VIKASIETOINEN VIRTUAALIPALVELINJÄRJESTELMÄ

Juha Turpeinen
Opinnäytetyö
Syksy 2010
Tietoliikennetekniikan koulutusohjelma
Oulun seudun ammattikorkeakoulu

Oulun seudun ammattikorkeakoulu
Tietotekniikan koulutusohjelma, tietoliikennetekniikka

Tekijä: Turpeinen Juha
Opinnäytetyön nimi: Vikasietoinen virtuaalipalvelinjärjestelmä
Työn ohjaaja: Rahikainen Markku
Työn valmistumislukukausi ja -vuosi: Syksy 2010 Sivumäärä: 41

TIIVISTELMÄ

Virtualisointi on viime vuosien aikana yleistynyt yritysmaailmassa huimasti. Virtualisoinnin avulla yrityksissä haetaan säästöjä niin energian kuin laiteresurssienkin kustannuksissa. Lisäksi virtualisointi mm. nopeuttaa uusien järjestelmien käyttöönottoa sekä mahdollistaa käyttöönotettavien järjestelmien testauksen ilman uusien laitteiden hankintaa. Virtualisointi valjastaa käytännössä palvelinlaitteiston täydelliseen suorituskuormaan.

Työssä mallinnettiin pk-yrityksen tyypillinen palvelinkokonaisuus virtuaalisesti sekä tarjottiin vaihtoehtoinen Linux-pohjainen Zarafa-sähköpostipalvelin yleisesti käytetyn Microsoft Exchangen tilalle. Rakennettu toimialueympäristö konfiguroitiin minimivaatimusten mukaan siten, että yrityskäyttöön kokonaisuutta siirrettäessä jouduttaisiin järjestelmä määrittämään tarkemmin asiakkaan tarpeiden mukaan.

Tietoperustana käytettiin pääasiassa työelämässä muutamien vuosien aikana karttunutta käytännön kokemusta sekä Internet-lähteitä ja -artikkeleita. Niitä löytyikin huomattavasti enemmän, kuin paperiversioita; lisäksi alan nopea kehitys tekee kirjamuotoisesta tiedosta aika ajoin vanhentunutta.

Työssä saavutettiin haluttu lopputulos järjestelmän toimivuuden sekä käytettävyyden kannalta. Lisäksi opinnäytetyön valmistuminen on kartutti jo aiempaa osaamista itse virtualisoinnista sekä etenkin Linux-ympäristöstä.

Valmiin järjestelmän toimivuus on hyödynnettävissä täysin pk-yritysmaailmaan. Tämän johdosta työn aikana kypsyi idea alkaa markkinoida tuotetta eteenpäin. Tämä puolestaan johti oman yrityksen perustamissuunnitelmaan, jonka mukaan toiminta on tarkoitus aloittaa vielä vuoden 2010 kuluessa. Järjestelmän kehittäminen sekä tietotaidon kartuttaminen jatkuu siis varmasti asian tiimoilta vielä vuosia.

Asiasanat:

Virtualisointi, virtuaalipalvelin, VMWare, domain, Zarafa, vikasietoinen toimialue

Oulu University of Applied Sciences
Information Tehcnology, Telecommunications

Author: Turpeinen Juha
Title of thesis: Fault Tolerant Server Domain Using Virtualization
Supervisor: Rahikainen Markku
Term and year when the thesis was submitted: Autumn 2010 Number of pages: 41

ABSTRACT

During past years, virtualization has become a very common way to implement enterprise's server systems. By virtualizing servers and other services, an enterprise gains remarkable savings in consumed energy and hardware investments. Virtualization also makes new system deployments quicker and makes possible to test them without aquiring new hardware.

The purpose of this thesis work is to create a model of a small-enterprise's domain and provide an alternative e-mail service with full functionality compared to Microsoft's Exchange, which is Linux-based Zarafa. The created system is configured only using minimum settings to make everything work. When implementing system in practise, more configurations are needed to be done by depending on customer's demands.

Main sources of information used in this thesis are web-based and gained expertise from few years in working life. Bookish information were not used because virtualization industry developes in accelerating pace, which makes a lot written information outdated. Also web-based information is much more easily achievable.

Main goal of this thesis was achieved in every possible way. The created system was fully functional in every way that was planned. Lots of new expertise was gained in virtualization matters as well in Linux-environment.

As a conclusion, a fully functional, self-created environment gave many new ideas concerning virtualization. Last but not least, this thesis work gave an inspiration to market this product forward. Efforts to found a new company has already been done, and hopefully new work will begin during year 2010. You can say for sure, that studying and developing virtual systems will continue for years; thanks to this thesis work.

Keywords:

Virtualization, virtual server, VMWare, domain, Zarafa, fault tolerant domain

LYHENTEET JA TERMIT

AD	Active Directory; Microsoftin aktiivihakemisto mikä mahdollistaa toimialueen- sekä käyttäjähallinnan.
Administrator	Järjestelmän pääkäyttäjä
BDC	Backup Domain Controller; toimialueen varaohjauskone
Boot	Tietokoneen käynnistäminen; re(-)boot = uudelleen käynnistäminen.
CentOS	Ilmainen Linux-ytimeen pohjautuva käyttöjärjestelmä.
Daemon Tools	Työaseman virtuaalisen asemamäärityksen mahdollistava ohjelmisto.
DC	Domain Controller; toimialueen ohjauskone
DFS	Distributed File System; Windows Server -järjestelmän replikointiominaisuus.
DHCP	Dynamic Host Configuration Protocol; verkkoprotokolla, jonka tärkein tehtävä liittyy verkon IP-osoitteiden jakamiseen.
DHCP-pool	IP-osoitteiden ”allas”, josta reitin tai palvelin jakaa vapaita IP-osoitteita verkon laitteille.
DNS	Domain Name System; Internetin nimipalvelujärjestelmä, joka muuntaa verkkotunnukset IP-osoitteiksi. Toimii myös sähköpostin reitityksessä.
Domain	Toimialue, joka sisältää esim pk-yrityksen palvelimet, työasemat, käyttäjätunnukset sekä näiden kaikkien hallinnan.
ESX-palvelin	Maksullinen VMWaren virtualisointialusta yrityskäyttöön.
ESXi-palvelin	Ilmainen VMWaren virtualisointialusta, soveltuu myös yrityskäyttöön.
Exchange	Microsoftin sähköpostipalvelinohjelmisto.
Explorer	Web-selain
GP	Group Policy; toimialueen sääntö AD-ympäristössä.
Konfiguraatio	Asetus
Kytkin	Verkon laitteita yhdistävä komponentti.
Image	Datamuotoon tallennettu esim. DVD-levy tai palvelin.
IP-osoite	Verkon laitekohtainen tunnistesarja; liittyy olennaisesti *verkkomaskiin*.

LDAP	Verkkoprotokolla, jonka pääasiallinen tehtävä on käyttäjätunnistus.
Linux	Pidemmälle viety versio *Unix*ista, osa versioista maksullisia.
NAT	Network Access Translation; tekniikka, jolla säästetään tai piilotetaan julkisia IP-osoitteita.
PDC	Primary Domain Controller; ts. DC
RAID	Redundant Array of Independent Disks; kiintolevyjärjestelmä
Reititin	Laite joka yhdistää tietoverkot toisiinsa esim. lähiverkon ja Internetin.
Replikointi	Tiedostojen automaattinen kopiointi toiseen kohteeseen, ks. *DFS*.
Snapshot	Eräänlainen nopeasti otettava varmuuskopio järjestelmästä.
Unix	Laitteistoriippumaton ilmainen käyttöjärjestelmä.
Verkkomaski	Network Mask; määrittää alaverkossa olevien mahdollisten koneiden maksimimäärän. Liittyy *IP-osoitteeseen*.
VMWare	VMware Inc; virtualisointiohjelmistojen valmistaja.
VMware Server	Virtualisointiohjelmisto kevyempään mallintamiseen Windows-alustalle.
VMware vSphere	Laaja kokonaisuus VMWaren ohjelmistoja yrityskäyttöön.
Webmin	Linux -järjestelmän web-hallintasovellus.
Windows	Työaseman käyttöjärjestelmä; eri versioita kuten XP/Vista/7
Windows Server	Palvelimen käyttöjärjestelmä; versioita mm. 2000/2003/2008
Zarafa	Ilmainen sähköpostiohjelmisto Linux -alustalle.

ALKUSANAT

Haluan aluksi antaa kiitokset kahdelle yhteistyökumppanille avusta, jota ilman lopputyön tekeminen olisi ollut käytännössä erittäin vaikeaa: konsultoinnissa järjestelmäasiantuntija Jarmo Jokelalle (Way 4 U Oy) sekä ICT Services Manager Matti Tuomikoskelle (WinWinD Oy) ohjelmistoavaimien käytöstä.

Oulussa 26.9.2010

Juha Turpeinen

SISÄLLYS

TIIVISTELMÄ....3
ABSTRACT....4
LYHENTEET JA TERMIT....5
ALKUSANAT....7
1 JOHDANTO....10
2 VIRTUALISOINTI....11
2.1 Yleisesti....11
2.2 VMware Server -ohjelmisto....11
3 DOMAIN ELI TOIMIALUE....13
3.1 Määritelmä....13
3.2 Toimialueen osat....13
3.2.1 Domain Controller....13
3.2.2 Active Directory AD....14
4 PALVELINJÄRJESTELMÄN SUUNNITTELU JA TOTEUTUS....15
4.1 Työssä käytetyt laitteet ja ohjelmistot....15
4.2 Ympäristön luonti....16
4.2.1 VMware Server 2.0....16
4.2.2 Snapshot....18
4.2.3 Verkko-osoitteet....18
4.2.4 Yhteyden testaus....19
4.3 Palvelimet....20
4.3.1 DC....20
4.3.2 File....22
4.3.3 Zarafa....23
4.4 Sähköpostin testaus....25
4.5 Tiedonvarmistus ja vikasietoisuus....28
4.5.1 Yleistä järjestelmistä....28
4.5.1 DFS-replikointi....29
4.5.2 Snapshot-menetelmä....30
4.5.3 RAID-levyjärjestelmä....30

4.5.4 Nauha-asemat 31
4.5.5 Shadow copy -palvelu 31
4.5.6 VMware vSphere -kokonaisuus 32
5 JOHTOPÄÄTÖKSET JA POHDINTA 33
LÄHTEET 35
LIITE 1 37

1 JOHDANTO

Tämän opinnäytetyön tavoitteena oli rakentaa minimivaatimuksilla toimiva virtuaalinen domain eli toimialue, joka pystytään tarvittaessa hyödyntämään pk-yrityskäyttöön sekä tarjota Linux -pohjainen ilmainen Zarafa-sähköpostipalvelin perinteisen Microsoft Exchangen tilalle. Työssä on hyödynnetty VMware Server -ohjelmistoa, jonka käyttö on ilmaista. Kun järjestelmä halutaan ottaa yrityskäyttöön muuttuu käytettävä alusta ESX Server -pohjaiseksi, jolloin järjestelmän tehokkuus korostuu. VMware Server -ohjelmisto on siis tarkoitettu vain kevyeen mallinnukseen eikä raskaaseen ammattikäyttöön. ESX Server -ympäristöön siirryttäessä järjestelmän käyttö kuitenkin säilyy suhteellisen samanlaisena kuin VMware Server -alustaa käytettäessä.

Linux-ympäristön mukaan ottaminen tuo omat haasteensa, sillä työn tekijän aikaisempi käyttökokemus järjestelmästä on vähäinen, joskaan ei olematon. Sähköpostipalvelin Zarafa on rakennettu juuri Linux-järjestelmän päälle ja oikein konfiguroituna se korvaa täysin yleisesti käytössä olevan Microsoft Exchangen, vähentää merkittävästi yrityksen kustannuksia nykyään kalliissa lisenssimaksuissa.

Virtualisointi on käytännössä järkevä tapa hoitaa yrityksen palvelinratkaisut, kun halutaan puhua vihreästä IT-alasta. Virtualisoinnin avulla voidaan moniajaa esimerkiksi viittä palvelinta yhdessä laitteistotason palvelimessa sen sijaan, että käytettäisiin samaan tarkoitukseen viittä eri laitteistotason palvelinta. Tämä vähentää uusien palvelimien hankintakustannukset lähes nollaan sekä säästää energiankulutuksessa huomattavia summia vuositasolla. Myös vuosia vanhan palvelinlaitteiston voi korvata virtualisoinnilla, jolloin järjestelmän suorituskyky kasvaa, koska emuloitava virtuaalilaitteisto on yleensä tehokkaampaa suorituskyvyltään kuin vanhentuneet palvelimet. Lisäksi palvelimen iän aiheuttamat mekaanisen rikkoutumisen riskit pienenevät.

