Päivi Saarimäki

Yhteisön viestintäsovelluksen rakentaminen Azure-ympäristöön

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikka

Insinöörityö

19.3.2016

Metropolia

Tekijä(t) Otsikko Sivumäärä Aika	Päivi Saarimäki Yhteisön viestintäsovelluksen rakentaminen Azure-ympäristöön 38 sivua + 2 liitettä 19.3.2016
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Tietoverkot
Ohjaaja(t)	Yliopettaja Kari Järvi

Työssäni tarkastelin SharePoint 2013 -sivuston käytettävyyttä ja soveltuvuutta vuokralaisyhteisön kommunikaatiovälineeksi. Tutustuin Azure PowerShell -työkalun käyttöön Azure ”Resource Manager” -mallin mukaisten palvelimien luonnissa. Palvelinten käyttöjärjestelmä- ja tiedostolevyt suojattiin BitLocker-salauksella. Salausavainten hallintaan käytettiin Azuren Key Vault -sovellusta.
Aluksi selvennettiin pilvipalvelun käsitteitä ja teknologioita. Palvelun hyötyjä ja uhkia pohdittiin sekä liiketaloudellisesti että teknologisesti. Esittelen tarkemmin Amazon Web Services EC2- ja Microsoft Azure -palvelut sekä näiden teknologisia ratkaisuja.
Toteutuksessa luotiin SharePoint 2013 -farmiin tarvittavat kolme palvelinta käyttäen sekä PowerShell-skriptejä että Azure-portaalia. SharePoint-palvelimen toteutus ei onnistunut suunnitellulla tavalla. Microsoft edellyttää, että palvelimella olisi vähintään 4 prosessoriydintä. Käytössä olleessa kokeilulisenssissä oli neljän CPU:n raja. SharePoint-palvelimelle allokoitiin yksi CPU, mikä aiheutti virheilmoituksia asennuksessa sekä hidasti palvelinta.
Palvelua varten luotiin uusi aktiivihakemistometsä, johon kaikki palvelimet liitettiin. SharePoint-sovelluksen suorittamista varten luotiin kolme käyttäjätunnusta. Tunnukset rekisteröitiin SharePoint-sovellukseen hallituiksi tileiksi palvelusovellusten käyttöön.
SharePointin verkkosovelluksen sivustokokoelma julkaistiin Azuren pilvipalvelussa. Sivustokokoelman käytettävyyttä testattiin eri käyttäjätunnuksilla. Käyttäjätunnusten oikeustasot olivat sivustokokoelmassa erilaiset. Sivustokokoelman elementteihin annettiin käyttäjäryhmille oikeuksia ja testattiin rajoitusten toiminnallisuus.
Tulosten tarkasteluissa sivuston käyttöoikeudet toteutuivat suunnitellusti. Hakupalvelusovellus ei tuonut näkyviin kuin tulokset, joihin käyttäjällä on lukuoikeus. SharePoint-sivuston sosiaalisen median elementit soveltuvat yhteisöviestintään hyvin. Palvelun kallis hinta tekee palvelusta soveltumattoman. SharePoint Online -palvelu tai Azuren verkkosivut ovat parempia ratkaisuja.
PowerShell-skriptit edistävät Azure-palvelun käytettävyyttä osana automaatiota. Luotaessa useita palvelimia skriptit säästävät aikaa ja parantavat hallittavuutta. Levyjen Bitlocker-salaus ei aiheuttanut merkittävää I/O-latenssia palvelimissa. Pilvipalveluiden kustannusten minimoimiseksi tulisi palvelun suorituskykyä ja resursseja seurata säännöllisesti. Ilman valvontaa voivat säästöt huveta resurssien ylikäytöstä aiheutuvaan laskuun.

Avainsanat	Microsoft Azure, SharePoint, PowerShell

Author(s) Title Number of Pages Date	Päivi Saarimäki Building Community Used Web Solution into Azure 39 pages + 2 appendices 19 March 2016
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	IT Networks
Instructor(s)	Kari Järvi, Principal Lecturer

The purpose of the study was to evaluate if a SharePoint 2013 site collection can be used as a sharing portal for a housing committee. The second objective was to test the Azure PowerShell tool. Azure RM PowerShell scripts and portal were used to create virtual servers using the "Resource Manager" mode. To enhance security Bitlocker encryption was used for both the operating system and data disks. The Azure Key Vault application was used for storing and managing the encryption keys.

First some key cloud concepts and technologies are introduced. The advantages and disadvantages of cloud services both on economical and on technological aspects are considered. Then the Amazon Web Services EC2 and Microsoft Azure technology behind their service offerings are discussed.

At the implementation phase three virtual servers were created in order to use AD authentication on the SharePoint 2013 farm. The Azure subscription was based on a "Free Trial"-license, which caused problems in the test setup. The license only allowed the use of 4 CPU's and resulting in having only one CPU for the SharePoint server in the end. This CPU level is below Microsoft SharePoint server requirements and caused errors when creating the farm. The setup was adequate to do the testing but would not be acceptable in real world.

A local AD forest was created and all computers were joined to this domain. To run the SharePoint service applications three service accounts were created and registered as managed accounts. The search account was given only read level access to the web application. The site collection was published in Azure cloud by using alternative access mapping and public IP of the SharePoint server. Three different access levels were implemented on the site by using AD groups. The web site contained several social media elements and web parts for testing rights and sharing. The search displayed results only at the user read level as expected. SharePoint delivered an easy way to publish and share information but the price tag of the service is too high for the community in question with limited economical resources. There are other solutions even in Azure that can accomplish the same with fewer costs.

