



Pilvipalvelut

Case: WPK-verkko

Tapio Rantanen

Opinnäytetyö
Huhtikuu 2012
Tietojenkäsittelyn koulutusohjelma
Tietoverkkopalvelut

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tietojenkäsittelyn koulutusohjelma
Tietoverkkopalveluiden suuntautumisvaihtoehto

RANTANEN, TAPIO:

Pilvipalvelut

Case: WPK-verkko

Opinnäytetyö 31 sivua, joista 5 sivua liitteitä

Huhtikuu 2012

Opinnäytetyön tavoitteena on tutkia eri pilvipalveluja ja luoda kuvaus erilaisista pilvipalveluista ja niiden toiminnasta. Tavoitteena on antaa kattava yleiskuva siitä, minkälaisia pilvipalveluita on olemassa, mihin niitä käytetään ja tuoda esiin niiden edut ja haitat sekä esitellä toimeksiantajalle toteutettu infrastruktuuripilvipalvelu.

Opinnäytetyössä tutkitaan IaaS-, PaaS- ja SaaS-pilvien eroavaisuuksia ja niiden tarjoamia etuja sekä niille sopivia käyttötarkoituksia. Erilaisista pilvityypeistä kerrotaan markkinoilla olevia, yleisesti tunnettuja kaupallisia esimerkkejä. Työssä esitellään Microsoftin tekniikoita, joilla luodaan IaaS-tyypin pilvipalvelu.

Toimeksiantajalle toteutettiin WPK-verkossa toimiva IaaS-pilvipalvelu WPK-verkon käyttäjien käyttöön. Työn tekemisen aikana huomattiin pilvipalvelun huomattavat laitevaatimukset ja tämä asettikin toteutetun ympäristön hyödyntämiseen suuret rajoitteen. Pilvipalvelun toiminnan etujen havainnollistamiseksi ja ympäristön toiminnan tehostamiseksi olisi tarvittu vain pilvipalvelun käyttöön omistettuja palvelimia.

Avainsanat: pilvipalvelut, IaaS, self-service portal

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
Degree Programme in Business Information Systems
Option of Data Network Services

RANTANEN, TAPIO:

Cloud Computing

Case: WPK network

Bachelor's thesis 31 pages, appendices 5 pages

April 2012

The objective of this thesis was to study and offer a general picture about different kinds of cloud computing technologies. The thesis also looks at the pros and cons of cloud computing and to give few examples of several commercial cloud computing services.

The thesis also explains what IaaS, SaaS and Paas clouds are and when to implement them. The IaaS-environment built for the client is described in this thesis. This hands-on approach gave a better understanding of the requirements and work needed for implementing a cloud computing service.

The massive memory, processor and storage resource requirements were realized during the installation of the cloud computing environment. Because of the limitations of the resources, the cloud computing environment and the advantages of cloud computing were restricted. A few servers dedicated for the cloud would have improved the results and the usefulness of the environment.

Keywords: cloud computing, IaaS, self-service portal

SISÄLLYS

SISÄLLYS	4
TERMIT	5
1 JOHDANTO	6
2 PILVIPALVELUT, NIIDEN EROT JA TIETOTURVA	7
2.1 Yleisesti pilvipalveluista	7
2.2 Virtuaalisointi	8
2.3 Palvelumallit	9
2.3.1 Julkinen pilvipalvelu	9
2.3.2 Yksityinen pilvipalvelu	10
2.3.3 Sovelletut pilvipalvelut.....	10
2.4 Palveluarkkitehtuurit	11
2.4.1 Infrastruktuuri pilvipalveluna	11
2.4.2 Alusta pilvipalveluna.....	12
2.4.3 Ohjelmisto pilvipalveluna	13
2.5 Pilvipalvelut, tietoturva ja -suoja	14
2.5.1 Pilvipalveluiden tietoturva.....	14
2.5.2 Tietosuoja pilvipalveluissa	15
3 TOTEUTETTU YMPÄRISTÖ	16
3.1 IaaS-pilvipalvelun perusrakenne	16
3.2 Toteutetun pilvipalvelun osat.....	17
3.3 WPK-verkon alkutilanne	17
3.4 Pilvipalvelun rakentaminen	19
3.4.1 IaaS-pilvipalvelun osien asennus	20
3.4.2 Asetusten teko.....	21
3.4.3 Valmiin pilvipalvelun toiminnan testaus.....	23
4 JOHTOPÄÄTÖKSIÄ JA POHDINTA.....	24
4.1 Työn onnistuminen.....	24
4.2 Toimeksiantajan ympäristön puutteet, rajoitukset ja kehitysehdotukset.....	24
4.2.1 Puutteet ja rajoitukset	24
4.2.2 Kehitysehdotukset.....	25
LÄHDELUETTELO.....	26
LIITTEET.....	27

TERMIT

AD	Active Directory on käyttäjätietokanta ja hakemistopalvelu Windows-toimialueelle.
DNS	Domain Name Service on nimipalvelinjärjestelmä, joka muuttaa verkkotunnuksia IP-osoitteiksi
Hypervisor	Rautapohjainen virtuaalisointitekniikka, jossa kaikki käyttöjärjestelmät, mukaan lukien isäntäkäyttöjärjestelmä, ajetaan virtuaalisointialustalla.
Hyper-V	Hyper-V on Microsoftin hypervisor-tekniikkaan perustuva virtuaalisointijärjestelmä.
Klusteri	Klusterilla tarkoitetaan tietotekniikassa mallia, jossa yksi kone jakaa esimerkiksi laskentatyötä useamman palvelimen koneen kesken.
WPK-verkko	TAMKin tietoverkkopalveluiden laboratorioverkko.
Hosting	Erilaisten palvelintroolien ja -palveluiden tarjoaminen Internetin välityksellä.

1 JOHDANTO

Pilvipalvelut ovat kasvattaneet suosiotaan viime vuosina merkittävästi, ja niiden suosion kasvu on ollut tasaista. Yksittäinen innovaatio ei selitä pilvipalveluiden suosion kasvua, vaan kasvun takana on useamman osan summa. Toimintaympäristöt ovat muuttuneet ja samalla muutokset ovat luoneet erilaisia tarpeita, kuten kustannussäästöt tai joustavampien palveluiden tarve. Pilvipalvelu on enemmänkin uusi ajattelumalli tarjota palveluita, kuin mikään yksittäinen tekninen tai periaatteellinen ratkaisu.

Kasvaneet tietoliikennesurssit sekä kehittyneemmät selaimet ovat pikkuhiljaa siirtäneet palveluiden painopisteen Internetiin ja pilvipalvelut vievät tätä ajattelumallia vielä eteenpäin. Pilvipalvelut siirtävät laitteistonkin pois käyttäjän vastuulta ja tarjoavat yksinkertaista, helppokäyttöistä, nopeaa ja joustavaa ratkaisua vapauttaen käyttäjän palveluiden tarvitseman laitteiston jatkuvalta ylläpidolta ja kehitystyöltä.

Opinnäytetyön tavoitteena on tutkia eri pilvipalveluita ja luoda kuvaus erilaisista pilvisistä ja niiden toiminnasta. Tavoitteena on antaa kattava yleiskuva siitä, minkälaisia pilvipalveluita on, mihin niitä käytetään ja tuoda esiin niiden hyödyt ja haitat, käyttäen apuna yleistä teoriaa pilvipalveluista sekä kaupallisia esimerkkejä. Pilvipalveluissa käytettävät tekniikat, kuten virtuaalisointi ja erilaiset toimintojen automatisoinnit, käydään työssä läpi, pilvipalveluiden vaatimusten ja luonteen ymmärtämiseksi. Koska pilvipalveluiden perusluonteena ja kilpailuvalttina pidetään saatavuutta ja pilvipalvelut toteutetaan usein keskittämällä palvelut isoihin datakeskuksiin, usein ulkomaille, niin työssä käydään myös läpi tietosuojan ja -turvan asettamia vaatimuksia ja rajoitteita.

Toimeksiantajan osuudessa esitellään TAMKIn WPK-verkkoon toteutettu infrastruktuuripilvipalvelu, käydään läpi siihen käytetyt tekniikat ja esitellään muita vastaavia tekniikoita eri valmistajilta kuin työssä käytetyt. Toteutukseen kuului myös antaa selvitys ympäristön mahdollisesta hyödyntämisestä WPK-verkon kurssien opetuksessa, esimerkiksi toimien palvelinkoneiden alustana fyysisten koneiden sijaan.

2 PILVIPALVELUT, NIIDEN EROT JA TIETOTURVA

2.1 Yleisesti pilvipalveluista

Pilvipalvelu tarkoittaa yleisesti Internetistä hankittua tietokonekapasiteettia, sovelluksia tai muita palvelusuoritteita. Pilvipalvelut ovat enemmänkin ajattelutapa kuin jokin tietty tekninen ratkaisu. Pilvipalveluiden käytöllä voidaan luopua fyysisistä konesaleista (Heino 2010, 32). Pilvi-sanana käyttö juontaa juurensa puhelinoperaattorien tavasta symboloida asiakkaan ja operaattorin hallitsemien laitteiden rajapintaa pilven kuvalla.

