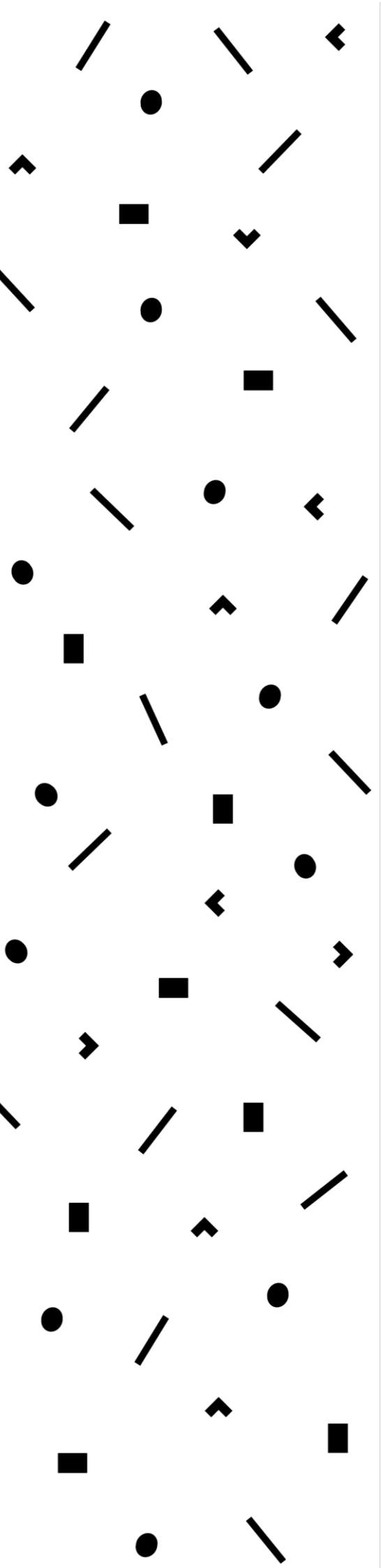


LAMK Lahden ammattikorkeakoulu
Lahti University of Applied Sciences

Pienyrityksen palvelimien ylläpitoratkaisu

LAHDEN
AMMATTIKORKEAKOULU
Tekniikan ala
Tietotekniikan koulutusohjelma
Tietoliikennetekniikka
Opinnäytetyö
Kevät 2016
Olli Metsähukala

Lahden ammattikorkeakoulu
Tietotekniikan koulutusohjelma

METSÄHUKALA, OLLI: Pienyrityksen palvelimien ylläpitoratkaisu

Tietoliikennetekniikan opinnäytetyö, 47 sivua

Kevät 2016

TIIVISTELMÄ

Opinnäytetyön tavoitteena oli vertailla pienyrityksen palvelimien erilaisia ylläpitoratkaisuja ottaen huomioon erityisesti kustannustehokkuuden, teknisen puolen mahdolliset haasteet sekä eri ylläpitoratkaisuihin liittyvien riskien arvioimisen.

Työssä vertaillaan kolmea eri vaihtoehtoa, joilla voidaan toteuttaa Miradore Oy:n palvelimien ylläpito. Näitä vaihtoehtoja ovat palvelimien ylläpito toimeksiantajan puolesta, kolmannen osapuolen hosting-palvelun ostaminen tai vaihtoehtoinen ratkaisu, jossa yhdistellään kahta aiemmin mainittua toteutustapaa. Vertailusta saadun tuloksen perusteella voidaan yritykselle suositella hosting-palvelun hyödyntämistä osana palvelimien ylläpitoratkaisua, koska yritykselle kriittisten palveluiden toimivuuden varmistaminen on parempi tässä ylläpitoratkaisussa.

Toisena tavoitteena oli tutkia fyysisiä palvelimia, virtualisointia sekä pienyrityksen tyypillisesti ylläpitämiä palveluita teoriassa. Fyysiset palvelimet toimivat alustana, jotka mahdollistavat virtualisoitujen palveluiden luomisen ja ylläpitämisen. Virtualisointi tarkoittaa palvelimen fyysisen tason resurssien jakamista useampaan suoritusympäristöön. Virtualisoinnin hyötyinä voidaan mainita palvelimien komponenttien parempi käyttösuhde, joka myös vähentää tarvetta suurelle määrälle fyysisiä palvelimia. Palvelinvirtualisointi on virtualisoinnin alaluokka, jota käyttämällä suurin osa nykyajan yrityksien palveluista on tuotettu. Pienyrityksen ylläpitämät palvelut vaihtelevat riippuen yrityksen henkilöstön määrästä ja toimialasta, mutta tyypillisesti ylläpidettyihin palveluihin kuuluvat käyttäjätietokanta, sähköpostipalvelin, nimipalvelin, tiedostopalvelin ja päivitysten keskitetty hallinta.

Yrityksen kannalta oikean ylläpitoratkaisun valitseminen vähentää yritykseen kohdistuvia riskejä imagon ja taloudellisen tappion suhteen. Tämän lisäksi se mahdollistaa paremman palveluiden toiminnan takaamisen, joka on jokapäiväisen työn jatkuvuuden kannalta tärkeää.

Asiasanat: palvelinympäristö, ylläpitoratkaisu, virtualisointi

Lahti University of Applied Sciences
Degree Programme in Information Technology

METSÄHUKALA, OLLI: Server hosting solution for small businesses

Bachelor's Thesis in Telecommunications Technology, 47 pages

Spring 2016

ABSTRACT

The objective of the thesis was to compare several server hosting solutions for a small to medium-sized company. This comparison was made in order to find out which solution offers the best cost-efficiency, in addition to being a low-risk method combined with an enterprise level data security.

Three options for making the upkeep of necessary services possible were compared to each other. These options were: either the company hosts their own physical servers and services, or they buy a hosting-service, or they use a solution that combines buying a hosting-service and hosting some of the servers by themselves. The result of this comparison is that utilizing a hosting-service as a part of the hosting solution can be recommended to the company due to it ensuring a better operability of critical services.

The secondary objective of this thesis was to examine physical servers, virtualization as a technique, and also study the services that are typically virtualized and hosted on a server. Physical servers act as a platform that enables the creation and upkeep of virtualized services. Server virtualization is a virtualization subclass that allows the distribution of a server's physical resources to several operating systems located in a single server. The advantage of using server virtualization is that it enables better use of physical server components, which leads to saving company resources by reducing the number of required servers. The types of services implemented by a small company depend on the size of the staff, and the business they are in. Typically implemented virtualized services include a directory service, a mail server, a name server, a file server and centralized management of updates for software.

Choosing the correct hosting solution for the company in question reduces the risks of bad publicity and financial loss. In addition, it guarantees a better operability of implemented services, which is important for the continuity of every day work in a company.

Key words: server environment, hosting solution, virtualization

1 JOHDANTO 1

2 PALVELIMET 2
2.1 Yleisesti fyysisistä palvelimista 2
2.2 Suoritin 3
2.3 Massamuisti 5
2.4 Keskusmuisti, virtalähde, verkkokortti 7

3 VIRTUALISOINTI 9
3.1 Yleisesti virtualisoinnista 9
3.2 Virtualisoinnin historiaa 9
3.3 Palvelinvirtualisoinnin toimintaperiaatteet 11
3.3.1 Hypervisor ja virtuaalikone 11
3.3.2 Palvelinvirtualisoinnin toteutusmenetelmät 14
3.4 Virtualisoinnin hyödyt 16
3.5 Virtualisointiohjelmistot 18

4 PALVELINYMPÄRISTÖ PIENYRITYKSESSÄ 22
4.1 Pienyrityksen palvelinympäristön rakenne 22
4.2 DNS 22
4.3 Domain controller 24
4.4 Tiedostopalvelin 26
4.5 Ohjelmistojen ja päivitysten keskitetty hallinta 27
4.6 Sähköpostipalvelin 28
4.7 Varmuuskopiointi 30

5 PALVELIMIEN YLLÄPITORATKAISU 32
5.1 Nykytilanne yrityksessä 32
5.2 Hosting-palvelu 35
5.3 Vertailu oman hostingin ja hosting-palvelun välillä 36
5.4 Vaihtoehtoratkaisu palvelimien ylläpitoon 38
5.5 Vertailu palvelimien ylläpitoratkaisuiden välillä 40

6 YHTEENVETO 42

LÄHTEET 44

LYHENNELUETTELO

AD	Active Directory, toimialueen käyttäjätietokanta.
CIFS	Common Internet File System, tiedostonjakoprotokolla
CPU	Central Processing Unit, prosessori tai suoritin
DAS	Direct Attached Storage, tietokoneeseen liitetty massamuisti
DNS	Domain Name System, nimipalvelujärjestelmä
HA	High Availability, järjestelmän korkea saatavuus
IT	Information Technology, informaatioteknologia
LDAP	Lightweight Directory Access Protocol, verkkoprotokolla
MTBF	Mean Time Between Failures, tilastollinen vikaantumisaika
NAS	Network Attached Storage, verkkotallennusmedia
NFS	Network File System, tiedostonjakoprotokolla
RAID	Redundant Array of Inexpensive Disks, vikasietoisuustekniikka kiintolevyille
RAM	Random Access Memory, keskusmuisti
SAN	Storage Area Network, tiedostopalvelintekniikka
SAS	Serial Attached SCSi, tietokoneväylä
SCSI	Small Computer System Interface, tietokoneväylä
WSUS	Windows Server Update Services, Windows-koneiden keskitetyn päivityksien hallinnoimisen mahdollistava ohjelmisto.

1 JOHDANTO

Miradore Oy on suomalainen IT-alan ohjelmistoyritys, joka tarjoaa yrityksille ratkaisuja sekä työpöytälaitteiden että mobiililaitteiden hallintaan työympäristössä. Ohjelmiston hallintaominaisuuksiin kuuluu fyysisellä tasolla laitteiden tarkkojen tietojen tarkastelu helpossa formaatissa, ohjelmistojen ja käyttöjärjestelmien automatisoidut rutiinitoimenpiteet, tietojen varmentaminen sekä etähallinta. Vuonna 2006 perustetun yhtiön tuotteita hyödynnetään kymmenissä maissa, tuhansissa laitteissa. Henkilöstömäärä liikkuu alle 50 henkilön tienoilla, joten tämän perusteella yritys voidaan luokitella pieneksi PK-yritykseksi.

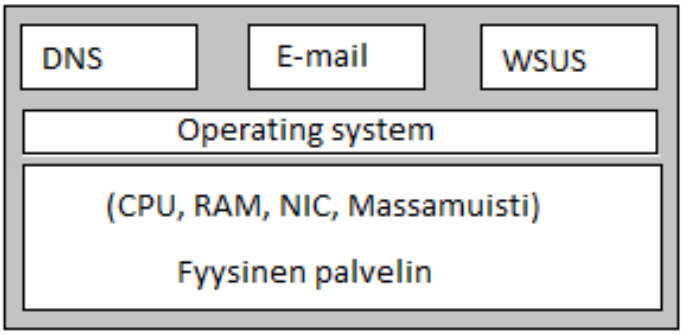
Työn tavoitteena on vertailla Miradoren palvelimien erilaisia ylläpitoratkaisuja ottaen huomioon erityisesti kustannustehokkuuden, teknisen puolen mahdolliset haasteet sekä riskien arvioimisen. Tavoitteena on myös selvittää, mitä etuja ja haittoja kukin vaihtoehto tuo mukanaan, ja tästä vertailusta saadun informaation myötä päätyä yrityksen kannalta parhaaseen mahdolliseen ratkaisuun.

Työssä käydään läpi yksityiskohtaisesti palvelinympäristöä, jota tavallisesti hyödynnetään IT-alan pienyrityksissä. Opinnäytetyöstä tulee selville fyysinen kokoonpano komponenteista lähtien ja fyysisen tason päälle rakennettavat virtualisoidut palvelut, kuten käyttäjätietokanta, nimipalvelin, sähköpostipalvelin sekä käyttöjärjestelmän ja ohjelmistojen keskitetty päivitystenhallinta. Lisäksi tutustutaan eri menetelmiin, joilla voidaan hoitaa datan varmuuskopiointi. Käytännön osuudessa otetaan selvää hosting-palveluiden tarjoamista vaihtoehdoista ja vertaillaan niiden kustannuseroja ja riskejä yrityksen nykyiseen ylläpitoratkaisuun. Vaihtoehtoisena ratkaisuna tarkastellaan skenaariota, jossa ostetaan hosting-palvelua samalla jättäen osan laitteista ja palveluista yrityksen ylläpidettäväksi.

2 PALVELIMET

2.1 Yleisesti fyysisistä palvelimista

Nykypäivänä yrityksen työntekijöiden lukumäärän ja liiketoiminnan kasvaessa tarvitaan monesti ylimääräistä IT-infrastruktuuria, jotta voidaan tarjota palveluita sisäverkon puolelle omalle henkilökunnalle sekä esimerkiksi www-sivuja tai nettikauppoja ulkoverkon puolelle asiakkaita varten. Näiden palveluiden luomista ja käyttämistä kutsutaan server-client-malliksi, jossa yksi palvelin voi palvella useaa käyttäjää samanaikaisesti ja yksi käyttäjä voi hyödyntää useamman palvelimen palveluita yhtä aikaa. Tässä kohtaa verkkoympäristön pääpainona toimivat palvelimet, jotka ovat joko ohjelmistoa sisältäviä fyysisiä tietokoneita tai hypervisoreita, joilla voidaan virtualisoida palvelinympäristöjä. Tyypillisesti organisaatioiden palvelimilla hoidetut palvelut liittyvät erityisesti tietokantojen hallintaan, keskitettyyn ja jaettuun tiedostojen tallentamiseen, www-palveluiden sekä eri sovellusten rakentamiseen ja ylläpitoon. (Dell 2016, 1.)



