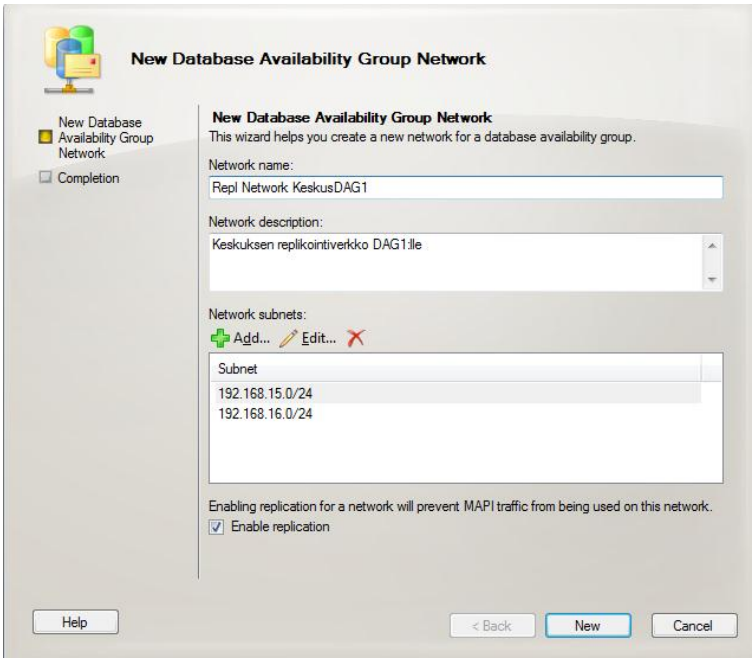
Exchange Management Shell -komentokehotteessa voidaan listata kaikki DAG-ryhmät komennolla ”Get-DatabaseAvailabilityGroup”. Kuviossa 8 on näkymä tämän komennon antamisen jälkeen. Ryhmään voidaan lisätä Mailbox-palvelimia komennolla: ”Add-DatabaseAvailabilityGroupServer -Identity DAGNimi -Mailboxserver LisättäväPalvelin”. Ryhmästä voidaan vastaavasti poistaa Mailbox-palvelimia komennolla: ”Remove-DatabaseAvailabilityGroupServer -Identity DAGNimi -Mailboxserver PoistettavaPalvelin”. (Stanek 2010, 294.)



KUVIO 8. Shell-näkymä, jossa listattuna DAG-ryhmät ja niiden jäsenet

5.5 DAG-verkon hallinnointi

DAG-verkko lisätään avaamalla Exchange-hallintakonsoli ja laajentamalla ”Organization Configuration”, josta valitaan ”Mailbox”. Seuraavaksi valitaan ”Database Availability Group” -välilehti. Tämän paneelin alaosasta nähdään verkot, jotka on liitetty DAG-ryhmään. Seuraavaksi valitaan oikealla klikkaamalla DAG-ryhmä, jota halutaan muokata ja valitaan ”New Database Availability Group Network”. Näytölle tulee kuvion 9 mukainen näkymä. (Stanek 2010, 296 - 297.)



KUVIO 9. Näkymä uuden DAG-verkon luonnista

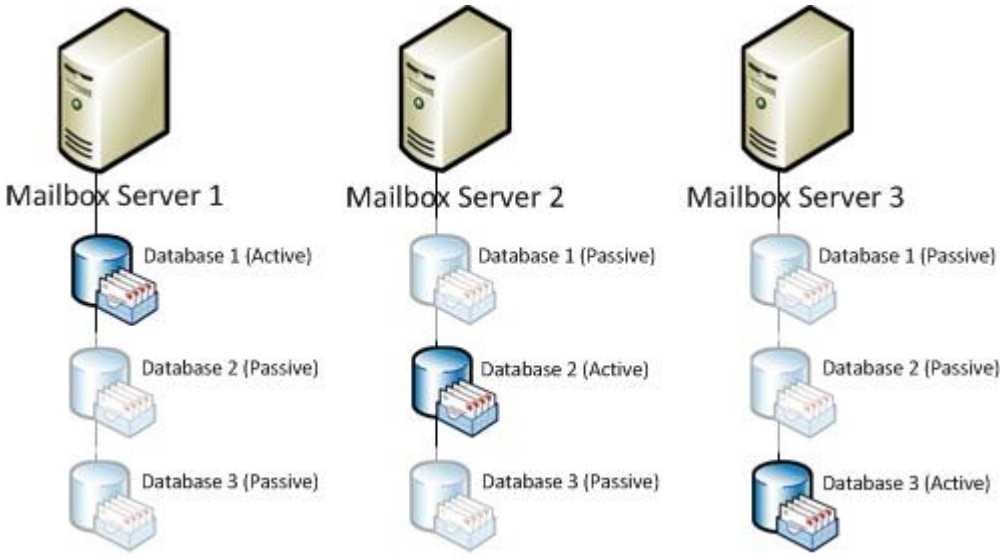
”New Database Availability Group Network” -sivulla annetaan verkolle ”Network name” -kohtaan yksilöllinen nimi ja lisäksi voidaan halutessa antaa ”Network description” -kohtaan kuvaus verkosta. ”Network Subnets” -kohdassa valitsemalla

”Add”, lisätään aliverkot DAG-verkolle. Aliverkot tulisi antaa IPv4 osoitteille muodossa ”IPv4Osoite/Aliverkonmaski”, esimerkiksi ”192.168.15.0/24”. IPv6 -osoitteille muodossa ”IPv6Osoite/Aliverkon etuliite”. Jotta verkosta tulee replikointiverkko, valitaan ”Enable Replication” -valintaruutu. Jos tätä ei valita, verkosta tulee viestintäverkko. Seuraavaksi valitaan ”New”, jolloin DAG-verkko luodaan. Loppusivulta nähdään yhteenveto ja oliko operaatio onnistunut.
DAG -verkko voidaan poistaa kun avataan Exchange-hallintakonsoli ja laajennetaan ”Organization Configuration”, josta valitaan ”Mailbox”. Seuraavaksi valitaan ”Database Availability Group” -välilehti. ”Network subnets” -listasta valitaan poistettava verkko ja painetaan punaista ruksia, jolloin verkko poistuu. (Stanek 2010, 296 - 297.)