Heino (2010, 48) ehdottaa viittä kohtaa aidon pilvipalvelun tunnistamiselle:

1. Pilvipalveluissa on elastinen provisiointi eli palvelun käyttöönotto ja irtisanominen ovat helppoa sekä palvelun kapasiteetin kasvattaminen onnistuu myös vaihatta.
2. Palvelut on toteutettu jaetussa multitenant-ympäristössä eli samoilla fyysisillä laitteilla on useamman käyttäjän palvelut. Dedikoituja ympäristöjäkin on ja siksi tämän kohdan vaatiminen on enemmän kaupallinen kuin tekninen seikka pilvipalvelun kannalta.
3. Tarjotut palvelut ovat yksinkertaistettuja bulkkituotteita ja volyymitaan isoja. Palveluiden räätälöintiin on annettu vähän, jos lainkaan, tilaa.
4. Pilvipalvelut ovat päätelaitteesta ja käyttöpaikasta riippumattomia. Tätä pidetään pilvipalveluiden isoimpana vahvuutena, sillä se mahdollistaa palveluiden monipuolisemman ja joustavamman käytön.
5. Pilvipalveluiden toimintaa voidaan mitata. Tämä on erittäin tuttua myös perinteisten käyttöpalveluiden puolelta, mutta pilvipalveluissa monesti tämä on ainut laskutusperuste sillä mitään fyysisiä laitehankintoja ei asiakkaalle koidu.

Heino (2010, 48-49), kuitenkin muistuttaa että pilvipalveluiden määrittelyllä ei ole toiminnan kannalta juurikaan arvoa, vaan merkitys on lähinnä akateeminen. Se, mikä pilvipalveluissa on kuitenkin tärkeää, on niiden tuottama hyöty palvelun käyttäjälle verrattuna perinteisiin ratkaisuihin, kuten käyttäjän itse hallitsemaan palvelinsaliin.

Siirryttäessä pois omista konesaleista ja pilvipalveluiden käyttämiseen haittana on palveluiden hallittavuuden ja muokattavuuden menetys. Salo (2010, 46-47) antaa kuusi kohtaa, joissa kontrollin määrä on suurin kohdassa ja yksi ja pienin kohdassa kuusi.

1. *itse kehitetty sovellus omalla alustalla (oma palvelinkeskus)*
2. *ostettu sovellus omalla alustalla (oma palvelinkeskus)*
3. *itse kehitetty sovellus ulkoistetulla palveluntarjoajan alustalla (perinteinen hosting)*
4. *ostettu sovellus ulkoistetulla palveluntarjoajan alustalla (perinteinen hosting)*
5. *itse kehitetty sovellus pilvialustalla (PaaS, IaaS)*
6. *ostettu sovellus pilvialustalla (SaaS)*

Pilvipalveluista ei kuitenkaan voida sanoa yhtä ja parasta ratkaisu kaikkeen, sillä erilaiset pilvipalvelut tarjoavat erilaisia ominaisuuksia. Pilvipalveluita käyttöönottaessa pitääkin huomioida, että kuinka paljon on valmis tuottamaan itse sekä kuinka paljon on valmis luopumaan sovellusten muokattavuudesta (Salo, 2010, 19-20).

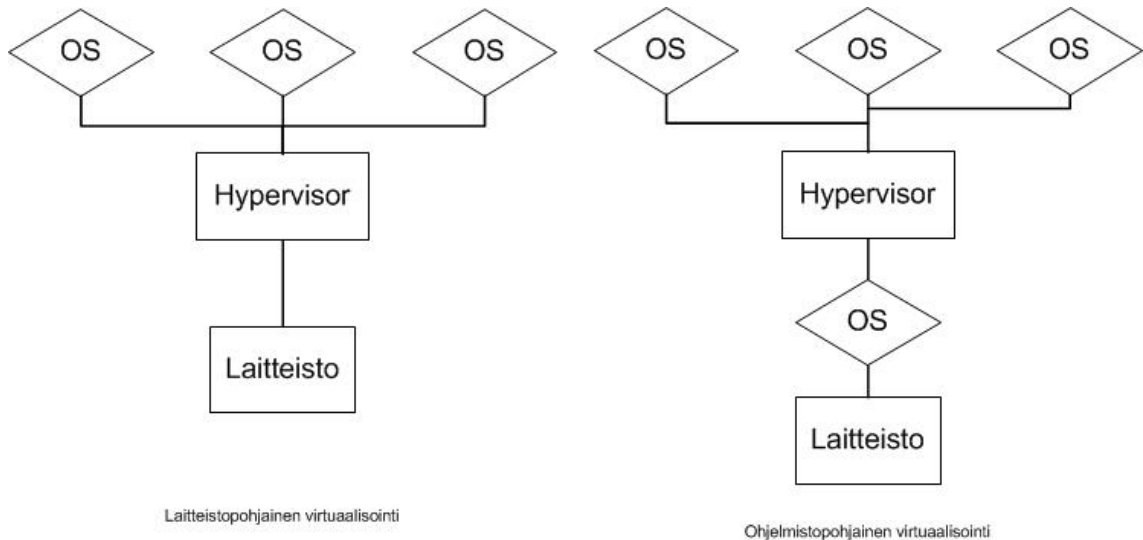
2.2 Virtuaalisointi

Virtuaalisoinnin tekniikan kehitys onkin isoin yksittäisistä pilvipalvelut mahdollistavista tekniikoista. Ilman virtuaalisointia ei olisi pilvipalveluita tarkoittaen, että pilvipalveluiden suurten resurssi- ja skaalautumistarpeiden takia näitä vaatimuksia ei pystytä fyysisillä laitteilla toteuttamaan kustannustehokkaasti. Virtuaalisointi tarkoittaa tekniikkaa, jolla jonkin fyysisen resurssin tekniset piirteet piilotetaan muilta järjestelmiltä, sovelluksilta ja loppukäyttäjiltä, jotka käyttävät näitä resursseja. Yksi fyysinen resurssi voi näkyä useana loogisena resurssina tai päinvastoin useampi fyysinen resurssi näkyy järjestelmille, sovelluksille ja loppukäyttäjille yhtenä. (Salo, 2010, 47.)

Isoin etu, joka virtuaalisoinnilla saavutetaan, on fyysisten resurssien käyttöasteen huomattava kasvu. Tämä kasvu johtaa säästöihin laitehankinnoissa ja energiakulutuksessa sekä nopeuttaa vikatilanteista selviämistä. Haittapuolena virtuaalisointi tuo yhden kerroksen lisää arkkitehtuuriin, joka heikentää järjestelmien tietoturva huomattavasti (Salo, 2010, 48). Tietoturvan heikkoudet kohdistuvat tämän fyysisen ja virtuaalisen resurssin väliin tulevan rajapinnan toimintaan (Heino, 2010, 60).

Virtuaalisoinnissa käytettävää rajapintaa kutsutaan nimellä *hypervisor*. Sana *hypervisor* on johdettu ohjelmistopuolella käytetystä sanasta *supervisor*, joka tarkoittaa ohjelmaa

joka hallitsee muita ohjelmia. *Hypervisor* on erittäin kevyt rajapinta ja se sijoittuu fyysisen laitteiston ja käyttöjärjestelmän väliin tai sitä ajetaan käyttöjärjestelmän osana. Yleisempi ja tehokkaampi sekä paremman yhteensopivuuden tarjoama käytäntö on ajaa *hypervisor* fyysisen laitteen ja käyttöjärjestelmän välissä (Heino, 2010, 60-61). Kuvassa 1 on esitetty laitteisto- ja ohjelmistopohjaisen virtuaalisoinnin toimintaperiaatteet.



Kuva 1. Laitteisto- ja ohjelmistopohjaisen virtuaalisoinnin toimintaperiaatteet

Isäntäkoneen (kone, joka toimii alustana virtuaalikoneille) resurssit voidaan tuoda virtuaalikoneille käytettäväksi kahdella tapaa: joko täytenä virtuaalisointina tai osittaisena eli niin sanottuna paravirtuaalisointina. Täydessä virtuaalisoinnissa käyttöjärjestelmä suoritetaan isäntäkoneella muuttumattomana. Osittaisessa virtuaalisoinnissa virtuaalikoneet käyttävät *hypervisorin* tarjoamaa API-rajapintaa (Application programming interface, ohjelmointirajapinta) ja kutsuu "hyperkutsuilla" laitteistopalveluita *hypervisorilta*. Virtuaalikoneen käyttöjärjestelmää pitää osittaisessa virtuaalisoinnissa muokata ja tämä asettaakin rajoituksia sen suhteen, mitä käyttöjärjestelmiä on mahdollista eri virtuaalisointitekniikoilla käyttää.

2.3 Palvelumallit

2.3.1 Julkinen pilvipalvelu

Julkinen pilvipalvelu on Internetissä käytettävä pilvipalvelu eli käytännössä ainoa, mitä käyttäjä julkisen pilvipalvelun käyttämiseen tarvitsee, on päätelaite ja Internet-yhteys. Useasti käytetään myös jonkinlaista VPN-yhteyttä (Virtual Private Network, yksityisverkko) liikenteen salaamiseen, mutta tämä ei ole pakollista palvelun toiminnan kannalta, sillä käyttäjän ja palveluntarjoajan välinen liikenne voidaan salata esimerkiksi

SSH:lla (Secure Shell, salattu verkkoliikenneprotokolla). Palvelu toteutetaan usein multitenant-ympäristössä eli useiden käyttäjien palveluita suoritetaan samalla laitteistolla. (Heino, 2010, 54-55.)

2.3.2 Yksityinen pilvipalvelu

Yksityinen pilvipalvelu toimii nimensä mukaisesti yksityisessä lähiverkossa tai muulla tapaa luotetuksi tehdyssä verkossa, kuten VPN-yhteydellä. Yksityisessä pilvipalvelussa ei siis välttämättä tarvita Internet-yhteyttä sen käyttämiseen (Heino, 2010, 55-56).

Jos yksityisen pilven koko infrastruktuuri, eli palvelin-, verkko- ja tallennuslaitteisto, on käyttäjän omissa tiloissa ja sen hallinnointi on kokonaan käyttäjän vastuulla, voidaan tästä pilvipalvelusta käyttää nimitystä sisäinen pilvipalvelu. (Salo, 2011, 32.)