KUVIO 1. Fyysisen palvelimen kolmikerroksinen toimintamalli

Fyysiset palvelimet eivät näytä eroavan suuresti työpöytäkäyttöön tarkoitetuista tietokoneista, sillä molemmat käyttävät prosessoria, keskusmuistia sekä kovalevyjä datan tallentamista varten. Eri konetyypit eroavat erityisesti käyttötarkoituksen mukaan – palvelimilla ei ole yleensä tarkoituksenakaan ajaa graafisesti intensiivisiä sovelluksia kuten kokonaisversiota käyttöjärjestelmistä vaan päinvastoin. Palvelimet käsittelevät taustalla raskaita prosesseja, joiden tarkoituksena on tarjota erinäisiä palveluita käyttäjille, ja tällöin palvelimen hallintanäkymän ei

haluta vievän turhaa tehoa pois järjestelmän tärkeimmiltä työtehtäviltä. Yleisenä käytäntönä palvelimiin asennetaan riisuttu versio halutusta käyttöjärjestelmästä tai sovelluksesta, johon tehdään oleelliset konfiguraatiot manuaalisesti paikan päällä, ja tämän jälkeen loput muokkaukset voidaan tehdä etänä verkon kautta. Tämän käyttöjärjestelmän päälle voidaan tehdä halutut verkkoa koskevat yleiset käytännöt ja asentaa tarvittavat sovellukset palveluiden tarjoamista varten. Kuviossa 1 on kuvailtu fyysisen palvelimen kolmikerroksinen toimintamalli. (Dell 2016, 1 - 2.)

Yrityskäyttöön tarkoitetut fyysiset palvelimet voidaan jakaa kahteen ryhmään koon perusteella: räkkipalvelimiin ja tornipalvelimiin. Räkkipalvelimet asennetaan nimensä mukaisesti kaappimaiseen palvelimille tarkoitettuun laitetelineeseen mutterien, ruuvien ja kiskojen avustuksella. Räkkipalvelimet on yleensä tarkoitettu suuremman työkuorman prosessointiin ja ovat hyvä vaihtoehto isommalle yritykselle, jossa palveluita käytetään paljon. Tämän takia niiden komponentit ovat laadukkaampia sekä kalliimpia, ja tämä yhdistettynä palvelinkaapin pakolliseen hankintaan tekevät niistä kustannustehokkudeltaan huonomman vaihtoehdon pienemmälle yritykselle. Tornipalvelimet ovat hieman pöytäkonetta suurempia, joten niiden sijoittaminen organisaatiossa on helpompaa, sillä ne eivät välttämättä tarvitse omaa tilaa tai erillistä laitekaappia. (Dell 2016, 3.)

2.2 Suoritin

Suoritin (CPU) on tietokonekomponenttien keskeisin osa, joka suorittaa eri ohjelmistojen antamia käskyjä. Palvelinkäyttöön tarkoitettu suoritin eli prosessori eroaa pöytäkoneiden vastaavasta komponentista siten, että sen välimuisti, johon säilötään useasti pyydettyä dataa, on huomattavasti suurempi kooltaan kuin pöytäkoneversion. Prosessori pystyy täten käsittelemään suuremman määrän pyyntöjä lyhyemmässä ajassa, ja juuri tämän vuoksi palvelimien prosessorissa halutaan olevan suuri määrä välimuistia. Käytetyt prosessorit eroavat myös rakenteeltaan, sillä

raskaampaan käyttöön halutaan suuri määrä ytimiä, jolloin pyyntöjen ja tiedon prosessointi nopeutuu. Palvelinkäytössä moniydin-prosessori pystyy myös hyödyntämään kaikkia ytimiään tasaisemmin ja isommalla taakalla kuin yleisessä käytössä olevat tietokoneet. (Dell 2016, 1.)

Nykyajan palvelimissa käytetään monesti Intelin suorittimia siksi, että ne hyödyntävät hypersäikeistystä (Hyperthreading technology, HTT). Hypersäikeistyksellä varustettu prosessori hyödyntää resursseja tehokkaammin kuin vastaava prosessori ilman kyseistä teknologiaa. Käytännössä tämä tarkoittaa sitä, että hypersäikeistys tuo ohjelmistotasolle näkyviin yhtä monta virtuaalista ydintä kuin mitä prosessori sisältää fyysisiä ytimiä. Esimerkkinä Intelin i7-prosessorit sisältävät neljä ydintä hypersäikeistyksellä, joten käyttöjärjestelmä näkee tässä tapauksessa käytössä olevan kahdeksan ydintä, joita voidaan hyödyntää eri tehtäville. Hypersäikeistysteknologian myötä prosessorien suorituskyky nousee joitain kymmeniä prosentteja aiemmasta. (Intel 2016a.) Tämä yhdistettynä turbo boost -teknologiaan, joka voi nostaa hetkellisesti suorittimen kellotaajuutta yli luvatun määrän, nostaa tuottavuutta suorittamalla enemmän käskyjä ja tehtäviä samanaikaisesti lyhyemmässä ajassa (Intel 2016b).

Suurin osa nykypäivän suorittimista käyttävät joko x86-arkkitehtuuria, joka on yleinen nimitys Intelin 80286-mikroprosessoria seuranneille samaa arkkitehtuuria hyödyntäville suorittimille, tai sen 64-bittistä versiota. X86-arkkitehtuuri on nykyajan CPU-markkinoita hallitseva sovellusalusta, jota myös palvelinkäyttöön suunnatut prosessorit käyttävät. Prosessorityyppiä yhdistää suunnittelu, jonka tärkein periaate on ollut aikaansaada taaksepäin yhteensopiva arkkitehtuuri, jossa vanhoille prosessoreille tehtyjä sovelluksia voidaan käyttää sellaisenaan uudemmissakin malleissa. Myös muut valmistajat, kuten AMD, tekevät x86-arkkitehtuurilla toimivia prosessoreja. (Rouse 2006.)

2.3 Massamuisti

Massamuistin tehtävänä on toimia pysyvänä säilytys- ja tallennuspaikkana tietokoneen sisältämälle datalle. Yleisesti käytössä olevien tietokoneiden ja palvelimien yksi suurimmista fyysisten komponenttien eroista sijaitsee tallennusjärjestelmässä. Pöytäkoneissa käytetään yleisesti yhdestä kahteen erillistä kiintolevyä datan tallentamista varten, mutta palvelimissa tarvitaan monesti suurempi määrä tallennuskapasiteettia, jonka tulisi olla mahdollisimman vikasietoista palveluiden toimivuuden varmistamista varten. Tämän lisäksi kiintolevytyypit ja nopeudet eroavat eri ympäristöjen välillä. Esimerkiksi palvelimissa voidaan käyttää SAS-(Serial Attached SCSI) tai SCSI (Small Computer System Interface) -levyjä suuremman siirto- ja lukunopeuden takia. (Dell 2016, 2.)

Vikasietoisuuden aikaansaamiseksi voidaan käyttää hyödyksi RAID-tekniikkaa (Redundant Array of Inexpensive Disks), jolla voidaan yhdistää useita fyysisiä kiintolevyjä näkymään yhtenä loogisena tallennusmediana. RAID-tekniikkaa käytetään yksittäisten kiintolevyjen vikaantumisen tai korruptoitumisen suojaamiskeinona, jolloin yhden kiintolevyn hajotessa data ei häviä kokonaan, sillä muut järjestelmässä sijaitsevat tallennusmediat sisältävät saman datan. Tätä tekniikkaa voidaan hyödyntää eri tavoilla, jotka jaetaan RAID-tasoihin riippuen käytetystä vikasietoisuustavasta ja asteesta. Käytetyimmät näistä tasoista ovat RAID 0, RAID 1, RAID 10, RAID 5, RAID 6, RAID 50 ja RAID 60. (Dell 2016, 2.)

RAID 0

RAID 0 perustuu lomituskäytäntöön, jolloin data kirjoitetaan kiintolevyille tasaisesti. Tällä tavalla saavutetaan nopeampi suoritusteho, mutta menetetään vikasietoisuus, sillä dataa ei kopioida eikä peilata muualle. Mikäli yksikin pakan kovalevyistä hajoaa, menetetään kovalevyn sisältämä data lopullisesti. RAID 0 on toimiva käytäntö suurille tiedostoille ympäristössä, jossa vikasietoisuus ei ole tärkeää. (Cisco 2016a.)

RAID 1

RAID 1 hyödyntää peilaamista, eli kyseinen tekniikka tallentaa saman datan useammalle eri kiintolevylle. Kyseisellä teknologialla saavutetaan vikasietoisuus, sillä yhden levyn hajotessa täsmälleen sama data löytyy muualta. Haittapuolena voidaan mainita tallennustilan menettäminen, joten tämä tapa on hyödyllinen pienille tietokannoille tai muille sovelluksille jotka vaativat kahdennuksen, mutta eivät vie suurta määrää tilaa. (Cisco 2016a.)

RAID 10

RAID 10 yhdistää RAID 0- ja RAID 1 -teknologian, joka käytännössä lisää nopeutta sekä vikasietoisuutta, mutta sisältää myös niiden heikkouksia kuten ylimääräisen tallennustilan menettämisen peilaamisen myötä. RAID 10 lomittaa datan peilatuissa pareissa, eli se vaatii vähintään neljä levyä ja niistä levypareista vähintään toisen tarvitsee olla toimintakuntoinen, jotta dataa ei menetetä. (Cisco 2016a.)

RAID 5

RAID 5 on edellisiä tekniikoita monimutkaisempi ja vaatii vähintään kolmen levyn olemassaolon pakassa, mutta sitä hyödyntämällä ei menetetä dataa riippumatta siitä mikä pakan yksittäisistä levyistä vikaantuu. Kaikkiin levyihin tallennetaan tasaisesti hajautettu pariteettidata, jolla vikasietoisuus saadaan toteutettua. (Cisco 2016a.)

RAID 6

RAID 6 on kehittyneempi versio RAID 5 -teknologiasta, jossa tallennetaan suurempi määrä pariteettidataa, joka mahdollistaa jopa kahden yksittäisen levyn hajoamisen pakasta ilman datan menettämistä (Cisco 2016a).

RAID 50

RAID 50 yhdistää RAID 5- ja RAID 0 -teknologiaa eli lomitusta ja pariteettidatan tallentamista ylimääräisille levyille. (Cisco 2016a.)

RAID 60

RAID 60 yhdistää RAID 6- ja RAID 0 –teknologiaa, eli sen voidaan sanoa olevan suoraan kehittyneempi versio RAID 50-menetelmästä. (Cisco 2016a.)

Osa RAID-tasoista mahdollistavat hot sparen käytön, joka tarkoittaa ylimääräistä levypakassa sijaitsevaa kiintolevyä, joka on valmiustilassa odottamassa mahdollista käytössä olevan levyn vikaantumista, jolloin ylimääräinen kiintolevy ottaa automaattisesti tämän paikan levyjärjestelmässä. Tämä operaatio toimii automaattisesti ilman järjestelmänvalvojan tai ylläpitäjän vaatimia toimenpiteitä. Hot sparen käyttö on mahdollista kaikissa edellämainituissa RAID-tasoissa paitsi RAID 0:ssa. (Cisco 2016a.)

Hot sparen lisäksi voidaan suorittaa hot swap -operaatio tietyissä tämän ominaisuuden sisältävissä palvelimissa, jolloin manuaalisesti vaihdetaan levypakassa sijaitseva epätoiminnassa oleva levy uuteen ilman järjestelmän sammuttamista. Uuden levyn asennuksen jälkeen järjestelmä osaa uudelleenrakentaa vanhalla levyllä olevan datan uuteen, jolloin vikasietoisuus on saavutettu jälleen. (Cisco 2016a.)

2.4 Keskusmuisti, virtalähde, verkkokortti

Loput palvelinosat nouduttavat samoja periaatteita kuin prosessori ja tallennusmediat, eli halutaan suorittaa useita pyyntöjä mahdollisimman nopeasti ja samanaikaisesti sekä tehdä tämä vikasietoisesti. Keskusmuisti (RAM) on tapa toteuttaa ohjelmistoille ja sovelluksille nopeaa, hetkellistä tallennuskapasiteettia, joka tavallisesti tyhjenee laitteiston virtojen katketessa. Varsinkin tärkeitä palveluita ylläpitävällä palvelimella keskusmuistina käytetään kellotaajuudeltaan korkeaa eli nopeaa ECC-RAMia (Error-correcting code memorya), joka ehkäisee yksittäisten bittien aiheuttamat virheet ja täten estää korruptoidun datan syntymisen. Hinnaltaan ECC-RAM on kalliimpaa kuin ECC:tä sisältämätön

keskusmuisti, mutta on oleellinen osa tärkeiden palveluiden vikasietoisuuden takaamista. (Dell 2016, 3.)

Virtalähteet on suunniteltu vikasietoisuutta silmällä pitäen, jolloin palvelin sisältää useasti vähintään kaksi eri virtalähdettä, jotka takaavat palvelimen virransaannin yhden virtalähteen vikaantuessa. Tavanomaisessa tilanteessa molemmat virtalähteet toimivat suunnitellusti. Kaikki palvelimet eivät sisällä vikasietoisuutta virtalähteiden suhteen, mutta hieman suurempia yrityksiä ja palveluita ajatellen virtalähteiden kahdentaminen on yksi datan varmistuskeino lisää. (Dell 2016, 3.)

Verkkokortilta halutaan mahdollisimman nopeat yhteydet, mikä nykypäivänä tarkoittaa vähintään gigabitin liityntää. Palvelimien verkkokortit hoitavat tiettyjä verkkoon liittyviä tehtäviä itse, jotta suorittimelle jää enemmän aikaa tehdä tärkeämpiä laskelmia raskaan kuormituksen aikana. Mikäli palvelimessa on useampi verkkokortti, niin liitynnät voidaan yhdistää, jolloin saadaan huomattavasti nopeampi yhteys palvelimelta ulos. Lopputuloksena saadaan siirrettyä suurempi määrä dataa nopeammin kuin pöytäkoneen vastaavaa verkkoliityntää hyödyntämällä. (Dell 2016, 4.)

3 VIRTUALISOINTI

3.1 Yleisesti virtualisoinnista

Palvelimien fyysisten osien kehitys on ollut erittäin nopeaa jo monien vuosien ajan. Mooren laki viittaa Gordon E. Mooren vuonna 1965 tekemään havaintoon, jonka mukaan prosessorien sisältämä transistorien lukumäärä kaksinkertaistuu tietyn aikavälin kuluttua. Tätä aikaväliä yleensä pidetään noin 18 - 24 kuukauden pituisena. Mooren laki selittää fyysisten palvelinosien nopean kehityksen ja kehityksen vaikutuksesta seuranneen ilmiön, jossa normaalien palvelinohjelmistojen ja palveluiden ajaminen fyysisen tason päällä aiheuttaa vain pienen suorituskäytön. (Golden 2007.)