2 VIRTUALISOINTI

2.1 Yleisesti

Virtualisoinnilla tarkoitetaan yleisesti jonkun tietyn resurssin, kuten palvelimen, kiintolevyn, tietoverkon jne., simulointia jonkin ohjelmiston avulla ilman oikeaa laitetason ratkaisua. Esimerkiksi tavallinen työasema voidaan tehdä virtuaalisesti siten, että fyysiseen työasemaan asennetaan virtualisoinnin mahdollistava ohjelmisto, jonka avulla luodaan uusi virtuaalinen työasema ilman, että uutta laitteistoa tarvitsee hankkia. Tämän mahdollistavia ohjelmistoratkaisuja on useampia, mutta tämä työ käsittelee aihetta ainoastaan VMwaren valmistamien tuotteiden pohjalta. (1.)

Virtuaalisen työaseman luominen esimerkiksi testikäyttöön on huomattavasti nopeampaa, edullisempaa ja vaivattomampaa kuin oikean tietokoneen käyttö tähän tarkoitukseen. Työaseman käyttöönotto vie yleensä vain murto-osan ajasta verrattuna fyysiseen koneeseen, koska virtuaalisen työaseman laitteet emuloivat isäntäkoneen laitetason ratkaisuja. Nopeusetu tulee myös nopeasti esille virtualisointia käytettäessä: Windows XP/Vista/7/Server-järjestelmiä joutuu aika ajoin uudelleen käynnistämään (boottaamaan) ja virtualisoituna työaseman re-boot-aika on useita kertoja pienempi, kuin fyysisen koneen. Käytännössä virtuaalisen työaseman käyttö ei poikkea normaalista mitenkään, koska luotu työasema on täysin itsenäinen tietokone, jota vain ajetaan ikkunamoodissa esimerkiksi tavallisen Windows-järjestelmän työpöydällä.

2.2 VMware Server -ohjelmisto

Työn toteutuksessa käytetty VMware Server on virtualisoinnin mahdollistava ohjelmisto, joka asennetaan suorituskykyiseen työasemaan. Ohjelmisto soveltuu erityisesti erilaisten pienen kokoluokan palvelinkokonaisuuksien mallintamiseen työpöytäkäytössä. Haittapuolena palvelinten virtualisoinnissa on luonnollisesti suorituskyvyn laskeminen verrattuna oikeaan laitetason ratkaisuun; tosin sillä ei ole suurta merkitystä esimerkiksi kohtuukuormitetuilla lisenssi-, tietokanta- tai sähköpostipalvelimilla.

Kevyemmän mallinnuksen käydessä riittämättömäksi VMware tarjoaa Server-ohjelmiston tilalle ESX Server -käyttöjärjestelmän, mikä optimoi laitteiston käytön huomattavasti tehokkaammin kuin

VMware Server -ohjelmisto. Käytännössä yritysten virtuaalipalvelinratkaisut toteutetaan ESX Server -alustalla (tai jonkun muun valmistajan ratkaisulla).

Virtuaalikoneiden luonti on tehty suhteellisen helpoksi alaa tuntevan kannalta. Itse ohjelmaa ajetaan Javascriptin pohjalta Internet-selaimessa, esimerkiksi Internet Explorerissa. Virtuaalikonetta luotaessa siihen määritellään perusasiat laitetasolla, kuten prosessoriytimien määrä, muistin määrä, kiintolevyn koko jne. Määrittelyssä onkin tärkeää ottaa huomioon isäntäkoneen resurssit. Muistia kuluu runsaasti, sillä esimerkiksi työssä käytetyille Windows 2008 Server -käyttöjärjestelmälle suositellaan vähintään 1 Gt muistia, jonka virtuaalikone ottaa suoraan käyttöön isäntäkoneen RAM-muistista.

3 DOMAIN ELI TOIMIALUE

3.1 Määritelmä

Domainilla voidaan tarkoittaa muutamaa eri asiaa. Tässä työssä kyseessä on Windows Server Domain eli toimialuekokonaisuus. Yrityskäytössä domainin muodostavat keskitetysti hallittava joukko työasemia, palvelimet sekä erilaiset verkon laitteet. Jokainen työasema sekä palvelin on toimialueen järjestelmävalvojan hallittavissa.

Jokaisella toimialueen käyttäjällä on henkilökohtainen käyttäjätili, joka on määritelty esimerkiksi Windows Server -käyttöjärjestelmän Active Directory (myöhemmin AD) -ohjelmistokokonaisuudessa. Käyttäjätilin perusteella voidaan jakaa erilaisia käyttöoikeuksia toimialueen työasemiin ja palvelimiin sekä mm. verkkoresursseihin. Toimialueen luonti yrityksissä on erittäin suositeltavaa, sillä se helpottaa järjestelmän hallintaa sekä antaa mahdollisuuden lähes täydelliseen tietoliikenteen hallintaan, joka koskee kyseisen toimialueen koneita. (2.)

3.2 Toimialueen osat

3.2.1 Domain Controller

Toimialueen tärkein laite on Domain Controller (myöhemmin DC) eli ohjauskone. Se vastaa toimialueen sisällä käytännössä kaikesta, mikä liittyy käyttäjätilin tai työaseman toimintaan lähiverkossa.

Pienemmissä yrityksissä riittää yleensä kun DC:itä on yksi kappale. Toiminnan kasvaessa halutaan yleensä järjestelmään lisää vikasietoisuutta, jolloin voidaan ottaa käyttöön useampia toimialueen ohjauskoneita. Tällaisessa tapauksessa luodaan yksi isäntäkone Primary Domain Controller (PDC), joka on muiden ohjauskoneiden yläpuolella. Alemman tason toimialueen ohjauskoneet eli Backup Domain Controllerit (BDC) voivat sisältää erilaisia palveluita, jotta PDC ei kuormittuisi liikaa ja hidastaisi työasemien toimintaa verkon sisällä. Tällaisia palveluita, joita voidaan hajauttaa BDC:ille, ovat esimerkiksi DHCP, DNS sekä verkkotulostuksen hallinta.

Rakennettaessa järjestelmää vikasietoisemmaksi, esimerkiksi tilanteessa, jossa PDC sammuu tai rikkoontuu, voidaan jokin tietty BDC asettaa ottamaan toimialueen PDC-rooli (priorisointi). Tällöin

toimialueen käyttökatkos on suhteellisen lyhyt, eivätkä verkon käyttäjät tipahda ”tyhjän päälle”. (3.)

Tässä opinnäytetyössä toimialue toteutettiin ainoastaan yhdellä DC:llä, johtuen työn tekijän rajallisista resursseista. On myös hyvä ottaa huomioon, että PDC sijaitsisi rautapalvelimella eikä sitä toteutettaisi virtuaalisesti. BDC:t puolestaan voi toteuttaa huoletta virtualisoinnilla, kuitenkin siten, että yhdellä ESX Server-palvelimella sijaitsee vain yksi BDC. Tämä lisää järjestelmän vikasietoisuutta tilanteissa, joissa esimerkiksi PDC ja priorisointitasolla 1 oleva BDC sammuvat tai rikkoontuvat.

DC:n rooleja ja ominaisuuksia ei tässä työssä käsitellä tämän tarkemmin, koska aihe on todella laaja eikä niillä olisi merkitystä työn suorittamisen kannalta.

3.2.2 Active Directory AD

Toimialueen käyttäjä- ja resurssihallinnan kannalta tärkein komponentti on Active Directory eli AD (aktiivihakemisto). Se on laaja keskitetty hallintakokonaisuus ja tietokanta, jossa määritetään mm. toimialueen käyttäjätilit, käyttäjäryhmät, toimialueen työasemien ominaisuuksiin vaikuttavat käytäntöryhmät eli Group Policyt (GP) jne. GP:n avulla voidaan hallita esimerkiksi yli tuhatta (1000) eri ominaisuutta, jotka koskevat käyttäjää tai työasemaa. Käytäntöryhmiä käyttämällä saadaan aikaan mahdollisimman standardi sekä helposti hallittava ja ylläpidettävä it-käyttöympäristö.

IT-Pro määrittelee AD:n seuraavasti: ”Aktiivihakemisto toimii käyttäjien ja muiden toimialueresurssien keskitettynä hallintapisteenä. Käyttäjät tunnistautuvat työasemilta aktiivihakemistoon käyttäjiksi. Tunnistautuminen voidaan toteuttaa perinteisellä käyttäjätunnus-salasanaparilla, mutta aktiivihakemisto tukee myös varmenteisiin (PKI) perustuvaa käyttäjän tunnistamista.” (4.)

Käyttäjä siis kirjautuu työasemaansa tunnuksella, joka on luotu AD:ssä. Kirjautumisen yhteydessä AD tunnistaa käyttäjän, jonka jälkeen tätä tunnistetietoa käytetään esimerkiksi tiedostojärjestelmän oikeuskäytännöissä. Lisäksi käyttäjätunnuksiin pystytään AD:ssä määrittämään yli 70 eri attribuuttia, joita eri käyttäjät pystyvät tarkistamaan oikeuksiensa mukaan. Näitä voivat olla esimerkiksi nimi, osoite, sähköpostiosoite, puhelinnumero jne.

4 PALVELINJÄRJESTELMÄN SUUNNITTELU JA TOTEUTUS

4.1 Työssä käytetyt laitteet ja ohjelmistot

Resurssien rajallisuudesta johtuen työ suoritettiin tavallisella, suhteellisen suorituskykyisellä kotityöasemalla. Laitteiston tärkeimmät ominaisuudet olivat seuraavanlaiset: Prosessorina 4 -ytiminen Intel Quad Core Q6600, RAM-muistia 4 Gt sekä kovalevytilaa 15 Gt/virtuaalikone. Luotaessa virtuaalikoneeseen kiintolevyä, määritetty 15 Gt varataan yhdeksi isoksi varastoksi eikä sitä pysty hyödyntämään normaalissa tietokoneen työpöytäkäytössä, vaan kaikki tila varataan ajettavaa virtuaalikonetta varten.

Verkkoyhteytenä toimi normaali 100/10 Mb:n yhteys, joka rajoitti mm. sähköpostin testausta, koska operaattori on sulkenut sähköpostin lähettämiseen vaaditun portin, eikä olisi järkevää avata käyttöön sopivaa liittymää pelkästään tämän työn suoritusta varten. Käyttöön soveltuisi operaattorin puolelta yritysliittymä, mutta kustannukset nousisivat kohtuuttoman suuriksi. Tämän vuoksi myöhemmin suoritettava sähköpostin testaus on tehty paikallisesti, tarkoitushan on vain todistaa järjestelmän toimivuus.

Verkkolaitteet muodostuvat 5-porttisesta hallitsemattomasta gigabit-kytkimestä sekä 4-porttisesta hallittavasta 100/10 megabitin langattomasta tukiasemasta, jonka ominaisuuksia on hyödynnetty verkon luonnin osalta. Jotta koneet saataisiin toimimaan mahdollisimman yksinkertaisesti ja helposti, konfiguroitiin tukiaseman taakse DHCP-verkko 10.20.1.0 verkkomaskilla 255.255.255.0. DHCP-pooli määritettiin alkamaan osoitteesta 10.20.1.10 alkaen, koska tuosta alaspäin olevat osoitteet voidaan asettaa palvelimiin kiinteästi, mikä on ehdoton vaatimus. Tukiasemasta eteenpäin tietoliikenne käytää NATia, joka mahdollistaa usean verkossa olevan koneen ulospäin näkymisen vain yhtenä IP-osoitteena. Tässä tapauksessa ulospäin näkyvä IP-osoite on tukiaseman operaattorilta saama IP-osoite.

Työaseman käyttöjärjestelmänä on 64-bittinen Microsoft Windows 7 Enterprise. VMware -ohjelmistoista käyttöön on valittu VMware Server 2.0.2, joka on ilmaiseksi ladattavissa osoitteesta www.vmware.com ja kohdasta Downloads.

Virtuaalikoneiden käyttöjärjestelminä toimii Windows Server 2008 Enterprise, joihin on saatu aktivointiavainten käyttöoikeus Matti Tuomikoskelta (WinWind Oy). Käyttöjärjestelmät on aktivoitu, vaikka Server 2008 -järjestelmässä on ilmainen rajoitetun ajan käyttöoikeus, koska tämä saattaa vaikuttaa järjestelmän tiettyihin ominaisuuksiin. Sähköpostipalvelimen käyttöjärjestelmäksi on valittu CentOS 5.5 (eräs Linuxin versio), koska postin välitykseen käytettävä Zarafa-ohjelmisto ei toimi Windows-pohjaisilla palvelimilla. Toinen syy, miksi Linux -ympäristö on otettu työhön mukaan on sen hyödyllisyys ja yleinen esiintyminen ammattikäytössä, josta työn tekijällä ei ole paljon kokemusta. Se siis toimii samalla oivana opetteluympäristönä tulevaisuutta ajatellen.