While using the PowerShell scripts it was found out that they can improve the automation of cloud services but the benefits would be seen by the customer with heavy use of the Azure. Bitlocker encryption was not found to cause significant I/O latency on the disks.

Keywords	Microsoft Azure, SharePoint, PowerShell

Sisällys

Lyhenteet

AAID	Azure AD Application ID eli Azuren sovellusidentiteettitunnus. Tätä tunnusta vasten tapahtuu salauksen ja purun luvan tarkistaminen.
ABE	Attribute Based Encryption. Tiedon salausteknologia, jossa jokaiselle tiedostolle määritetään attribuutit, ja käyttäjän salausavaimen on vastattava attribuuttien ehtoja, jotta tiedosto puretaan käytettäväksi.
AWS	Amazon Web Services. Amazon Oy:n verkkopalvelu.
Azure	Microsoft Azure -pilvipalvelu
CSS	Cross Site Scripting on nettisivujen haavoittuvuuksia hyväksikäyttävä hakkeroimistekniikka.
FRC	Fraudulent Resource Consumpion. Resurssien vilpillinen väärinkäyttö, jonka tarkoituksena on aiheuttaa asiakkaille taloudellisia menetyksiä.
IaaS	Infrastructure as a Service. Palvelussa ulkoistetaan alustan ja sen päivitysten ylläpito palvelun tuottajalle.
Key Vault	Microsoft Azuressa oleva avainten hallintapalvelu.
PaaS	Platform as a Service. Palvelussa ulkoistetaan alustan ylläpito palvelun tuottajalle.
SaaS	Software as a Service. Palvelussa ulkoistetaan sovelluksen tuottaminen ulkoiselle tuottajalle.
SecretKeyID	Azure AD:n määrittämä salaisuus, jota käytetään sovelluksen salausavaimissa Key Vaultissa.
WAWS	Windows Azure Web Sites. Microsoft Azuren tarjoama verkkosivupalvelu, jossa sivut voidaan luoda esimerkiksi valmiista malleista.

1 Johdanto

Insinöörityössä arvioidaan Microsoft Azure SharePoint -toteutuksen käyttötapoja yksittäisen yhteisön tiedon jakamisen välineenä. Käytännön esimerkki on vuokrataloni talotoimikunnan viestintäkanavan tekeminen, joka mahdollistaa tiedostojen jaon sekä erilaisia sosiaalisia viestintätapoja, joita ovat wiki, blogi, RSS-syötteet jne. Talotoimikunnalla on tarve viestittää talon tapahtumista, välittää naapuriapua sekä antaa neuvoja asukkaille. Vuokranantajalla ei ole tarjota käyttöömme viestintäkanavaa, joten halusimme testata, tarjoaako Microsoft Azure SharePoint tähän ratkaisun.

Toteuttamiseen valikoitui Microsoft Azure SharePoint, jolla haluan testata, miten hyvin se toimii yksityisessä käytössä ilman kompleksista organisaatiota taustalla. Toinen vaihtoehto Microsoft Azure SharePointin tilalle olisi ollut tehdä nettisivut käyttäen sähköisen ilmoitustaulun (BBS) valmista mallia ja julkaista se Azuren Web Sites (WAWS) -toiminnon kautta [1, s. 1 -10]. SharePoint Azure -toteutuksessa saan samalla tutustua eri tapoihin luoda palvelimia Azuren pilveen. Tässä työssä haluan perehtyä automatisointiin tarkoitetun Windows PowerShell -työkalun käyttöön palvelimien toteuttamisessa. Tein palvelimia sekä nettiportaalin kautta että PowerShellillä, jotta voin tarkastella toteuttamistapojen eroja. Omien palvelimien toteutuksessa pystyn samalla kokeilemaan, mitä tietoturvaa parantavia asetuksia Microsoftin Azuressa voidaan käyttää.

Työskentelen tällä hetkellä IT-alan yrityksessä, joka tarjoaa yksityistä pilvipalvelua asiakasyritystensä käyttöön. Työntekijöitä kannustetaan automatisoimaan esimerkiksi palvelinten tuotannon operointeja. Työni vuoksi minua kiinnostavat pilvipalveluiden automatisointi sekä yritysten pilvipalveluiden käytön liiketaloudelliset päätökset ja toteutukset. Halusin tutustua Microsoftin Azure palveluun tarkemmin, sillä sen toteutukset ovat keskittyneet Windows-palvelimiin. Tällä hetkellä se on nousemassa Amazonin Web Servicen rinnalle IaaS- ja PaaS-palveluiden tarjoajana.

Työssäni käyn läpi pilvipalvelun merkitystä yrityksen liiketaloudelle, pilvipalvelun teknologiaa sekä palvelun käsitteitä. Tarkastelen pilvipalveluun liittyviä tietoturvariskejä sekä mahdollisia keinoja niiden minimointiin. Selvitän nykyisiä pilvipalvelun tarjoajia (IaaS- ja PaaS-tasolla) ja tarjottuja ratkaisuja. Käytännön toteutuksessa kerron rakennetusta SharePoint-farmista, sivustosta sekä palvelinten toteuttamisesta ja suojaamisesta. Tulosten tarkastelussa käyn läpi Azure SharePointin soveltuvuutta

yhteisöjen käyttöön sekä arvioin automatisoinnin toteutusta. Lopuksi pohdin pilvipalveluiden teknologisia mahdollisuuksia sekä sitä, mikä tulevaisuudessa voisi kiinnostaa itseäni.