Virtualisoinnilla viitataan käsitteeseen, joka tarkoittaa tietokoneen komponenttitason resurssien jakamista useampaan suoritusympäristöön käyttämällä yhtä tai useampaa seuraavista teknologioista: osittainen tai täysimittainen tietokonesimulaatio, emulaatio ja sovellustason tai komponenttitason jakaminen osiin (Williams & Garcia 2007).

Käytännössä virtualisointia hyödynnetään nykypäivän tietotekniikassa siten, että yhdellä palvelimella voi olla käytössä useampi käyttöjärjestelmä samanaikaisesti, jotka jakavat resursseja isäntäkoneen komponenteista suorittaakseen toimintoja. Nämä vieraskäyttöjärjestelmät eivät ole tietoisia toisistaan vaan käyttäytyvät kuin ne olisivat suoraan asennettuna fyysisen alustan päälle pääkäyttöjärjestelmäksi, vaikka todellisuudessa ne toimivat virtualisointiohjelmiston päällä. Näihin virtualisoituihin vieraskäyttöjärjestelmiin voidaan asentaa halutut palvelut. (Golden 2007.)

3.2 Virtualisoinnin historiaa

Virtualisoinnin kehitys lähti liikkeelle 1960-luvulla; tosin virtualisointi tunnettiin eri nimellä ja tarkoitusperäkin erosi nykypäivän käsitteestä. Alkuperäisessä muodossaan virtualisointi tunnettiin termeinä ”time sharing” ja ”multiprogramming”. Christopher Strachey toi termit esiin

tutkielmassaan Time Sharing in Large Fast Computers. Käytännössä nämä termit tarkoittivat moniajotekniikkaa, jolla yksi ohjelmoija voisi kehittää ohjelmaa omassa konsoli-ikkunassaan samalla kuin toinen ohjelmoija debugaisi omaansa. Tarkoituksena tällä tekniikalla oli välttää ylimääräinen odotusaika, joka johtui ajan hitaasta tietokoneteknologiasta. Tästä syntyi muita nykypäivän virtualisointiteknologiaa ajatellen mullistavia ideoita, joista kaksi tärkeintä ovat Atlas ja IBM M44/44X. (Williams & Garcia 2007.)

Atlas oli yksi 1960-luvun alun ensimmäisistä supertietokoneista, joka hyödynsi Christopher Stracheyn ideoimia teknologioita. Atlas oli yksi aikansa nopeimmista tietokoneista, koska käyttöjärjestelmäprosessit ja käyttäjäprosessit erotettiin eri osiin. Supervisor hallitsi tietokoneen avainresursseja ja ympäristöä, joka vastasi käyttäjätason käskyistä. Atlaksessa oli myös erotettu käyttöjärjestelmätason muisti käyttäjätason sovelluksien käyttämästä muistista. Supervisorin voidaan ajatella vastaavan ideologialtaan nykypäivän virtualisoinnin hypervisoria. (Williams & Garcia 2007.)

IBM vastasi Atlas-supertietokoneeseen omalla projektillaan, joka sai nimen M44/44X. Tämä arkkitehtuuri oli ensimmäinen, joka käytti termiä virtuaalikone ja oli samalla IBM:n ensimmäinen panostus ”time-sharing”-teknologiaa hyödyntävälle supertietokoneelle. (Williams & Garcia 2007.)

IBM jatkoi virtualisoinnin kehitystä 1960- ja 1970-luvuilla. 1960-luvun lopulla IBM julkaisi ensimmäisen onnistuneen käyttöjärjestelmän, joka tuki täysvirtualisointia (CP-40). 1980-luvulla ja 1990-luvun alkupuolella virtualisoinnin kehitys hidastui merkittävästi, mikä johtui tietokoneiden yleistymisestä ja siitä seuranneesta trendistä. Fyysisiä tietokoneita ja palvelimia pidettiin tarpeeksi tehokkaina, joten yhden palvelimen raudan käyttöasteen parantamista virtualisoinnin avulla ei havaittu tarpeelliseksi. Vuonna 1999 VMware julkaisi aiemmin mahdottomana pidetyn x86-arkkitehtuurin täysvirtualisointimenetelmän. Tämä toimi osaltaan virikkeenä muille yrityksille alkaa kehittämään vastaavaa tuotetta. (Williams & Garcia 2007.)

3.3 Palvelinvirtualisoinnin toimintaperiaatteet

Palvelinvirtualisointi on yksi suurimmista virtualisoinnin nykypäivän trendeistä ja syystäkin. IT-alan organisaatiot ovat kärsineet palvelinsalien tilanpuutteesta ennen virtualisoinnin yleistymistä. Fyysisten palvelimien viedessä suuren määrän tilaa ja laajentamismahdollisuuksien heikentyessä on ollut haasteellista yrityksille tarjota asiakkaiden tarvitsemia resurssimääriä. (Golden 2007.)

Ratkaisuna ongelmaan on palvelinvirtualisointi, jossa asennetaan palvelimelle hypervisor eli virtuaalikoneiden hallintaohjelmisto, joka toimii välikerroksena erottaen fyysisen tason ja ohjelmistotason. Hypervisorin päälle voidaan rakentaa virtuaalikoneympäristö, joka ylläpitää tarvittavia palveluita. Virtualisoitujen palvelimien lisääntyessä tarve ylläpitää suurta määrää fyysisiä palvelimia vähenee. (Golden 2007.)

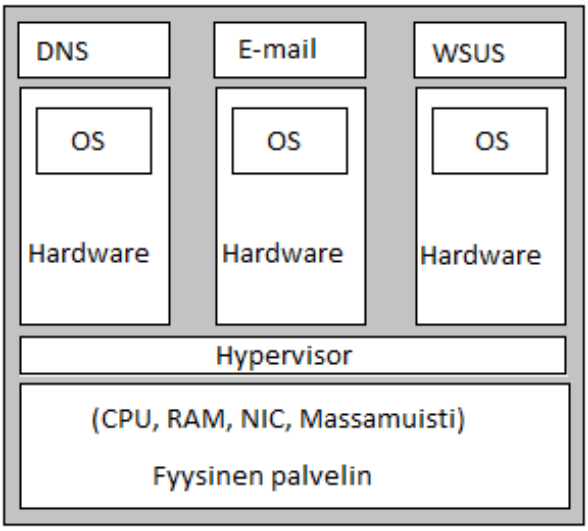
3.3.1 Hypervisor ja virtuaalikone

Hypervisor on virtuaalikoneiden hallintaohjelmisto (Virtual Machine Manager, VMM), joka mahdollistaa useamman vieraskäyttöjärjestelmän eli virtuaalikoneen samanaikaisen olemassaolon hyödyntäen isäntäkoneen fyysisiä resursseja. Jokaisella virtuaalikoneella näyttää olevan käytössä isäntäkoneen eli palvelimen fyysiset osat kokonaisuudessaan, vaikka todellisuudessa hypervisor hallitsee ja jakaa isäntäkoneen resursseja määriteltyjen tehojen mukaan virtuaalikoneille. Fyysisten prosessorien sijaan ohjelmisto turvautuu näyttämään virtuaalisia esityksiä komponenteista, eli virtuaalikoneet käyttävät esimerkiksi niin sanottuja virtuaaliprosessoreita (vCPU). (Rouse 2015a.)

Virtualisoidut tietokoneresurssit jaetaan yksittäisiin instansseihin, eli virtuaalikoneisiin, joihin voidaan asentaa käyttöjärjestelmiä ja sovelluksia, kunhan käytetty arkkitehtuuri tukee niitä. Jokainen virtuaalikone toimii eristetyissä instansseissa, jolloin yksittäisen virtuaalikoneen ongelmat eivät vaikuta toisiin virtuaalikoneisiin. Yksi palvelin voi toimia isäntäkoneena usealle eri virtuaalikoneelle, jolloin fyysisien resurssien

käyttö on kustannustehokkaampaa suurella käyttöasteella. Virtuaalikoneisiin asennettava käyttöjärjestelmäkin voi erota isäntäkoneen vastaavasta, mikä johtaa siihen, että saadaan enemmän aikaan pienemmällä komponenttimäärällä. (Rouse 2015a.)

Hypervisor voidaan jakaa kahteen ryhmään riippuen sen sijainnista palvelinvirtualisoinnin toimintamallissa. Type 1 -luokan hypervisor, eli ”bare-metal”-hypervisor asennetaan suoraan fyysisen tason päälle ilman varsinaista käyttöjärjestelmää, jolloin hypervisor pystyy hallitsemaan vieraskäyttöjärjestelmiä käyttäen vähemmän resursseja. Vieraskäyttöjärjestelmät toimivat prosesseina taustalla. Tällä tavalla hyötysuhde on parempi, saadaan aikaan parempi suorituskyky ajettaville virtuaalikoneille ja sen laajennettavuus paranee, sillä hypervisorilla on suora pääsy laitteiston fyysisiin resursseihin. Type 2 -luokan hypervisor, eli ”hosted architecture” voidaan asentaa jo olemassa olevan ja asennetun käyttöjärjestelmän päälle ja siten hypervisor tukee suurta määrää olemassaolevia fyysisen tason kokoonpanoja, mutta tämän tyypin hypervisor kuluttaa samalla enemmän resursseja. (VMware 2016b.)

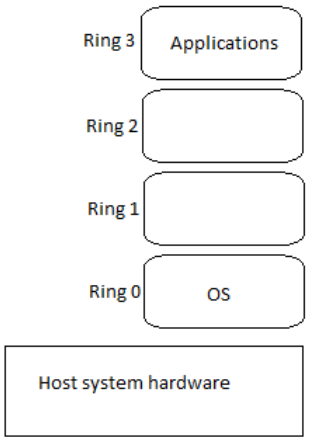


KUVIO 2. 1-tason hypervisorin sijoittuminen täysvirtualisoituun palvelinmalliin

Kuviossa 2 on visualisoitu täysvirtualisoidun palvelimen toimintamalli, jossa fyysisen tason päälle on asennettu suoraan tyypin 1 hypervisor.

Hypervisor hallitsee ja jakaa kolmelle eri virtuaalikoneelle resursseja isäntäkoneen prosessorista, keskusmuistista, verkkokorteista ja massamuistista riippuen tarvittavasta ja valitusta määrästä. Virtuaalikoneet sisältävät jonkin tietyn vieraskäyttöjärjestelmän, jonka päälle halutut palvelut on rakennettu. Tässä esimerkkitapauksessa virtuaalikoneille on asennettu sähköpostipalvelin, nimipalvelin ja WSUS-palvelin. (VMware 2016b.)

Hypervisor kehiteltiin, jotta laitteistovirtualisointi olisi mahdollista x86-arkkitehtuurin käyttöjärjestelmissä. X86-arkkitehtuuria hyödyntävät käyttöjärjestelmät on suunniteltu käytettäväksi suoraan fyysisen tason päällä ja käyttöjärjestelmät olettavat kaikkien fyysisen tason komponenttien olevan täysin käyttöjärjestelmän käytettävissä. X86-arkkitehtuuri koostuu neljästä eri oikeustasosta, jotka tunnetaan nimillä Ring 0,1,2 ja 3. Nämä tasot hallitsevat pääsyä käyttämään fyysisiä tietokoneosia. Käyttöjärjestelmä vaatii suoraa kontaktia muistiin ja muihin komponentteihin, joten sen käskyt tulee suorittaa Ring 0 -tasolla. Käyttäjän ohjelmistot sijaitsevat yleensä Ring 3 -tasolla. Kuviossa 3 on kuvailtu x86-arkkitehtuurin oikeustasojen hierarkia ennen virtualisointia. Virtualisointikerroksen, eli hypervisorin sijoittaminen käyttöjärjestelmän alapuolelle tässä hierarkiassa oli edellytyksenä virtualisoinnin mahdollistamiselle. Tämän aikaansaamiseksi on kehitelty eri menetelmiä, joilla palvelinvirtualisointi voidaan suorittaa. (VMware 2016b.)



KUVIO 3. x86-arkkitehtuurin oikeustasojen hierarkia ennen virtualisointia

3.3.2 Palvelinvirtualisoinnin toteutusmenetelmät

Palvelinvirtualisointia voidaan harjoittaa neljällä eri menetelmällä: täysvirtualisoinnilla, paravirtualisoinnilla, laitteistoavusteisella virtualisoinnilla tai käyttöjärjestelmätason virtualisoinnilla. Nämä menetelmät jakavat toistensa kanssa yhteisiä piirteitä termien suhteen, mutta teknologiat, joilla virtualisointi toteutetaan käytännössä, eroavat toisistaan. (VMware 2016b.)

Täysvirtualisoinnissa vieraskäyttöjärjestelmä on täysin eristetty fyysisestä tasosta virtualisointikerroksen avulla. Vieraskäyttöjärjestelmä ei siis ole tietoinen virtualisoimisesta, vaan vieraskäyttöjärjestelmä olettaa olevansa suoraan tekemisissä palvelinlaitteiston kanssa ja täten vieraskäyttöjärjestelmä ei vaadi ylimääräistä muokkaamista yhteensopivuuden takaamiseksi, kunhan ne ovat samalle laitteistoarkkitehtuurille suunniteltuja. (VMware 2016b.)

Täysvirtualisointi on ainoa palvelinvirtualisoinnin menetelmä, joka ei vaadi laitteistolta tai käyttöjärjestelmältä avustusta eri komentojen virtualisoimiseen. Hypervisor kääntää kaikki käyttöjärjestelmätason komennot lennossa ja siirtää useasti käytetyn tiedon välimuistiin ja tarjoaa samalla käyttäjätason käskyille normaalitason nopeuden. Täysvirtualisoinnin hyötyinä voidaan mainita parempi tietoturva täysin eristettyjen virtuaalikoneintanssien myötä ja helposti skaalautuva virtuaalikoneympäristö, joka voidaan yksinkertaisilla toimenpiteillä siirtää tarvittaessa toiseen järjestelmään. Esimerkkinä täysvirtualisointia käyttävästä alustasta on VMwaren virtualisointituotteet sekä Microsoft Hyper-V. (VMware 2016b.)