2.3.3 Sovelletut pilvipalvelut

Yksityinen pilvipalvelu voidaan myös jakaa useammalle, mutta rajatuille, käyttäjäryhmille. Tällöin kyseinen pilvipalvelu on community cloud eli yhteisöpilvipalvelu. Pilveä käyttää siis useampi käyttäjäryhmä yhden sijaan, joka asettaa kovemmat vaatimukset alustan resursseille ja niiden jakamisen toteuttamiselle, mutta samalla myös jakaa kustannukset useammalle. (Heino, 2010, 56.)

Yhdistelemällä yksityistä ja julkista pilvipalvelua saadaan aikaiseksi hybridipilvipalvelu. Yksityinen pilvipalvelu, tai sen osia, yhdistetään tietoliikenneyhteyksien välityksellä julkiseen pilvipalveluun muodostaen näin hybridipilvipalvelun. Hybridipilvipalvelua voidaan käyttää esimerkiksi siten, että pilvipalvelun kehitysalusta on yksityinen pilvipalvelu ja käyttäjille tarjotaan julkista pilvipalvelua.

Muita pilvipalvelumalleja on *Wired*-lehden toimittajan Kevin Kellyn (2007) esittämä *intercloud*, pilvien pilvi. Intercloud-mallissa käyttäjät saivat kaikki palvelut pilvipalveluista. *Intercloud*-mallin erottaisi muista pilvipalveluista se, että tässä mallissa yksittäinen pilvipalvelu voisi tarvittaessa hyödyntää muiden pilvien resursseja, luoden illuusion rajoittamattomista resursseista.

Finnetin Supermatrix (2012) on pilvipalvelumalli, jossa käyttäjälle tarjotaan fyysinen kone palveluna. Tallennus-, muisti- ja laskentakapasiteetti on palveluntarjoajan palvelinsaleissa, joista sitä jaetaan käyttäjille nopeiden tietoliikenneyhteyksien ylitse. Käyttäjän ei siis tarvitse hankkia kallista ja tehokasta tietokonetta, vain pelkän näyttöpäätteet,

näppäimistö sekä hiiren. Nämä laitteet kytketään palveluntarjoajan antamaan linjamuuntimeen tai kevyeen Linux-koneeseen, joka on yhteydessä palvelinsalin resursseihin. Tämänkaltaisen palvelumallin isoin vaatimus on erittäin nopeat tietoliikenneyhteydet, kuten valokuituyhteys.

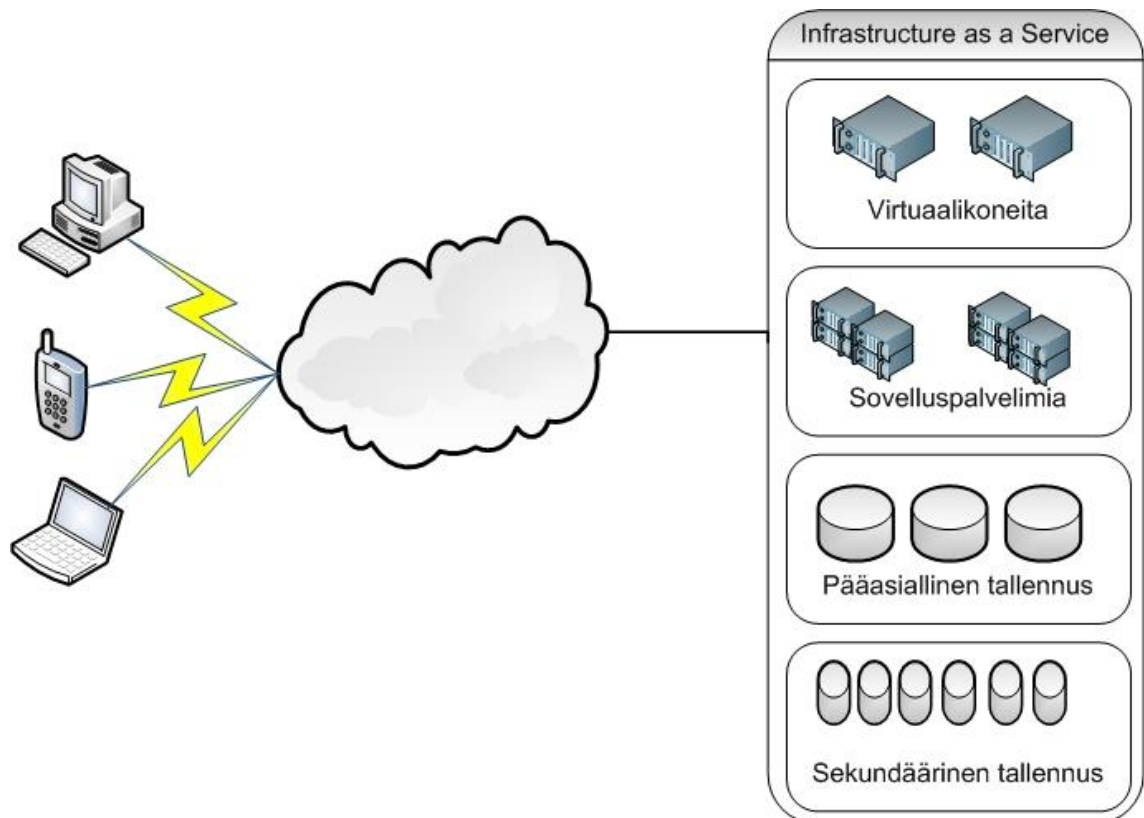
2.4 Palveluarkkitehtuurit

2.4.1 Infrastrukturi pilvipalveluna

IaaS-pilvipalvelussa (Infrastructure as a Service, infrastruktuuripilvipalvelu) tarjotaan käyttäjälle virtuaalista konesalia tai -saleja, joihin voidaan asentaa halutut ympäristöt. Yksinkertaisimmillaan käyttäjälle tarjotaan muisti-, prosessori-, ja tallennuskapasiteettia. Virtuaaliympäristön mahdollisuudet ja rajoitukset riippuvat käytetystä laitteistosta ja virtuaalisointitekniikoista.

Tämä pilvipalvelun tyyppi vaatii käyttöönotolta ja ylläpidolta eniten, sillä virtuaalikoneiden lisäksi hallittavana on itse pilvipalvelu, jonka kapasiteettia pitää tarpeen mukaan muuttaa. Itse fyysiseen laitteistoon ei käyttäjä pääse käsiksi, mutta pilvipalvelun resurssit ovat, palveluntarjoajasta riippuen, laajasti säädettävissä ja mukautettavissa (Salo, 2010, 26). Jos käyttäjä hankkii itse laitteiston, jonka päälle pilvipalvelu toteutetaan, niin tämä laitteiston ylläpito lisää ympäristön kokonaisylläpidon määrää. Pilvipalvelun hallinnan käyttöliittymissä on paljonkin eroja, sillä jotkut tarjoavat komentorivipohjaisia työkaluja toisten tarjotessa selainpohjaisia graafisia hallintatyökaluja.

Palveluntarjoajasta riippuen pilvipalvelun koneet voidaan liittää osaksi käyttäjän jo olemassa olevaa verkko, luoda pilvipalvelun koneille kokonaan oma verkko tai käyttää koneita Internetin yli. Tarjottava kapasiteetti voidaan tuottaa dedikoiduilla palvelimilla multitenant-mallin sijaan, mutta tällöin ei täyty Heinon (Heino 2010, 48) esittämien pilvipalvelun vaatimusten kohta kaksi. Kuvassa 2 on esitetty yksinkertaistettu kuvaus IaaS-pilvipalvelusta.

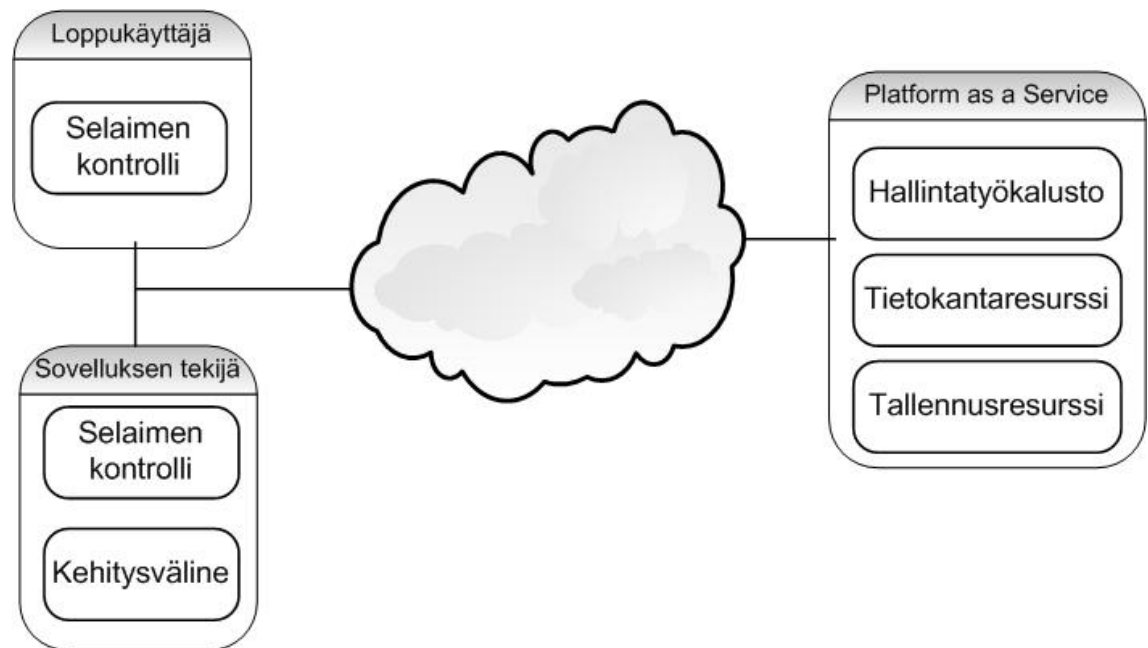


Kuva 2. IaaS-pilvipalvelun yksinkertaistettu toimintaperiaate

Tunnettuja kaupallisia IaaS-palveluja ovat Amazonin Web Services sekä Elisan eCloud. Elisan eCloud- sekä Amazonin Web Services -ympäristön hallinta tapahtuu selaimen avulla. Näistä palveluista Web Services on maailmanlaajuinen ja eCloud toimii pääasiassa vain Suomessa.