4.2 Ympäristön luonti

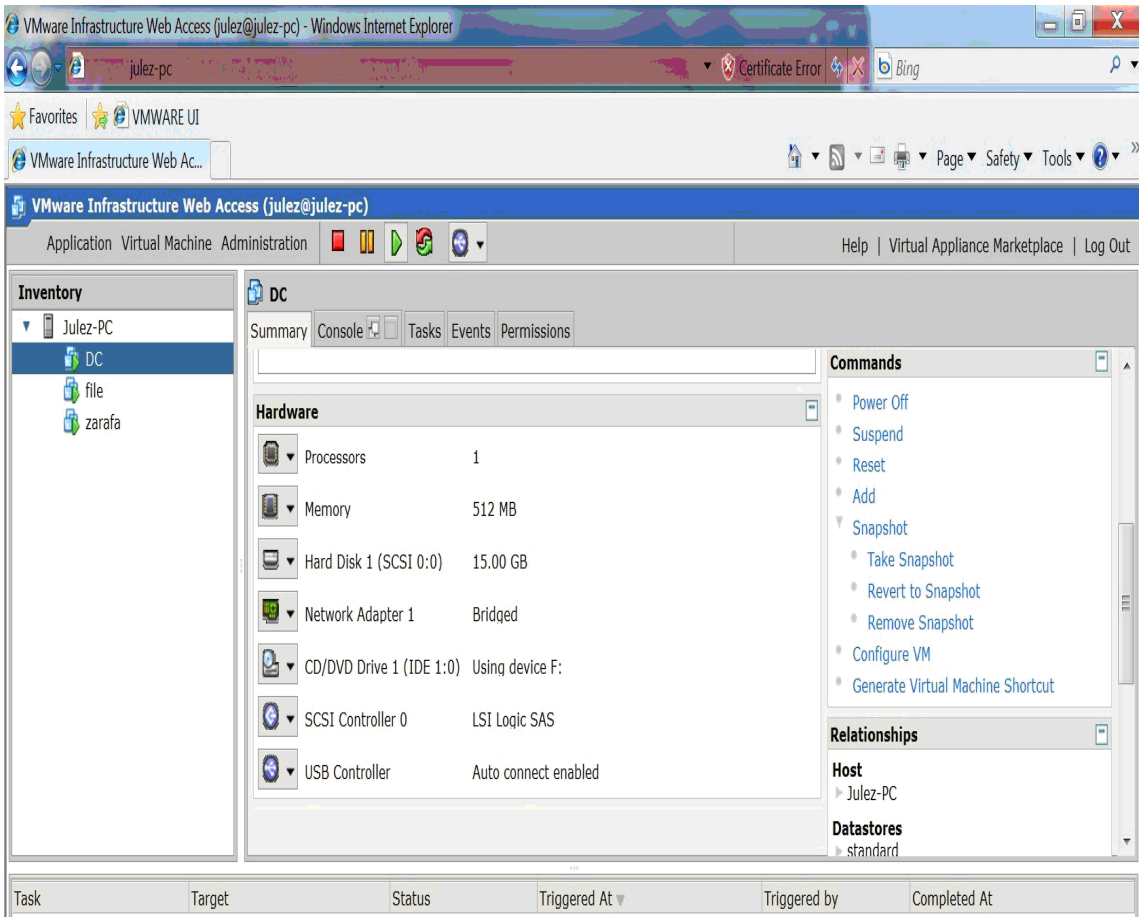
4.2.1 VMware Server 2.0

VMware Server 2.0 -ohjelmiston asennuksen jälkeen päästiin luomaan itse virtuaalista ympäristöä. Asennusvaiheessa VMware Server -ohjelmistoon määriteltiin käyttäjätili sekä salasana, jolla kirjaudutaan itse selainpohjaiseen järjestelmään. Kirjautuminen tapahtui normaalin internet-selaimen avulla kirjautumalla osoitteeseen https://localhost:8333/ui , jossa localhost on työaseman nimi ja 8333 portti.

Sisäänkirjautumisen jälkeen luotiin itse virtuaalipalvelimet. Tämä tapahtui kohdasta Virtual Machine/Create Virtual Machine. Tässä kohdassa koneeseen tehtiin tarvittavat määritykset niin käyttöjärjestelmän, kuin emuloitavan laitteiston ominaisuuksienkin puolesta.

Windows 2008 Server -järjestelmän suositeltu minimivaatimus muistin osalta on 1024 Mt, mutta työaseman muistikapasiteetin ollessa rajallinen sekä tulevan ympäristön vähäisen kuormituksen johdosta on tyydytty 512 megatavuun. Kiintolevytilaksi on määritelty 15 Gt sekä prosessoriytimien määräksi yksi. Verkkokortit on luotu käyttämään sillattua yhteyttä isäntäkoneen kautta. Järjestelmän kaikki kolme palvelinta ovat ”fyysisiltä” ominaisuuksiltaan samanlaisia.

Virtuaalikoneita luotiin siis kolme, jotka nimettiin niiden tulevan domain-nimen mukaan: dc (domain controller), file (tiedostopalvelin) ja zarafa (sähköpostipalvelin). Luodut koneet tulivat näkymään hallintaikkunan vasempaan reunaan, josta aktivoimalla pystyttiin muokkaamaan rajoitetusti koneen ominaisuuksia sekä käynnistämään ne yksitellen (kuvio 1).



KUVIO 1. VMware Serverin hallintaikkuna

Palvelimet voitaisiin myös konfiguroida käynnistymään heti VMware Serverin käynnistyttyä, mutta tässä työssä ne käynnistetään manuaalisesti yksitellen, jolloin isäntäkoneen resursseja säästyy muuhun käyttöön. Käyttöjärjestelmän asennus virtuaalikoneeseen voi tapahtua useammalla eri tavalla; seuraavassa on esitelty kaksi useimmin käytettyä. Tässä työssä Windows-palvelimet luotiin tavalla yksi ja Linux-palvelin tavalla kaksi.

Tapa yksi

Windows Server -käyttöjärjestelmän asennus-DVD on ladattu Microsoftin lisensointiportaalista licensing.microsoft.com. Tiedostomuoto on normaali levyimage eli .ISO. Latauksen jälkeen asennuslevy määritetään isäntäkoneen (työasema) virtuaaliseen DVD-asemaan, joka on toteutettu yleisesti käytössä olevalla Daemon Tools -ohjelmistolla. Virtuaalikone on määritetty käyttämään isäntäkoneen levymääritystä, joten tässä tapauksessa riittää, kun käynnistämme aikaisemmin luodun koneen DC, jolloin käyttöjärjestelmän asennus käynnistyy normaalisti aivan kuin käytettäisiin normaalia DVD-asemaa.

Tapa kaksi

Uudemmissa VMware Server -ohjelmistoissa on mahdollista käyttää .ISO-tunnisteisen levyn suoraa määritystä. Tämä asetuskohta löytyy virtuaalikoneen asetuksista hardware/dvd-drive/connection/iso.

4.2.2 Snapshot

Järjestelmän käytettävyyden sekä turvallisuuden lisäämiseksi kaikista palvelimista on otettu snapshot eli levynkuva heti asennuksen jälkeen. Snapshotiin tallentuvat järjestelmän kaikki sen hetkiset tiedot, mitä yksi palvelin sisältää. Jos palvelimeen tulee toimintahäiriö, virus, järjestelmän sekoittava päivityspaketti tai virhekonfiguraatio jne., voidaan muutokset kumota palauttamalla aiempi snapshot. Tapa muistuttaa normaalin Windows-järjestelmän palautuspistettä, mutta siinä tallennetaan huomattavasti enemmän dataa muistiin kuin pelkässä palautuspisteen luomisessa. Lisäksi palvelimen palautus snapshotista on nopeampaa, kuin Windowsin omaa palautuspistettä käytettäessä.

Testiympäristössä käytetty VMware Server -ohjelmisto on mm. snapshot-ominaisuuksiltaan hieman niukempi, kuin itse ammattikäytössä oleva ESX-Server. VMware Server mahdollistaa ainoastaan yhden snapshotin ottamisen kerrallaan. Tästä on hieman haittaa esimerkiksi tilanteessa, jossa järjestelmässä olevissa kymmenestä palvelimesta halutaan kaikista ottaa varmuustiedosto. ESX-Server mahdollistaa tämän sekä toisen käyttökelpoisen ominaisuuden: virtuaalikoneiden kloonauksen. Kloonausta voidaan käyttää esimerkiksi tilanteessa, kun halutaan viisi samanlaista palvelinta. Tällöin jokaista palvelinta ei tarvitse asentaa erikseen, vaan voidaan kloonata yksi valmiiksi asennettu useammaksi, mikä voi säästää aikaa ja vaivaa jopa kymmeniä tunteja. (5.)

4.2.3 Verkko-osoitteet

Osoiteavaruuden suunnittelu näin pieneen järjestelmään on helppo, koska palvelimia ei ole kuin kolme kappaletta, tosin valmis järjestelmä kykenee hallitsemaan isoakin alaverkkoa. Verkko-osoitteet on valittu privaattiverkosta 10.20.1.0 maskilla 255.255.255.0. Tämä mahdollistaa alaverkon laitteiden määräksi 254.

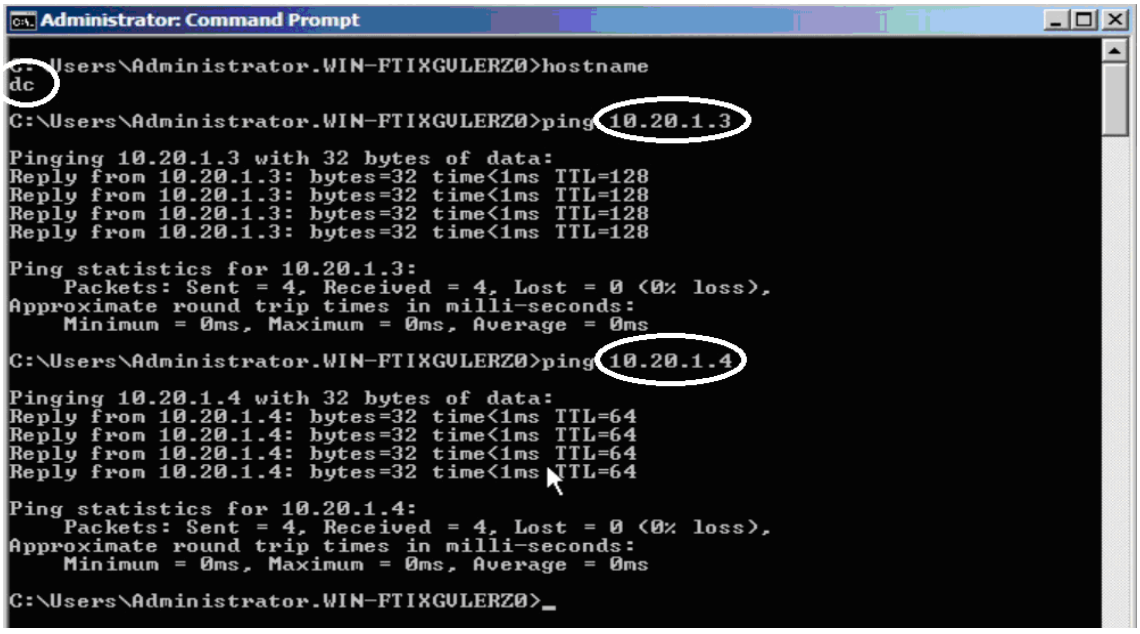
Kiinteiden IP-osoitteiden mahdollistamiseksi otettiin käyttöön ihan perinteinen Buffalon 4-porttinen langaton tukiasema, joka oli kytetty tavalliseen hallitsemattomaan kytkimeen ja siitä eteenpäin suoraan internetiin. Langaton reititin toimi tässä tapauksessa myös koneiden yhdyskäytävänä (gateway) osoitteessa 10.20.1.1. Reititin saa ulkoisen IP-osoitteensa suoraan palveluntarjoajalta, tässä tapauksessa Soneralta, jolloin tukiasema huolehtii alaverkon internet-liikenteen ohjaamisesta. Reitittimen DHCP pooli asetettiin alkamaan osoitteesta 10.20.1.10, jolloin osoitteet 10.20.1.2—10 jäivät käyttöön kiinteille IP-osoitteille.

Palvelimien IP-osoitteet olivat seuraavat: DC=10.20.**1.2**, file=10.20.**1.3**, zarafa=10.20.**1.4**. Verkkoon lisättävät testityöasemat saivat osoitteensa DHCP:stä.

4.2.4 Yhteyden testaus

Yksinkertaisin tapa testata palvelinten väliset sekä muut yhteydet on Windows-komento **ping**. Siinä lähetetään pieniä paketteja lähdekoneelta kohdekoneelle, jotka kohdekone palauttaa automaattisesti lähettäjälle. Toimintatapaa voi ajatella yksinkertaisimmillaan pöytätenniksen pelaamiseksi: jos pallo palautuu toiselta puolelta takaisin, on yhteys kunnossa. (6.)