Paravirtualisointi on vaihtoehtoinen lähestymistapa, jossa koko tietokonejärjestelmän emuloimisen sijaan käytetään hallintaohjelmistoa tai hypervisoria, joka tekee yhteistyötä virtuaalikonekäyttöön muokatun käyttöjärjestelmän kanssa. Paravirtualisointiarkkitehtuuri voidaan kuvailla seuraavasti: ”bare-metal”-hypervisorin päälle asennetaan suoraan vieraskäyttöjärjestelmä. Hypervisor ei itsessään sisällä laitteistoajureita,

vaan sen sijaan hypervisor sisältää vieraskoneen ”Domain0”, joka ajetaan vierasoikeuksilla sisältäen suorat oikeudet palvelinosien resursseihin. Muut vieraskäyttöjärjestelmät pääsevät käsiksi samoihin resursseihin Domain0:n kautta. Domain0 on käytännössä normaali käyttöjärjestelmä, kuten Red Hat Enterprise Linux, joka on muokattu koordinoimaan resurssienhallintaa hypervisorin kanssa. (Golden 2007.)

Paravirtualisaatiolla saavutetaan tehokkaampi virtualisointijärjestelmä, joka on kustannustehokkuudeltaan ja skaalautuvuudeltaan parempi vaihtoehto kuin laitteistoa emuloivat virtualisointimenetelmät. Heikkoutena paravirtualisoinnissa on joustavuus käyttöjärjestelmien suhteen, sillä se vaatii monimutkaisia käyttöjärjestelmän kernelitasoon tehtäviä muutoksia, jotta se on yhteensopiva paravirtualisoidun ympäristön kanssa. (VMware 2016b.)

Kolmas menetelmä on laitteistoavusteinen virtualisointi. 2000-luvun puolivälin tienoilla AMD ja Intel alkoivat kehittää virtualisointituen sisältäviä prosessorimalleja markkinoille. Käytännössä tämä tarkoittaa x86-oikeustasojen hierarkiassa sitä, että virtualisointituen sisältävillä prosessorien uudella CPU suorituskäytännöllä hypervisoria pystytään ajamaan root-tasolla ring 0 -tason alapuolella. Laitteistoavusteisessa virtualisoinnissa ei siis tarvita täysvirtualisoinnissa käytettäviä paravirtualisointimetodeja tai binäärimuunnoksia siirrettäessä käskyjä vieraskäyttöjärjestelmätasolta hypervisorille ja laitteistolle. (VMware 2016b.)

Laitteistoavusteisesta virtualisoinnista on seurannut useita eri hyötyjä yrityksillä, jotka ovat olleet kiinnostuneet virtualisoinnin toteuttamisesta ympäristössään. AMD-V tai Intel VT-x -virtualisointituen sisältämät mikropiirit ovat tehneet virtualisoimisprosessista sulavamman verrattuna aikaisempiin toteutustapoihin, sillä laitteisto on jälleen hallinnassa resurssien jakamisesta eri virtuaalikoneille pelkän ohjelmistopohjaisen mallin sijaan. (Rouse 2015a.)

Intelin ja AMD:n valmistavat laitteistoavusteista virtualisointia tukevat prosessorimallit ovat myös suoraan x64-arkkitehtuurille yhteensopivia, joten tämän teknologian käyttäminen saattaa mahdollistaa yritykselle siirtymisen nykyaikaisempaan arkkitehtuuriin. Esimerkkinä voidaan mainita Microsoftin Hyper-V-palvelinvirtualisointiteknologia, joka vaatii 64-bittisen yhteensopivuuden laitteistolta toimiakseen. Laitteistoavusteinen virtualisointi on nopeampaa ja vähemmän laitteistoresursseja vaativaa kuin ohjelmistopohjainen virtualisointi. Tämä virtualisointimenetelmä antaa myös käyttäjälleen paremman mahdollisuuden vaihtaa virtualisointiohjelmistosta tai alustasta toiseen niin halutessaan. (Rouse 2015a.)

Käyttöjärjestelmätason virtualisointi on palvelinvirtualisoinnin menetelmä, jolla tarkoitetaan useamman samalla käyttöjärjestelmällä varustetun virtuaali-instanssin yhtäaikaista käyttöä. Nämä eristetyt instanssit mahdollistavat laitteiston paremman hyödyntämisen, sillä vain yksi käyttöjärjestelmä vastaa fyysisten komponenttien resurssikäskyistä. Samalla se toimii rajoittavana tekijänä ympäristöissä, joissa tarvitaan eri käyttöjärjestelmien virtualisointia. (Rouse 2014.)

3.4 Virtualisoinnin hyödyt

Virtualisointi tuo mukanaan useita eri hyötyjä, joista ensimmäinen on palvelinlaitteiston käyttöasteen parempi hyödyntäminen. Nykyajan palvelinkeskusten fyysisten palvelimien laitteistoresursseista ei käytetä kuin 10 – 15 % ohjelmistojen ja palveluiden tuottamiseen. Suurin osa resursseista jää käyttämättä ympäristössä, jossa virtualisointia ei ole otettu käyttöön. Mahdollistamalla usean käyttöjärjestelmän samanaikaisen ajon yhdellä laitteistolla saadaan laitteiston käyttöaste nostettua 70 – 80 %:n välille. Tämä johtaa kustannustehokkaampaan palvelinkeskukseen, jossa samoilla fyysisillä resursseilla saadaan moninkertaisesti enemmän aikaiseksi. (Golden 2007.)

Internetin eksponentiaalinen yleistyminen 1990-luvulta lähtien sai aikaan liiketoimintaa harjoittavien yritysten siirtymisen paperiajasta

tietokoneistettuihin ympäristöihin. Nykyään yritykset haluavat pystyä suoraan kommunikointiin yhteistyökumppanien sekä asiakkaiden kanssa ja sitä pidetäänkin norminmukaisena käytäntönä. Tietokoneistuminen yritysmaailmassa on johtanut palvelimien määrän räjähtävään kasvuun, jolloin fyysisen laitteiston tarvitsemasta tilasta on ollut pulaa. Tilan-puutteen lisäksi järjestelmän hallitsemisesta on tullut hankalampaa ja kalliimpaa suuren laitemäärän vuoksi. Laitteiston määrän noustessa kasvaa myös energiantarve, jolloin palvelinkeskusten ylläpitämiseen vaadittavat rahamäärät ovat kasvaneet suurentuneen sähkönkulutuksen ja sähkön hinnan noustessa. Virtualisointi voi korvata osan fyysisestä ympäristöstä saaden aikaan enemmän säästöjä, ja samalla sähkönkulutus, tilan tarve, ylläpitokustannukset sekä jäähdytyksen tarve pienenevät. (Golden 2007.)

Skaalautuvuus, siirrettävyys, vikasietoisuus ja tietoturva ovat palvelinympäristöjä käyttäville yrityksille tärkeitä käsitteitä ja virtualisointi mahdollistaa niiden paremmin aikaansaamisen IT-infrastruktuurissa. Virtuaalikoneille voidaan määrittää enemmän resursseja, mikäli huomataan sen tarvitsevan alkuperäistä määrää suurempia tehoja, muistia tai kovalevytilaa. Virtuaalikoneiden nopea ja helppo luominen sekä hallitseminen mahdollistavat järjestelmänhallitsijan tuottamaan palveluita suuremmalle ihmismäärälle tarpeen mukaan. (Steele 2010.)

Palvelinympäristön siirrettävyys kasvaa huomattavasti asetusten ja palveluiden sijaitessa virtuaalikoneen vieraskäyttöjärjestelmässä, josta voidaan tehdä malli (template) ja siirtää se isäntäkoneelta toiselle. Osa virtualisointiohjelmistoista mahdollistaa myös niin sanotun live migration -ominaisuuden, jolla virtuaalikone voidaan siirtää fyysisten isäntäkoneiden välillä ilman toteutettujen palveluiden käytettävyyden katkeamista. (Steele 2010.)

Palveluiden vikasietoisuus saadaan aikaiseksi hyödyntämällä High Availabilitya (HA) tai sitä vastaavaa teknologiaa, joka voidaan konfiguroida tietyille virtuaalikoneille käytettäväksi. Esimerkkinä voidaan käyttää VMwaren High Availabilitya. Käytännössä tämä HA käynnistää

virtuaalikoneen toiselle fyysiselle palvelimelle, mikäli järjestelmä huomaa ensisijaiseksi isäntäkoneeksi määritellyn palvelimen vikaantumisen. Jos virtuaalikoneen käyttöjärjestelmä vikaantuu, niin HA-teknologia osaa uudelleenkäynnistää sen samalle fyysiselle palvelimelle. (VMware 2009.)

Yksittäisten palveluiden tietoturva on parempi virtualisoidussa ympäristössä eristettyjen instanssien vuoksi. Samalla fyysisellä palvelimella sijaitseva saastunut virtuaalikone ei vaikuta muilla virtuaalikoneilla toimiviin palveluihin. Mahdollisesti saastunut tai vikaantunut virtuaalikone voidaan palauttaa aiempaan versioon snapshot-teknologialla. Snapshot tallentaa sillä hetkellä virtuaalikoneeseen tehdyt asetukset, muistin ja massamuistin sisällön ja tekee kyseisestä tilanteesta kopion, joka voidaan tarvittaessa palauttaa eli ottaa uudelleen käyttöön. (Bigelow 2010.)

3.5 Virtualisointiohjelmistot

Vuonna 2015 lähes 75 % x86-arkkitehtuurin palvelimien työmäärästä on virtualisoitua, kun yritykset ovat etsineet ratkaisuja edellä mainittuihin teknologisiin haasteisiin ja sitä kautta saavuttaneet monia virtualisoinnin kautta saatuja hyötyjä. Gartner on tehnyt vertailun virtualisointiteknologioita myyvistä yrityksistä ja niiden tuotteista ottaen huomioon tuotteiden etevyyden suorittaa tarvittavia toimenpiteitä sekä kokonaiskuvan tekniikoiden tulevaisuudennäkemyksestä. Tästä vertailusta nähdään virtualisoinnin markkinoita johtavan VMwaren, jonka perässä tulee vahvasti Microsoftin Hyper-V-tuote. Muiden yrityksien tarjoamat virtualisointiratkaisut täyttävät joitakin tiettyjä markkinarakoja, mutta niiden markkinaosuus ja ominaisuudet eivät ole yhtä merkittäviä verrattuna johtavassa asemassa oleviin vaihtoehtoihin. (Gartner 2015.)

KUVIO 4. Gartnerin markkinatutkimus virtualisointiohjelmistoista (Gartner 2015.)

Microsoftin Hyper-V on x-86-64-arkkitehtuurille suunniteltu 1-tyypin hypervisor, joka mahdollistaa virtuaalikoneiden luomisen ja hallitsemisen. Hyper-V on alun perin julkaistu Windows Server 2008 -käyttöjärjestelmän mukana, minkä jälkeen se on ollut mukana kaikissa uudemmissa palvelinkäyttöön tarkoitetuissa käyttöjärjestelmissä sekä useissa Windows-versioissa asennettavana roolina ilman erillistä maksua. (Microsoft 2015.)

Windowsin mukana tulleissa Hyper-V clienteissä ei tosin ole mukana kaikkia ominaisuuksia, jota palvelinkäyttöön tarkoitettu versio sisältää, kuten live migration-tekniikkaa tai jaettuja virtuaalikovalevyjä. Hyper-V clientin muistin käyttöä hallitseva malli on erilainen, sillä näillä isäntäkoneilla arvellaan käytettävän muitakin sovelluksia virtuaalikoneiden hallitsemisen lisäksi. Hyper V:n sisällyttäminen moneen käyttöjärjestelmään on osaltaan auttanut Microsoftia aikaisempaa suuremman markkinaosuuden ja antanut paremman mahdollisuuden kilpailla VMwaren kanssa. (Microsoft 2015.)

Hyper-V-virtualisointiohjelmisto on varsinaisesti 1-tyypin hypervisor, vaikka hypervisorin asennusta varten tarvitaankin toimivan Windowsin käyttöjärjestelmän olemassaoloa. Tämä selittyy sillä, että Hyper-V-roolia asennetaan ikään kuin tämän käyttöjärjestelmän alle, jolloin hypervisor valvoo sitäkin, eli isäntäkoneen käyttöjärjestelmän voi kuvitella virtuaalikonemaiseksi käyttöjärjestelmäksi tässä hierarkiassa. (Microsoft 2015.)

Hyper-V:n Windows Server 2012 R2- version tärkeimpiin ominaisuuksiin kuuluu virtuaalikoneiden lisenssien automaattinen aktivointi, virtuaalikoneiden tiedonvarmistus, snapshotit, dynaaminen muisti, virtuaalikonepakettien migraatio virtuaaliympäristöstä pois ja sisään sekä live migration -ominaisuus. Näiden ominaisuuksien hyödyntämiseen ja Hyper-V:n toimintaan vaaditaan x64-arkkitehtuuria tukeva prosessori, laitteistoavusteisen virtualisoinnin tuki sekä vähintään 4 GB keskusmuistia. (Microsoft 2015.)

VMware on palvelinvirtualisoinnin edelläkävijä. 1990-luvun lopulla yritys oli ensimmäinen, joka onnistui kehittämään toimivan täysvirtualisoidun ratkaisun x86-arkkitehtuurille. Yritys tarjoaa virtualisointiratkaisuja työpöytämuodossa VMware Workstation -ohjelmistolla sekä yritysluokan 1-tyypin hypervisoreita palvelimille (vSphere), joista erityisesti vSphere on Hyper-V:n suurin kilpailija. Tämä ratkaisu eroaa muista kilpailijoistaan sillä, että sen mukana tai sitä hyödyntääkseen ei tule erillistä käyttöjärjestelmää vaan hypervisor asennetaan suoraan fyysisen tason päälle, minkä jälkeen sitä voidaan käyttää etähallintatyökalun kautta. (VMware 2016c.)

vSpheren perusversio (ESXi) on ilmaiseksi ladattavissa, mutta tämä versio ei sisällä kaikkia ominaisuuksia kuten keskitettyyn hallintaan liittyviä työkaluja. Näiden ominaisuuksien käyttöön ottamista varten tarvitsee hankkia VMwarelta maksullinen lisenssi. Muihin tärkeisiin ominaisuuksiin kuuluu muun muassa high availability, vMotion (live migration-ominaisuus), datan suojaus, vikasietoisuus ja vShield Endpoint-tietoturva tekniikka. (VMware 2016c.)