2.4.2 Alusta pilvipalveluna

PaaS-pilvipalvelussa (Platform as a Service, alusta pilvipalveluna) tarjotaan täysin virtuaalinen palvelinympäristö, josta käyttäjälle osoitetaan hänen haluamiaan palveluita. PaaS-ympäristössä käyttäjä hyödyntää ympäristön kapasiteettia ja työkaluja API-ohjelmointirajapinnan välityksellä ja tekee ympäristöä hyödyntävät sovellukset. Tämä pilvipalvelumalli sopii sellaisille käyttäjille, jotka osaavat itse tehdä tai pystyvät teettämään haluamansa sovellukset. Käytetyt rajapinnat ovat usein kevyitä ja tunnettuja mahdollisimman laajan ja ongelmattoman yhteensopivuuden saavuttamiseksi. Kuvassa 3 on esitetty PaaS-pilvipalvelun toimintaperiaate.



Kuva 3. PaaS-pilvipalvelun yksinkertaistettu toimintaperiaate

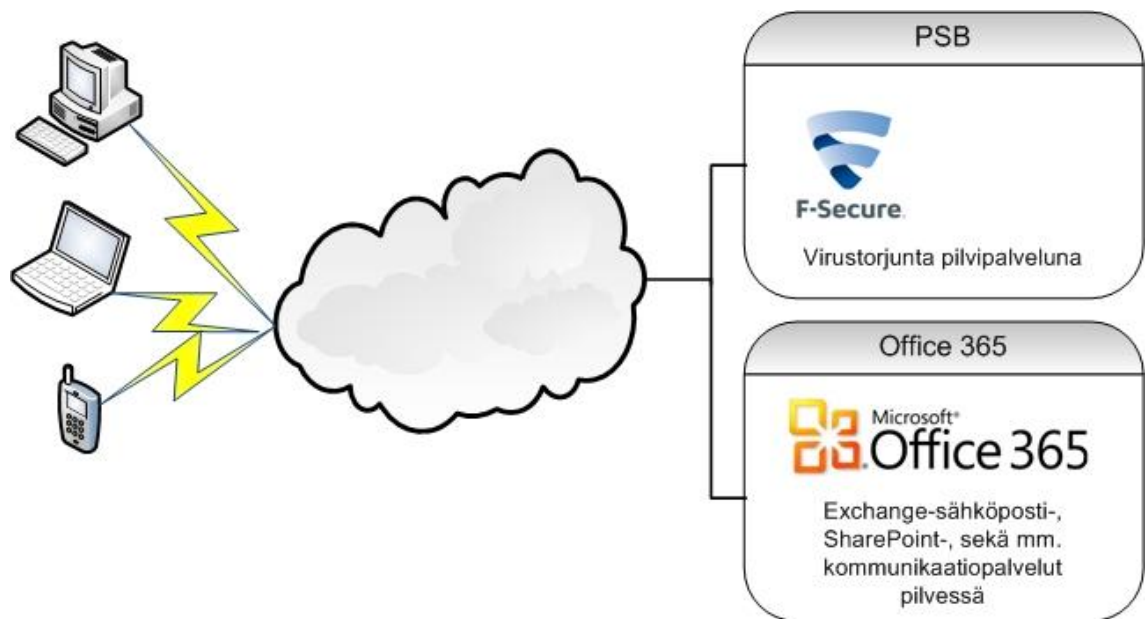
Esimerkkejä kaupallisista PaaS-ympäristöistä ovat Googlen AppEngine, Microsoftin Azure sekä Salesforceen Force.com -palvelut. Nämä palvelut tarjoavat monipuolisen rajapinnan pilvipalveluna omien sovellusten suorittamiseen.

2.4.3 Ohjelmisto pilvipalveluna

SaaS-pilvipalvelussa (Software as a Service, ohjelmisto pilvipalveluna) tarjotaan käytettävää ohjelmistoa pilvipalveluna paikallisten asennusten ja erilaisten alustojen sijaan. Ohjelmistopilvipalvelua käytetään perinteisesti selaimen kautta eli tietoliikenneyhteys, useimmiten Internet-yhteys, on käyttäjän ja palveluntarjoajan välillä pakollinen.

SaaS-pilvipalvelun etuna on sen helppous käyttäjälle, sillä sovellusta voidaan käyttää välittämättä sen laite- ja resurssivaatimuksista tai versiopäivityksistä ja niiden tuomista yhteensopivuusongelmista. Tämä etu vapauttaa käyttäjän resurssit varsinaiseen toimintaan ylläpidon sijaa ja tämä onkin SaaS-pilvipalveluiden tarkoitus, sillä ovat suunnattu liiketoimintaa ajatellen (Salo, 2010, 29).

SaaS-pilvipalveluiden tarjonta on kasvanut huomattavasti viime aikoina, sillä monet yritykset tarjoavat tuotteitaan perinteisten jakelumallien lisäksi myös SaaS-mallisenä palveluna. SaaS-pilvipalveluista onkin enemmän kyse palvelun tai ohjelmiston tarjoajan jakelutavan muutoksesta, kuin suoranaisesti laitteiston muutoksesta. Kuvassa 4 on esitetty SaaS-pilvipalvelun toimintaperiaate ja käytetty esimerkkinä kahta pilvipalveluiden tarjoajaa.



Kuva 4. Esimerkki SaaS-pilvipalveluista

Esitetyissä esimerkeissä käyttäjälle tarjotaan samat palvelut ja ohjelmistot, mitkä saisi-
vat asentamalla samat ohjelmistot käyttäjän omille palvelimille. F-Secure tarjoaa selain-
pohjaisen virustorjuntapalvelun, josta voidaan suorittaa samoja toimintoja kuin vastaa-
valla palvelintuotteella. Koska kommunikointi suojattavan koneen ja virustorjuntapalve-
lun välillä tapahtuu Internetin välityksellä, voidaan koneita hallita mistä vain. Perinteis-
essä mallissa, jossa virustorjunnan hallinta tapahtuu paikallisella palvelimella, pitää
hallittavan koneen olla samassa verkossa kuin palvelimen.

2.5 Pilvipalvelut, tietoturva ja -suoja

2.5.1 Pilvipalveluiden tietoturva

Pilvipalveluissa tietoturvan vaatimukset ei laitteiston puolella suuresti eroa "perinteisis-
tä" ratkaisuista, sillä käytettävä laitteisto, alustat ja sovellukset ovat pitkälti samoja, ai-
noastaan niiden sijainti ja saatavuus käyttäjän näkökulmasta. Koska pilvipalveluiden
käyttöliittymä on web-pohjainen, sen tietoturvavaatimukset eivät ole oleellisesti erilaiset
kuin perinteisessä web-palvelimessa. Palvelimet usein karaistaan eli poistetaan käytöstä
tarpeettomat järjestelmäpalvelut ja tietoliikenneportit, jolloin palvelimen tietoturvan ta-
so nousee huomattavasti. Tähän palvelinten kovettamiseen on erilaisia työkaluja, mutta
ylläpitäjän on tehtävä se usein käsin ja oman ammattitaidon varassa. Loppukäyttäjän

osalta käytettävien ohjelmistojen tietoturvapäivitykset tulevat käyttöön automaattisesti ja ilman toimintakatkoksia tai yhteensopivuusongelmia.

Pilvipalvelun ja Internetin, jos pilvipalvelua käytetään Internetin välityksellä, välissä on palomuri ja hyvin usein myös IDS (Intrusion Detection System, tunkeutumisen havaitsemisjärjestelmä) tai jopa IDPS (Intrusion Detection and Prevention System, tunkeutumisen havaitsemis- ja estojärjestelmä) suojaamassa verkkoa ei toivotulta verkkoliikenteeltä.

Tietoturvan riskit ovat pilvipalveluiden käyttötavasta johtuen hieman erilaiset, kuin mitä esimerkiksi omissa tiloissa sijaitsevalla palvelimella. Isoin riski on tietoliikenneyhteyksien katkeaminen, sillä se pysäyttää Internetin kautta käytettävien pilvipalveluiden käytämisen täysin. Tätä riskiä voi pienentää hankkimalla esimerkiksi useamman tietoliikenneyhteyden eri operaattoreilta. Ylläpidolliset virheet pilvipalvelun tarjoajan puolelta ovat todennäköisiä riskejä ja näihin virheisiin käyttäjä ei voi vaikuttaa. Muut erityiset riskit liittyvät joko pilvipalveluntarjoajan toiminnan loppumiseen tai heidän laitteiston tuhoutumiseen luonnonmullistuksen tai muun katastrofin seurauksena.