Palvelinten väliset yhteydet on testissä todettu toimiviksi (kuvio 2). Jokainen palvelin sai ping-komennolla yhteyden toisiinsa. Lisäksi internet-liikenne testattiin jokaisessa koneessa toimivaksi, eli verkko ja reititys oli alaverkon osalta kunnossa.



KUVIO 2. Yhteyden testaus ping-komennolla

4.3 Palvelimet

4.3.1 DC

Kuten jo aikaisemmin on todettu, Domain Controller on toimialueen tärkein ohjauskone. Kun toimialueen palvelut, nimet jne. on suunniteltu ja valittu, DC:n konfigurointi pystytään aloittamaan.

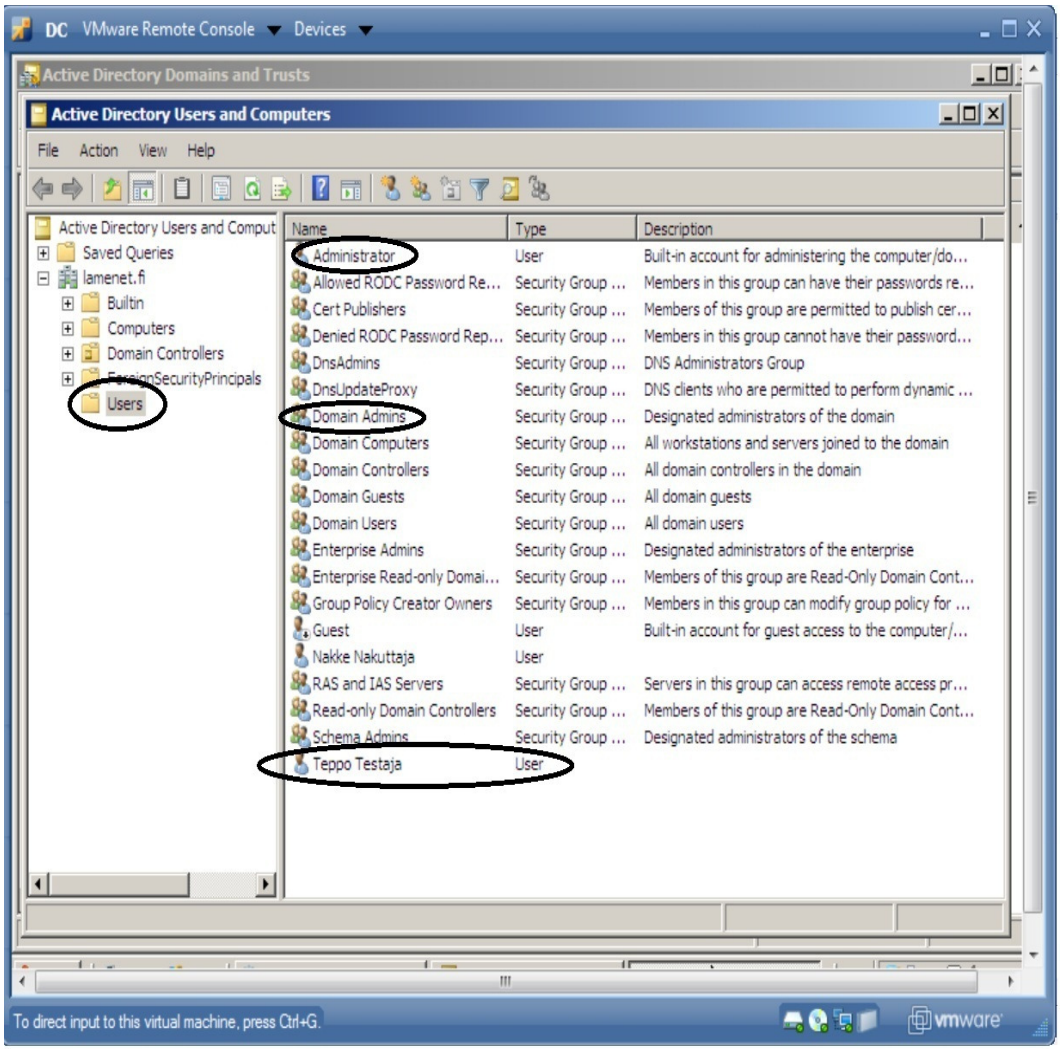
Työssä käytetyn toimialueen nimeksi valittiin lamenet.fi, joka on internetissä toistaiseksi rekisteröimätön domain. Rekisteröimättömästä domainista on hieman haittaakin internet-liikenteessä, koska esimerkiksi sähköpostien ohjaus ei toimi oikealla tavalla. Lisäksi tämä voisi vaikuttaa kotisivujen tekoon, jos sellaiset tehtäisiin. Työssä päätettiin kuitenkin käyttää keksittyä nimeä, koska domain-nimien rekisteröinti on maksullista.

Kun Server 2008 -käyttöjärjestelmä asennettiin, saatiin kaikki palvelut täysin käyttöön aktivoimalla Windows. Tämä tapahtui kohdasta Control Panel/Change product key, jolloin uuden avaimen syöttö aktivoi järjestelmän automaattisesti.

Aktivoinnin jälkeen tehtiin DC:stä virallisesti toimialueen ohjauskone käyttämällä komentokehotteessa **dcpromo**-käskyä. Tämä komento luo Domain Controllerin ja sen kaikki ominaisuudet ja roolit, joita myös myöhemmin pystytään muokkaamaan. (7.)

Koska palveluita ja rooleja on todella paljon, konfiguroitiin DC käyttämään vain minimimäärää palveluista, jotta toimialue saataisiin vain toimimaan oikein. Tärkein rooli DC:llä on Active Directory Domain Services, joka määrittää lähes kaiken toimialueella tapahtuvan toiminnan. Jotta toimialuetta sekä kaikkia sen jäseniä pystyttäisiin hallitsemaan halutulla tavalla, täytyi tehdä tunnukset sitä varten.

Administrator-tunnus on yleinen järjestelmänvalvojan käytettävissä oleva käyttäjätili. Tämä tunnus lisättiin AD:n Domain Admins-ryhmään, jolloin tällä tunnuksella pystyi kirjautumaan ja hallitsemaan toimialueen laitteita järjestelmänvalvojan oikeuksin. Testikäyttöön luotiin tunnus Teppo Testaaja, jolla on toimialueen rajoitetut oikeudet. Tätä tunnusta käytettiin myöhemmin esim. tiedostojaon sekä sähköpostin toimivuuden testaamiseen. Kuvio 3 näyttää hallintaikkunan, jossa nämä toimet on suoritettu.



KUVIO 3. Active Directory:n hallintaikkuna

Yleensä DC konfiguroidaan myös toimialueen sekä DNS- että DHCP-palvelimeksi. Tässä tapauksessa nämä roolit asennettiin, mutta jätettiin hyödyntämättä, koska langaton reititin hoitaa kyseiset palvelut. Tällä menetelmällä vältetään myös alaverkon sisäisiä kommunikaatio-ongelmia, koska järjestelmä on mahdollisimman yksinkertainen.

Moni hyödyllinen, muttei elintärkeä palvelu jäi nyt siis hyödyntämättä tässä järjestelmässä yksinkertaisesti siksi, että niitä ei tarvita. Jos järjestelmä siirrettäisiin valmiina yrityskäyttöön, niin mukaan otettavia palveluita olisi runsaasti, koska valittavana on kymmeniä eri mahdollisuuksia. Muutamia käyttökelpoisia palveluita pk-yritykselle voisivat olla esimerkiksi

1) WSUS (Windows Server Update Service), joka mahdollistaa Windowsin päivityspakettien keskitetyn jakamisen verkon jokaiselle työasemalle ilman, että jokainen työasema lataisi ne erikseen oman Internet-yhteytensä kautta

2) Web Server (IIS), jonka avulla pystyttäisiin jakamaan verkon käyttäjille web-pohjaisia sovelluksia

3) Windows Deployment Services, joka mahdollistaa nopeasti työaseman uudelleenasennuksen verkon kautta esim. ylitsepääsemättömissä vikatilanteissa

4) Print Services, jolla hallitaan verkon tulostimia.

4.3.2 File

Tiedostopalvelin on nimensä mukaan verkon datakeskus, johon käyttäjät ovat yhteydessä. Työssä tiedostojen verkkojako toteutettiin yksinkertaisella kansion jakamisella, joka mahdollisti tiedostojen tallentamisen verkkolevylle. Yleensäkin kaikki tärkeämpi data yritysverkoissa tallennetaan verkkoasemalle, koska ne on varmennettu usein jopa moninkertaisesti eri laitteistoratkaisuissa. Tässä työssä laitetason ratkaisua tiedostojen varmentamiseen ei käytetty, vaan tiedonvarmennus on suoritettiin teoreettisesti kahden virtuaalipalvelimen välillä käyttämällä Windows Serverin replikointiominaisuutta (DFS), josta löytyy lisäinformaatiota luvusta 4.4.

Tiedostonjako kannattaa yleensä toteuttaa jakamalla kansio tietylle ryhmälle. Ryhmälle jaettuna kansioon on helppo antaa oikeuksia AD:n kautta, mikä helpottaa ja nopeuttaa työtä huomattavasti verrattuna siihen, että jokaiseen kansioon annettaisiin oikeudet manuaalisesti. Tämä tulee parhaiten esille silloin, kun yritykseen tulee uusi työntekijä ja verkko-oikeuksia aletaan määrittää.

Ryhmän luonti tapahtui siis AD:ssä eli tässä tapauksessa dc-palvelimella. Yksinkertaistettuna tämä toimii siten, että ensin luodaan itse ryhmä, jonka jälkeen käyttäjä lisätään tuohon luotuun ryhmään. Tämän jälkeen sitten määritetään jako-oikeudet itse kansioon Windowsin resurssienhallinnan kautta.

Ryhmäjako toimii parhaiten silloin, kun oikeuksin hallittavia kansioiden alatasoja on ainoastaan yksi. Haluttaessa jakaa oikeuksia myös alakansioihin sekä niiden alatasoille on hyvä ottaa nämä seikat huomioon jo kansiorakennetta suunniteltaessa.

Järjestelmään luotiin aluksi nämä kaksi palvelinta, dc ja file. Palveluita ei asennettu kumpaankaan minimimäärää enempää. Tällaisessa pienessä järjestelmässä voitaisiin asentaa suurin osa palveluista file-palvelimelle ja jättää dc hoitamaan itse toimialuetta, jolloin kaikki sen resurssit olisivat käytössä siihen tarpeeseen, mihin se on luotu.

Järjestelmien toteutustapoja sekä varmistusmetodeja ym. on lukuisia: file-palvelin voisi aivan hyvin toimia dc:n varakoneena, backup domain controllerina (BDC). Lisäksi on myös hyvä muistaa, ettei virtualisointi sovellu kovinkaan hyvin suuren rasituksen alla olevan tiedostopalvelimen alustaksi, koska suorituskyky on huomattavasti laitetason ratkaisua heikompi. Päivittäisen tiedonsiirron jäädessä palvelimen ja työasemien välillä korkeintaan muutamiin gigatavuihin on virtuaalinen tiedostopalvelin tällöin oiva ratkaisu.

4.3.3 Zarafa

Sähköposti alkaa nykypäivänä olemaan yksi tärkeimmistä työvälineistä työelämässä. Yritysten sähköpostiratkaisuihin on tarjolla useita vaihtoehtoja aina omasta palvelimesta palvelun vuokraukseen tai ulkoistamiseen. Jo hieman isommissakin pk-yrityksissä on yleensä oma sähköpostipalvelin, mikä on jo hallittavuudenkin kannalta järkevä ratkaisu. Yleisimmin käytössä on Microsoft Exchange Server, joka on jo pelkästään hinnaltaan suuri investointi pk-yritykseen. Pelkkä järjestelmä voi maksaa tuhansia euroja sekä noin 100 € jokaista käyttäjää kohden, koska Exchange vaatii CAL-lisenssin, joka on yksinkertaisesti selitettynä tuotteen henkilökohtainen käyttöoikeus. Tämän tiedon puitteissa Zarafa tarjoaa varteenotettavan ja käytännössä ilmaisen vaihtoehdon Microsoft Exchangelle, sillä kustannukset ovat vain muutamia euroja käyttäjää kohti vuodessa.

Tässä työssä käytetty Zarafa on erittäin hyvä vaihtoehto pienelle yritykselle, koska se mahdollistaa kaikki samat palvelut kuin Exchange Serverkin. Käyttäjät voivat työskennellä Microsoft Outlookin kanssa täysin normaalisti, mutta käyttäjiä on enemmän kuin kolme, tarvitsevat ylimääräiset käyttäjät muutaman euron hintaisen vuosikohtaisen lisenssin. Käytännössä Zarafan käyttö on siis ilmaista verrattuna Exchangeen.