2 Pilvipalveluista

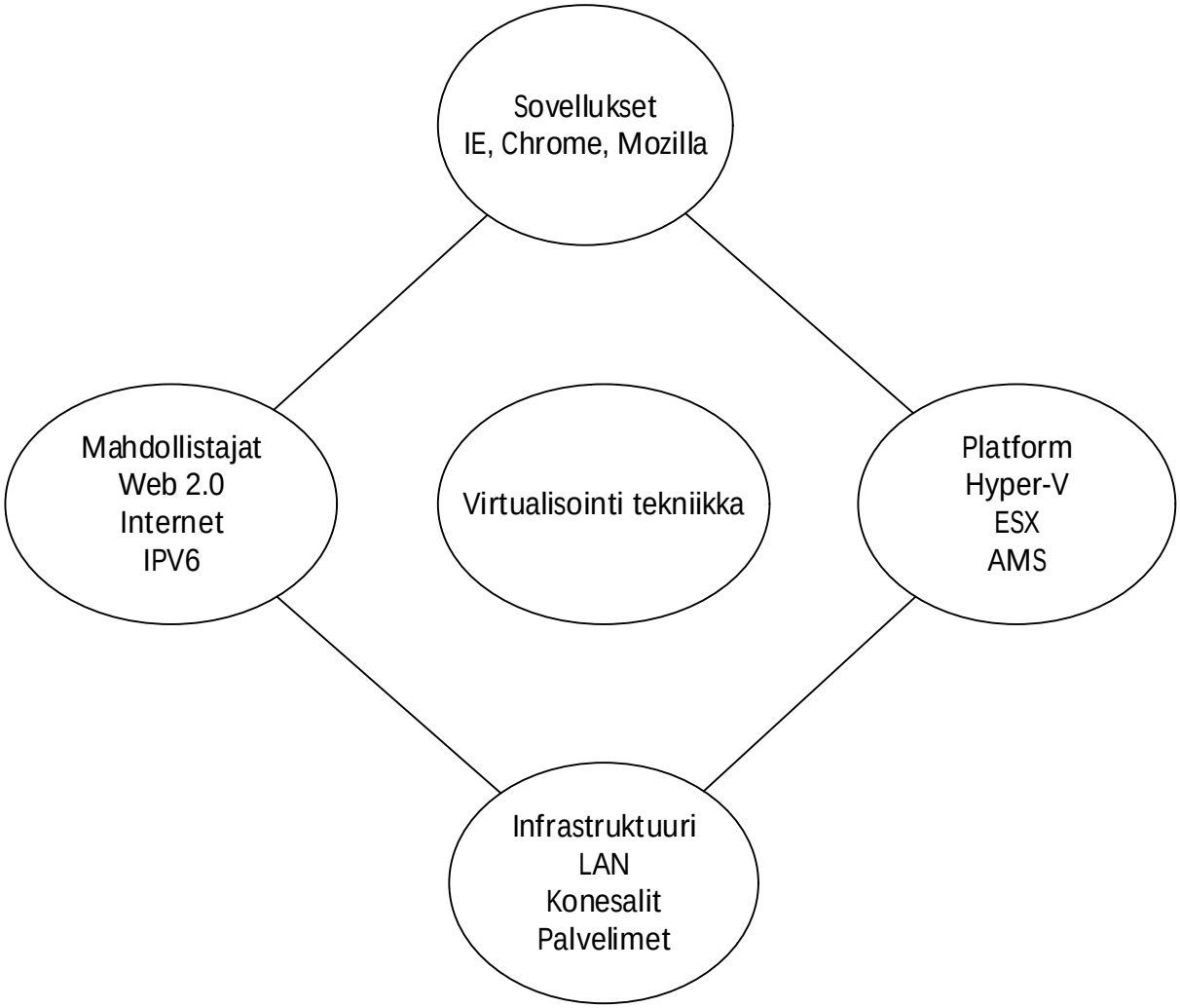
Pilvipalveluita tuotetaan sekä yksityisille että yrityksien käyttöön. Pilvipalveluille ei ole olemassa standardisoitua määritelmää, mutta esimerkiksi Salo käyttää seuraavaa National Institute of Standards and Technologyn (NIST) määritelmää pilvipalveluista:

> ”Cloud computing on toimintamalli, joka mahdollistaa pääsyn vapaasti konfiguroitaviin ja skaalautuviin tietotekniikkaresursseihin, jotka voidaan ottaa käyttöön tai poistaa käytöstä helposti ja nopeasti.” [2, s. 17.]