5.6 Palveluiden saatavuuden varmistaminen

Mailbox-palvelimien saatavuuden parantamisessa ja siinä, ettei viestejä tarvitse palauttaa varmuuskopioista on useita tekniikoita. Näitä ovat tietokantakopiot, poistettujen osien säilytys (Deleted item retention), poistetun sähköpostilaatikon säilytys (Deleted mailbox retention), sähköpostilaatikoiden säilytyssäännöt ja useat sähköpostitietokannat. (Stanek 2010, 570.)

Tietokantojen kopiomenetelmässä (KUVIO 10) jokainen jäsenpalvelin DAG-ryhmässä voi ylläpitää yhtä kopiota tietokannasta, jonka isäntänä toimii toinen DAG-jäsenpalvelin, jossa tietokanta on aktiivisena. Exchange käyttää jatkuvaa replikointia luodakseen ja ylläpitääkseen tietokantojen kopioita. (Stanek 2010, 570.)



KUVIO 10. Vain yksi Mailbox-palvelin voi pitää aktiivisena tiettyä tietokantaa, mutta muut DAG-ryhmän jäsenet voivat ylläpitää varalla yhtä kopiota tästä tietokannasta (Cunningham 2010)

Poistettujen osien säilytys mahdollistaa käyttäjän palauttaa yksittäinen viesti tai koko kansio Outlook-sähköpostiohjelmassa. Poistettujen sähköpostilaatikoiden säilytys mahdollistaa ylläpitäjän palauttaa poistettuja postilaatikoita ilman, että niitä tarvitsee palauttaa varmuuskopioista. (Stanek 2010, 570.)

Arkisto-sähköpostilaatikoita käytetään varastoimaan käyttäjien vanhoja viestejä, joita voidaan tarvita. Viestejä voidaan joutua säilyttämään esimerkiksi yrityksen sääntöjen, viranomaisten tai lain takia. (Stanek 2010, 570.)

Säilytyssäännöt lisätään vahvistamaan viestien säilytysasetuksia. Kun viestit saavuttavat säilytysrajan, Exchange käsittelee ne toimien mukaan, jotka on ennalta määritelty. Tämä mahdollistaa viestien arkistoinnin, poiston tai merkitsemisen käyttäjän huomioimiseksi. (Stanek 2010, 570.)

Käyttämällä useita sähköpostitietokantoja, konfiguroimalla tallennusmuisti asianmukaisesti ja jakamalla käyttäjät näihin tietokantoihin voidaan huomattavasti vähentää yhden tietokannan menettämisen vaikutusta. Tämä mahdollistaa myös nopeamman palautumisen vikatilanteessa. (Stanek 2010, 570.)

Käyttämällä näitä ominaisuuksia ja konfiguroimalla ne asianmukaisesti, ei välttämättä tarvita tietokannoista perinteisiä ajoitettuja varmuuskopiointeja tai pitkän aikavälin tallennustilaa nauha-asemalla. Korkean saatavuuden takaamiseksi, Microsoft suosittelee pitämään vähintään kolmea korkean saatavuuden tietokantakopiota. Tällöin yksi kopio on aktiivinen ja vähintään kaksi kopiota on passiivisena. Korkean saatavuuden kopio tarkoittaa kopiota, jolla ei ole viiveaikaa ja jota ei ole ylläpitäjän toimesta estetty aktivoitumasta. Tämä tarkoittaa, että tarvitaan vähintään kolme Mailbox-palvelinta jokaisessa korkean saatavuuden DAG -ryhmässä. (Stanek 2010, 570 - 571.)

Kokonaisuus, jossa on käytössä tietokantojen kopiot, ”hold policy”-sääntö ja ”Single page restore”, jättävät ongelmaksi vain erittäin harvinaisen, mutta vakavan tietokannan korruptoitumisen. Tästä korruptoitumisesta ja muista katastrofeista palautumiseksi suositellaan vähintään neljää tietokantakopiota. Tällöin yksi on aktiivinen kopio, kaksi on korkean saatavuuden passiivista kopiota ja yksi on viivästetty kopio. Tällöin tarvitaan vähintään neljä Mailbox-palvelinta DAG-ryhmässä. Viivästetty kopio on kopio, jolla on aikaeroa. Se auttaa tilanteissa, joissa korruptoitunut tietokanta on replikoitunut DAG-ryhmässä ja tarvitsee palata aikaisempaan tilaan. Poistettujen osien säilytys ja ”hold policy”-sääntö ovat ensisijainen puolustus palauttaa vahingossa poistetut postilaatikot tai postilaatikoiden tiedot. (Stanek 2010, 570 - 571.)

Jos aktiivisista tietokannoista on useita kopioita, halutaan yleensä yhden näistä kopiosta olevan pitkällä aikaerolla. Ajan tulisi olla niin pitkä, että ongelma ehditään paikallistamaan ja aloittaa palautus. Ympäristössä, jossa ylläpitäjä on aina paikalla, sopiva aikaero voisi olla 12, 24 tai 48 tuntia riippuen tarpeista. Muissa ympäristöissä sopiva aikaero olisi useampia päiviä. (Stanek 2010, 571.)

Osana Exchange-organisaation suunnittelua, pitäisi jokaisessa AD-toimipaikassa olla vähintään yksi Mailbox-palvelin. Koska mikä tahansa DAG-ryhmä voidaan ulottaa useille toimipaikoille, ei välttämättä tarvita useita Mailbox-palvelimia jokaisella toimipaikalla. Useampi toimipaikka Mailbox-palvelimille voi auttaa suojautumaan tietokeskukselle sattuvilta vioilta. Esimerkiksi jos toimipaikka A:han ei saada yhteyttä, mutta toimipaikka B:hen on yhteys, käyttäjät, jotka normaalisti ot-

taisivat yhteyden sähköpostilaatikoihinsa toimipaikka A:ssa, ohjattaisiin automaattisesti sopivaan Mailbox-palvelimeen toimipaikka B:ssä. (Stanek 2010, 571.)

Kun tietokantakopiota luodaan tai konfiguroidaan käyttäen komentoja ”Add-MailboxDatabaseCopy” tai ”Set-MailboxDatabaseCopy”, voidaan ne määritellä parametrilla ”-ReplayLagTime”. Tällä komennolla voidaan määrätä, kuinka kauan ”Exchange Information Store” -palvelun tulee odottaa, enne kuin lokitiedostot tyhjennetään. Parametrilla ”-TruncationLagTime” voidaan määritellä, kuinka kauan Exchangen replikointipalvelun tulisi odottaa, ennen kuin kaikki lokitiedostot, jotka on tutkittu kaikissa kopioissa, korvataan. (Stanek 2010, 571.)