Ennen kuin Zarafa pystyttiin asentamaan ja konfiguroimaan, täytyi ensin luoda virtuaalipalvelin, jonka käyttöjärjestelmäksi valittiin konsultoinnin pohjalta avoimen lähdekoodin CentOS 5.5, joka perustuu maksulliseen Red Hat Linux Enterpriseen. Erona näillä kahdella Linuxilla on pääosin se, että CentOSiin ei löydy virallista tukikanavaa, vaan ongelmatilanteet ratkaistaan käyttäjien ja asiantuntijoiden keskuudessa Internetin eri foorumeilla sekä ohjelmistopäivitykset toimivat hieman eri tavalla kuin Red Hat Linuxissa. CentOS kuitenkin tarjoaa mitä parhaimman käyttöympäristön Zarafalle. (8.)

Itse käyttöjärjestelmän asennus oli suhteellisen helppo, kun valittiin verkkoasennus. Siinä käyttäjä sai valita tietyt järjestelmän osaset, jotka asennettaisiin. Kaikki turhat ominaisuudet karsittiin tästäkin järjestelmästä jo asennusvaiheessa manuaalisesti sekä valittiin tietyt komponentit, joita vaadittiin sähköpostipalvelimen pystyttämiseen ja toimintaan.

Itse Zarafan konfigurointi suoritettiin komentorivin kautta SSH-yhteydellä. Lisäksi Zarafan asennukseen olisi ollut käytettävissä valmiita skriptejä, jotka mahdollistaisivat automatisoidun asennuksen, mutta tässä niitä ei käytetty, koska tarkoituksena oli myös opiskella ja tutustua Linux -ympäristöön. Sen sijaan käytettiin osittain valmiita konfiguraatiotiedostoja, jotka liittyvät itse ohjelmiston konfigurointiin. Osittain valmiiden konfiguraatiotiedostojen käyttöön päädyttiin siksi, että työn tarkoitus ei harhailisi liikaa, sillä noiden tiedostojen sisältö on satoja rivejä puhdasta unix-ohjelmakoodia.

Myöhemmässä vaiheessa CentOS-palvelimeen asennettiin myös Webmin-lisäosa, joka mahdollistaa palvelimen hallinnan selainikkunan kautta. Koska opinnäytetyötä ei ole tarkoitettu manuaaliksi, on ainoastaan osa asennuskomentoriveistä selityksineen sekä osa konfiguraatiotiedostoista julkaistu liitteessä 1.

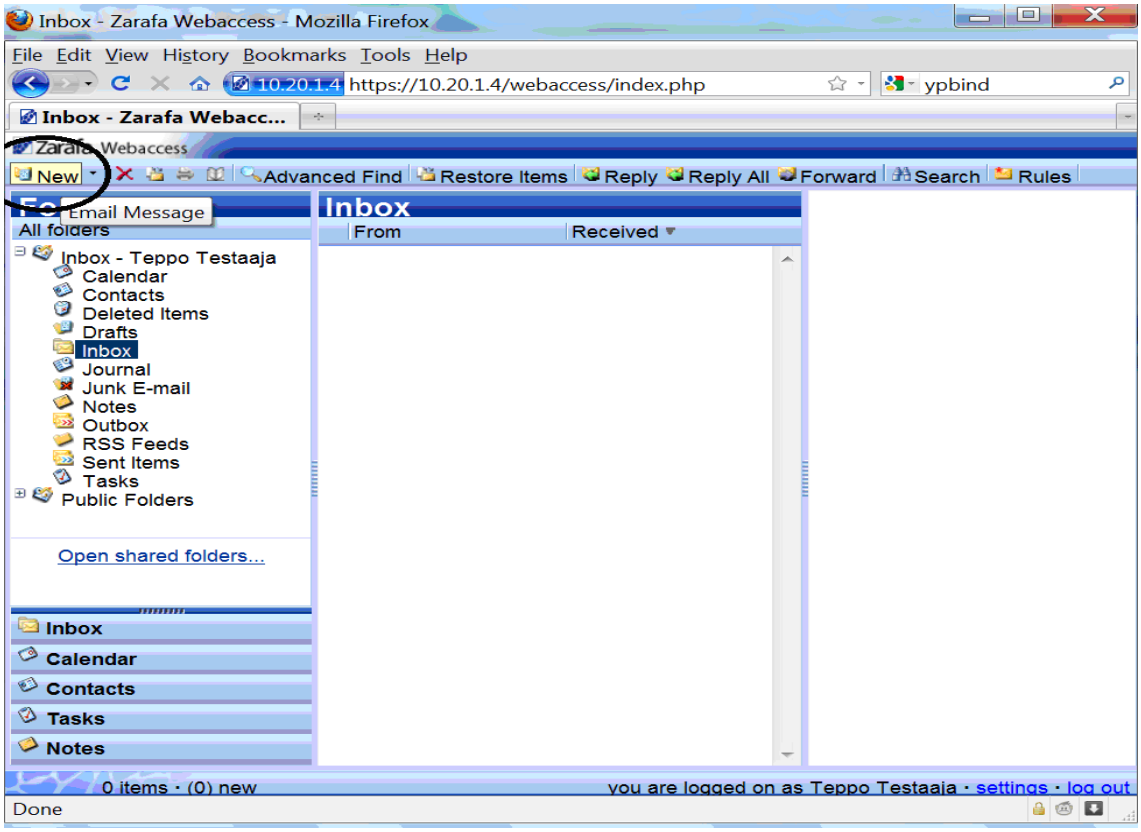
Maininnan kofiguraatiosta ansaitsee Zarafan ominaisuus, jota ei kuitenkaan ole tässä hyödynnetty. Testikäyttöön luotu tunnus on tehtiin itse Zarafa-palvelimella, mutta mahdollista olisi käyttää myös LDAP-tunnistusta. LDAP-tunnistusta käytettäessä Zarafa pystyisi etsimään käyttäjätunnukset suoraan AD:n tietokannasta ja luomaan sähköpostitunnukset lähes automaattisesti. Tätä ominaisuutta ei ole hyödynnetty tässä työssä sen vuoksi, koska sen opettelu veisi runsaasti ylimääräistä aikaa, joskin asian opiskelu jatkuu myöhemmässä vaiheessa.

Sähköpostin toimintaa teoriatasolla verkon sisällä sekä sähköpostipalvelimen eri komponenttien toimintaa postin kulun kannalta ei myöskään ole tarpeen käsitellä tässä työssä enempää, koska se on epäolennaista järjestelmän toimivuuden kannalta.

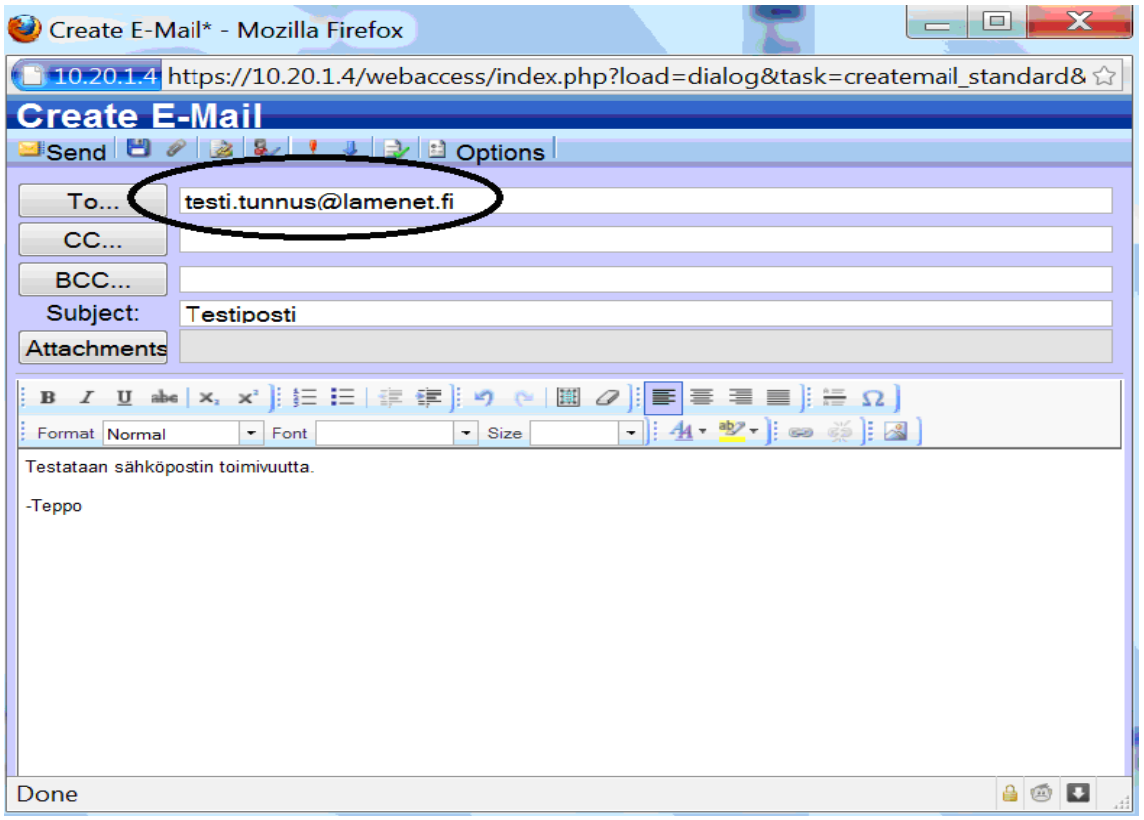
4.4 Sähköpostin testaus

Kun kohdassa 4.3.2 ja liitteessä 1 olevat toimet saatiin suoritettua, oli sähköpostijärjestelmä valmis testattavaksi. Seuraava kuvasarja osoittaa postin testauksineen toimivaksi. On syytä ottaa huomioon, että postin vastaanottaminen ulkopuolelta on tässä tapauksessa mahdotonta, koska operaattori on sulkenut sähköpostiliikenteessä käytettävän SMTP-portin 25 yksityisliittymistä. Jotta posti saataisiin kulkemaan maailmanlaajuisesti, tulisi liittymätyyppi Internet-yhteydelle v sekä rekisteröidä domain lamenet.fi virallisesti.

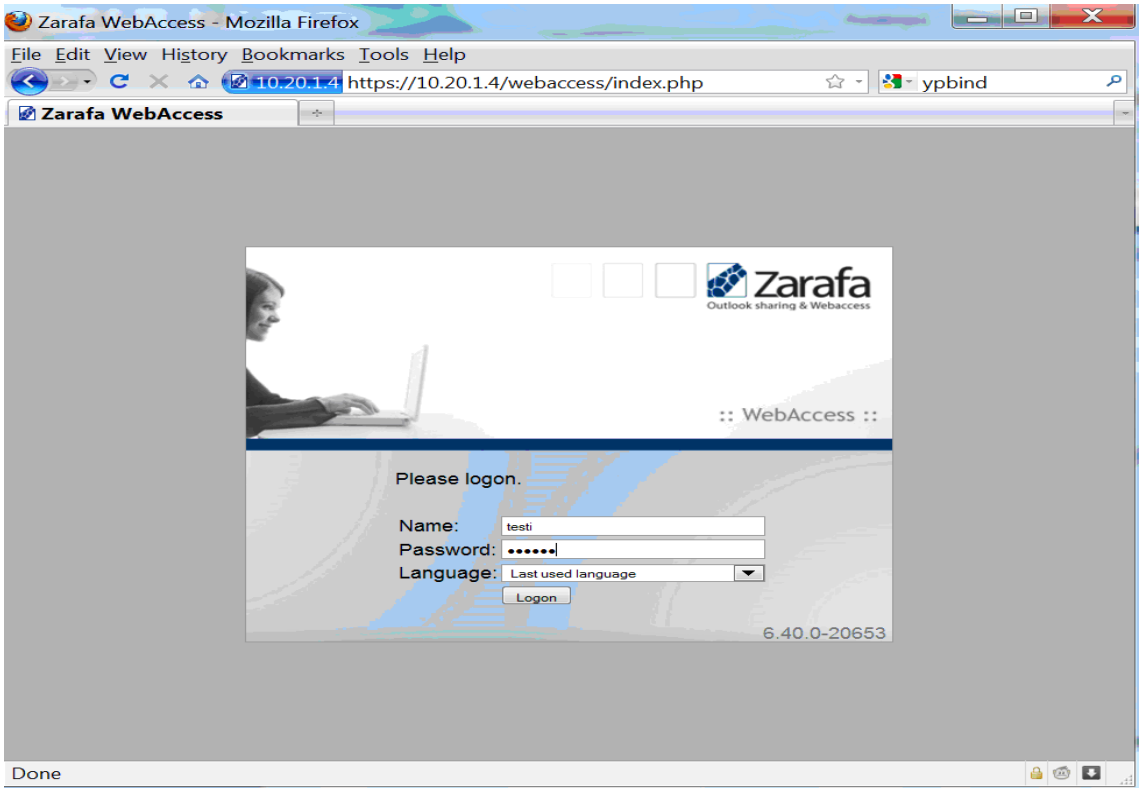
Kuviot 5—9 kuvaavat perinteistä sähköpostin lähettämistä web-selaimen kautta. Postia lähetettiin Teppo Testaaja -tunnuksella Testi Tunnukselle. Viimeisin kuva on postin otsikkotaulu, josta nähdään miten posti on kulkenut ja mitä sille on matkan varrella tehty.