Sovelluksien käyttö palveluna (Software as a Service SaaS) on ollut mahdollista jo vuodesta 2006 lähtien. Teknologisena murroskohtana pidetään vuotta 2010, jonka jälkeen erityyppiset jaetut palvelut yleistyivät IT-alalla. [3, s. 61.] Yksityisille käyttäjille tuotettuja palveluita ovat esimerkiksi Facebook, LinkedIn, MySpace, Microsoft Live jne. [2, s. 38]. Kun käyttäjät oppivat uusia työskentelytapoja, he edellyttävät usein samoja palveluita yrityksen IT-osastoilta, ja yritysten ratkaisujen on oltava joustavasti saatavilla ja käytettävissä internetissä tai kotoa käsin. IT-osastoille asetetaan yhä kovempia vaatimuksia kustannusten laskemisesta sekä käytettävyyden parantamisessa, mutta samalla ohjelmistojen toiminnallisuudet halutaan käyttöön nopeammin. Pilvipalveluiden on nähty tarjoavan vastauksia tähän kysyntään, ja hankintaesitykset ovat usein lähtöisin sisäisiltä asiakasyksiköiltä tai substanssiosaajilta. Perinteisen IT-osaston rooli on muuttumassa, kun se tuottaa palvelua julkisesta tai yksityisestä pilvestä. [3, s. 99; 37.]

Pilvipalvelu on usean teknologian ja komponentin yhdistelmä, jossa sovellusta tai palvelua käyttää internetyhteyden kautta useampi käyttäjä yhtä aikaa. Pilvipalvelun käytön mahdollistivat internetin yleistyminen, palvelinten ja muun infrastruktuurin virtualisointia edistävä hypervisor-teknologia ja palvelinarkkitehtuuri. Pelkästään internetyhteyksien lisääntyminen ei riitä pilvipalveluiden käyttöön. Sen lisäksi eri selaimet, selainteknologiat ja näiden ominaisuudet tukevat palveluiden käyttöä. Teknologisesti pilvipalvelu käsitetään usein synonyymina virtualisoinnille, mutta ne ovat kuitenkin kaksi eri käsitettä. Virtualisointitekniikalla parannettiin sekä laajennettavuutta että kustannustehokkuutta jakamalla fyysisten palvelinten resursseja usean eri virtuaalisen palvelimen käyttöön. Ilman palvelinten, verkkokytkimien tai palomuurien

virtualisointia ei kuitenkaan voinut olla nopeita, kattavia pilvipalveluita. Kuvassa 1 on esitetty yleisellä tasolla niitä tekijöitä, jotka ovat mahdollistaneet pilvipalveluiden käytön, eli uudentyyppiset sovellukset, erilaiset alustat, virtualisointi ja hypervisorit, infrastruktuuri ja taustalla olevat mahdollistajat. [3, s. 11 -21.]

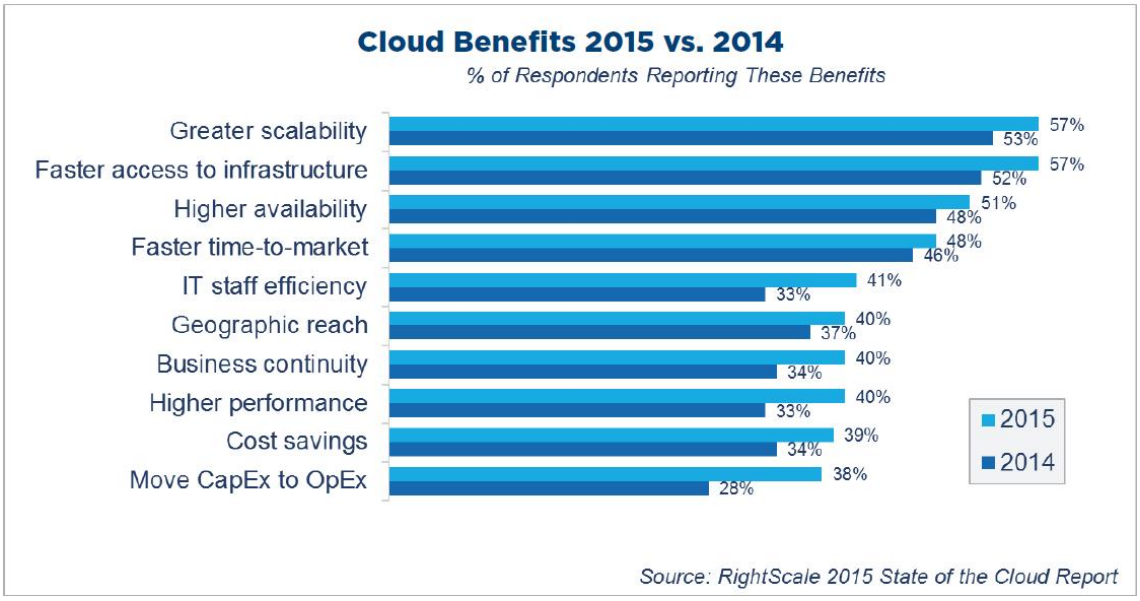


Kuva 1. Pilvipalveluiden neljä tukipilaria [3, s. 11]

Tietoturvanäkökulmasta pilvipalvelut ovat alttiita kaikille käytössä olevien teknologioiden periytyville sekä omille tietoturvariskeille. Riski- ja tietoturva-analyyseissä on otettava periytyvyys huomioon, esimerkiksi erilaiset SSL-haavoittuvuudet voivat kohdistua sovellukseen tai alustan ESX-käyttöjärjestelmään. Molemmat on korjattava ennen kuin haavoittuvuus on tilkitty. [4, s. 14.]