Vaikka tietokantakopiot voivat poistaa tarpeen ajoitetuille tietokantojen vedoksille (snapshot), ne eivät poista tarvetta pitkän aikavälin varmuuskopiolle. Jotta näiden varmuuskopioiden tarvetta voidaan vähentää, tulee toteuttaa poistettujen osien säilytys ja ottaa käyttöön poistettujen sähköpostilaatikoiden säilytys. Suurimmassa osassa tapauksista halutaan poistettujen osien ja postilaatikoiden säilyvän vähintään 30, 60 tai 90 päivää. Lisäksi voidaan lisätä säilytyssääntö vahvistamaan viestien säilytysasetuksia ja konfiguroida arkistointi. (Stanek 2010, 572.)

6 TESTIYMPÄRISTÖN TOTEUTUS

6.1 Testiympäristön asennus

Luodun testiympäristön tarkoituksena on simuloida kaikkia yleisimpiä toimintoja, joita tullaan käyttämään varsinaisessa Päijät-Hämeen koulutuskonsernin tuotantoympäristössä. Sen tarkoituksena on myös selvittää mahdollisia toimintatapoja sekä ongelmatilanteita, joita saattaa tulla esille. Tässä opinnäytetyössä edellä käydyn teorian tueksi kokeiltiin joitain toimintoja käytännössä.

Testiympäristössä oli käytössä palvelin, johon oli valmiiksi asennettu Active Directory- ja DNS-palvelut. Tälle palvelimelle oli käytettävissä laajat Enterprise Admins -tason tunnukset, joita tarvittiin muun muassa Exchange-oikeuksien muuttamiseen. Jos tätä palvelinta ei olisi ollut, olisi nämä palvelut täytynyt asentaa, koska Exchange Server 2010 tarvitsee niitä. Tämä olisi tapahtunut asentamalla palvelimelle Windows Server 2008 -käyttöjärjestelmä ja lisäämällä palvelimelle ”Add Roles Wizard” -toiminnolla ”Active Directory Domain Services” -rooli. Tämän jälkeen olisi käynnistetty ”Active Directory Domain Services Installation Wizard”, jossa ”Configure Domain Name System Client Settings” -ikkunassa valittaisiin, että asennus ottaa DNS-palvelun automaattisesti käyttöön. ”Deployment Configuration” -ikkunassa valittaisiin ”Create a new domain in a new forest”. Tämän jälkeen olisi annettu haluttu FQDN-nimi ja valittu metsän toimintatasoksi ”Windows Server 2008”, jonka jälkeen asennus olisi ottanut AD- ja DNS-palvelut käyttöön.

Työasemina testiympäristössä toimi kaksi kannettavaa tietokonetta, joille asennettiin Windows 7 -käyttöjärjestelmä ja Microsoft Office 2007. Tämän jälkeen ne lisättiin käytössämme olevaan ”cd.lpt.fi”-toimialueeseen. Työasemia käytettiin testeissä AD:n ja Exchangen hallintaan, virtuaalipalvelimien ohjelmistojen asennukseen sekä etäkäyttöön. Lisäksi niillä käytettiin Outlook-sähköpostiohjelmaa.

Testiympäristön Exchange-palvelimien asennuksessa noudatettiin Microsoftin Exchange 2010 -koulutusmateriaalia. PHKK:n VMware-virtuaaliympäristöstä

saimme käyttöömme kaksi 64-bittistä virtuaalikonetta: ”exch-demo” ja ”exch-demo2”. Kummallakin virtuaalikoneella oli käytössään 4 Gt keskusmuistia, mikä riitti testiympäristön tarpeisiin. Näille virtuaalikoneille asennettiin 64-bittinen Windows Server 2008 R2 Enterprise -palvelinkäyttöjärjes-telmä. Asennuksen jälkeen koneille annettiin käytössä olevasta verkosta IP-osoitteet ja DNS-palvelimeksi asetettiin saamamme DNS-palvelimen IP-osoite.

Exchange Server 2010 -asennusmedian tiedostot purettiin virtuaalipalvelimien levyille. Tämän jälkeen asennettiin Exchange 2010:n tarvitsemat Net Framework 3.5.1 -ohjelmistokomponenttikirjasto, ISS -palvelu sekä roolien tarvitsemat Windows -ominaisuudet. Nämä ominaisuudet voitiin kaikki asentaa Powershell-komennolla: ”Add-WindowsFeature 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 -Restart”. Tämän jälkeen virtuaalipalvelimet liitettiin jäseniksi käytössämme olevaan ”cd.lpt.fi”-toimialueeseen.

Varsinainen Exchange-roolien asennus käynnistettiin palvelimien komentokehotteessa Exchange 2010 -mediakansiossa komennolla: ”setup.com /prepareAD /organizationname: demoexch”. Tällä komennolla pystyttiin lisäksi antamaan Exchange-organisaatiomme nimeksi ”demoexch”. Asennuksessa valittiin kummallekin virtuaalikoneelle Client Access-, Hub Transport- ja Mailbox-roolit. Nämä annettiin sen takia, että ne ovat tarvittavat Exchange-roolit toimivaan sähköpostijärjestelmään ja ne asennettiin kaikki samoille virtuaalikoneille, jotta testiympäristö olisi yksinkertainen. Tällöin saatiin tarvittavat toiminnot ja koska roolit olivat kummallakin virtuaalikoneella, voitiin testata myös vikasietoisuutta. Testiympäristön asennus sujui onnistuneesti ja ilman suurempia ongelmia.

6.2 Exchange 2010 -ominaisuuksien ja toiminnan testaus

Testijärjestelmässä kokeiltiin tärkeimpiä ja yleisimpiä Exchange 2010:n ominaisuuksia ja mahdollisia toimintoja mitä varsinaisessa järjestelmässä käytetään. Näihin liittyivät myös palvelimien vikasietoisuuden testaus sekä viestin ja tietokantojen palautus.

Aluksi tutkimme Exchange Management -konsolin näkymää Exchange 2010 -organisaatiosta. Siellä näimme organisaation asetukset ja roolien asetukset ja organisaatioon kuuluvat palvelimet ja näiden asetukset. Lisäksi konsolista nähtiin myöhemmin muun muassa käyttäjien postilaatikot, DAG-ryhmät, postituslistat sekä erilaisia oikeussääntöjä.