Vaihtoehtoisista virtualisointiratkaisuista voidaan mainita Citrixin XenServer, joka on avoimeen lähdekoodiin perustuva täysin ilmainen 1-tyypin hypervisor. Citrix tarjoaa maksua vastaan XenServerille tuki- ja hallintapalvelua, mutta kaikki toiminallisuus on maksutonta. XenServer ei ole ominaisuuksiltaan yhtä monipuolinen kuin kilpailijansa, ja sen hallintatyökalut sekä päivitysten jakaminen eivät ole yhtä helppokäyttöisiä kuin vastaavissa tuotteissa. Linuxiin pohjautuvana hypervisorina sen käyttäminen ympäristöissä, joita Microsoftin käyttöjärjestelmät ja ohjelmistotuotteet hallitsevat, tekee siitä hankalamman toteuttaa. (Siebert 2016.)

4 PALVELINYMPÄRISTÖ PIENYRITYKSESSÄ

4.1 Pienyrityksen palvelinympäristön rakenne

Palvelinympäristön optimaalinen rakenne riippuu halutuista palveluista, asiakasryhmän koosta ja yrityksen toimialasta sekä henkilöstömäärästä. Yhden tai muutaman henkilön yrityksessä harvemmin tarvitsee omaa fyysistä palvelinta tarjoamaan työntekijöille verkkoympäristöä ja erilaisia sisäisiä palveluita, jollei tämä liity olennaisesti firman toimenkuvaan tai liiketoiminnan kasvuun. (Brown 2012.)

Näitä palvelimien tarjoamia ominaisuuksia ja palveluita voidaan vaihtoehtoisesti ostaa suoraan alan yrityksiltä palvelintilana, palveluna tai pilvipalveluna. Astetta kookkaampien organisaatioiden kannattaakin jo harkita omien palveluiden ylläpitoa ja siihen sijoittamista. Tällöin on tärkeää ymmärtää eri järjestelmien ja sovelluksien toimintaperiaatteet ja vaikutukset kokonaisympäristöön. (Brown 2012.)

4.2 DNS

Domain Name System (DNS) on tärkeä osa tapaa, jolla laitteet kommunikoivat toistensa kanssa TCP/IP-protokollan yli tietoliikenneverkoissa, kuten Internetissä tai yksityisissä intraneteissa. Tämän dynaamisen nimipalvelujärjestelmän tarkoituksena on yhdistää helposti muistettavat verkkotunnukset numeerisiin IP-osoitteisiin, joilla liikennöinti varsinaisesti tapahtuu. Liikennöinti ilman nimipalvelun toteuttamista olisi käytännössä hyvin haasteellista, sillä yksinkertaisia tehtäviä vartenkin tulisi muistaa ulkoa numeeriset osoitteet jokaiselle laitteelle, johon käyttäjä haluaa olla yhteydessä. Esimerkiksi palveluiden siirtäminen fyysiseltä alustalta toiselle vaihtaisi myös www-palvelun osoitetta. (Microsoft 2008.)

Yrityksen verkkoympäristöissä nimipalvelun tuottaminen hoidetaan DNS-palvelimella, jonka toteuttaminen kulkee tiiviisti liitettynä toimialueen käyttäjätietokannan ja hakemistopalvelun (Active Directory) kanssa. Active

Directoryn (AD) toiminta on riippuvainen verkossa sijaitsevasta oikein konfiguroidusta nimipalvelujärjestelmästä, joten useasti nämä palvelut toteutetaan samaan virtualisoituun instanssiin. Yleisen mallin mukaan palveluita halutaan ylläpitää erillisillä virtuaalikoneilla, sillä virtuaalisten instanssien eristäminen auttaa osoittamaan ongelman lähteen vianratkontatapauksissa. Vaikka nimipalvelujärjestelmän ja Active Directorya toimivuuden kannalta ei ole vaatimusta integroida niitä samaan järjestelmään, niin integroiminen helpottaa verkkoympäristön konfiguroimista, sillä kyseiset järjestelmät kommunikoivat toistensa kanssa aktiivisesti. Integroimisella saavutetaan hyötyjä verkkoliikenteen tarvitseman kaistan vähentymisellä sekä mahdollisuudella säilöä domainin nimitietoja suoraan Active Directoryyn (Active Directory-Integrated Zones, ADI). (Microsoft 2014a.)

DNS query eli nimikysely lähtee liikkeelle, kun käyttäjä syöttää sovellukseen kuten selaimeen jonkin verkkotunnuksen. Tietyt sovellukset sisältävät oman välimuistinsa, johon ne keräävät aiempiin kyselyihin saatuja vastauksia. Jos vastausta ei ole saatavilla sovelluksen omasta välimuistista, on seuraava kyselyn paikka DNS client (resolver), joka etsii järjestelmän tietyistä staattisista tiedostoista vastausta kyselylle ja ohjaa kyselyn eteenpäin järjestelmän osoittamalle nimipalvelimille, mikäli sitä ei löydy. Varsinaiset nimipalvelimet voidaan jakaa rekursiivisiin nimipalvelimiin sekä autoritäärisiin nimipalvelimiin. (Cisco 2016b.)

Rekursiivisen nimipalvelimen saadessa kyselyn tietyn osoitteen sijainnista, nimipalvelin järjestelmällisesti lähettää pyyntöjä juurinimipalvelimille. Juurinimipalvelimet ovat Internetin ylimmän tason nimipalvelimia, jotka sisältävät tiedot seuraavan tason palvelinten osoitteista (top level domain). Rekursiivisen nimipalvelimen lähettäessä kyselyn www.esimerkki.fi-verkkosivun osoitteesta juurinimipalvelimelle, vastaa se .fi-aluetta hallitsevan nimipalvelimen osoitteella, jota kautta saadaan aina astetta tarkempi vastaus ja lopulta pyydetyn sivun osoite. Rekursiivisella nimipalvelimella saattaa olla tieto osoitteesta välimuistissa, jolloin se lähettää vastausviestissä suoraan tietämänsä osoitteen resolverille. (Cisco 2016b.)

Autoritäärinen nimipalvelin huolehtii vain sen hallinnassa olevien alueiden kyselyistä. Palvelin pystyy vastaamaan suoraan kyseisen autoritäärisen nimipalvelimen vastuussa olevien alueiden nimipalvelukyselyihin aikaansaaden nopeampia vastausaikoja. Mikäli palvelimen tiedossa ei ole vastausta saatuun kyselyyn, niin palvelin delegoi tämän tehtävän toiselle palvelimelle, johon resolverille lähetetyssä vastausviestissä viitataan. (Cisco 2016b.)

4.3 Domain controller

Domain controller on palvelimelle ohjelmiston kautta määriteltävä rooli, joka mahdollistaa sisäverkon resurssien, kuten käyttäjätilien ja tietokoneiden keskitetyn hallinnan. Domain controllerin kautta onnistuu käyttäjätilien autentikointi, käyttäjien siirtäminen eri ryhmiin ja niiden perusteella oikeuksien ja eri käytäntöjen määrittäminen. Käyttäjällä on oikeus ennaltamääriteltyihin toimialueen tarjoamiin resursseihin yhtä tiliä käyttämällä laitteesta riippumatta. Suosituin tapa toteuttaa domain controller on Microsoftin Active Directory Windows -käyttöjärjestelmiä sisältävässä ympäristössä. Vaihtoehtoisesti voidaan käyttää Sambaa, joka on avoimen lähdekoodin Linuxiin perustuva ohjelmistoratkaisu. Sambaa ja Active Directorya yhdistää saman verkkoprotokollan (LDAP) hyödyntäminen autentikoimiseen ja käyttöoikeuksien tarkastamista varten, ja tämän kautta ne pystyvät myös kommunikoimaan keskenään. (Rouse 2005a.)

Halutun domain controllereiden määrän päättäminen riippuu yrityksen toimialueen verkon fyysisestä topologiasta. Pienemmät yritykset, joilla on yksi fyysinen sijainti pienehköllä verkkototeutuksella ja laitemäärällä, voivat pärjätä yhdellä domainilla ja siihen liitetyllä kahdella domain controllerilla. Nämä kaksi erillistä domain controlleria mahdollistavat pääasiallisen kontrollerin tietokantojen kopioimisen toissijaiselle domain controllerille saaden aikaan vikasietoisemman autentikointipalvelun. Active Directoryssa tämä on toteutettu replikoinnilla. Domain controllerin

vikaantuessa koko toimialueen palveluiden käyttäminen keskeytyisi ilman vikasietoisuutta. (Microsoft 2016a.)

Active Directory on Microsoftin tarjoama hakemistopalvelu ja käyttäjätietokanta, joka on tarkoitettu Windows-toimialueen resurssien keskitettyä jakamista ja hallitsemista varten. Ohjelmisto on sisältynyt erillisenä asennettavana roolina Microsoftin valmistamiin palvelimille tarkoitettuihin käyttöjärjestelmiin Windows 2000 Server -versiosta lähtien. Active Directoryn toimialueiden hallinta on rajoitettu vain Windows-alustalla toimiviin koneisiin. (Microsoft 2016a.)

Active Directoryn toiminta voidaan jakaa eri loogisiin tasoihin, jotka ovat forest, domain tree, domain ja Organizational Unit (OU). Forest on ylin looginen taso ja forest sisältää kaiken, mitä yksi kokonainen Active Directory instanssi pitää sisällään. Active Directoryn sisältämä tieto jaetaan forestin sisällä, jolloin forest toimii yhden instanssin rajana, jonka sisällä pysyy turvattu tieto. Domain tree on kokoelma toimialueita, joita yhdistää hierarkkinen rakenne. Kun puuhun lisätään toimialue, tulee siitä child domain kyseiselle tree root domainille. Child domainin nimi yhdistetään parent domainin nimeen, jolloin sille muodostuu oma uniikki DNS-nimi. Toimialueet ovat kasa hallinnollisesti yhdistettyjä objekteja, jotka jakavat hakemiston yleisen tietokannan ja tietoturvakäytännöt. Organizational Unit (OU) on järjestelmän ylläpitäjiä varten luotu ryhmä, joka auttaa järjestelemään objekteja, kuten käyttäjiä, eri tasoille. Tämä helpottaa objektien löytämistä ja hallinnointia. (Microsoft 2016a.)

Active Directory on toimialueen ylläpitäjien tärkein työkalu, sillä se toimii runkona, jonka sisältämiä palveluita ja informaatiota muut verkon palvelut käyttävät hyödykseen. AD mahdollistaa toimialueeseen liitettyjen laitteiden, käyttäjien ja käyttäjätilien tarkan tietojen tarkastelemisen ja hallinnan helposti käsiteltävässä formaatissa. Jokaiselle käyttäjälle voidaan luoda oma käyttäjätili, liittää se haluttuun käyttäjäryhmään ja määrittää tälle ryhmälle haluttu määrä oikeuksia ja rajoituksia verkon resurssien käytöstä. Tällä tavoin voidaan rajoittaa oikeuksia suorittaa esimerkiksi asennus- ja päivitystoimenpiteitä laitteistolla sijaitseville

ohjelmistoille yleisessä käytössä oleville tunnuksille ja samalla antaa oikeudet kyseisiin toimenpiteisiin työntekijöiden tunnuksille. Kaikki verkon objektit saadaan näkyville hierarkisessa luettelossa, jota voidaan käyttää apuna määritellessä muille verkon palveluille vaadittavat oikeudet. (Microsoft 2016a.)

Vikasietoisuus voidaan toteuttaa replikoinnilla, jossa jokainen forestin sisällä toimiva domain controller synkronoi tietokantansa muiden domain controllereiden kanssa, jotka kopioivat tehdyt muutokset muistiinsa. Tätä prosessia kutsutaan nimellä multi-master replication, joka tapahtuu hallitusti järjestelmän päättämällä systemaattisella tavalla, joka takaa tiedon varmistamisen. Toinen palvelin voidaan määrittää asennuksen yhteydessä toissijaiseksi Active Directory -palvelimeksi, joka toimii palvelun jatkuvan toteuttamisen varmistuskeinona. (Microsoft 2016a.)

4.4 Tiedostopalvelin

Tiedostopalvelin on yrityksen tiedostojen yhteinen tallennuspaikka, jolloin tallennettua dataa päästään keskitetysti tarkastelemaan, siirtämään ja hallitsemaan laitteiden ja käyttäjien välillä. Tiedostopalvelin mahdollistaa tiedostojen siirtämisen ilman fyysistä datansiirtoa ulkoisella medialla. Yksinkertaisimmillaan tiedostopalvelin voi olla tietokone, joka on määritetty jakamaan tallennuskapasiteettia verkon ylitse. Yritysmaailmassa tämä ratkaisu ei välttämättä ole tietoturvaltaan, kapasiteetiltaan ja halutuilta ominaisuuksiltaan paras mahdollinen. Tällöin ratkaisuna voidaan käyttää esimerkiksi NAS- tai SAN-järjestelmiä. (Rouse 2005b.)

Network attached storage (NAS) on tallennusjärjestelmä, jonka kautta on mahdollista tallentaa, jakaa ja siirtää dataa tietoverkon ylitse. Perinteisten suoraan tietokoneeseen tai palvelimeen kiinnitettävien direct-attached storagen (DAS) sijaan NAS on kytketty verkkoon omalla IP-osoitteella, jolloin sen käyttäminen etänä on mahdollista. NAS sisältää joko yleisesti käytetyn käyttöjärjestelmän, kuten Microsoft Windowsin, laitevalmistajan omistaman käyttöjärjestelmän tai nimenomaan tiedostonsiirto-ominaisuuksiltaan optimoidun muokatun käyttöjärjestelmän. FreeNAS on

esimerkki tiedostopalvelimen käyttöjärjestelmäksi muokatusta Unix-käyttöjärjestelmästä, jonka tiedostonjakoon liittyviä ominaisuuksia on paranneltu. Fyysisiltä osiltaan tämä menetelmä sisältää vähintään yhden kovalevyn, mutta useamman kovalevyn hyödyntäminen mahdollistaa RAID-teknologian hyödyntämisen paremman tiedon varmistusasteen takaamiseksi. NAS-järjestelmä mahdollistaa verkkoon liitetyn Windows-koneiden tiedostonjaon CIFS-protokollalla ja Linux- tai Unix-pohjaista käyttöjärjestelmän sisältävän koneen tiedostonjaon NFS-protokollaa käyttämällä. (Rouse 2015b.)