2.1 Pilvipalveluiden liiketaloudelliset merkitykset yrityksille

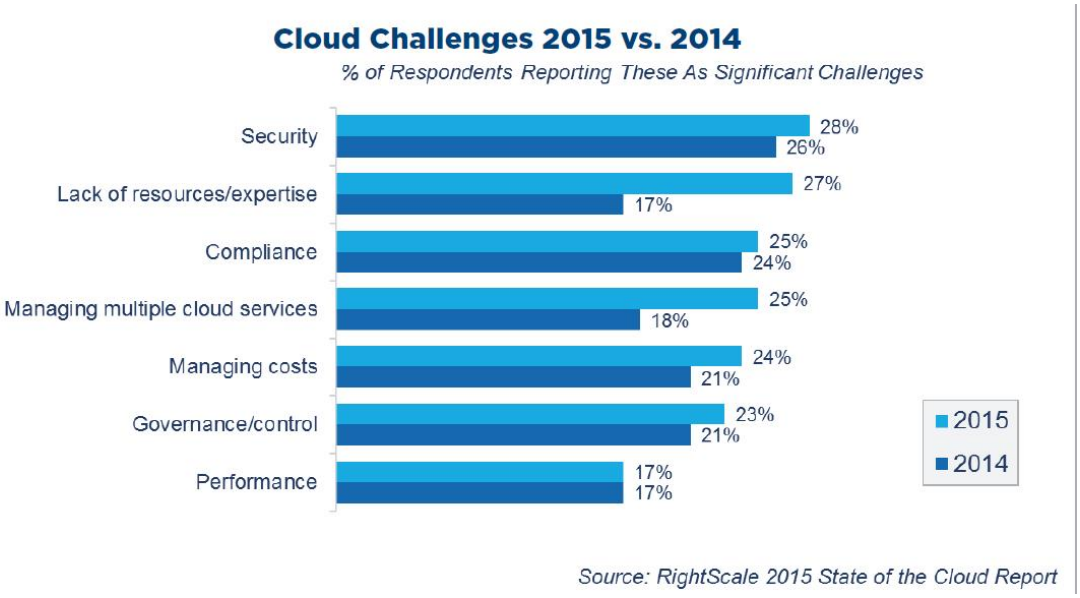
Pilvipalvelut tarjoavat yrityksille mahdollisuuden tuottaa kustannustehokkaasti ja nopeammin palveluita käyttäjille, vähentää omia IT-järjestelmiä ja IT-kustannuksia sekä vapauttaa resursseihin sidottua pääomaa. Kun laskutus tapahtuu käytössä olevien resurssien käytön mukaan, pysyvät kustannukset alhaisina hiljaisimpinakin aikoina. Sovellusten käyttöönottoaika nopeutuu, kun muutoksia voidaan hioa ja testata virtuaalisessa testiympäristössä ja tuotanto voidaan tehdä vastaamaan testiympäristöä. [3, s. 29–32, 5.] Vuoden 2016 alussa RightScale-yrityksen tekemässä tutkimuksessa palveluiden korkea saatavuus sekä suorituskyky olivat tärkeimmät kriteerit pilvipalveluiden valinnalle [6].



Kuva 2. Pilvipalvelun etuja [5.]

Tietoturvariskit ovat olleet suurimpana esteenä yritysten siirtymisessä käyttämään pilvipalveluita. Tiedon suojaaminen palvelun muilta asiakkailta ja tuottajilta on ollut suurin riski. Palvelun kypsyessä on kehitetty uusia tapoja esimerkiksi salata tiedot ilman levylatenssin kasvamista. Teknologisesti asiakkuudet pystytään eriyttämään jo alustapalvelimella riittävästi, jotta tiedot olisivat turvassa vilpilliseltä käytöltä. Esimerkiksi Amazon Web Service (AWS) ilmoittaa, että sen alustapalvelut ovat PCI DSS -standardin mukaisia. Tiedon suojaaminen pilvipalveluissa on nykyään turvallisempaa kuin yrityksen omissa järjestelmissä, joihin käyttäjillä on usein suojaamaton pääsy omalta työpisteeltään. [3, s. 32–36; 7; 8.] Yrityksille on ollut hankalaa jäsentää sitä kontrollin puutetta, mikä heillä on suhteessa palveluntuottajiin. Alustaan kohdistuvat toimet eivät

ole läpinäkyviä asiakkaille. Tietämättömyys, resurssien puute ja osaamattomuus ovat nousseet RightScalen vuoden 2016 tutkimuksessa suurimmaksi haasteeksi pilvipalvelun käyttämisessä. Vuoden 2014 tutkimuksissa vain 17 % vastaajista piti osaamattomuutta negatiivisena puolena. Vuonna 2015 osaamattomuuden koki haasteena jo 27 % vastaajista. [5.] Vuoden 2016 tutkimuksessa tiedon turvaaminen ei ensimmäistä kertaa enää ollut pahin haaste, vaan osaamattomuus pilvipalveluista oli 32 % vastaajien mielestä pahin ongelma. Rightscalen vuoden 2016 pilvipalveluiden käytön tutkimuksessa resurssien mitoitus nähtiin ongelmana. Yrityksillä on huoli, että niiden palvelut ovat yli- tai alimitoitettuja. Ostetaan esimerkiksi omistettuja instansseja, vaikka vähemmillä resursseilla pärjättäisiin varsinkin hiljaisina aikoina. [6.] Muuttuva yrityskulttuuri ja toimintatavat muuttavat IT-osaajien työtä. Tuotantotaloutta pitää ymmärtää, ja on osattava laskea menoja, sekä lukea palvelusopimuksien ehtoja. Ostettua palvelua on valvottava, jotta suorituskyvystä saadaan kaikki hyöty irti. Tietotekniikka tarvitsee rinnalleen liiketaloudellista osaamista pilvipalveluiden kanssa työskenneltäessä.