Aloitimme Exchangen ominaisuuksien testaamisen luomalla käyttäjälle sähköpostilaatikon. Tämä onnistui Exchange management -konsolista ”Recipient Configuration” ja Mailbox-välilehden alta valitsemalla ”New Mailbox”. Ohjatussa toiminnossa valittiin ”User Mailbox” ja valittiin ”Existing User”, joka lisättiin listaan. Ohjatussa toiminnossa voidaan myös valita tietokanta, johon postilaatikko tulee. Toiminnon kautta voidaan myös luoda uusia käyttäjiä, joille tulee suoraan postilaatikko. Tällöin annetaan käyttäjälle nimi ja salasana. Loimme myös uusia sähköpostilaatikoita laitteille sekä huoneille. Toimintatapa oli samantyylinen kuin käyttäjille.

Vaihdoimme käyttäjien sähköpostilaatikoiden kokorajoituksia Exchange Management -konsolista valitsemalla ”Microsoft Exchange On-Premises/ Organization Configuration/ Mailbox/Database Management” -välilehdeltä haluttu tietokanta ja avaamalla sen asetukset ”Properties”-kohdasta. Tämän jälkeen avautuvassa ikkunassa valittiin ”Limits”-välilehti, jolla näkyi kokorajoituskentät. Nämä kolme kenttää vaikuttavat siihen milloin järjestelmä ilmoittaa postilaatikon täyttymisestä, milloin se estää lähettämisen ja milloin se estää lähettämisen ja vastaanottamisen. Vastaavat muutokset voidaan tehdä myös yksittäiselle postilaatikolle. Muutimme kummallakin tapaa arvoja ja kokeilimme niiden toimintaa.

Kokeilimme lisätä testikäyttäjällemme oikeuden lähettää myös toisesta postilaatikosta kuin käyttäjän omasta. Tämä onnistui Exchange Management -konsolista ”Microsoft Exchange On-Premises/Recipient Configuration/Mailbox” -välilehdeltä, jossa valittiin postilaatikko josta käyttäjä saa lähettää. Postilaatikon ”Manage Send As Permissions” -listaan lisättiin testikäyttäjä. Tämän jälkeen kokeilimme onnistuneesti lähettää käyttäjällä postia lisätystä postilaatikosta, jolloin lähettäjän osoitteessa näkyi postilaatikon sähköpostiosoite. Lisäksi kokeilimme antaa testikäyttäjälle oikeuden lähettää sähköpostia toisen käyttäjän puolesta. Tällöin viestiin tuli merkintä, että käyttäjä on lähettänyt viestin toisen käyttäjän puolesta. Tämä oikeus lisätään postilaatikkoon, josta halutaan antaa muiden lähettää postia. Se tehtii Exchange Management -konsolista ”Microsoft Exchange On-Premises/Recipient Configuration/Mailbox” -välilehdeltä valitsemalla postilaatikko ja sieltä ”Properties”. Avautuvassa ikkunassa valitiin ”Mail Flow Settings” ja siellä ”Delivery Options” -listaan lisättiin käyttäjä, joka sai lähettää postia kyseisestä postilaatikosta.

Tämän jälkeen loimme jakelulistan, johon lähettämällä postia kaikki listaan lisätyt saavat viestin. Jakelulista luotiin Exchange Management -konsolista ”Microsoft Exchange On-Premises/Recipient Configuration/Distribution Group” -välilehdeltä valitsemalla ”New Distribution Group”. Avautuvassa ikkunassa valittiin uusi ryhmä, jolle annettiin nimi ja valittiin ”Distribution”. Listaa voitiin tämän jälkeen hallita valitsemalla se ja avaamalla ”Properties”. ”Members”-välilehdeltä voitiin lisätä jakelulistaan käyttäjiä valitsemalla ”Add”. Listoille voitiin antaa myös muita ominaisuuksia, kuten esimerkiksi listalle lähetetyn viestin hyväksyminen ryhmän ylläpitäjän toimesta, ennen viestin lähetystä muille listalla olijoille.

Loimme myös dynaamisen jakelulistan, joka muuttuu määriteltyjen sääntöjen mukaan. Exchange Management -konsolista valitsimme ”Recipient Configuration\ Distribution Group” -välilehdeltä ”New Dynamic Distribution Group”. Avautuvassa ikkunassa valitsimme organisaatioyksikön, johon jakelulista luotiin. Annoimme listalle nimen sekä aliaksen ja määrittelimme tasoksi käytetyn toimialueen, mistä käyttäjiä haetaan dynaamiseen jakelulistaan. Valitsimme jakelulistalle säännöksi ”Recipient is in a Department” ja kirjoitimme tälle osastoksi ”Tietohal-

linto”. Listalle ilmestyi odotetusti kaikki käyttäjät, jotka kuuluivat osastoon ”Tietohallinto”. Jos osastoon lisätään uusia käyttäjiä, tulevat ne automaattisesti listalle.

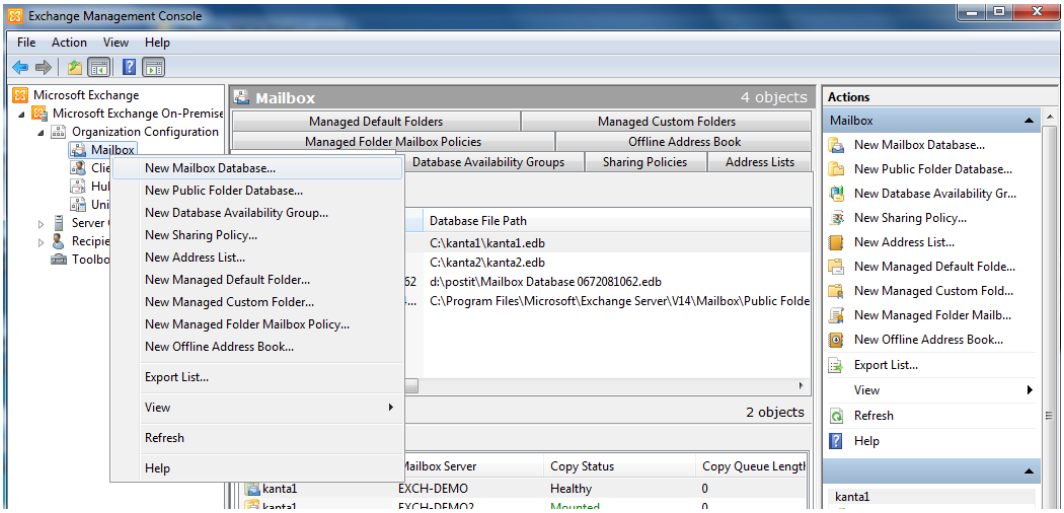
”Email Address Policies” -säännöillä muutettiin kuinka sähköpostiosoitteet luodaan käyttäjille automaattisesti. Exchange Management -konsolista valittiin ”Microsoft Exchange On-Premises/Organization Configuration/Hub Transport/ E-mail Address Polcies” välilehdeltä ”New E-mail Address Policy”. Avautuvassa ikkunassa annettiin säännölle nimi ja valittiin organisaatioyksikkö. Lisäksi säännölle voidaan valita myös tarkempia kriteerejä, kuten käyttäjän sijainti tai osasto. Tämän jälkeen valitaan listasta tyyli, jolla sähköpostiosoite muodostetaan. Valitsimme tyylin, jossa sähköpostiosoitteen alku muodostuu henkilön etu- ja sukunimestä ja niiden välissä on piste. Sitten valitsimme toimialueen, joka määrittelee osoitteen loppuosan. Havaitsimme, että uusien käyttäjien osoitteet muodostuivat säännön mukaisesti.