2.5.2 Tietosuoja pilvipalveluissa

Koska pilvipalveluissa laitteistot, tai osa niistä, saattavat sijaita eri puolilla maailmaa, aiheuttaa se hankalan tilanteen tietosuojan kannalta. Eri maiden erilaiset lait määrittelevät käytännöt miten tallennettua tietoa pitää säilyttää ja miten sitä saa käsitellä sekä mitä tietoa saa ylipäättään tallentaa. Tietojen vuotaminen on iso riski ja vaadittavan tietosuojan tarjoaminen on hankalaa juuri erilaisten käytäntöjen takia.

Joissakin maissa viranomaisilla, kuten Ruotsissa, on oikeus salakuunnella verkkoliikennettä omassa maassaan ilman erillistä lupaa (Salminen, J. 2009). Salakuuntelusta aiheutuvan ongelman voi ratkaista kryptaamalla kaiken datan. Ongelmana kryptauksessa on se, että tämä jää usein käyttäjän vastuulle, sillä pilvipalveluntarjoaja ei kryptausta tarjoa. Kryptaus vaatii aina salausavaimen, jolla data kryptataan. Palveluntarjoaja ei tätä avainta voisi pitää hallussaan, koska kyseinen toimintatapa ei takaisi tietojen salausta, koska silloin sekä kryptattu data että datan salausavain olisivat pilvipalveluntarjoajan hallussa. Kryptaukseen erikoistuneita yrityksiä on, jolloin salausavainten huolehtiminen siirtyy tämän yrityksen vastuulle. Tästä on kuitenkin seurauksena käyttökustannusten nousu ja datan purkamisen monimutkaistuminen.

3 TOTEUTETTU YMPÄRISTÖ

3.1 IaaS-pilvipalvelun perusrakenne

Infrastruktuuripilvipalvelun perusrakenne on samanlainen riippumatta siitä, minkä valmistajan tuotteista on kysymys. Tämä perusrakenne on selvitetty vertailemalla eri valmistajien tuotteita keskenään. Vertailuun käytettiin kahta kaupallista (VMware vCloud ja Microsoft System Center Virtual Machine Manager) ja yhtä vapaan lähdekoodin (Xen Cloud Platform) ratkaisua. Havaitut peruskomponentit ovat esitetty taulukossa 1.

Komponentti	Komponentin toimenkuva
Virtuaali-isäntä	Antavat virtuaalirajapintansa resurssit pilven käyttöön
Virtuaali-isäntien hallintapalvelin	Hallitsee kaikkia pilvipalveluun liitettyjä virtuaali-isäntiä
Tietokantapalvelin	Tallentaa pilvipalvelun eri tietoja riippuen käytettävistä sovelluksista
Hallintapalvelimen hallintatyökalu	Tällä hallitaan pilvipalvelun laitteistoa ja määritellään pilvipalvelun toimintoja
Pilvipalvelun käyttöliittymä	Toimii loppukäyttäjän käyttöliittymänä pilvipalveluun

Taulukko 1. IaaS-pilvipalveluiden peruskomponentit

Näillä komponenteilla on valmistajakohtaisia tuotenimiä, mutta kaikkien toimintaperiaate on samanlainen. Riippuen valmistajan rajoituksista, niin kaikki peruskomponentit voidaan asentaa yhdelle fyysiselle palvelimelle, joten jokaiselle toiminnolle ei tarvitse hankkia omaa fyysistä laitetta. Tietokantapalvelimena voidaan käyttää erilaisia ratkaisuja, riippuen valmistajasta, mutta se ei ole rajattu tietyn tyyppiseen palvelimeen. Tällä helpotetaan pilvipalvelun rakentamista ympäristöihin, joissa tietokantapalvelin on jo olemassa ja ei haluta luoda uutta.

3.2 Toteutetun pilvipalvelun osat

Pilvipalvelualustan tekniikoiden valinnassa päädyttiin Microsoftin tuotteisiin, koska toimeksiantajan ympäristö on pääasiassa toteutettu Microsoftin System Center -tuotteilla. Edut käytettäessä System Center -tuotteita:

- Yhteensopivuus muiden ympäristön osien kanssa.
 - Virtuaalisoinnissa käytetään Hyper-V-teknologiaa.
 - Palvelimet ovat Windows Server 2008 R2.
 - Virtuaalisoitavat koneet ovat pääasiassa Windows-koneita.
- Toimintaympäristö on tuttu.
- Laaja tuki.
- Kattavat ja ajantasaiset dokumentaatiot.

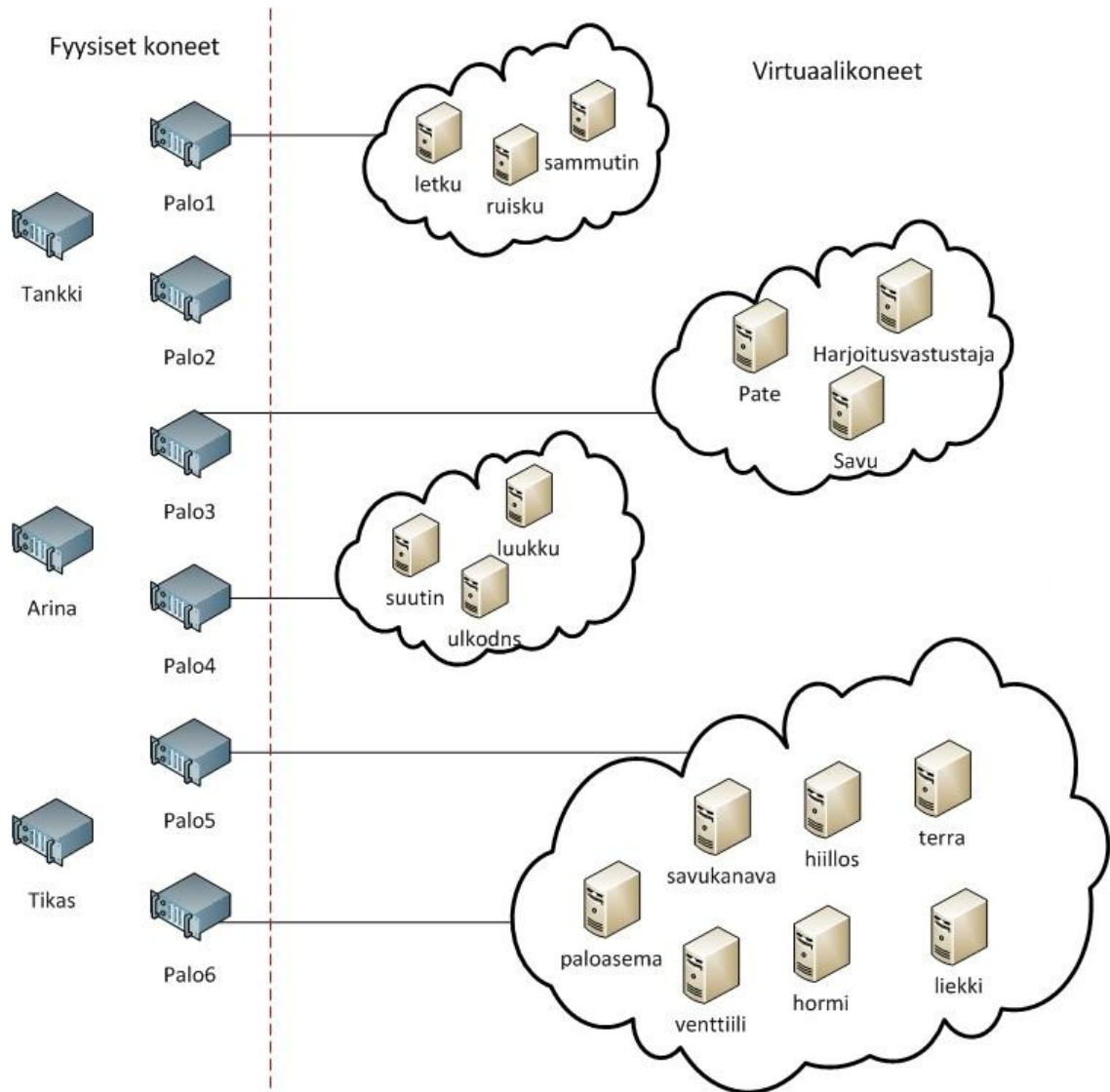
Kohdassa 3.1 esitetyt IaaS-pilvipalvelun yleisiä osia vastaavat nimitykset Microsoftilla ovat (Microsoft Corporation, 2010) esitetty taulukossa 2:

Komponentti	Microsoft-tuote
Virtuaali-isäntä	Hyper-V ja System Center Virtual Machine Manager Agent, SCVMM Agent
Virtuaali-isäntien hallintapalvelin	System Center Virtual Machine Manager, SCVMM
Tietokantapalvelin	Useita vaihtoehtoja, työssä käytettiin SQL Server 2005 Express
Hallintapalvelimen hallintatyökalu	System Center Admin Console
Pilvipalvelun käyttöliittymä	System Center Virtual Machine Manager Self-Service Portal, SCVMM SSP

Taulukko 2. Microsoft IaaS-pilvipalvelun osat

3.3 WPK-verkon alkutilanne

WPK-verkko koostuu muutamista fyysisistä palvelimista ja useista virtuaalipalvelimista. Tarkempi palvelinten määrä ja roolit on kerrottu kuvassa 5.



Kuva 5. WPK-verkon fyysiset ja virtuaaliset palvelimet

Fyysisten ja virtuaalisten palvelinten roolit ovat esitetty kuvassa 6.