Kuva 3. Pilvipalvelun haasteita. [5.]

Pilvipalveluiden käyttäjiksi ei voida ryhtyä ilman esivalmisteluja. Vanhat sovellukset pitää muokata ja koodata uudestaan, jotta voidaan siirtyä käyttämään virtuaalista ympäristöä tai pilvipalveluita. Pilvipalveluihin on helppo siirtyä yrityksen elinkaaren mukaan. Pienet, juuri perustetut yritykset valitsevat usein jo alussa pilvipalveluiden käytön, tai sitten ne pitäytyvät omissa IT-ratkaisuissa. Keskikokoiset yritykset, joilla on omaa IT-infrastruktuuria, voivat olla potentiaalisesti siirtymässä pilvipalveluihin, kun niiden IT-

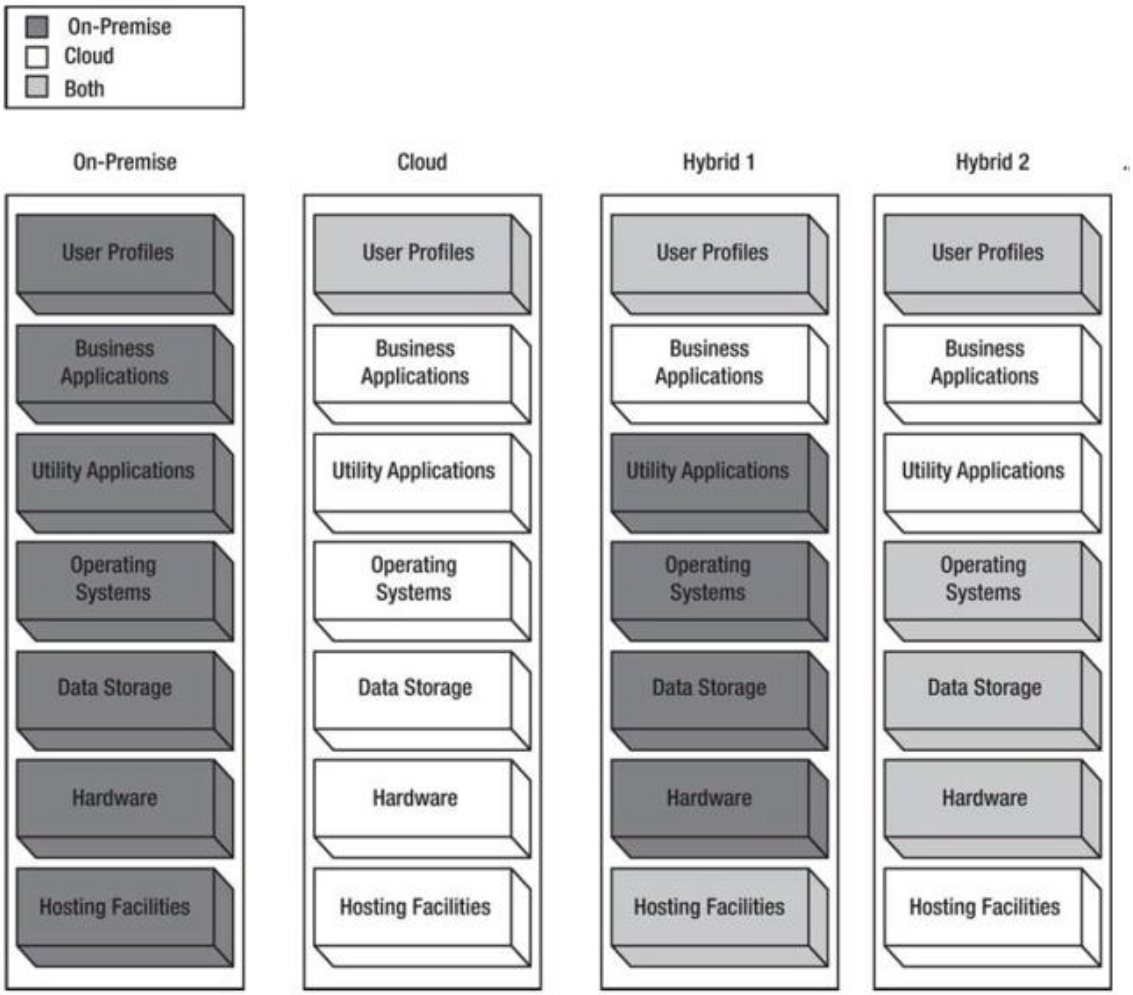
investointien elinkaari on loppumaisillaan. Isot, vakiintuneet, suuria järjestelmiä käyttävät yritykset, joilla voi olla paljon myös vanhentunutta, omaa IT-infrastruktuuria, ovat vasta siirtymässä pilvipalveluihin. Näiden yritysten kohdalla on pilvipalveluihin siirryttäessä otettava huomioon sekä teknologiset että liiketoimintaprosessien muutokset. Isojen linkitettyjen järjestelmäsovellusten siirtyessä pilveen on tehtävä yhteistyötä substanssiosaajien ja IT-osastojen kanssa, jotta muuttuneet toiminnallisuudet ja kehitystoimet voidaan sisällyttää muutoksen yhteyteen. Yrityksen sisäiset vastuut ja päätöksentekijät on aina syytä selvittää ennen siirtymistä pilveen. Palvelun jatkuvuussuunnitelmat on tehtävä ennen kuin palvelua siirretään pilveen. [3, 109 -151.]