Käyttäjille lisättiin myös ylimääräisiä SMTP-osoitteita, jolloin käyttäjälle voitiin lähettää postia usealla osoitteella. Uuden osoitteen lisääminen onnistui Exchange Management -konsolista ”Microsoft Exchange On-Premises/Recipient Configuration/Mailbox” -välilehdeltä, josta valittiin sähköpostilaatikko ja sen ominaisuudet. Avautuvan ikkunan ”E-Mail Addresses”-välilehdeltä valittiin ”Add” ja lisättiin haluttu osoite. Jotta uusi sähköpostiosoite näkyy vastaanottajille, tulee valintaruutu ”Automatically update e-mail addresses based on e-mail policy” tyhjentää ja asettaa sähköpostiosoite ”Set as Reply” -tilaan.

Koska Päijät-Hämeen koulutuskonsernin käyttäjät ovat valmiiksi AD:ssa, tuli löytää yksinkertainen tapa luoda kaikille käyttäjille sähköpostitunnukset Exchange-sähköpostijärjestelmään. Tähän soveltui Exchange Management Shell, jolla voidaan hakea käyttäjät AD:n tietokannasta ja luoda jokaiselle sähköpostiosoite annettujen sääntöjen mukaan. Kokeilimme luoda testikäyttäjille onnistuneesti sähköpostiosoitteet Shell-komennolla: ”Get-User -OrganizationalUnit cd.lpt.fi/ testiou/users/marketti | Where-Object {$_.recipienttype -eq "User"} | Enable-Mailbox -Database “kanta””. Komento hakee kaikki objektit, jotka ovat tyyliä ”käyttäjä” ja ovat organisaatioyksikössä ”Marketti” ja luo sähköpostilaatikon tietokantaan ”kanta”.

Uuden osoitekirjan laitteille saimme luotua Exchange Management Shell -komennolla: ”New-AddressList -name 'Kaikki laitteet' -RecipientFilter {(ResourceType -eq 'Equipment')}”, joka luo osoitekirjan nimeltä ”Kaikki laitteet” ja rajaa vastaanottajat laitteiksi suodattimella ”Equipment”.

Kokeilimme luoda uusia sähköpostitietokantoja oletustietokannan lisäksi. Tämä onnistui Exchange Management -konsolilla, josta avattiin kuvion 11 mukaisesti ”Organization Configuration\Mailbox” ja valittiin ”New Mailbox Database”. Uudelle tietokannalle annettiin nimi ja valittiin palvelin, jolle kanta luodaan. Lisäksi määriteltiin sijainti levyllä, jonne tietokanta ja lokitiedostot tallentuvat.



KUVIO 11. Exchange Management -konsolin näkymä luotaessa uutta tietokantaa

Tämän jälkeen testasimme käyttäjien sähköpostilaatikoiden siirtoa tietokannasta toiseen. Tämän onnistui valitsemalla käyttäjän sähköpostilaatikko Exchange Management -konsolissa ja valitsemalla valikosta ”New Local Move Request”. Avatuvassa ikkunassa valittiin selaus, joka näytti käytettävissä olevat tietokannat. Valitsimme sähköpostilaatikolle uuden tietokannan ja hyväksyimme siirron. Siirto tapahtuu taustalla ja voi kestää jonkin aikaa riippuen laatikon koosta. Siirto onnistui ilman ongelmia.

Exchange Web-käyttöliittymä on oletuksena käytössä käyttäjille. Sen asetukset voitiin nähdä Exchange Management -konsolissa ”Server Configuration\Client

Access\Outlook Web App” -välilehdeltä, valitsemalla asetukset. Muutimme asetuksista käyttöliittymään kirjautumista ”Use forms-based authentication” -kohdasta niin, että toimialueen etuliitettä ei tarvinnut kirjoittaa, valitsemalla ”User name only”. Asetuksista otettiin käyttöön myös WebReady, joka näyttää Word, Excel, PowerPoint ja PDF tiedostot selaimessa. Kirjautuminen Web-käyttöliittymään toimi ilman ongelmia ja WebReadyn tukemat dokumentit aukesivat selaimessa.

Jotta käyttäjät näkisivät toistensa kalentereista, milloin toisilla on menoa tai ovat vapaina, täytyy kalenteri jakaa. Valitsimme Outlookista ”File\Folder\Change Sharing Permissions” -asetukset ja muokkasimme ”Default”-käyttäjän oikeuksia. Sille valittiin ”Read\FreeBusy time, subject, location”, jolloin kaikki voivat lukea, milloin käyttäjä on varattu tai vapaa sekä kalenterimerkinnän otsikon. Kokeilimme onnistuneesti samaa myös Outlook Web App:n kautta.

Määrittelimme Exchangelle SMTP-asetukset ulkopuolelta tulevaa postia varten. Loimme alitoimialueen ”foo.prv.phkk.fi”, jossa MX-tietue viittaa ensisijaisesti ”mail.prv.phkk.fi”-toimialueeseen. Hub Transport -palvelimelle luotiin uusi ”Accepted domain”, jossa määriteltiin postien vastaanottaminen luodulle ”foo.prv.phkk.fi”. Pääkäyttäjälle luotiin SMTP-osoite ”administrator@ foo.prv.phkk.fi” ja sallittiin Hub Transport -palvelimen ”Receive connector” -asetuksissa nimettömät lähettäjät. Saimme tämän jälkeen onnistuneesti lähetettyä sähköpostia käytössä olleesta Groupwise-järjestelmästä Exchange-järjestelmäämme.