SAN (Storage area network) on tiedostojen tallennusverkko, joka keskittää erilliset massamuistilaitteet jaettuun yhteiseen käyttöön. SAN on hyvä vaihtoehto yrityksille, jotka siirtävät suurta määrää dataa useasti. Tallennusmedian siirtäminen omaan itsenäiseen verkkoon mahdollistaa jaetun tallennuskapasiteetin näkymisen palvelimille ikään kuin tallennusmedia olisi osa palvelimen paikallista tallennuskapasiteettia, jolloin vapaata tilaa voi käyttää helpommin useilta eri palvelimilta. RAID-teknologian hyödyntäminen on mahdollista ja oletuskäytäntö myös SAN-toteutuksessa. (Rouse 2015b.)

4.5 Ohjelmistojen ja päivitysten keskitetty hallinta

Toimialueen laitteiden ohjelmistojen päivitysten keskitetty asentaminen ja jakelu ovat tärkeä osa domainin järjestelmänhallitsijan työtehtäviä. Active Directoryn antaessa työkalut toimialueen käyttäjien ja laitteiden hallinnointiin tarvitaan erillinen ohjelmisto, jolla voidaan kontrolloida käyttöjärjestelmän ja ohjelmistojen päivityksiä. Päivitysten keskitetty hallinta auttaa ylläpitämään palveluita aina yhtä tehokkaina ja vakaina kokonaisuuksina sekä vähentää järjestelmän heikkouksia tietoturvan näkökulmasta. Pitämällä ohjelmistot päivitettynä uusimpaan suositeltuun versioon vähennetään yrityksen ympäristöön kohdistuvia uhkia. (Microsoft 2016a.)

Windows Server Update Services -ohjelmisto (WSUS) antaa mahdollisuuden Microsoft-tuotteiden keskitettyyn päivitysten jakamiseen

yritysympäristössä. WSUS on nimenomaan Microsoftin tuotteiden päivitysten hallintaa ja automatisointia varten luotu ohjelmisto. Ylläpitäjät voivat automatisoida tietyn tasoisia järjestelmän päivityksiä ja hyödyntää AD:n ryhmäsääntöjä varmistaakseen päivitysten asentamisen käyttäjien tietokoneille. (Microsoft 2014c.)

Eräs ominaisuuksiltaan laajempi vaihtoehto on Miradore Management Suite, jolla voi hallita eri ohjelmistojen päivityksiä ja asennuksia. Management Suite sisältää monia muita ominaisuuksia päivitysten hallinnan lisäksi, joita palvelinympäristön ylläpitäjä voi käyttää saadakseen paremman kuvan ympäristön sisältämistä laitteista ja ohjelmistoista. Näitä ominaisuuksia ovat muun muassa yksityiskohtainen listaus toimialueen käyttäjien ohjelmistoista ja laitteista sekä niiden statuksesta, käyttöjärjestelmien ja sovellusten automatisoitu etäasennus, asennuspakettien rakentaminen sekä endpoint backup. Management Suite ei myöskään ole rajoitettu vain Windows-tuoteperheen hallintaan, vaan se tukee myös Linux- tai OSX-pohjaista käyttöjärjestelmää hyödyntäviä ympäristöjä. (Miradore 2016.)

Tietoturvan keskitettyyn hallintaan löytyy myös omia sovelluksia, kuten F-secure-tuoteperheen käsittelyä varten kehitetty F-secure policy manager -ohjelmisto. Policy manager tarjoaa usean eri käyttöjärjestelmällä toimivien sovelluksien tietoturvahallinnan yhdestä paikasta. Sillä voi määrittää ja jakaa tietoturvakäytäntöjä, asentaa ohjelmistoa toisessa lokaatiossa sijaitsevaan järjestelmän ja varmistaa käytäntöjen toteutumisen monitoroimalla järjestelmiä. (F-Secure 2016.)

4.6 Sähköpostipalvelin

Sähköpostipalvelun valitseminen on yrityksen sisäistä toimintaa ja kommunikaatiota ajatellen yksi keskeisistä tekijöistä. Pienemmät yritykset saattavat harkita ulkopuoliselta taholta ostettua sähköpostipalvelua, kun taas isommat organisaatiot voivat hyötyä enemmän oman sähköpostipalvelimen ylläpitämisestä. Windows-ympäristöissä paljon käytetty ratkaisu sähköpostipalvelimen perustamiseen on Microsoft

Exchange -komponentti, joka asennetaan palvelimen käyttöjärjestelmän päälle, ja tämä komponentti toimii hyödyntäen Active Directoryn sisältämiä tietokantoja säilöäkseen ja jakaakseen informaatiota. Sähköpostipalvelimelle voidaan helposti konfiguroida AD-käyttäjille omat sähköpostitilit, eri postituslistoja, suodattimia ja niiden avulla keskitetyt sähköpostilaatikot, joihin pääsee yhdistämään selaimen kautta. Uusin versio Microsoft Exchangesta on Exchange 2016, jonka järjestelmävaatimukset ovat kohtuullisen pienet (Microsoft 2016b.):

- prosessori: x64-arkkitehtuurin kanssa yhteensopiva Intelin tai AMD:n suoritin.
- keskusmuisti: 4 GB Edge Transport -roolin omaavalle palvelimelle
- keskusmuisti: 8 GB Mailbox-roolin omaavalle palvelimelle
- vähintään 30 GB tilaa massamuistimedialla
- NTFS-tiedostojärjestelmällä formatoidun kovalevyosion
- palvelimelle asennetun Windows Server 2012 tai Windows Server 2012 R2-käyttöjärjestelmän, joka on liitetty oikeaan Active Directory forestiin.

Exchange 2016 -palvelin jaetaan kahteen eri rooliin riippuen kyseisen palvelimen sijainnista yrityksen verkkototeutuksessa ja siltä halutuista ominaisuuksista. Mailbox-roolin sähköpostipalvelin sisältää sähköpostin siirtämistä varten tarvittavat palvelut sekä käyttäjien sähköpostidatasta koostuvan tietokannan. Edge Transport -roolin tehtävänä on sähköpostin kuljettaminen organisaatiosta ulospäin. Tämän roolin sisältävä palvelin halutaan sijoittaa verkon ulkoreunalle tai omaan erilliseen demilitarisoituun alueeseen parannetun tietoturvan vuoksi. Tällä tekniikalla saadaan piilotettua varsinainen verkko, jossa Mailbox-roolin omaavat palvelimet sijaitsevat ja vähentävät mahdollisuuksia hyökätä niihin ulkoapäin. (Microsoft 2016c.)

Exchange 2016 tarjoaa yritykselle mahdollisuuden toteuttaa palvelu vikasietoisena DAG-ominaisuudella. Database Availability Group (DAG) on joukko Mailbox-palvelimia, jotka ylläpitävät jaettua kokoelmaa tietokannoista. Tällä automatisoidulla HA-ominaisuudella voidaan välttää

verkon tai laitteiden vikaantumisesta johtuvan tiedon häviämisen aiheuttamat tappiot. DAG-ominaisuuden käyttäminen vaatii vähintään kahta Exchange-palvelinta, mutta se tukee tiedon replikointia jopa 16 palvelimen välillä. (Microsoft 2016b.)

4.7 Varmuuskopiointi

Varmuuskopioinnilla tarkoitetaan toimenpiteitä, joilla tärkeät tiedostot tai tietokannat kahdennetaan eli kopioidaan varmuuden vuoksi toiselle kiintolevylle tai muulle tallennusmedialle. Tällä toimenpiteellä pyritään varjelemaan datan olemassaoloa, mikäli alkuperäinen massamuistimedia vikaantuu syystä tai toisesta. Vikatapauksessa data voidaan palauttaa alkuperäiseen muotoon varmuuskopioista. Liiketoimintaa koskevan tai siihen liittyvän tiedon varmuuskopiointi on elintärkeää yrityksen toiminnalle. (Rouse 2009.)

Varmuuskopiointi on mahdollista eri tekniikoilla esimerkiksi verkkoyhteyksiä hyödyntäen toisessa sijainnissa olevalle palvelimelle tai paikalliseen massamuistiin. Eri palveluntuottajat tarjoavat ratkaisuja varmuuskopioinnille, mikäli yritys haluaa ulkoistaa tämän palvelun. Toimialueen koneille voidaan myös tehdä eri skriptejä, jotka automatisoivat varmuuskopioinnin esimerkiksi palveluntarjoajan etäpalvelimelle tietyn aikavälin kuluttua. Verkon yli pilveen tai etäpalvelimen kiintolevylle varmuuskopioiminen varmuuskopiointi on lisäkeino, jolla vältetään datan korruptoitumisesta tai muusta ulkoisesta tekijästä johtuva tietojen menettäminen pääasiallisessa palvelinsalissa. (Rouse 2005c.)

Yritysluokan paikallisen varmuuskopioinnin toteuttamisessa voidaan hyödyntää varmistusnauha-asemia. Nauha-asemat tarjoavat kustannustehokkaan ja luotettavan tavan arkistoida ja kopioida tarvittavia tiedostoja varmempaan muotoon, josta ne on mahdollista palauttaa. Nauha-asemat useasti sisältävät suuren määrän tallennuskapasiteettia yhdellä nauhalla, jolloin hieman suuremmankin yrityksen varmuuskopiointiin liittyvät tarpeet täyttyvät kapasiteetin suhteen. Lisäksi

mahdollisuus 256-bittiseen AES-kryptattuun mediaan tekee datan arkistoimisesta tietoturvallista. (HP 2016.)

5 PALVELIMIEN YLLÄPITORATKAISU

Käytännön osuuden tarkoituksena on vertailla Miradoren palvelimien erilaisia ylläpitoratkaisuja ottaen huomioon erityisesti kustannustehokkuuden, teknisen puolen mahdolliset haasteet sekä riskien arvioimisen. Tavoitteena on selvittää, mitä etuja ja haittoja kukin vaihtoehto tuo mukanaan, ja tästä vertailusta saadun informaation myötä päätyä yrityksen kannalta parhaaseen mahdolliseen ratkaisuun. Pääasiassa tämä vertailu tehdään organisaation nykyisen palvelimien ylläpitoratkaisun ja hosting-palvelun tarjoaman vaihtoehdon välillä.

5.1 Nykytilanne yrityksessä

Tällä hetkellä yritys ylläpitää omia palvelimiaan vuokraamassaan laitetilassa, joka sijaitsee lähellä varsinaista konttoria toisessa toimipisteessä. Tässä toimintamallissa yritykselle kuuluu kaikki ylläpitotoimet, joita ovat asennustoimenpiteet, ohjelmistojen päivitykset sekä mahdolliset vianselvitystilanteet - eli ulkopuolisten yritysten tarjoamiin palveluihin ei turvauduta normaalitilanteessa palvelimien vuokraamista lukuun ottamatta.

Ulkoistetuiksi harkittuja fyysisiä palvelimia on kolme kappaletta. Niillä toimivat tärkeimmät palvelut, joiden toiminnan takaaminen on jokapäiväisen työn jatkuvuuden kannalta tärkeää. Tämän lisäksi paikan päällä on myös muita palvelimia tuotteen kehitystä ja testaamista varten. Palvelimilla ylläpidettyihin palveluihin kuuluvat seuraavat:

- tiedostopalvelin
- tuotekehityspalvelin
- OBS (Open Build Service)
- lähdekoodinhallinta
- domain controller ja DNS-palvelin
- WSUS-palvelin & F-secure policy manager.

Tiedostopalvelimella jaetaan työntekijöille tallennustilaa eri tiedostojen säilyttämistä ja siirtämistä varten. Palvelimissa voidaan hyödyntää nopeita lähiverkkoyhteyksiä, koska ne sijaitsevat lähellä toimipistettä, joten tiedostopalvelimen käyttäminen on huomattavasti nopeampaa kuin ulkoistetussa mallissa. Tämä säästää työaikaa ja vaivaa esimerkiksi suurten image-tiedostojen siirtämisessä.

Tuotekehityspalvelin on yrityksen kehittämän ohjelmiston hallintapalvelin. OBS-palvelinta hyödynnetään Linux clienttien kääntö- ja asennuspakettien luomista varten.

Lähdekoodinhallintaan käytetään TFS-palvelinta (Microsoft Team Foundation Server), joka antaa työkalut helpomman yhteistyön tekemiseen suuremmissakin ohjelmistoprojekteissa. TFS:n sisältämällä versionhallinnalla voidaan hallita ja muokata lähdekoodia tarvittavaan muotoon. Versionhallinnalla varmistetaan, että dokumentaatioon tai lähdekoodiin tehdyistä muutoksista pidetään yllä lokia. Tällä tavoin saadaan vähennettyä riskiä, että useampi henkilö tekisi yhtä työtehtävää samanaikaisesti, ja samalla parannetaan dokumentaatiota.

Domain controllerilla hallitaan sisäverkon tietokoneita, käyttäjätilejä ja oikeuksia Windows domainin sisällä. Tässä hyödynnetään Microsoftin Active Directorya, jolla saadaan luotua ympäristö, jossa halutuilla käyttäjätileillä on tietyt määritetyt oikeudet. Täten voidaan jakaa resursseja keskitetysti käyttäjille sekä suojata sisäverkkoa ja verkon resursseja autentikoinnin avulla. Domain controllereita on kaksi kappaletta, joista toinen toimii varalla. Samalla palvelimella on toiminnassa DNS-palvelin, joka muuntaa IP-osoitteita verkkotunnuksiksi

WSUS (Windows Server Update Services) on työkalu, joka mahdollistaa Microsoftin tuotteiden päivitysten hallitun asennuksen järjestelmänvalvojalle. WSUS lataa nämä päivitykset Windows Updaten kautta ja asentaa päivitykset halutuille koneille haluttuun aikaan.