Työssäni ulkoistettuna Windows-järjestelmien ylläpitäjänä olen törmännyt sovelluksiin, joita ei ole optimoitu alustalle (fyysiselle tai virtuaaliselle), mutta ne on vain haluttu siirtää ajettavaksi virtuaalisiksi palvelimiksi. Tämä on aiheuttanut ongelmia sovelluksen suorituskyvylle, ja resursseja on jouduttu useasti lisäämään tai muokkaamaan, jotta ympäristöstä on tullut käyttäjiä tyydyttävä. Joskus ongelmana ovat olleet käyttäjän tavat käyttää sovellusta, eli on haettu *.* -sanoilla hakuja eikä alusta ole tarjonnut riittäviä resursseja. Tosin joskus näitä tapoja on hankala kitkeä pois. Näiden ongelmien selvittely voi olla haastavaa jos asiakasyrityksellä ei ole selkeätä sisäistä toimintatapaa ja -prosessia ongelmien selvittämiseksi.

2.2 Pilvipalveluiden arkkitehtuuri ja tuotantomallit

Pilvipalvelu on palvelun tuottamista asiakkaalle käyttäen jaettuja laskennallisia resursseja, ja asiakasta laskutetaan vain käytettyjen resurssien osalta (pay-as-you-go) sovitun palvelutason mukaisesti. Asiakkaita voivat olla yritykset, sekä yrityksen sisäiset tai ulkoiset asiakkaat. Resurssien ja vastuiden jakaminen toimittajan ja asiakkaan välillä määrittää, minkä tyyppisestä pilviarkkitehtuurista on kyse: julkisesta, yksityisestä vai hybridipilvestä. Julkisessa pilvessä ulkoistettu palvelun tuottaja toimittaa ja vastaa kaikista palvelun komponenteista, fyysisistä/virtuaalisista verkoista, levykapasiteetista, palvelininfrastruktuurista, jne. aina sovelluksen ylläpitoon asti. Resurssit ovat yleensä useamman eri asiakkaan kanssa jaettuja. Julkisessa pilvessä asiakas itse vastaa sovelluksen käyttäjistä ja heidän toimintavaltuuksistaan palvelun käyttäjänä. Sovellus, lisenssit ja ylläpito ovat palvelun tuottajan vastuulla, joten näitä asiakkaalla ei yleensä ole mahdollista muokata tai yksilöidä. [9, s. 3–4.]

Yksityisessä pilvessä palvelua tuotetaan yrityksen sisällä vain yrityksen sisäisille asiakkaille ja resurssit on jaettu yrityksen omien käyttäjien kesken. Ylläpito tapahtuu IT-osaston toimesta ja sovelluksilla on käytössä yrityksen oma infrastruktuuri kuten AD, sähköposti, tiedostojaot, jne. Usein yksityinen pilvi on tehty erilaisten virtuaalisten käyttöjärjestelmien päälle, jolloin alustaa voidaan käyttää usean palvelimen ajamiseen. [9, s. 5.]



Kuva 4. Eri pilvipalveluiden tuottajien vastuualueet eri skenaarioissa, on-premise=yrityksen omistamat ja hallinnoimat palvelut, cloud= pilvipalvelun tuottajan omistamat ja hallinnoimat palvelut, both= molempien yhdessä omistamat ja hallinnoimat palvelut. [9, s. 7.]

Hybridipilviratkaisuissa palvelukokonaisuuden elementtejä tuotetaan eri tahoilla ennalta sovitusti. Julkisesta pilvestä voidaan tuottaa esimerkiksi nettisovelluksen alustan palvelut (käyttöjärjestelmä + valmiiksi asennettu nettisovellus), mutta käyttäjän lataama tieto tallentuu yrityksen omassa hallinnassa olevaan levyjärjestelmään tai tietokantaan. Tällöin tuotantovastuut räätälöidään asiakkaan ja toimittajan kanssa yhdessä. Kehitystyö ja vianetsintä tehdään alustapalvelun toimittajan ja asiakkaan kanssa yhdessä. Asiakas

on vastuussa käyttäjien hallinnasta muiden mahdollisten komponenttien lisäksi. [9, s. 3–7.]

Yrityksillä on nykyään useita pilvipalvelun tuottajia eli niillä voi olla oma yksityinen pilvipalvelu. Sen lisäksi ne ostavat julkisia ja hybridipalveluita. [6.]

Pilvipalveluiden toimittajat luokitellaan tarjotun palvelun mukaan SaaS-, PaaS- ja IaaS -palvelun tuottajaksi. Pilvipalveluiden tuottajista käytetään muotoa ”* as a Service”, esimerkiksi ”Security as a Service” tarkoittaisi tuottajaa, joka tarjoaa tietoturvallisuuspalveluita. [2, s. 8.]