Loimme kahdelle Mailbox-palvelimellemme DAG-ryhmän, jolloin toisen vikaantuessa toiselta voidaan hakea sähköpostitietokannat. Uusi DAG-ryhmä luotiin Exchange-hallintakonsolista avaamalla ”Organization Configuration” -ryhmä ja valitsemalla Mailbox-rooli. Seuraavaksi valittiin pikavalikosta ”New Database Availability Group”, jolloin ohjattu asennus käynnistyi. Ryhmälle annettiin nimeksi ”KeskusDAG”. Todistajapalvelimeksi valittiin toinen virtuaalikoneista. Todistajakansioksi annettiin jaettu kansio tällä virtuaalikoneella ja varmistettiin, että Exchangella on riittävät oikeudet tähän kansioon. Tämän jälkeen

”Manage Database Availability Group Membership” -listaan lisättiin halutut Mailbox-palvelimet, jolloin niistä tuli osa DAG-ryhmää ja ryhmä sai oman IP-osoitteen. Kantojen replikoitumisen jälkeen DAG-ryhmän toimintaa testattiin sammuttamalla aktiivista tietokantaa ylläpitävä Mailbox-palvelin. Exchange-hallintakonsolista näkyi, että tietokanta toisella Mailbox-palvelimella muuttui muutamassa sekunnissa aktiiviseksi ja sähköpostit voitiin lukea normaalisti.

Testasimme vikasietoisuuden toteuttamista myös käyttäjien pääsystä vastaavalle Client Access -palvelimelle luomalla ”Client Access Array” -ryhmän. Kummallekin ”exch-demo” -palvelimelle asennettiin ”Windows Network Load Balancing” -palvelu. Tämä asennettiin Windowsin ”Add Features” -työkalun kautta. Loimme Client Access -taulua varten DNS-palvelimelle uuden A-tietueen ”192.168.101.165 mail.cd.lpt.fi”. Tämän jälkeen kuormatasauspalvelun asetuksissa luotiin uusi klusteri ja lisättiin tähän kummatkin palvelimet antamalla palvelimien nimet ja IP-osoitteet. Seuraavaksi annettiin klusterille verkkotunnus ”mail.cd.lpt.fi” ja valittiin toimintatavaksi ryhmälähetys. Valitettavasti kuormatasausryhmän luonti epäonnistui, koska palvelimet oli liitetty jo palvelinklusteriin DAG-ryhmän takia, eivätkä samat palvelimet voi olla kummassakin.

Testasimme Exchange-palvelimen varmuuskopiointia Windows Server Backup -ohjelman avulla. Jos palvelin kuuluu DAG-ryhmään, tulee siltä aluksi poistaa käytöstä ”Microsoft Exchange Replication service VSS writer”. Käynnistimme Windows Server Backup -ohjelmiston ja valitsimme yhden kerran varmuuskopioinnin. Ohjatussa toiminnossa valitsimme varmuuskopioinnin kohteeksi palvelimen C-aseman ja kohteeksi paikallisen D-aseman. Seuraavaksi valitsimme ”Advanced Settings” -ikkunasta ”VSS Settings” -välilehdeltä ”VSS full Backup”. Tällöin koko kiintolevystä tehdään kopio, Exchange siirtää lokitiedostot tietokantoihin, poistaa lokitiedostot ja Exchange-palvelut voivat toimia taustalla operaation ajan. Seuraavaksi käynnistimme varmuuskopioinnin painamalla ”backup”.

Onnistuneen varmuuskopioinnin jälkeen kokeilimme tietokannan palautusta ”Microsoft Server Backup:n Volume Sanpshot -varmuuskopioista. Testissä poistimme käyttäjältä viestin purge-toiminnolla ja yritimme palauttaa sen käyttäjälle. Koska sähköpostilaatikkoon ei oltu määritelty ”Single Item Recovery”

-palautustoimintoa päälle, niin ainoa vaihtoehto oli palauttaa kansio ja viesti varmuuskopiosta. Avasimme Windows Server Backup -ohjelman ja painoimme ”palauta”. Avautuvassa ohjatussa toiminnossa valitsimme uusimman varmuuskopion. Varmuuskopio tyypiksi valitimme ”ohjelmisto” ja ohjelmistoksi valitsimme Exchangen. Palautus kohteeksi valitsimme D-aseman. Onnistuneen palautuksen jälkeen D-asemalla näkyi kansio, jossa sijaitsi kopiot Exchangen tietokannoista. Varmuuskopiointi ottaa huomioon vain aktiiviset tietokantakopiot eli sellaiset joiden tila on ”mounted”. Kansion ”kanta3” alta löytyi tietokanta (.edb) sekä lokitiedostot omassa kansiossaan. Avasimme Exchange-komentokehotteen ja siirryimme palautettuun kansioon. Kansiossa ajoimme komennon ”eseutil /MH ”kanta3.edb”, joka kertoo tietokannan tilan. Kannan tila oli ”Dirty Shutdown”, jolloin jouduimme kirjoittamaan tiedot lokeista kantaan komennolla ”eseutil /R E04 /l ”d:\C_\kanta3\lokit” /i /d”. Tarkistimme uudestaan kannan tilan ja nyt se oli “Clean Shutdown” -tilassa.