Koneiden roolit		
Fyysiset palvelimet	Virtuaalipalvelimet	
Palo1	Letku	Paloasema
-DHCP	-OCS	-F-Secure
-WDS		
-Print Service	Ruisku	Savukanava
-MS SQL Server 2008 R2	-OCS	-Vanha Share
Palo2	Sammutin	Hiillos
-DHCP	-LAMP	-SCMM
-NPS		
-vara-DC	Pate	Terra
Palo3	-Exchange 2010	-Linux
-DC	Savu	Venttiili
-sisäDNS	-IIS	-TFTP
Palo4	Harjoitusvastustaja	-Cisco-ympäristöä
-DC	-Windows 7	Hormi
-sisäDNS		-SharePoint 2010
Palo5	Luukku	Liekki
-Virtualisointiklusteri	-NPS	-Windows 7
	-CertServer	
Palo6	Suutin	
-Virtualisointiklusteri	-OCS	
Tankki	UlkoDNS	
-WSUS	-ulkoDNS	
Arina		
-Linux		
Tikas		
-VPN		

Kuva 6. WPK-verkon palvelinten roolit

WPK-verkko on pääasiassa TAMKIn tietojenkäsittelyn opiskelijoiden käytössä ja verkossa järjestetään opetusta, niin verkon muut toiminnot eivät saaneet pilvipalvelun rakentamisesta häiriintyä. Toimeksiantaja antoi tiukat rajaukset palvelinten resurssien käytöstä ja pilvipalvelun rakentamiseen saatiin käyttöön vain kaksi fyysistä palvelinta, joilla oli myös muita virtuaalisoituja koneita.

Käyttöön saadut palvelimet olivat Palot5 ja Palo6. Nämä palvelimet ovat klusteroitu virtuaalisoinnin osalta eli niiden virtuaalisointiin käytettävät resurssit näkyvät yhtenä kokonaisuutena. Muut palvelimet eivät joko soveltuneet pilvipalvelun virtuaalisointisännäksi tai niiden roolit olivat liian tärkeitä WPK-verkon toiminnalle, jotta niiden resursseja voitaisiin käyttää pilvipalvelussa.

3.4 Pilvipalvelun rakentaminen

Pilvipalvelun luomisella pyrittiin saamaan aikaiseksi palvelinalusta, joka voitaisiin ottaa nopeasti käyttöön ja sen uudelleen asentaminen olisi erittäin nopeaa. Näitä ominaisuuksia tarvittaisiin etenkin palvelinkursseilla, jossa koneita muokataan opiskelun aikana ja

ympäristön uudelleen asentamiseen on työlästä fyysisillä laitteilla. Fyysisten laitteiden uudelleen asentamisen sijaan laitteet voitaisiin palauttaa nopeasti alkuperäiseen tilaan.

Pienen koon takia pilvipalvelun palvelinkomponentit asennettiin yhdelle palvelimelle, koska useammalle palvelimelle asentamisessa ei tämän kokoisessa ympäristössä saavuteta mitään etua. Pilvipalvelun komponenttien laitteistovaatimukset ovat kerrottu liitteessä 1. Molemmat käyttöön saadut palvelimet ovat identtisiä ja niiden kokoonpano ylittää reilusti Microsoftin asettamat laitteistovaatimukset:

- Prosessori: 2kpl, Intel® Xeon® 2 GHz tuplaytimellä (x64)
- RAM-muisti: 22 GB
- Massamuisti: >1TB

Palveluiden osat vaativat käyttäjätunnuksen, jolla on järjestelmänvalvojan oikeudet kaikille pilvipalveluun liitetyille virtuaali-isännille, tietokanta- tai hallintapalvelimille. Koska käytössä oli vain osa WPK-verkon palvelimista, luotiin käyttäjä *wpk_sccm* jolle annettiin paikalliset järjestelmänvalvojan oikeudet pilvipalveluun liitetyille palvelimille.

3.4.1 IaaS-pilvipalvelun osien asennus

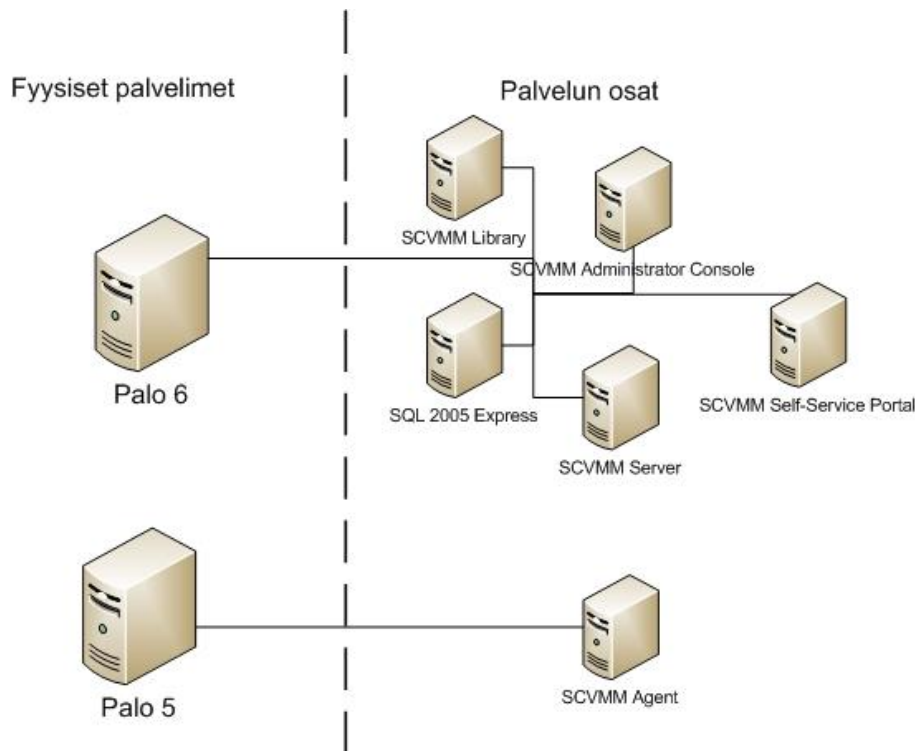
Ensimmäisenä asennettiin virtuaali-isännät. Edellä esitetystä kuvasta 6 selviää, että palvelimet Palo5 ja Palo6 ovat virtuaali-isäntiä. Tästä johtuen Hyper-V-rajapintaa ei palvelimille tarvitse asentaa, mutta Palo5:lle asennettiin SCVMM Agent, joka kommunikoi Palo 5:n ja virtuaali-isäntien hallintapalvelimen välillä. Palo6:lle ei asennettu SCVMM Agent -komponenttia, koska siihen asennetaan SCVMM Server ja SCVMM Server sisältää SCVMM Agent -komponentin toiminnot.

Seuraavaksi asennettiin Palo6:lle virtuaali-isäntien hallintapalvelin, SCVMM. Hallintapalvelimen ohjelmistovaatimukset löytyvät liitteestä 1. Hallintapalvelimen asennus vaatii tietokantapalvelimen ja tämä asennettiin samalla Palo6:n hallintapalvelimen asennuksen yhteydessä. Tietokantapalvelimeksi asennettiin Microsoftin SQL Server 2005 Express, joka sopii yhden hallintapalvelimen pilvipalveluun hyvin keveyden ja asennuksen helppouden johdosta.

Hallintapalvelimen hallintatyökalu, SCVMM Admin Console, asennettiin Palo6:lle. SCVMM Admin Console voidaan asentaa mille tahansa koneelle, sillä se kommunikoi hallintapalvelimen kanssa verkon välityksellä. SCVMM Admin Consolea käytetään ko-

ko pilvipalvelun hallintaan. Sen avulla muun muassa lisätään uusia virtuaali-isäntiä, laske-
 kenta-
 resursseja, luodaan virtuaalikoneita sekä hallitaan käyttäjien ja käyttäjäryhmien
 oikeuksia pilvipalvelussa. Hallintakonsoli asennettiin Palo6:lle sen takia, koska ympä-
 ristön työasemia asennetaan säännöllisen väliajoin uusiksi ja tällöin se pitäisi asentaa
 jokaisen uudelleenasetuksen yhteydessä.

Ympäristön koon pienyydestä johtuen myös pilvipalvelun käyttöliittymä asennettiin Pa-
 lo6:lle. Pilvipalvelun käyttöliittymä käyttää alustanaan Microsoft Internet Information
 Services 7 -palvelua (IIS), joten tämä asennettiin ennen käyttöliittymäkomponentin
 asennusta. Kuvassa 7 esitellään pilvipalvelun fyysiset palvelimet ja niille asennetut roo-
 lit.



Kuva 7 - Pilven palvelimet ja niille asennetut komponentit

3.4.2 Asetusten teko

SCVMM Server ja sen tietokantapalvelin asennettiin käyttäen oletusasetuksia, niin tie-
 tokannan kuin SCVMM Serverin käyttämän kirjaston suhteen. Ainoa itse määritelty
 asetus oli kirjaston käyttämä levytila. Komponenttien oletusarvojen muuttamisella
 asennuksen yhteydessä ei nähty tarvetta. Levytilaksi määritettiin Palo5:n ja Palo6:n yh-
 teinen, virtuaalikoneille tarkoitettu, verkkolevy. Palo5 ja Palo6 asetettiin toimimaan pil-
 vipalvelun virtuaali-isäntinä. Koska palvelimet ovat asetettu toimimaan klusterissa

WPK-verkon vaatimusten tähden, niin niiden resurssit näkyvät yhtenä kokonaisuutena kahden erillisen palvelimen sijaan.