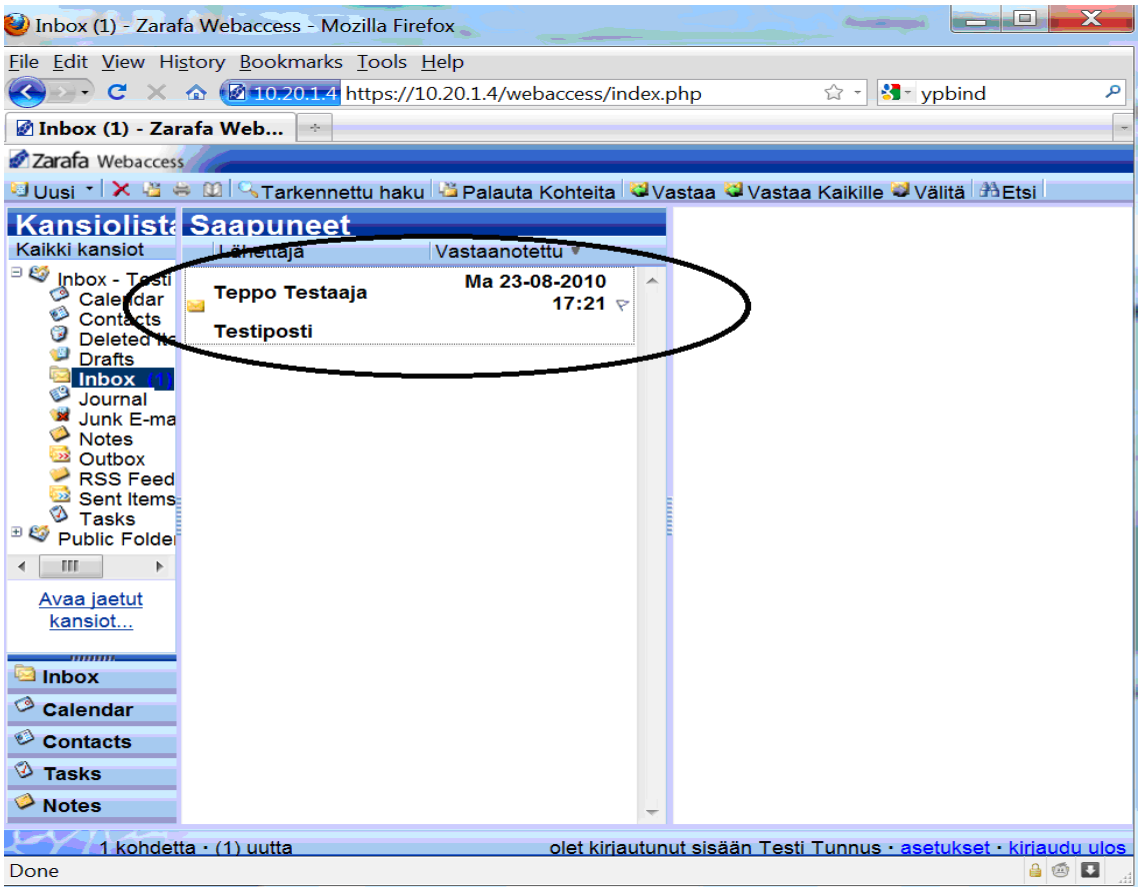
KUVIO 4. Luodaan uusi sähköpostiviesti



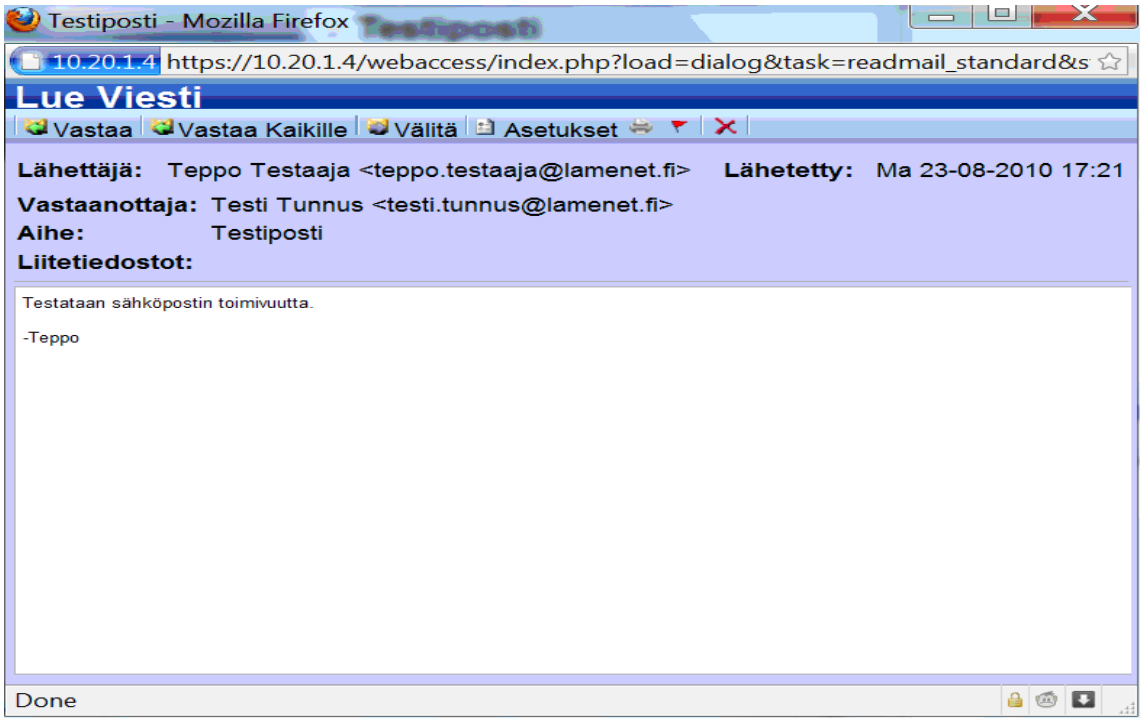
KUVIO 5. Lisätään vastaanottaja sekä otsikko ja viesti



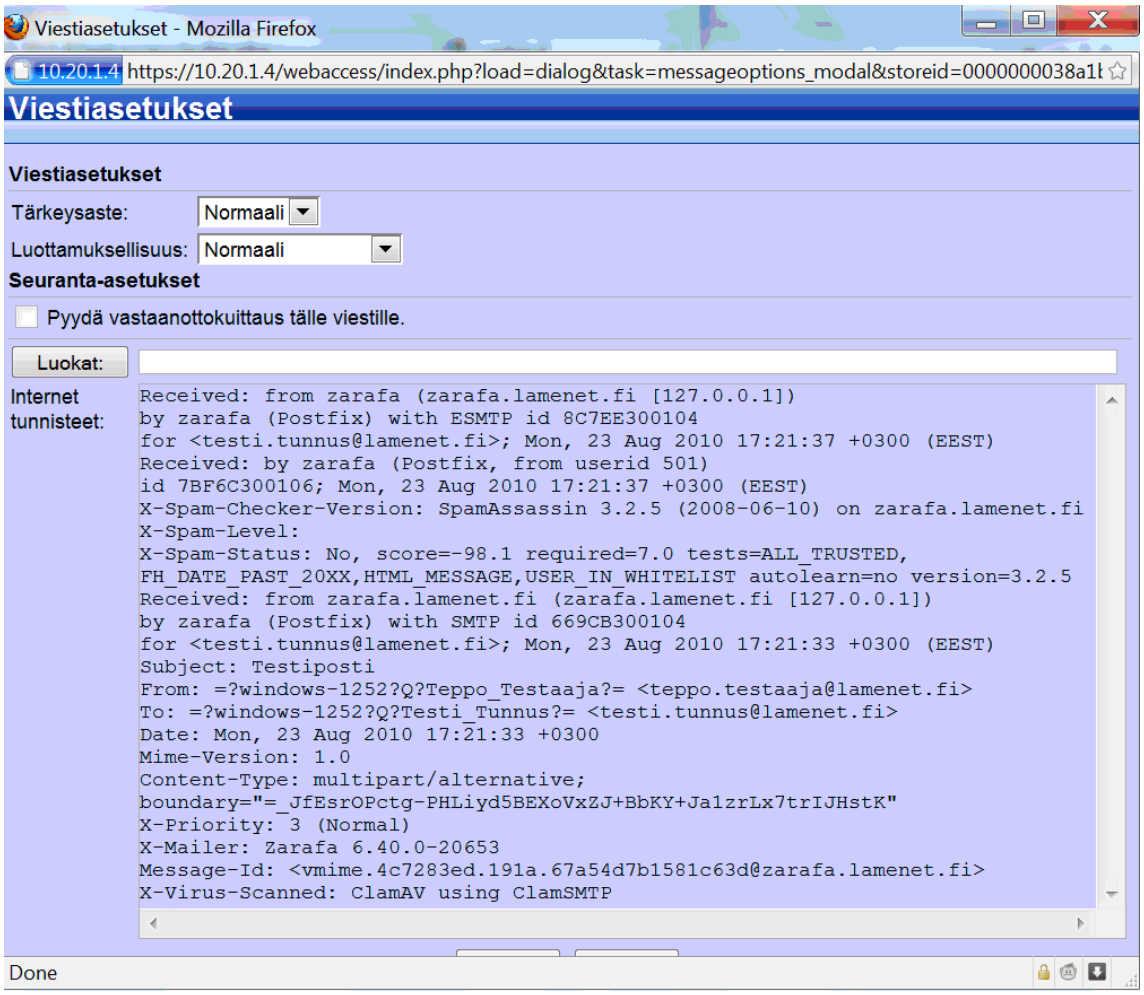
KUVIO 6. Kirjaudutaan sisään toisella tunnuksella



KUVIO 7. Avataan vastaanotettu sähköposti



KUVIO 8. Vastaanotetun viestin sisältö



KUVIO 9. Vastaanotetun postin otsikkotiedot

4.5 Tiedonvarmistus ja vikasietoisuus

4.5.1 Yleistä järjestelmistä

Tiedonvarmistus ja järjestelmien vikasietokyky ovat erittäin tärkeä osa yritysten IT-strategiaa. Järjestelmien haavoittuvuuden suunnittelussa voidaan mennä äärimmäisyyksin, kun varajärjestelmille rakennetaan omat varajärjestelmät. Tällöin järjestelmistä tulee monimutkaisia sekä kalliita. Pääasiassa suuret yritykset pelaavat varman päälle tässäkin asiassa, varsinkin kun palvelimien käytettävyyden tulee olla lähes 100 %. PK-yritysmaailmassa tullaan toimeen vähemmällä, eikä suurta varmennusverkkoa tarvitse rakentaa, vaan pärjätään ”normaalilla” varmennuksella. (9.)