F-secure policy manager on keskitetyn tietoturvan hallintatyökalu, jolla voidaan etänä asentaa tietoturvaan liittyviä päivityksiä, hallita ja tarkastella verkon laitteiden ja palvelimien tilaa yhdestä näkymästä.

Fyysisisiin palvelimiin on asennettu Hyper-V virtualisointiohjelmistoksi, jonka päälle on luotu useampi virtuaalikone ylläpitämään tarvittavia palveluita. On luontevaa pitää mahdollisimman monta osaa ympäristöstä niin hyvin yhteensopivina jo valmiiksi kuin mahdollista, joten käytössä on monia saman valmistajan eli Microsoftin tuotteita.

Varmuuskopiointi hoidetaan pääasiallisesti nauha-asemalla, joka tarjoaa useamman teratavun tallennuskapasiteetin pakattuna yhdelle nauhalle. Nauha-asema sisältää myös 256-bittisen AES-kryptauksen tiedon turvaamiseksi. Lisäksi osa tiedoista on kopioitu normaaleille kovalevyille ristiin järjestelmien välillä välttäen single point of failure -tapaukset varmistuksien välillä.

Kokonaisuudessaan nykyinen ylläpitoratkaisu on hyvinkin kustannustehokas monelta kannalta. Palvelimien käytössä kulutetusta sähköstä ei jouduta maksamaan juurikaan mitään ylimääräistä, sillä vuokrattujen neliöiden määrä määrittää sähkön hinnan. Arviolta voidaan puhua korkeintaan kymmenistä euroista kuukaudessa. Samantapainen tilanne on myös Internet-yhteyden kanssa, koska palvelimille käytetään samaa yhteyttä kuin muulle toimistolle ja tämän Internet-yhteyden hinta on työntekijämäärästä riippuvainen. Palvelimille vuokrattu laitetilakin on kustannuksiltaan pieni ja sijainniltaan hyvä. Palvelintilan sijainti lähellä fyysistä toimipistettä mahdollistaa nopean lähiverkkoyhteyden hyödyntämisen. Fyysiset palvelimet on hankittu vuokraamalla niitä muutaman vuoden ajan, jonka jälkeen vuokrasopimuksen päättyessä osa niistä on ostettu omaan käyttöön. Vanhimmat palvelimet ovat siis noin 5 vuotta vanhoja.

Nykyisen ylläpitoratkaisun haittapuolena ovat useat riskit, joita vanhentunut laitteisto tuo mukanaan. Vanhempien palvelinlaitteiden elinikää on vaikea, ellei lähes mahdotonkin arvioida. Tilastollisesti voidaan

laskea MTBF-lukuja komponenteille (Mean Time Between Failure), mutta suurista fyysisen tason, palvelinympäristön ja käyttötarkoituksien erosta johtuen laitevalmistajat harvemmin nykyään edes julkaisevat MTBF-lukuja. Laitteiston rikkoutuessa on yrityksen asiakkaille tarjoamilla palveluilla tehotonta työaikaa, kunnes fyysiset komponentit saadaan toimintakuntoon joko tilaamalla uusi palvelin tai huollattamalla vanha. Samalla organisaatio tekee taloudellista tappiota, josta voi esimerkkinä mainita työntekijöiden palkat, joita on maksettava, vaikka käytännössä työtehtäviä olisi mahdotonta suorittaa ilman tarpeellista infrastruktuuria. Palvelimen yllättävä vikaantuminen tai sen toiminnan lakkaaminen toisi myös mahdollisesti vakaviakin riskejä yritykselle imagotappion ja huonon pr-maineen muodossa.

5.2 Hosting-palvelu

Hosting-palvelulla tarkoitetaan ulkopuolisen toimitsijan tarjoamaa ylläpitoratkaisua, jossa nykyisessä käytössä olevat virtuaalikoneiden imaget siirretään nykyaikaiseen konesaliin ylläpidettäväksi. Palvelu tarjoaa siis jaetusta kapasiteetista virtuaalipalvelimia. Yrityksen ei tarvitsisi enää huolehtia fyysisistä palvelinkomponenteista, vaan yritys voisi keskittyä pelkästään ohjelmistopuolen tehtäviin.

Hosting-palvelut tarjoavat eri palvelutasoja tarpeiden mukaan. Palvelutasoilla vaihtelevat erityisesti käytettävyysprosentti ja vikojen korjaamiseen liittyvät vasteajat. Yleisesti luvataan 99 % - 99,9 % käytettävyysprosentteja riippuen palvelutasoista. Tällä käytettävyysprosentilla tarkoitetaan juuri fyysisiä komponentteja, jotka hosting-palvelu tarjoaa käytettäväksi. Kriittisimmille palveluille voidaan ostaa esimerkiksi jokin kolmesta palvelutasosta, jolloin vakavampienkin vikojen korjaamiseen varattu vasteaika pienenee. Esimerkkinä palvelutasosta on 3-taso, jossa vasteaika olisi korkeintaan 10 tuntia. Datalle luvataan myös laadukasta varmennusta esimerkiksi offsite-kopiolla, joka toimitetaan toiseen konesaliin.

5.3 Vertailu oman hostingin ja hosting-palvelun välillä

Laskelmat on tehty tapauksessa, jossa jo ostetut palvelimet siirrettäisiin muihin tehtäviin ja vanhentuneen leasing-sopimuksen tilalle vuokrattaisiin kolme kappaletta uusia palvelimia ylläpitämään tarvittavia palveluita. Palvelimien vuokraaminen tulee maksamaan noin 200 € jokaisesta tornipalvelinta kohden. Jäähdytetyn palvelintilan vuokra on 200 €:n luokkaa, ja tila sijaitsee toimiston viereisessä rakennuksessa. Tämän lisäksi uusien palvelimien asennustöihin voidaan karkeasti arvioida menevän yhdestä kahteen työpäivää.

Microsoftin palvelinlisenssit kustantavat 341 kahta prosessoria kohden yhden vuoden ajan, ja tällä paketilla voi käyttää isäntäkonetta sekä kahta virtuaalikonetta. Toisella lisenssillä saadaan lisättyä kaksi virtuaalikonetta isäntäkoneeseen. Yhteishinnaksi tulee 682 € vuodessa, joka tekee 56,8 € kuukausihinnaksi.

Varmistukseen käytetään LTO-5 Ultrium -varmistusnauhoja, joita menee vuodessa neljä kappaletta. Yhden varmistusnauhan hinta on 23,3 €, josta saadaan kuukausihinnaksi 7,7 €. Nauha-aseman puhdistamiseen käytetään HP Ultrium-puhdistusnauhaa, jonka hinta on 61,2 €. Kuukausitasolla varmistusnauhojen hinnaksi tulee 5,1€.

Palvelimien ylläpitoon käytetyt tunnit sisältävät varmistusnauhan vaihdon, ohjelmistotason ongelmat ja muut yllättävät tilanteet. Kustannus työntekijästä yritykselle on arvioilta noin 4500 €/kk. Yhteensä kuukausikulut uusilla vuokratuilla palvelimilla olisivat 1057 €. Kaikki laskemat on tehty arvolisäverottomina, jotta vertailu hosting-palvelun lukuihin on järkevää.

Hosting-palvelun tarjoamassa ylläpitoratkaisussa on vara domain controller jätetty laskuista pois, sillä varalla toimivaa AD-palvelinta ylläpidettäisiin yrityksen omissa toimistotiloissa pienellä palvelimella. Microsoft Active Directory -palvelin sekä yrityksen tuotteen tuotekehityspalvelin siirrettäisiin suoraan 3-tasolle, jotta mahdollisten vikojen ilmeentyessä, saadaan palvelimen toimimattomuusaika

mahdollisimman lyhyeksi. TFS, OBS ja WSUS-palvelimet toimisivat perustasolla ja niiden tasoa voi myöhemmin tarvittaessa nostaa korkeammalle. Tiedostopalvelin siirrettäisiin hosting-palvelun CIFS-tiedostopalveluun. Virtuaalikoneiden datan varmistus hoidetaan esimerkiksi offsite-kopioilla.

Hosting-palvelun käytön kokonaiskustannukset nousevat 2050 €:oon (ALV0) asti verrattuna oman ylläpidon 1057 €:n (ALV0) määrään. Tämän lisäksi palvelinten siirtoprojektiin kuuluvat suunnittelut, virtuaalipalvelimien migraatio, verkkoyhteyksien luominen ja mahdollinen tiedostopalvelimien siirto kustantavat noin 100-200 € tuntityöskentelynä. Vaikka kustannukset ovat suuremmat, niin samalla riskit vähenevät huomattavasti ja hyödyt ovat helposti huomattavissa. Yrityksen ja työntekijöiden ei enää tarvitsisi huolehtia palvelimien fyysisistä komponenteista, sillä niille on luvattu korkea käytettävyyslukema. Tällä myös vältetään skenaario, jossa palvelin lakkaa toimimasta ja työnteko keskeytyy pidemmäksi aikaa aiheuttaen turhia kustannuksia palkkojen ja käytetyn ajan suhteen. Ylipäätänsä henkilöstö pystyisi keskittymään ydinliiketoimintaan täysiaikaisesti eikä palvelimen ylläpitoon liittyviä tehtäviä tarvitsisi hoitaa itse.

Mahdolliset haittapuolet kustannuksien nousemisen lisäksi ovat hitaammat yhteydet CIFS-tiedostopalveluun, kun halutaan siirtää suurempia tiedostoja, mikä vuorostaan tekee työnteosta hieman hitaampaa. Lokaali työskentely myös keskeytyy täysin, mikäli Internet-yhteydet eivät toimi kunnolla, kun taas tämänhetkisessä mallissa sisäverkon kautta päästään kiinni lähdekoodinhallintaan, tiedostopalvelimeen, ja varalla oleva domain controller hoitaa ympäristön hallinnan. Tietoturvan heikkeneminen on myös mahdollista, kun puhutaan kolmannen osapuolen ympäristöstä, joka ei ole yritykselle ennestään tuttu.

5.4 Vaihtoehtoratkaisu palvelimien ylläpitoon

Vaihtoehtoisessa ratkaisussa käydään läpi malli, jossa yhdistetään molempien palvelimien ylläpitoratkaisujen hyödyt ja yritetään minimoida haitat. Tiedostopalvelin, lähdekoodinhallinta sekä varalla oleva domain controller jätettäisiin yrityksen omalle ylläpidolle sitä varten, että olemassa on pieni ympäristö, joka ei ole riippuvainen yhteyksistä ulkomaailmaan ja työnteko onnistuu jouhevasti tilanteessa kuin tilanteessa. Samalla hyödynnetään hosting-palvelun tarjoamia suuria käytettävyysaikoja, jotta vähennetään mahdolliset tilanteet alhaallaoloajan suhteen.

Hosting-palveluun migroitaisiin tuotekehityspalvelin, Open Build Service -palvelin, pääasiallinen Active Directory-domain controller ja WSUS & F-secure policy manager -palvelin. Näistä palvelimista domain controller sekä tuotekehityspalvelin nostettaisiin 3-tasolle niin kuin edeltävässä ratkaisussa, jossa kaikki palvelut siirrettäisiin hosting-palvelun hoidettavaksi. Syynä tähän on kyseisten palveluiden tärkeys infrastruktuurille ja niiden haluttu mahdollisimman suuri käytettävyysaste yhdistettynä lyhyeen vikojen korjaamiseen varattuun vasteaikaan. Näiden neljän migroitavan palvelimen ylläpitohinnaksi saadaan 750 €. Kolmannen osapuolen tarjoama datan varmistus laskisi määrältään 400 GB, ja tässä skenaariossa tuon datan backup-toimenpiteet hoidettaisiin Miradoren puolesta varmistusnauhoilla vanhaan tapaan. Hintaa datan varmistukselle tulisi hosting-palvelun puolesta 300 €. Hosting-palvelulta ostettujen lisenssien määrä vähenee yhdellä kolmeen kappaleeseen. Hinnaksi tälle ylläpitoratkaisun osalle tulisi 1125 €.

Miradoren vuokratut palvelimet vähentyisivät yhteen, koska sillä voidaan ylläpitää yritykselle jääviä ylimääräisiä palveluja, ja vanhempia jo ostettuja palvelimia voitaisiin hyödyntää joko testikäytössä tai varapalvelimina. Uuden palvelimen vuokraamisen kulut liikkuvat 200 € molemmin puolin. Jäähdytetyn palvelintilan vuokraamisen jatkaminen testipalvelimia ja lähdekoodinhallinta, vara domain controller ja tiedostopalvelin yhdistelmää varten on järkevää, jollei konttorin puolelta löydy palvelimille sopivaa tilaa. Palvelintilan kustannukset ovat 200 € kuukaudessa.

Itse ostetut palvelinlisenssit vähenevät yhteen kappaleeseen, jolla voi ajaa isäntäkonetta sekä kahta virtuaalikonetta. Microsoftin palvelinlisenssit kustantavat 341 € kahta prosessoria kohden yhden vuoden ajan, ja kyseisellä paketilla voi ajaa isäntäkonetta sekä kahta virtuaalikonetta. Tämä tekee kuukausihintana 28,40 €.

Varmistusnauhat on arvioitu yläkanttiin neljällä kappaleella, joita todellisuudessa saattaa uudella kokoonpanolla mennä määrällisesti vähemmän. Varmistukseen käytetään edelleen LTO-5 Ultrium -varmistusnauhoja. Yhden varmistusnauhan hinta on 23,3 €, josta saadaan kuukausihinnaksi 7,7€. Nauha-aseman puhdistamiseen käytetään HP Ultrium -puhdistusnauhaa, jonka hinta on 61,2 €. Kuukausitasolla se tekee hinnaksi 5,1 €.

Palvelimiin käytetyt työtunnit myös pienenevät muutamaan tuntiin kuukaudessa, jolloin työskentelyn tuottavuustaso nousee. Palvelimien ohjelmistoja tarvitsee päivittää harvemmin ja vianratkontaan liittyvien yllättävien tapauksien määrän voidaan olettaa vähenevän lineaarisesti käytettyyn aikaan nähden. Yrityksen omaan ylläpitoon jäävien palvelimien kustannukset tässä vaihtoehtoratkaisussa ovat noin 509 €.