Pilvipalvelun käyttöliittymä asetuksiin kuuluvat palvelun osoitteen määrittely sekä käyttäjiryhmien luonti ja käyttöoikeuksien asettaminen. Pilvipalvelun käyttöliittymän verkkosivuston osoitteeksi asetettiin pilvi.wpk.tpu.fi. Palvelun tietoturvan lisäämiseksi sivusto pakotettiin käyttämään SSL-yhteyttä. Käyttäjiryhmiä luotiin kaksi: pilvikäyttäjät ja pilviadminit. Pilvikäyttäjät-ryhmään lisättiin WPK-verkon toimialueen kaikki käyttäjät. Pilviadmin-ryhmään lisättiin WPK-verkon toimialueen järjestelmänvalvojaoikeudet omaavat käyttäjät. Taulukossa 3 on esitetty näiden kahden käyttäjiryhmän oikeudet pilvipalvelussa.

Toiminto	Pilvikäyttäjät	Pilviadminit
Virtuaalikoneen käynnistys	Sallittu	Sallittu
Virtuaalikoneen pysäytys	Sallittu	Sallittu
Virtuaalikoneen keskeytys	Sallittu	Sallittu
Virtuaalikoneen sammutus	Sallittu	Sallittu
Tarkastuspisteen luonti	Ei sallittu	Sallittu
Virtuaalikoneen varastointi	Ei sallittu	Sallittu
Varastoidun koneen käyttöönotto	Ei sallittu	Sallittu
Virtuaalikoneen poisto	Ei sallittu	Sallittu
Virtuaalikoneeseen yhdistäminen	Sallittu	Sallittu
Etätyöpöytäyhteyden luonti virtuaalikoneeseen	Sallittu	Sallittu

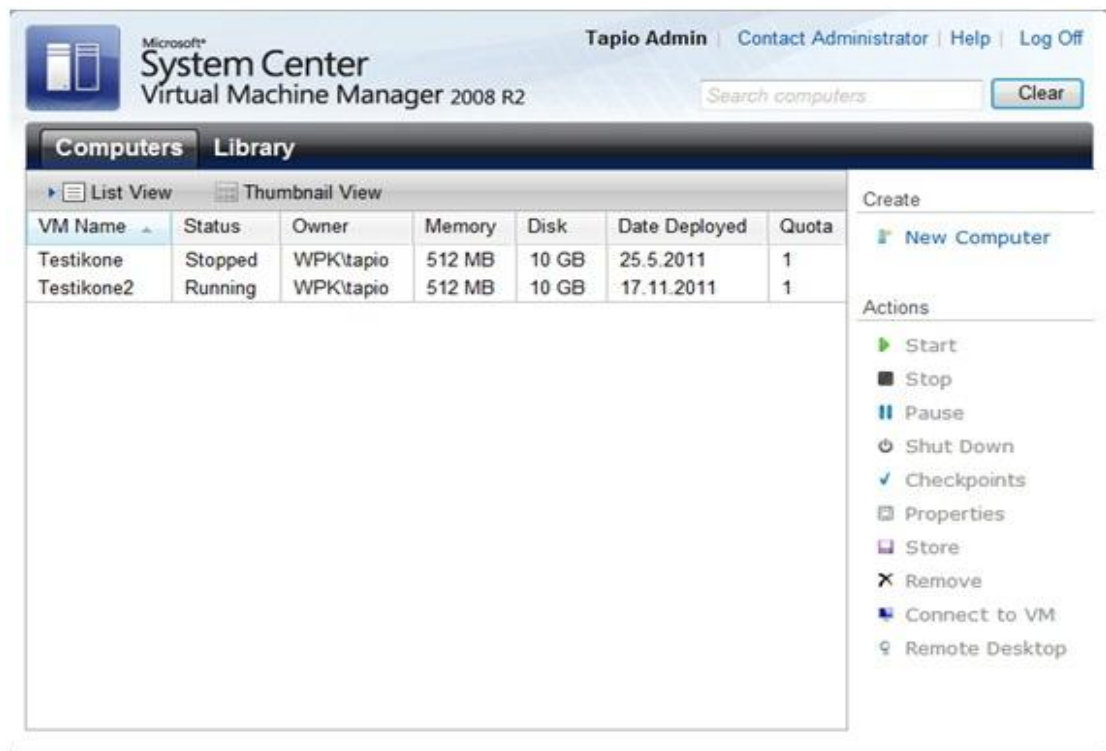
Taulukko 3. Käyttäjiryhmien oikeudet.

Pilvipalveluiden virtuaalikonepohjaksi luotiin yksi Windows 7 -käyttöjärjestelmällä varustettu virtuaalikone. Muistin määräksi ja prosessori tehoksi asetettiin Windows 7 mi-

nimivaatimuksia vastaavat arvot, koska pilvipalveluiden resurssit ovat erittäin rajalliset. Samalla asetettiin kiintiö sille, kuinka monta konetta pilvikäyttäjät voivat itselleen tehdä. Määräksi asetettiin kaksi konetta käyttäjää kohden.

3.4.3 Valmiin pilvipalvelun toiminnan testaus

Pilvipalvelun toiminnan varmistamiseksi palveluun kirjauduttiin sekä pilvikäyttäjänä, että pilviadmininä. Kirjautumisen jälkeen pilvipalveluun luotiin uusi kone ja luomisen jälkeen testattiin sen toimivuus. Käyttöoikeuksien rajoitteet testattiin yrittämällä suorittaa käyttäjältä kiellettyä toimintoa. Samalla testattiin virtuaalikoneiden kiintiö. Kuvassa 8 näkyy pilvipalvelun käyttöliittymä.



Kuva 8 - Pilvipalvelun käyttöliittymän avausnäky

Kun pilvipalvelun toimivuus varmistettiin, ilmoitettiin tästä toimeksiantajalle ja pyydettiin häntä testaamaan palvelun toimintaa. Toimeksiantajan palautteen perusteella pilvipalvelu todettiin toimivaksi ja luovutettiin toimeksiantajan hallintaan.

4 JOHTOPÄÄTÖKSIÄ JA POHDINTA

4.1 Työn onnistuminen

Työssä annetaan kattava peruskuva erilaisista pilvipalveluista ja niiden tietoturvasta. Jos eri pilvipalveluita olisi lähdetty käsittelemään laajemmin, niin se olisi ollut jo oman opinnäytetyönsä aihe. Etenkin tietosuojaa käsittelevästä osiosta olisi saanut paljon laajemman käsittelemällä Suomen tietosuojalakeja ja vertaamalla niitä esimerkiksi isoimpien palveluntarjoajien käyttämiin tietosuojaperiaatteisiin ja täten pilvipalvelun edut laajojen ympäristöjen alustana ei päässyt oikeuksiinsa. Pilvipalveluiden esittelyä olisi voinut kohdistaa enemmän yritys- tai kuluttajälähtöiseksi yleisen esittelyn lisäksi.

Toimeksiantajalle toteutettu ympäristö vastasi annettuja vaatimuksia, mutta sen käyttökelpoisuus jäi kyseenalaiseksi rajoitettujen resurssien takia. Toimeksiantajan rajaus käytettävien tuotteiden kohdalla oli myös iso takaisku, sillä vertailu esimerkiksi VMwaren vastaavien tuotteiden välillä olisi tuonut työhön paljon lisää. VMware on käytetyin virtuaalisointiympäristö maailmassa (Hess. 2010).

4.2 Toimeksiantajan ympäristön puutteet, rajoitukset ja kehitysehdotukset

4.2.1 Puutteet ja rajoitukset

WPK-ympäristössä isoimmaksi puutteeksi nousi palvelinten tarjoamat rajalliset resurssit. Tämä johtui pitkälti siitä, että palvelimilla pyöritetään muun toiminnan vaatimia virtuaalikoneita sekä erilaisia palveluita. Myös käytävissä olevien palvelinten rajaaminen kahteen fyysiseen palvelimeen supisti resursseja huomattavasti.

Miksi kaikkia palvelimia ei sitten voitu hyödyntää? Tämä johtui osittain toimeksiantajan ja osin ympäristön rajoitteista. Toimeksiantaja kielsi käyttämästä palvelimia Palo3 ja Palo4, sillä ne olivat verkon domain controllerit, ne hoitavat ympäristön keskitetyn käyttäjähallinnan, ja näiden palvelinten toimintavarmuutta ei haluttu riskeerata ottamalla niitä pilvikäyttöön.

WPK-ympäristön kahden muun palvelimen, Palo1 ja Palo2, resurssit olivat lähes kaikki jo käytössä, joten niitä ei päästy hyödyntämään pilven resursseina. Myös nämä palvelimet sisälsivät joitain erittäin tärkeitä ympäristön palveluja, joten niiden toimintavarmuuden riskeeraaminen ei ollut toivottua.

Käyttöliittymän yksinkertaisuus teki pilvipalvelun yksityiskohtaisemman hallinnan mahdottomaksi selainpohjaisesti. Käyttöliittymässä ei ole eri näkymiä käyttäjätason mukaan, vaan kaikki käyttävät samaa näkymää ja ainoastaan toiminnot ovat rajoitettu käyttäjäoikeuksien mukaan. Kaikki hallinta joudutaan tekemään hallintapalvelimelta käyttämällä erillistä hallintatyökalua.

4.2.2 Kehitysehdotukset

Pilvipalvelun toiminnan saattamiseksi sellaiseen kuntoon, että sillä voisi toteuttaa palvelinkurssien vaatimia ympäristöjä, vaatisi huomattavasti enemmän prosessori-, muisti- ja kovalevykapasiteettia. Tässä tulisi siis kyseeseen oma, pelkästään pilvipalvelun käyttöön tarkoitettu palvelinklusteri. Näin voitaisiin taata pilvipalvelulle riittävät resurssit ja sen häiriötön ja vikasietoinen toiminta.