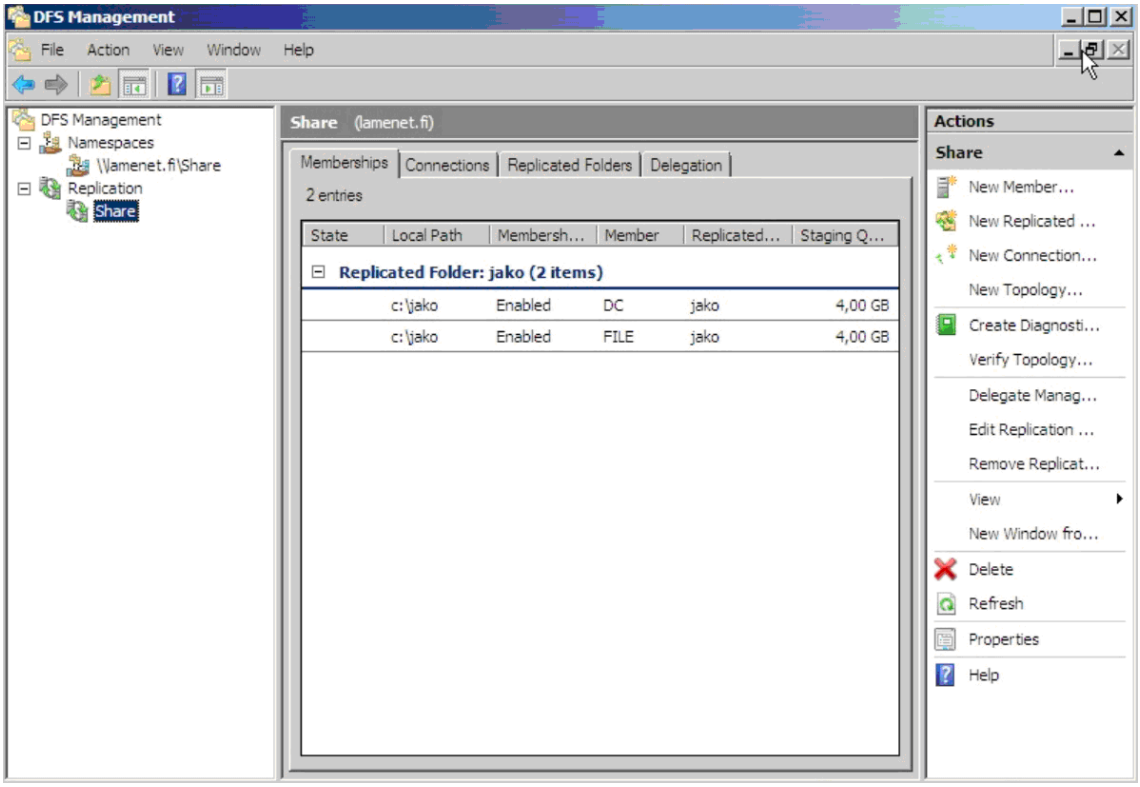
Laitetatason vikasietoisuus on otettu usein jo palvelimissa huomioon niitä hankittaessa. Useissa palvelimissa on kahdennetut virtalähteet, kovalevyt, verkkokortit jne. Lisäksi sähkökatkojen varalta useimmat järjestelmät varustetaan UPSilla, joka toimii kuin suuri akku, joka kykenee

pitämään tärkeät palvelimet päällä jopa useita tunteja. Suuriin konesaleihin taas on asennettu erilliset varavoimalähteet, jotka ovat riippumattomia yleisestä sähköverkosta. Seuraavassa on kuvailtu muutamia yleisiä tiedonvarmistustapoja, joista osaa myös hyödynnettiin tätä virtuaalista järjestelmää rakennettaessa.

4.5.1 DFS -replikointi

DFS-replikointi (Distributed File System) on Windows Server -käyttöjärjestelmään rakennettu lisäosa, joka on ollut mukana versiosta 2003 R2 lähtien. Se mahdollistaa tietojen automaattisen siirron esimerkiksi palvelimelta toiselle.

DFS on kätevä työkalu esimerkiksi kahden toimipisteen välisen tiedonsiirtoon tai yksinkertaiseen varmuuskopiointiin. DFS -nimiavaruus määritellään palvelimella (tässä DC:llä). Palvelun saa otettua käyttöön kohdasta control panel\administrative tools\DFS-management. Palvelun konfiguroinnissa määritellään nimiavaruus, kohdekansiot, jotka replikoidaan, sekä monia muita toimivuuteen vaikuttavia seikkoja. Muun muassa näitä ominaisuuksia voi tarkastella kuviosta 10.



KUVIO 10. DFS-hallintaikkuna

DFS ei siirrä kaikkea dataa, joka kansioon tallennetaan, vaan esimerkiksi Word-tiedostoa muokattaessa siirretään ainoastaan muuttunut data.

Kun kahden toimipisteen eli palvelimen välinen replikointi on saatu toimimaan halutulla tavalla, näkyy se käyttäjälle parhaiten verkkolevyjen nopeuden lisääntymisenä. ” Näin säästetään kaistaa, mutta taataan yhtenäisten tiedostoversioiden saatavuus yrityksenlaajuisesti.” (10.)

Tässä työssä hyödynnettiin tiedostojen varmentamiseen DFS:ää, koska muiden vaihtoehtojen käyttö olisi ollut käytännössä mahdotonta.

4.5.2 Snapshot -menetelmä

Jo aiemmin luvussa 4.2.2 sivuttiin snapshotin toimintaa, mutta menetelmää voidaan hyödyntää myös tiedonvarmennukseen. Koska palvelimet ovat yksi IT-järjestelmien kriittisimpiä osa-alueita, voidaan virtuaalipalvelimista ottaa snapshoteja ajastetusti esimerkiksi päivittäin tai viikoittain.

Kun järjestelmää päivitetään aika ajoin, palveluita lisätään ym., nuo muutokset tallentuvat myös snapshotiin. Lisäksi aina virtuaalipalvelinta päivitettäessä on hyvä ottaa snapshot ennen päivitystä, koska vikatilanteessa on helppo palata päivitystä edeltäneeseen tilaan. Tässä työssä ei hyödynnetty jatkuvaa snapshot-ominaisuutta, koska VMware Server ei sitä tue, joskin tämä ominaisuus voidaan toteuttaa laajemmalla VMware ESX Server -ohjelmistolla.

4.5.3 RAID -levyjärjestelmä

Kiintolevyjen varmennusratkaisuista yleisin on RAID (Redundant Array of Independent Disks). RAID-tasoja on useita, ja eri ratkaisuissa se vaatii tietyn määrän kiintolevyjä eli levypakan. RAIDilla saavutetaan myös huomattavasti parempi suorituskyky kuin yksittäisellä levyllä. Useat valmiit palvelimet on toteutettu jonkin asteisella RAID-ratkaisulla. RAID-järjestelmän tekee vikasietoiseksi se, että esimerkiksi yhden kiintolevyn rikkoutuessa yhtään dataa ei menetetä. Tämäkin tosin riippuu RAID-tasosta. Seuraavassa on esitelty muutamia yleisesti yritysmaailmassa käytettyjä vikasietoisia RAIDeja. (11.)

RAID 1 eli peilaus on yleisimmin käytetty taso, kun halutaan varmentaa kaksi samanlaista kiintolevyä. RAID 1 toimii siten, että sama data kirjoitetaan molemmille levyille. Tämä

mahdollistaa tilanteen, jossa toinen kiintolevy rikkoontuu, mutta dataa ei menetetä sekä teoriassa tämä taso kaksinkertaistaa kiintolevyjen lukunopeuden.

RAID 5 on ehdottomasti yleisimmin käytetty RAID-taso palvelimissa. Tämä taso vaatii vähintään kolme kiintolevyä, jolloin levypakka kestää yhden kiintolevyn rikkoontumisen. Luku- ja kirjoitusnopeus on nopeampi kuin RAID 1:ssä. Jos levypakasta rikkoontuu kaksi kiintolevyä, menetetään kaikki data.

RAID 6 on hieman kehittyneempi versio RAID 5:stä, joka mahdollistaa levypakassa kahden levyn rikkoontumisen ilman datan menettämistä. Käytetään ainoastaan erittäin kriittisissä sovelluspalvelimissa.

4.5.4 Nauha-asemat

Kun tarvitaan suurta kapasiteettia tiedontallennukseen, on nauha-asema (robotti) oiva ratkaisu. Nauhuritekniikka on kehittynyt huimasti viime vuosien aikana ja tallennuskapasiteetti näillä laitteilla lasketaan jo kymmenissä tai sadoissa teratavuissa. Vaihtoehtoja nauhurijärjestelmiin löytyy useisiin käyttötarkoituksiin. Nauharobottiin sijoitetuille magneettinauhoille tallennetaan haluttu data järjestelmän kiintolevyiltä, jolloin data on myöhemmin luettavissa. Tosin lukuaika on monta kertaluokkaa hitaampaa dataa palautettaessa kuin verrattaessa kiintolevyyn. Nauhajärjestelmät ovat kuitenkin hyvin yleisiä, mikä johtuu niiden suhteellisen edullisesta tallennuskapasiteetista.

Nauha-aseman käyttö tekee yrityksen tietojärjestelmästä vieläkin vikasietoisemman, vaikka käytössä olisi mikä tahansa RAID-järjestelmä. Ajastetut päivittäiset sekä viikoittaiset nauhavarmistukset tekevät vikatilanteista, joissa koko levypakka hajoaa, nopeasti ohimeneviä, eikä suuria taloudellisia tappioita pääse syntymään, kun järjestelmän kriittinen data pystytään palauttamaan takaisin suhteellisen nopeasti.

4.5.5 Shadow copy -palvelu

Jaettujen kansioiden yksinkertainen tiedonvarmennustapa on Windows Serverin ominaisuus *shadow copy*. Se ei virallisesti ole mikään vikasietoisuutta lisäävä ominaisuus, mutta tekee järjestelmän käyttämisen helpommaksi käyttäjän kannalta. Kun shadow copy -palvelu kytketään päälle, se mahdollistaa tiedon nopean palauttamisen käyttäjälle, eikä IT-osastoa tarvitse vaivata

tiedonpalautuksella lainkaan. Tällaisia tilanteita voisivat olla mm. vahingossa tapahtunut tiedoston poistaminen, virheellinen tallennus, korruptoitunut tiedosto jne.

Shadow copyn toimintatapaa voisi verrata esimerkiksi snapshotin toimintaan kansiotasolla, jossa tietyin väliajoin tallennetaan kansion sisältämä data. Tuota dataa käyttäjä pystyy sitten selaamaan tiettyyn päivämäärään ja aikaan asti sekä palauttamaan tiedoston helposti omin avuin normaalilla copy-paste-menetelmällä.

4.5.6 VMware vSphere -kokonaisuus

Virtuaalipalvelinjärjestelmän vikasietoisuus on tärkeä ominaisuus varsinkin, kun käytössä on useita tärkeitä palvelimia. Työssä käytetty VMware Server -ohjelmisto ei kykene kovinkaan kummoiseen vikasietotilanteeseen, mutta yrityskäyttöä varten on kehitetty ohjelmistokokonaisuus vSphere.

VSpherellä sen sijaan pystytään toteuttamaan järjestelmä, joka mahdollistaa virtuaalisen palvelinjärjestelmän primäärikoneen kaatumisen. Tuolloin luonnollisesti kaikki primäärikoneessa olevat palvelimet sammuvat. Järjestelmää konfiguroitaessa vSpheren avulla luodaan primäärikoneen rinnalle sekundäärinen palvelin. Molemmat koneet vaativat oman laitetason ratkaisun sekä virtuaalikoneiden levykuvien sijainnin samassa kovalevyjärjestelmässä, esimerkiksi suuressa kuitulevypakassa.

Kun sekundäärinen palvelin on luotu, se konfiguroidaan käytännössä tarkkailemaan primäärisen koneen toimintaa. Jos primäärinen palvelin jostakin syystä sammuu tai rikkoontuu, tarkkaileva kone osaa oikein konfiguroituna käynnistää kaikki primäärikoneen sisältämät virtuaalipalvelimet nopeasti uudelleen, jolloin toimintakatko jää erittäin lyhyeksi. (12.)

5 JOHTOPÄÄTÖKSET JA POHDINTA

Työn tavoitteeksi asetettiin suhteellisen haastava tehtävä pystyttää pienyrityksen palvelinjärjestelmä sekä Zarafa-sähköpostijärjestelmä. Vaikka osittaista työkokemusta asian tiimoilta löytyikin esimerkiksi uusien palvelimien luonnista sekä valmiiden virtuaalipalvelimien hallinnasta, oli tehtävä täynnä haasteita sekä opiskelua. Lisäksi Linux-ympäristöön tutustuminen oli erittäin mielenkiintoista ja vaativaa, koska hyvään Linuxin hallintaan vaaditaan jopa vuosien käytännön kokemusta.

Aiheen valinta ja yleensäkin opinnäytetyöpaikan saaminen lama-aikana oli erittäin vaikea tehtävä. Yli sata kirjoitettua hakemusta alan yrityksiin noin kolmen vuoden aikana ei tuottanut tulosta eikä koulukaan opinnäytetyötä pystynyt järjestämään. Aihe-ehdotus tuli sitten opiskelijalta itseltään, mikä ei ollut lainkaan huonompi idea. Ammattitaito karttui työtä tehdessä runsaasti ja työllä oli selvä tarkoitus. Se ei ollut mikään ”pakkopulla”, vain sen vuoksi että opinnäytetyö tulee olla tehtynä valmistumista ajatellen. Mielestäni tällainen omaa mielenkiintoa lähellä oleva aihe-ehdotus palvelee huomattavasti paremmin opiskelijan motivaatiota työskennellä kuin työ, mistä ei ole mitään käytännön hyötyä, puhumattakaan että opinnäytetyöprosessin aikana opittua ei voitaisi hyödyntää myöhemmin työelämässä.

Työn tuloksena saavutettiin toimintavalmis järjestelmä alkuvaatimusten mukaan. Työssä esiintyi myös ongelmia pitkin matkaa, kuten pieniä virheitä virtuaalikoneiden luonnista domainin konfigurointeihin, puhumattakaan Zarafan asennuksesta sekä toimintavalmiuteen saattamisesta. Työn suorittamista voisikin verrata hyvin normaalissa työelämässä tapahtuvaan alan toimintaan: virheiden kautta opitaan, jolloin niitä ei taatusti tee uudestaan seuraavalla kerralla.