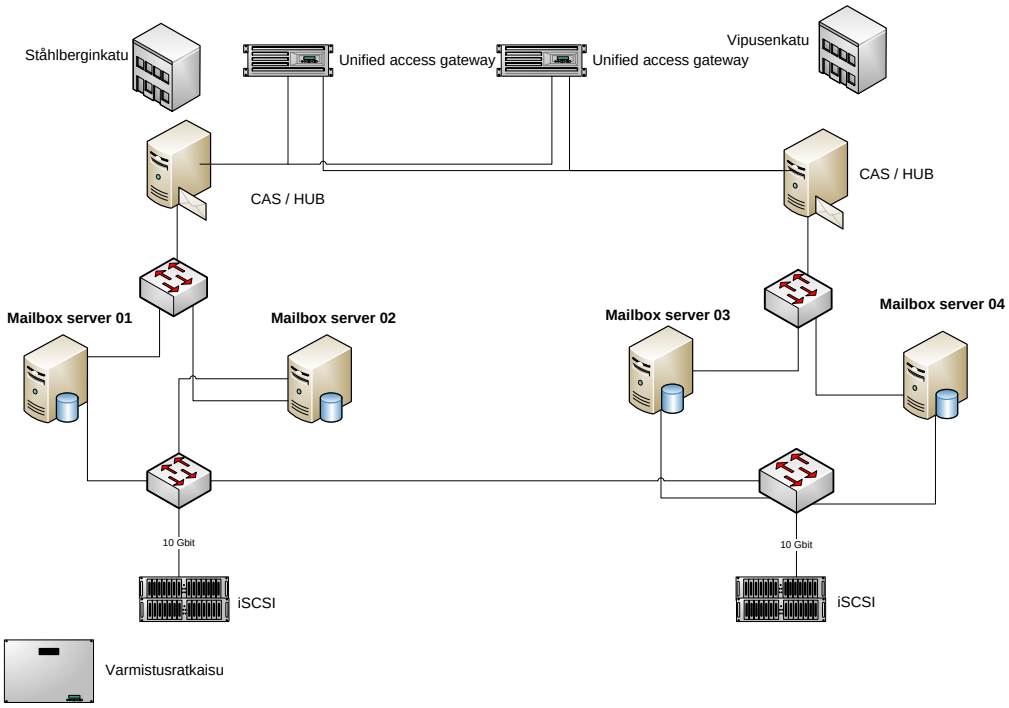
Loimme seuraavaksi uuden palautustietokannan Exchange Management Shell -komentokehotteesta komennolla ”New-MailboxDatabase -Name "Recovery Database" -Server exch-demo -EdbFilePath "d:\C_\kanta3\kanta3.edb" -LogFolderPath "d:\c_\kanta3\lokit\" -recovery”. Kanta tuli näkyviin Exchange-hallinnassa. Tämän jälkeen otimme tietokannan Exchangessa aktiiviseksi valitsemalla Exchange Management -konsolissa ”Mount Database”. Komentorivillä annoimme komennon ”Restore-Mailbox -Identity kosonjuk -RecoveryDatabase "recovery database" -RecoveryMailbox "Kosonen" -TargetFolder Recovery”, joka palautti varmistuksesta Kososen sähköpostilaatikon hänen nykyiseen sähköpostilaatikkoonsa ”Recovery”-kansioon. Tämän jälkeen kansio näkyi Outlook:ssa ja poistetut viestit näkyivät kansiossa. Palautus oli tällöin onnistunut.

Eräänä tärkeänä tavoitteena oli myös, että käyttäjät voisivat tuoda vanhasta Novell Groupwise -sähköpostijärjestelmästä omat kalenterimerkintänsä uuteen järjestelmään. Tämän toiminta testattiin avaamalla Groupwise-asiakasohjelma ja valitsemalla kalenteri. Valitsemalla ”Export” voitiin kalenteri tuoda ohjelmasta iCal-tiedostona. Tämä tiedosto voitiin Outlookissa ”Import and Export Wizard” -toiminnon avulla tuoda Outlookin kalenteriin. Siirto onnistui ilman ongelmia.

Exchange Server 2010 -sähköpostijärjestelmästä löytyi käyttäjille paljon samoja toimintoja kuin löytyy PHKK:n aikaisemmasta Novell GroupWise 8 -järjestelmästä. Exchange Server 2010:n etuina voisin nähdä tehokkuuden, laajennettavuuden, viestin palautuksen ja helpon tavan saavuttaa palveluiden korkea saatavuus. Tallennustilan tarve tulevassa Exchange-järjestelmässä tulee kuitenkin olemaan suuri, johtuen sähköpostilaatikoiden koosta, määrästä ja niiden tietokantojen passiivista ja viivästytetyistä kopioista. Mitään suuria ongelmia ei työssä ilmennyt eikä selvittämättömiä ongelmia testien jälkeen jäänyt varsinaisen järjestelmän testeihin. Varsinaisen järjestelmän lopullinen arkkitehtuuri ja palvelimien laitteisto jäi tämän työn ulkopuolelle ja vielä päättämättä.

6.3 Exchange 2010 -arkkitehtuuri

PHKK:n uuden Exchange Server 2010 -sähköpostijärjestelmän mahdollisessa arkkitehtuurissa (KUVIO 12) palvelimet olisi sijoitettu kahteen eri palvelinsaliin, jotka sijaitsevat eri fyysisissä pisteissä. Tällä voidaan ehkäistä koko sähköpostijärjestelmän toiminnan lakkaaminen, mikäli toisessa palvelinsalissa sattuu tulipalo, vesivahinko tai muu vastaava onnettomuus. Kummassakin palvelinsalissa tulee olla Exchangen toiminnalle välttämättömät Mailbox ja Client Access -roolit. Tällöin voidaan myös säilyttää palveluiden toiminta, vaikka jokin palvelin tai verkko vikaantuisi. Client Access ja Hub Transport -roolit voidaan sijoittaa samalle palvelimelle. Mailbox-palvelimien tulee olla DAG-ryhmässä, jotta kummallakin toimipaikalla olisi kaikkien käyttäjien sähköpostilaatikot ja ne olisivat ajan tasalla. Järjestelmässä ei välttämättä tarvita erillistä ajoitettua varmuuskopiointia sähköpostilaatikoille, johtuen usean Mailbox-palvelimen DAG-järjestelmästä ja jos viivästetyt kopiot sähköpostitietokannoista ovat käytössä. Viivästettyjen kopioiden saamiseksi tarvitaan neljä Mailbox-palvelinta. On hyvä ottaa myös käyttöön ”Deleted item retention”, jolloin vahingossa poistetut sähköpostit on helppo palauttaa. ”Microsoft Forefront Unified Access Gateway” on Microsoftin edustajan suosittama VPN-ratkaisu ja käänteinen välityspalvelin, jolla käyttäjät saavat turvallisen yhteyden sähköpostilaatikoihinsa organisaation ulkopuolelta.