Kokonaishinnaksi vaihtoehtoratkaisulle saadaan arvioitua 1634 € (ALV0). Kustannuksiltaan vaihtoehtoinen ratkaisu siis sijoittuu nykyisen ylläpitoratkaisun (1057 €) ja hosting-palvelun tarjoaman paketin (2050 €) välimaastoon. Parhaimpina puolina vaihtoehtoratkaisussa voidaan luetella varmempi käyttöaste tärkeimmille palveluille verrattuna yrityksen nykyiseen ylläpitoratkaisuun, sillä tuotekehityspalvelin, obs, domain controller sekä WSUS & F-secure policy manager -palvelin siirrettäisiin eri palvelutasoille hosting-palveluun. Tämän lisäksi olemassa olisi pieni ympäristö yrityksen sisällä, joka mahdollistaisi kohtuullisen työnteon esimerkiksi Internet-yhteyden vikaantuessa. Tällöin myös tiedostopalvelimen pysyessä omassa lähiverkossa olisi tiedostojen siirtäminen nopeampaa kuin puhtaassa hosting-skenaariossa.

Täysin haasteeton ei kyseinen ratkaisu ole, sillä yrityksen olisi silti ylläpidettävä vähintään yhtä palvelinta pienympäristön palveluita varten. Omaan ylläpitoon liittyvä työmäärä olisi huomattavasti pienempi kuin nykytilanteessa, mutta silti voidaan puhua useammasta tunnista kuukaudessa, jotka voisi hyödyntää tärkeimpiin työtehtäviin. Ylläpidettävän laitteiston vikaantuminen ei myöskään lamaannuttaisi työntekoa läheskään niin kriittisesti kuin nykytilanteessa eikä tuottaisi yrityksen ulkopuolelle näkyvää tappiota. Sisäisen pienympäristön hajoaminen hidastaisi työntekoa, mutta palveluiden takaisin ylösnostaminen ei kestäisi ajallisesti niin kauaa, että siitä koituisi suuria rahallisia tappioita ja hosting-palvelussa olevia palvelimia voitaisiin silti sillä välin hyödyntää täysin. Tämä ratkaisu tarjoaa hinnaltaan halvemman vaihtoehdon, joka yhdistelee nykyisen ylläpitotyylin ja hosting-palvelun parhaita puolia, samalla sisältäen pieniä riskejä ja ylimääräistä työtä palvelimien kanssa.

5.5 Vertailu palvelimien ylläpitoratkaisuiden välillä

Pelkät kustannukset huomioon ottaen nykyinen ylläpitoratkaisu on parempi kuin muut vaihtoehdot, mutta kokonaiskuvaa ajatellen ylläpitoratkaisu sisältää suuren määrän riskejä, jotka altistavat mahdollisesti suuremmille tappioille kuin mitä siitä saadut säästöt ovat. Hosting-palvelun tarjoama ratkaisu sisältää vähiten riskejä, mutta samalla se on hinnaltaan suurin ja kolmannen osapuolen hosting-palvelun mukana tulee silti haittapuolia liittyen tiedostopalvelimen tiedostojen siirtonopeuteen ja mahdollisiin yhteysongelmiin. Vaihtoehtoratkaisu on riskeiltään kohtuullisen pieni, ja ne riskit liittyvät enimmäkseen yrityksen sisäisen pienympäristön ongelmiin. Vaihtoehtoratkaisun haittapuolena oman palvelimen ylläpitäminen toimii häiriötekijänä muille työtehtäville tarvittavien päivitystöiden ja muiden vikatilanteiden ilmeentyessä. Taulukossa 1 on vertailtu eri ylläpitoratkaisuiden kustannuksia ja riskitasoja toisiinsa.

Yrityksen kannalta paras palvelimien ylläpitoratkaisu voidaan sijoittaa kolmannen osapuolen tarjoaman ylläpitopalvelun ja vaihtoehtoratkaisun

välille riippuen projektin budjetista ja siitä kuinka paljon oman henkilökunnan resursseja halutaan käyttää palvelimien ylläpitoon.

TAULUKKO 1. Vertailu ylläpitoratkaisuiden kuukausikustannuksien ja riskitasojen välillä

Vertailu vaihtoehtojen välillä			
	Oma ylläpitoratkaisu	Kolmannen osapuolen tarjoama ylläpitopalvelu	Vaihtoehtoratkaisu
Riski	Suuri	Pieni	Kohtalainen
Kokonaiskustannukset	1,057 €	2,050 €	1,634 €

6 YHTEENVETO

Opinnäytetyön tavoitteena oli tutustua Miradoren Oy:n fyysiseen palvelinympäristöön, kyseisen palvelinympäristön päälle toteutettuihin virtualisoituihin palveluihin ja tämän kokonaisuuden ylläpitoratkaisuihin. Tämän ympäristön nykyistä ylläpitoratkaisua verrattiin hosting-palvelun tarjoamaan ratkaisuun ja vaihtoehtoiseen ratkaisuun, jossa yhdistettiin aiemmista toteutuksista saatuja hyötyjä samalla minimoiden niiden tuomia haittoja. Nykyisessä ylläpitoratkaisussa fyysisten palvelimien ja palveluiden ylläpidosta vastaa yritys itse. Toisena vaihtoehtona on hosting-palvelun ostaminen, jolloin kaikki tai osa palvelimista siirrettäisiin kolmannen osapuolen tarjoamaan palvelinsaliin. Vaihtoehtoisessa ylläpitoratkaisussa osa palvelimista jäisi yrityksen omaan ylläpitoon ja loput siirrettäisiin hosting-palveluun. Miradore Oy tulee käyttämään tätä vertailua päättäessään mahdollisista palvelimien ylläpitoon tehtävistä muutoksista.

Toisena tavoitteena työllä oli selvittää, mistä komponenteista ja tekniikoista tuotantokäytössä oleva palvelinympäristö koostuu, ja antaa tästä ympäristöstä työn lukijalle realistinen kuva. Työssä käsiteltiin fyysisen palvelimen rakenne, syitä minkä takia virtualisointiteknologiaa hyödynnetään määrällisesti paljon nykypäivän palveluiden tuottamisessa, ja ohjelmistoja, joilla yrityksen sisäverkon palvelut voidaan toteuttaa. Samalla paneuduttiin myös näiden palveluiden välisiin yhteyksiin ja tapoihin toteuttaa niitä vikasietoisesti.

Työ saavutti sille asetetut tavoitteet, vaikka yrityskäytössä olevasta palvelinympäristöstä ei ollutkaan aiempaa kokemusta. Yhteenvetona voidaan mainita, että palvelimien ylläpitoon ei ole yhtä oikeaa ratkaisua. Henkilöstön määrä, asiakkaiden määrä, laitteiden määrä, laitetilan koko, ylläpidon kustannukset ja ratkaisun sisältämät riskit sekä monet muut tekijät vaikuttavat siihen mikä on kullekin yritykselle paras ratkaisu. Nämä tekijät yhdistettynä nykypäivän tietotekniikan standardeihin auttavat rajoittamaan vaihtoehtojen määrää, jolloin lopulta päädytään siihen ratkaisuun, joka vastaa eniten yrityksen tarpeita. Tässä tapauksessa

mahdolliset riskit ja kustannustehokkuuden huomioon ottaen voidaan suositella yritykselle vähintään osittaista palvelimien siirtämistä hosting-palveluun.

LÄHTEET

Bigelow, S. 2010. VM snapshop backup process explained [viitattu 25.3.2016]. Saatavissa: http://searchservervirtualization.techtarget.com/tip/VM-snapshot-backup-process-explained

Brown, M. 2012. How to choose a serveryou're your small business [viitattu 20.3.2016]. Saatavissa: http://www.pcworld.com/article/251993/how_to_choose_a_server_for_your_small_business.html

Cisco. 2016a. Cisco UCS Servers RAID Guide [viitattu 20.3.2016]. Saatavissa: http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/sw/raid/configuration/guide/RAID_GUIDE/IntroToRAID.html

Cisco. 2016b. DNS best practices, network protections, and attack identification [viitattu 1.4.2016]. Saatavissa: http://www.cisco.com/c/en/us/about/security-center/dns-best-practices.html

Dell. 2016. What Is a Server [viitattu 15.2.2016]. Saatavissa: http://www.dell.com/downloads/us/bsd/What_Is_a_Server.pdf

F-secure. 2016. F-secure policy manager [viitattu 17.4.2016]. Saatavissa: https://download.f-secure.com/corpro/pm/current/fspm-12.00-adminguide-eng.pdf

Gartner. 2015. Magic quadrant for x86 server virtualization infrastructure [viitattu 25.3.2016]. Saatavissa: https://www.gartner.com/doc/reprints?id=1-2JGMVZX&ct=150715&st=sb

Golden, B. 2007. Virtualization for Dummies

HP. 2016. HPE StoreEver LTO Ultrium Tape Drives [viitattu 18.4.2016]. Saatavissa: http://www8.hp.com/us/en/products/tape-drives-enclosures/product-detail.html?oid=5336462#!tab=features

Intel. 2016a. Intel Hyper Threading Technology. [viitattu 15.3.2016]. Saatavissa: http://www.intel.com/content/www/us/en/architecture-and-technology/hyper-threading/hyper-threading-technology.html

Intel. 2016b. Intel Turbo Boost Technology [viitattu 15.3.2016]. Saatavissa: http://www.intel.com/content/www/us/en/architecture-and-technology/turbo-boost/turbo-boost-technology.html

Microsoft. 2005a. Domain controllers [viitattu 15.4.2016]. Saatavissa: https://technet.microsoft.com/en-us/library/cc759623(v=ws.10).aspx

Microsoft. 2005b. Domains [viitattu 15.4.2016]. Saatavissa: https://technet.microsoft.com/en-us/library/cc780856(v=ws.10).aspx

Microsoft. 2008. DNS server role. [viitattu 15.4.2016]. Saatavissa: https://technet.microsoft.com/en-us/library/cc753635(v=ws.10).aspx

Microsoft. 2014a. How DNS support for active directory works [viitattu 15.4.2016]. Saatavissa: https://technet.microsoft.com/en-us/library/cc759550(v=ws.10).aspx

Microsoft. 2014b. What are domains and forests? [viitattu 15.4.2016]. Saatavissa: https://technet.microsoft.com/en-us/library/cc759073(v=ws.10).aspx

Microsoft. 2014c. Windows Server Update Services overview [viitattu 16.4.2016]. Saatavissa: https://technet.microsoft.com/en-us/library/hh852345.aspx

Microsoft. 2015. Hyper-V feature overviews [viitattu 26.3.2016]. Saatavissa: https://technet.microsoft.com/en-us/library/hh831564.aspx

Microsoft. 2016a. Active Directory [viitattu 18.4.2016]. Saatavissa: https://technet.microsoft.com/en-us/library/bb123715(v=exchg.160).aspx

Microsoft. 2016b. Exchange 2016 architecture [viitattu 18.4.2016]. Saatavissa: https://technet.microsoft.com/EN-US/library/jj150491(v=exchg.160).aspx

Microsoft. 2016c. Exchange 2016 system requirements [viitattu 18.4.2016]. Saatavissa: https://technet.microsoft.com/en-us/library/aa996719(v=exchg.160).aspx

Miradore. 2016. Miradore Management Suite for IT Systems Management [viitattu 27.4.2016]. Saatavissa: https://www.miradore.com/miradore-management-suite-for-it-systems-management/

Rouse, M. 2005a. Domain controller [viitattu 15.4.2016] Saatavissa: http://searchwindowsserver.techtarget.com/definition/domain-controller

Rouse, M. 2005b. File server [viitattu 16.4.2016]. Saatavissa: http://searchnetworking.techtarget.com/definition/file-server

Rouse, M. 2005c. Online backup [viitattu 18.4.2016]. Saatavissa: http://searchstorage.techtarget.com/definition/online-backup

Rouse, M. 2006. X86 [viitattu 16.3.2016]. Saatavissa: http://searchwindowsserver.techtarget.com/definition/x86

Rouse, M. 2009. Backup [viitattu 18.4.2016]. Saatavissa: http://searchstorage.techtarget.com/definition/backup

Rouse, M. 2014. Container-based virtualization [viitattu 26.4.2016]. Saatavissa: http://searchservervirtualization.techtarget.com/definition/container-based-virtualization-operating-system-level-virtualization

Rouse, M. 2015a. Hardware virtualization [viitattu: 23.3.2016]. Saatavissa: http://searchvmware.techtarget.com/definition/hardware-virtualization

Rouse, M. 2015b. Network-attached storage [viitattu 16.4.2016]. Saatavissa: http://searchstorage.techtarget.com/definition/network-attached-storage

Rouse, M. 2015c. RAID [viitattu 16.3.2016]. Saatavissa: http://searchstorage.techtarget.com/definition/RAID

Rouse, M. 2015d. Storage area network (SAN) [viitattu 16.4.2016]. Saatavissa: http://searchstorage.techtarget.com/definition/storage-area-network-SAN

Siebert, E. 2016. Choosing vSphere vs. Hyper-V vs. XenServer [viitattu 1.4.2016]. Saatavissa: http://searchitchannel.techtarget.com/feature/Choosing-vSphere-vs-Hyper-V-vs-XenServer

Steele, C. 2010. Virtual machine migration FAQ: Live migration, P2V and more [viitattu 23.3.2016]. Saatavissa: http://searchservervirtualization.techtarget.com/feature/Virtual-machine-migration-FAQ-Live-migration-P2V-and-more

Techtarget. 2016. Active Directory tutorial [viitattu 16.4.2016]. Saatavissa: http://searchwindowsserver.techtarget.com/tutorial/Active-Directory-Tutorial

VMware. 2009. VMware High Availability [viitattu 25.3.2016]. Saatavissa: http://www.vmware.com/files/pdf/ha_datasheet.pdf

VMware. 2016a. Server Consolidation [viitattu 15.2.2016]. Saatavissa: http://www.vmware.com/pdf/server_consolidation.pdf

VMware. 2016b. Understanding Full Virtualization, Paravirtualization, and Hardware assist [viitattu 23.3.2016]. Saatavissa: https://www.vmware.com/files/pdf/VMware_paravirtualization.pdf

VMware. 2016c. vSphere and vSphere with operational management [viitattu 26.3.2016]. Saatavissa: https://www.vmware.com/products/vsphere/compare.html

Williams, D. Garcia, J. 2007. Virtualization with Xen