Toinen ympäristön suurempi kehittämiskohde olisi sen käyttöliittymä. Tässä voitaisiin joko käyttää Microsoftin tarjoamaa SCVMM SSP 2.0 versiota tai tehdä koko käyttöliittymä itse. SSP:n veriossa 2.0 on laajemmat työkalut ympäristön hallintaan muun muassa mahdollistamalla erilaiset organisaatio- ja osastojaot, joille voidaan eriyttää omia osia pilvipalvelusta. Tämä tietysti vaatisi huomattavasti enemmän asennus- ja käyttöönotto-toimenpiteitä.

Jos käyttöliittymä tehtäisiin itse, niin siitä pystyttäisiin muokkaamaan toimeksiantajan käyttötarpeisiin parhaiten sopiva. Tämä vaihtoehto olisi kaikista työläin, mutta sen tulokset olisivat, työn onnistuessa, antoisimmat.

LÄHDELUETTELO

Heino, P. 2010. Pilvipalvelut. Talentum.

Olzak, T., Boomer, J., Keefer, R., Sabovik, J. 2010. Microsoft Virtualization. Burlington, USA. Syngress.

Salo, I. 2010. Cloud computing - palvelut verkossa. WSOYpro.

Salminen, J. 2009. Ruotsi aloitti verkkoliikenteen salakuuntelun: Mitä pitää tehdä ja tietää? Suomenkuvalehti.fi

Microsoft Corporation. 2010. Virtual Machine Manager 2008 R2 Deployment Guide. Luettu 20.4.2011

<http://technet.microsoft.com/en-us/library/cc917964.aspx>

Architecting a VMware vCloud. Version 2.0.1. 2011. VMware. Luettu 21.2.2012

<http://www.vmware.com/files/pdf/vcat/Architecting-VMware-vCloud.pdf>

Xen Cloud Platform Project. Luettu 21.2.2012

<http://xen.org/products/cloudxen.html>

F-Secure PSB - Aloitusopas. Luettu 25.2.2012

http://www.f-secure.com/system/fsgalleries/brochures/fpspb_gsg_pws_fin.pdf

Kelly, K. 2007. A Cloudbook for the Cloud. Luettu 24.2.2012

http://www.kk.org/thetechnium/archives/2007/11/a_cloudbook_for.php

Finnet Supermatrix. Tietotekniikan mahdollisuudet vaivattomina palveluina. Tallennettu 26.2.2012. <http://www.supermatrix.fi/jt3/index.php/projektin-esittely/projektin-ideat-paehkineaenkuoressa>

Hess, K. 2010. Top 10 Virtualization Technology Companies Luettu 21.2.2012

<http://www.serverwatch.com/trends/article.php/3877576/Top-10-Virtualization-Technology-Companies.htm>

LITTEET

Liite 1 Microsoft Corporation. 2010. Virtual Machine Manager 2008 R2 Deployment Guide.

Liite 1: 1 (5)

Self-Service Portal System Requirements

This section provides the minimum hardware and software requirements required for the self-service portal, whether you are installing all of the components on a single computer or distributing them across multiple computers. This section also indicates whether each component has any special hardware or software configuration requirements.

System Requirements: Single-Machine Deployment Scenario

As described previously, the single-machine deployment scenario requires installing all three VMMSSP components on a computer that is running the VMM Administrator Console and SQL Server 2008.

Hardware Requirements

The following table provides the minimum and recommended hardware requirements for a single-machine deployment.

Table 4. Required Hardware for a Single-Machine Deployment Scenario

Hardware Component	Minimum	Recommended
RAM	2 GB	4 GB
Available hard disk space	50 GB	50 GB

Software Requirements

Before you install the VMMSSP website component, install and configure the following software on the computer.

Table 5. Required Software for a Single-Machine Deployment Scenario

Software	Comments
Operating System: Windows Server® 2008 R2	Windows Server 2008 R2 Enterprise Edition and Windows Server 2008 R2 Datacenter Edition are supported.
Windows Server Internet Information Services (IIS) 7.0	<p>You must add the Web server role (IIS) and then install the following role services:</p> <ul style="list-style-type: none"> • Static Content • Default Document • ASP.NET • .NET Extensibility • ISAPI Extensions • ISAPI Filters • Request Filtering • Windows Authentication • IIS 6 Metabase Compatibility <p>Turn off Anonymous authentication. For more information, see Configure Windows Authentication in the IIS documentation.</p> <p>Use IIS v6.0 compatibility mode.</p>
Microsoft .NET Framework 3.5 SP1	Use Server Manager's Add Features wizard to add the .NET Framework 3.5 SP1 features.
Windows PowerShell 2.0	<p>Important If your extensibility scripts require specific Windows PowerShell snap-ins, install them when you install the VMMSSP server component. For information about extending the self-service portal with scripts, see the <i>Virtual Machine Manager Self-Service Portal 2.0 SP1: Extensibility Guide</i>.</p>
Message Queuing (also known as MSMQ)	<p>Use Server Manager's Add Features wizard to add Message Queuing.</p> <p>For more information, see What is Message Queuing? in the Windows Server 2008 R2 online documentation.</p>
VMM 2008 R2 Administrator Console	For more information about installing the VMM 2008 R2 Administrator Console, see the Virtual Machine Manager Deployment Guide .
SQL Server 2008	<p>You can use any of the following editions of SQL Server:</p> <ul style="list-style-type: none"> • SQL Server 2008 Enterprise (64-bit). • SQL Server 2008 R2 Enterprise (64-bit). • SQL Server 2008 R2 Datacenter (64-bit). • SQL Server 2008 Standard (64-bit). • SQL Server 2008 R2 Standard (64-bit).

System Requirements: VMMSSP Website Component

This section lists the hardware and software required for the VMMSSP website component if you install it on a dedicated web server.

Hardware Requirements

The following table provides the minimum and recommended hardware requirements for the VMMSSP website component.

Table 6. Required Hardware for the VMMSSP Website Component

Hardware Component	Minimum	Recommended
RAM	2 GB	4 GB
Available hard disk space	50 MB	2 GB

Software Requirements

Before you install the VMMSSP website component, install and configure the following software on the web server.

Table 7. Required Software for the VMMSSP Website Component

Software	Comments
Operating System: Windows Server 2008 R2	Windows Server 2008 R2 Enterprise Edition and Windows Server 2008 R2 Datacenter Edition are supported.
Windows Server Internet Information Services (IIS) 7.0	<p>You must add the Web server role (IIS) and then install the following role services:</p> <ul style="list-style-type: none"> • Static Content • Default Document • ASP.NET • .NET Extensibility • ISAPI Extensions • ISAPI Filters • Request Filtering • Windows Authentication • IIS 6 Metabase Compatibility <p>Turn off Anonymous authentication. For more information, see Configure Windows Authentication in the IIS documentation.</p> <p>Use IIS v6.0 compatibility mode.</p>
Microsoft .NET Framework 3.5 SP1	Use Server Manager's Add Features wizard to add the .NET Framework 3.5 SP1 features.

System Requirements: VMMSSP Server Component

This section lists the hardware and software required for the VMMSSP server component if you install it on a computer that is dedicated to the self-service portal and the VMM Administrator Console.

Hardware Requirements

The following table provides the minimum and recommended hardware requirements for the VMMSSP server component.

Table 8. Required Hardware for the VMMSSP Server Component

Hardware Component	Minimum	Recommended
RAM	2 GB	4 GB
Available hard disk space	50 MB	2 GB

Software Requirements

Before you install the VMMSSP server component, install and configure the following software on the computer that will run the server component.

Table 9. Required Software for the VMMSSP Server Component

Software	Comments
Operating System: Windows Server 2008 R2	Windows Server 2008 R2 Enterprise Edition and Windows Server 2008 R2 Datacenter Edition are supported.
Microsoft .NET Framework 3.5 SP1	Use Server Manager's Add Features wizard to add the .NET Framework 3.5 SP1 features.
Windows PowerShell 2.0	Important If your extensibility scripts require specific Windows PowerShell snap-ins, install the snap-ins with the server component. For information about extending the self-service portal with scripts, see the <i>Virtual Machine Manager Self-Service Portal 2.0 SP1: Extensibility Guide</i> .
Message Queuing (also known as MSMQ)	Use Server Manager's Add Features wizard to add Message Queuing. For more information, see What is Message Queuing? in the Windows Server 2008 R2 online documentation.
VMM 2008 R2 Administrator Console	Install the VMMSSP server component on a computer that already has the VMM Administrator Console installed. For more information about installing the VMM 2008 R2 Administrator Console, see the Virtual Machine Manager Deployment Guide .

System Requirements: VMMSSP Database Component

This section lists the hardware and software required for the VMMSSP database component if you install it on a dedicated SQL Server computer.

Hardware Requirements

The following table provides the minimum and recommended hardware requirements for the VMMSSP database component.

Table 10. Required Hardware for the VMMSSP Database Component

Hardware Component	Minimum	Recommended
RAM	2 GB	4 GB
Available hard disk space	50 GB	50 GB

Software Requirements

Before you install the VMMSSP database component, install and configure the following software on the SQL Server computer.

Table 11. Required Software for the VMMSSP Database Component

Software	Comments
Operating System: Windows Server 2008 R2	Windows Server 2008 R2 Enterprise Edition and Windows Server 2008 R2 Datacenter Edition are supported.
SQL Server 2008	You can use any of the following editions of SQL Server: <ul style="list-style-type: none">• SQL Server 2008 Enterprise (64-bit).• SQL Server 2008 R2 Enterprise (64-bit).• SQL Server 2008 Standard (64-bit).• SQL Server 2008 R2 Standard (64-bit).• SQL Server 2008 R2 Datacenter (64-bit).