KUVIO 12. PHKK:n Exchange Server 2010 -järjestelmän mahdollinen arkkitehtuuri

7 YHTEENVETO

Opinnäytetyössä perehdyttiin Microsoft Exchange Server 2010 -sähköpostijärjestelmään ja tutkittiin sen soveltumista Päijät-Hämeen koulutuskonsernin käyttöön. Opinnäytetyö perustuu PHKK:n koulutuskonsernin työntekijöiden toiveisiin uudistaa ja parantaa tämänhetkistä järjestelmää. Tavoitteina uudelle sähköpostijärjestelmälle oli muun muassa suuremmat sähköpostilaatikot, tuki mobiililaitteille, kalenteri, yhteystiedot sekä järjestelmän laajennettavuus, vikasietoisuus ja luotettavuus.

Työn teoriaosuudessa perehdyttiin Exchange 2010 -ohjelmiston käyttöönottoon liittyviin asioihin, kuten laitteisto- ja ohjelmistovaatimuksiin. Lisäksi selvitettiin eri roolien tarkoitukset ja niiden toiminta ja tutustuttiin hallintatyökalujen toimintaan. Työssä tutkittiin myös, kuinka Exchange liittyy AD:hen ja kuinka viestinvälitys toimii Exchange-järjestelmässä. Käyttöoikeuksien osalta tutkittiin roolipohjaisen oikeusmallin toimintaa ja oikeuksien antamista. Lisäksi perehdyttiin, kuinka järjestelmästä saadaan vikasietoinen, ja selvitettiin, miten DAG-ryhmä luodaan ja miten se toimii.

Käytännön osuudessa toteutettiin virtuaalikoneiden avulla Windows Server 2008 -testiympäristö, johon asennettiin Exchange Server 2010 -sähköpostijärjestelmä. Järjestelmässä testattiin työlle asetettuja tavoitteita ja käytiin etukäteen läpi varsinaisessa tuotantoympäristössä eteen mahdollisesti tulevia asioita.

Testijärjestelmässä testattiin Exchange-palvelimien asennusta, eri roolien toimintaa, sähköpostilaatikoiden tekoa, kalenterien ja ajanvarauksen toimintaa, jakelulistoja, Shell-komentosarjoja, vikasietoisuutta, varmuuskopiointia sekä tietokantojen luontia. Tavoitteista ainoastaan Exchangen toiminta mobiililaitteiden kanssa jäi testaamatta. Tämä johtui muun muassa siitä, että testijärjestelmään ei ollut mahdollisuutta saada yhteyttä Internetistä. Exchangen toiminta mobiililaitteiden kanssa ei pitäisi teoriatietojen pohjalta olla kuitenkaan ongelma varsinaisessa järjestelmässä.

Lopuksi suunniteltiin mahdollinen arkkitehtuurimalli PHKK:n tulevalle

Exchange-sähköpostijärjestelmälle. Mallin järjestelmä on vikasietoinen, se tarjoaa riittävät toiminnallisuudet ja on riittävä tulevaisuuden kasvutarpeita ajatellen.

Exchange Server 2010 soveltuu kaiken kokoisiin organisaatioihin ja sitä voidaan helposti laajentaa lisäämällä järjestelmään palvelimia tarvittavilla rooleilla. Se voidaan siis toteuttaa PHKK:n noin 2500 sähköpostilaatikon käyttöön. Vikasietoisuus on helppo saavuttaa ottamalla käyttöön useampia saman roolin palvelimia. DAG mahdollistaa käyttäjien pääsyn sähköpostilaatikoihin, vaikka jokin Mailbox-palvelin vikaantuisi. Client Access Array mahdollistaa käyttäjien käyttää Exchange-palveluja, vaikka jokin Client Access -palvelin vikaantuisi. Ajastettuja varmuuskopioita ei välttämättä tarvita jos tietokantakopioita on riittävästi ja yksi niistä on viivästytetty. Exchange tarjoaa yksinkertaisen, mutta hyvin kattavan roolipohjaisen oikeusmallin, jolla voidaan organisaatiossa antaa eri oikeudet eri ryhmille.

Mitään esteitä Microsoft Exchange Server 2010 -sähköpostijärjestelmän soveltuvuudelle PHKK:n käyttöön ei testiympäristössä ilmennyt. Kaikki PHKK:n antamat ja opinnäytetyöntyön alussa asetetut tavoitteet, niin käyttäjien kuin ylläpitäjienkin osalta voidaan toteuttaa. Siirtyminen Exchange-järjestelmään tuo siis mukanaan monia etuja, niin käyttäjille kuin ylläpitäjillekin.

LÄHTEET

Cunningham, P. 2010. Exchange Server 2010 Database Availability Group Installation Step by Step [viitattu 3.3.2011]. Saatavissa: http://exchangeserverpro.com/exchange-server-2010-database-availability-group-installation-step-by-step

Jarva, M. 2008. Case: Javerdel Oy:n toimialue ja Exchange. Opinnäytetyö. Tampereen ammattikorkeakoulu.

Kivimäki, J. 2005. Active Directory - Tehokas hallinta. Jyväskylä: Gummerus.

McBee, J. 2009. Mastering Microsoft Exchange Server 2007 SP1. Indianapolis, Indiana: Wiley.

McBee, J. & Elfassy D. 2010. Mastering Microsoft Exchange Server 2010. Indianapolis, Indiana: Wiley.

Microsoft TechNet. 2009. High level Exchange 2010 architecture [viitattu 3.3.2011]. Saatavissa: http://blogs.technet.com/b/ucedsg/archive/2009/06/29/high-level-exchange-2010-architecture.aspx

Microsoft TechNet. 2010. Understanding Exchange ActiveSync [viitattu 1.11.2010]. Saatavissa: http://technet.microsoft.com/en-us/library/aa998357.aspx

Microsoft. 2010. Exchange 2010 Overview [viitattu 1.11.2010]. Saatavissa: http://www.microsoft.com/exchange/2010/en/us/overview.aspx

Morimoto, R., Noel, M., Amaris, C., Abbate, A. & Weinhardt, M. 2010. Microsoft Exchange Server 2010 Unleashed. Indianapolis, Indiana: SAMS.

Posey B. 2007. How an Edge Transport server works [viitattu 1.3.2011]. Saatavissa: http://searchexchange.techtarget.com/tutorial/Step-1-How-an-Edge-Transport-server-works

Redmond, T. 2010. Microsoft Exchange Server 2010 Inside Out. Redmond, Washington: Microsoft Press.

Stanek, W. 2010. Microsoft Exchange Server 2010 Administrator's Pocket Consultant. Redmond, Washington: Microsoft Press.