Ongelmatilanteissa suurena apuna toimivat Internetin hakukoneet, keskustelufoorumit, erilaiset tietokannat sekä tietysti asiantuntijan konsultointi etenkin Linux-asioissa. Tiedonhaku oli joustavaa, joskin todella työlästä paikoitellen, koska yhden pienen asetuksen löytäminen Internetistä voi olla kuin neulan etsiminen heinäsuovasta. Pienet palaset koottuna yhteen tuottivat lopulta kuitenkin toivotun lopputuloksen ja näin ollen järjestelmä valmistui, vaikkakin välillä hieman hitaanlaisesti.

Asioita, joita näin myöhemmin tekisin eri tavalla, voisi olla esimerkiksi domainin nimeäminen. Nyt luotu lamenet.fi voisi aiheuttaa isommassa ympäristössä esimerkiksi nimipalveluongelmia, joten itse domainin nimi tulisi muuttaa esimerkiksi lamenet.local:iksi. Lisäksi suuremmassa ympäristössä Zarafan käyttöönotto vaatisi ehdottomasti LDAP-tunnistuksen käyttämistä, jolloin yrityksen kaikkia käyttäjätunnuksia ei tarvitsisi manuaalisesti luoda Zarafaan, vaan tunnistaminen voitaisiin tehdä suoraan AD:n kautta. Tämä on kuitenkin sen verran suuren luokan projekti, että se on jätetty opeteltavaksi tulevaisuutta varten.

Työn soveltaminen käytäntöön sekä jatkokehitys valmiiksi tuotteeksi yritysmaailmaan vaatii sekin runsaasti lisätyötä. Työtä aloitettaessa allekirjoittanut oli juuri jäänyt työttömäksi, joten ajankohtaisen ja mielenkiintoisen aiheen löydyttyä heräsi mielenkiinto myös jatkomahdollisuuksiin. Työn puolivälissä alkoi sivuprojektina idean vieminen eteenpäin sekä idea uuden yrityksen perustamisesta, jonka tarkoituksena on tarjota palvelin- sekä työasemavirtualisointia, Zarafa-vaihtoehtoa sähköpostiksi ja muuta tietotekniikkaan liittyvää palvelua. Työn ollessa loppusuoralla kehitystä ja opiskelua on jatkettu entisestään. Vielä toistaiseksi nimeä vailla oleva yritys on perustamisvaiheessa ja toiminta on suunniteltu alkavaksi vielä vuoden 2010 kuluessa. Voidaankin sanoa, että opinnäytetyöstä siirtyminen työelämään oli juuri se tarvittava lisäpotku, mitä vaadittiin. Alan tutkiminen ja kehittäminen tulee siis jatkumaan, toivottavasti vielä vuosia.

LÄHTEET

1. Rousku, K. 2004. Virtuaalisesti halvemmalla, MikroPC 11/2004. Hakupäivä 12.7.2010. http://mikropc.net/rml/arkisto/mikropc/pdf/2309200440.pdf.

2. Wikipedia. 2009. Windows Server Domain. Hakupäivä 24.4.2010. http://fi.wikipedia.org/wiki/Windows_Server_Domain.

3. Wikipedia. 2010. Domain controller. Hakupäivä 24.4.2010. http://en.wikipedia.org/wiki/Domain_controller.

4. IT-pro. 2010. IT-asiantuntijoiden portaali. Hakupäivä 7.5.2010. http://itpro.fi/wiki/sivut/Identiteetti%20ja%20hakemistot/Active%20Directory.aspx.

5. Davis, D. 2009. VMWare Snapshot. Hakupäivä 5.6.2010. http://www.petri.co.il/virtual_vmware_snapshot.htm.

6. Microsoft Technet. 2006. Using the ping command. Hakupäivä 5.6.2010. http://technet.microsoft.com/en-us/library/cc737478%28WS.10%29.aspx.

7. Microsoft Technet. 2010. DCPromo. Hakupäivä 5.6.2010. http://technet.microsoft.com/en-us/library/cc732887%28WS.10%29.aspx.

8. Wikipedia. 2010. CentOS . Hakupäivä 14.7.2010. http://en.wikipedia.org/wiki/CentOS.

9. Busk, K, 2010. Kuinka pitkä on odottavan aika. 9-11. Hakupäivä 6.8.2010. http://www.proact.fi/Global/FI/Proact.Storage/ProactStorageFI%2001_2010.pdf.

10. Hämäläinen, P. 2007, 63. Vikasietoiset NAS-palvelimet, virtuaalisia tietoja etätoimipisteisiin. Hakupäivä 9.8.2010. http://www.tietokone.fi/lehti/tietokone_3_2007/vikasietoiset_nas_palvelimet_virtuaalisia_tiedostoja_etatoimipisteisiin_1398.

11. Webopedia. 2008. RAID. Hakupäivä 9.8.2010.
http://www.webopedia.com/TERM/R/raid.html.

12. VMWare Inc. 2009. vSphere Availability Guide. 33-43. Hakupäivä 12.8.2010.
http://www.vmware.com/pdf/vsphere4/r40/vsp_40_availability.pdf.

LIITE 1

Zarafa-sähköpostipalvelimen asennus sekä osa konfiguraatioista

Linux-pohjainen Zarafa asennettiin komentorivin kautta ja yhteyden luontiin käytettiin SSH-yhteyttä tukevaa Putty-ohjelmaa. Seuraavassa on eritelty osa SSH-komentoikkunan käskyistä järjestyksessä selityksineen, joilla Zarafa on konfiguroitu toimintavalmiiksi.

- Muodostetaan SSH-yhteys 10.20.1.4, karsitaan tarpeettomat palvelut pois ”system services” -kohdasta sekä konfiguroidaan palomuuri.
setup
firewall asetuksista SEL linux DISABLED
firewall customize -kohdasta avataan Zarafan käyttämät portit 110pop, 143imap, 25smtp

- Tarkistetaan verkkoasennuksen aikana asennetut paketit että ne varmasti täsmäävät.
yum install php OK
yum install php-common OK
yum install mysql-server mysql OK

- Editoidaan konfiguraatiotiedostoa siten, että sähköpostin välittämiseen tarvittavien pakettien haku tapahtuu vain postfixistä, sendmail poistetaan myöhemmässä vaiheessa.

nano /etc/yum.repos.d/CentOS-Base.repo

[base]
exclude=postfix

[updates]
exclude=postfix

[centosplus]
enabled=1
includepkgs=postfix

- Tallennetaan ctrl+x
- Asennetaan postfix ennen kuin sendmail poistetaan, muutoin Sendmailin poisto tuhoaa Postfixin tarvitsemia tiedostoja.

yum install postfix
yum remove sendmail

- Asennetaan sysstat, jonka Zarafa tarvitsee toimiakseen.
yum install sysstat

Kun järjestelmään on saatu asennettua kaikki Zarafan vaatimat paketit, niin ladataan itse Zarafa www.zarafa.com:ista. Valitaan tässä tapauksessa versio ” RHEL i386 including 3 users outlook support.”. Tässä vaiheessa työasemaan on asennettu WinSCP-ohjelma, joka mahdollistaa drag&drop-tyylisen tiedostosiirron ftp-yhteyden ylitse. Tämän jälkeen ladattu Zarafa-paketti siirretään /root kansioon, jonka jälkeen zarafa.gz puretaan.

tar xfv zarafa.tar.gz (tar –help lisätietoa purkuohjelmasta)
cd zarafa

- Käynnistetään Zarafan asennustiedosto
./install.sh

- Tässä vaiheessa täytyy sql-serverille asettaa admin salasana, jotta asennusta pystytään jatkamaan. Asennetaan myös WEBMIN-lisäosa, jolla pystytään hallitsemaan unix-palvelinta web-selaimen kautta.

wget souceforge.net/…../webmin.rpm haetaan webmin-paketti

- Asennetaan rpm-muotoa oleva Webmin-paketti rpm-komennolla.

rpm –Uvh webmin…noarch.rpm (rpm:llä asennetaan .rpm tiedostoja) (rpm –help lisää tietoa)

- Käynnistetään mysql palvelu

/etc/init.d/mysqld start

- Käytetään Googlen hakukonetta, jotta saadaan suora komentorivi millä sql-salasana vaihdetaan. ”mysql root passwd” → **mysqladmin –u root password NEWPASSWORD** → copy paste SSH-ikunaan

- Avataan Webminille palomuurista portti 10000 (firewall configuration/customization/other ports 10000).
- Nyt pystytään hallitsemaan Linuxia web-selaimen kautta osoitteesta **http://10.20.1.4:10000**.

- Jatketaan Zarafan asennusta. Tuoteavainta ei tarvita, kun asennetaan community pack.

mysqlserver localhost [oletus]
mysql port 3306 [oletus]
mysql User root [oletus]
mysql password administrator [oletus]
database name zarafa [oletus]
log method (file or syslog) file [oletus]
log filename [oletus]
smtp server (ulospäin lähtevän postin palvelin) **mail.inet.fi**
log method file [oletus]
log filename [oletus]

monitor config (esim quota varoitus)
send interval 1 day [oletus]
log method [oletus}
log file [oletus]

zarafa gateway and ical YES
log method [oletus]
log file [oletus]
pop3 port 110 [oletus]
imap port 143 [oletus]
zarafa indexer service YES

start the server now YES
start the configured services YES
zarafa-admin (zarafan hallinta)
man zarafa-admin (zarafan hallintaohje)

- Nyt on saatu Zarafa toimimaan siihen pisteeseen asti, että pystytään kirjautumaan webmailiin osoitteessa https://10.20.1.4/webaccess .

- Haetaan ja asennetaan rpmforge (pakettivarasto), joka on lisäosa CentOSiin, software repository.

wget http://apt.sw.be/redhat/el5/en/i386/rpmforge/RPMS/rpmforge-release-0.3.6-1.el5.rf.i386.rpm
rpm -ivh http://apt.sw.be/redhat/el5/en/i386/rpmforge/RPMS/rpmforge-release-0.3.6-1.el5.rf.i386.rpm

- Haetaan sähköposteja varten virustorjuntaohjelmiston ClamAV asennuspaketti ja asennetaan se.
yum install clamav clamd clamav-db clamav-devel
YES
yum -y install rpm-build gcc make automake autoconf

- Tämän jälkeen ladataan ja asennetaan virustutka (ClamSMTP) smtp-protokollaan. Clamsmtp käyttää Clamav-moottoria, eli ClamSMTP on smtp-lisäosa itse Clamav:hen.

wget http://www.inet.lt/clamsmtp/clamsmtp-1.10-1.src.rpm
rpmbuild —rebuild clamsmtp-1.10-1.src.rpm
rpm -ivh /usr/src/redhat/RPMS/i386/clamsmtp-1.10-1.i386.rpm

- Sitten asennetaan roskapostisuodatin Spamassassin.

yum install spamassassin

Kun Spamassassin on asennettu, alkaa itse Zarafan asetuksien konfiguroiminen. Koska konfiguraatiotiedostot ovat satojen rivien mittaisia niin niitä ei tässä liitteessä erikseen julkaista. Noissa tiedostoissa kuitenkin on manuaalisesti määritelty mm. tietokanta-asetuksia, käyttäjätunnuksia ja salasanoja, domain-asetuksia, postin kulun kannalta tärkeitä postfix-ominaisuuksia (white list ym) jne. Järjestelmän toimintakuntoon saattamiseksi on suurimpana apuna ollut hakukone Google.

Tämän jälkeen luodaan tunnukset, jotta posti kulkee oikein. Vmail-tunnus toimii järjestelmän postioperaattorina joten se on määritelty tiedostossa rootiksi pystyen käyttämään kaikkia tietokantoja ilman salasanakyselyitä.
Adduser vmail
passwd vmail administrator
Adduser spamd
passwd spamd administrator

Jotta Zarafa toimisi oikein, täytyy jokaisen ”zarafa”- sekä ”clam”-alkuisen palvelun olla käynnissä, kuin myös ”spamassassin”, ”mysqld” ja ”httpd”. Nämä asetukset voidaan muokata Webminin kautta käynnistymään suoraan bootissa.

Zarafa on nyt siis konfiguroitu, joten voidaan tehdä testitunnus ja testata järjestelmän toimivuus.

zarafa-admin –c testi –f ”Teppo Testaaja” –e teppo.testaaja@lamenet.fi –P

Tämän jälkeen voidaan kirjautua Zarafan web-accessiin. Järjestelmän toimivuus saadaan selville, kun pystytään lähettämään sekä vastaanottamaan sähköpostia. Sähköpostin toiminta on testattu toimivaksi luvussa **4.3.3**.