PaaS eli ”Platform as a Service” -tuotantomallissa palveluntuottaja toimittaa alustan sovellukset eli ylläpitää käyttöjärjestelmää ja sen komponentteja. Asiakkaan vastuulle jää sovelluksen ylläpito ja päivittäminen. IaaS eli ”Infrastructure as a Service” -mallissa tuottaja omistaa ja hallinnoi asiakkaan käytössä olevan fyysisen ja loogisen infrastruktuurin kokonaan, asiakas tekee käyttöjärjestelmän päivitykset, sovelluksen päivitykset, datan hallinnan jne. [2, s. 21.]

SaaS eli sovellukset palveluina (Software as a Service) on laajin ja ajallisesti vanhin käytössä ollut palvelumalli. SaaS-palveluissa sekä alusta, data että sovellus ovat toimittajan hallussa. [2, s. 22.] Markkinoilla on useita erilaisia SaaS-sovelluksia, jopa tehdastuotannon mahdollistavia CAD- ja SAP-palveluita. CAD-palvelussa tekniset suunnittelijat pääsevät pilvipalvelun kautta käsiksi suoraan tuotantotehtaan CAD-kuviin selaimen kautta. Kuvista voidaan valikoida halutut osat muokattavaksi. Tuotantolinja voi tehdä muutoksia elementtiin ja/tai hyväksyttää muutokset toisella suunnittelijalla tai esimiehellä. Isojen kuvien muokkaukset voidaan tehdä nopeasti eikä kuvia tarvitse siirtää levyjakojen tai vastaavien kautta. Pilvipalvelussa oleva välikerroksen rajapinta toimii sekä pääsynhallinnan että tallennuksen määrittäjänä. Samalla eri operaattorit pystyvät näkemään muutokset heti näiden tapahtuessa. [10, s. 11.].

2.3 Pilvipalveluiden tietoturvariskit ja estäminen

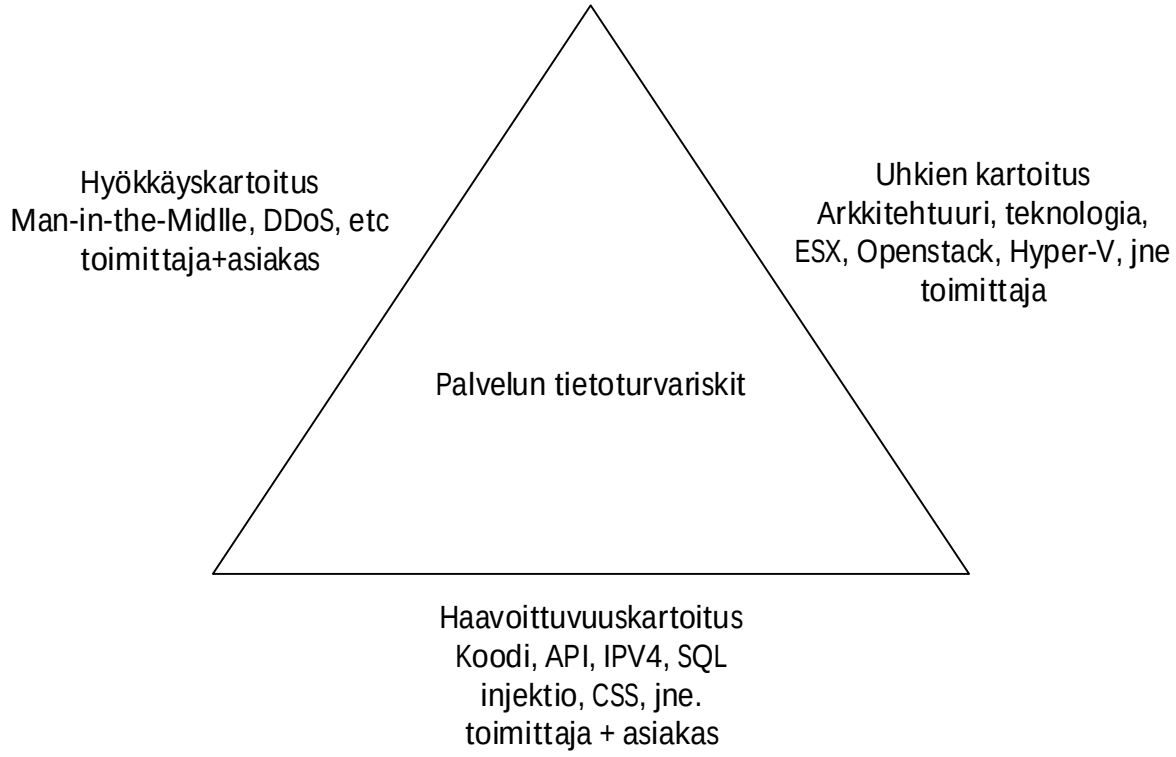
Suurimmaksi koettu uhka pilvipalveluihin siirtymiselle on ollut yrityksen tiedon suojaaminen pilvessä ja yrityksen sisällä. Luottamuksen pilvipalvelun tuottajaan on oltava vahva, yrityksen tieto pitää suojata eri syistä, ja tietovuodot ovat pahin mahdollinen skenaario. Suojattava materiaali voi olla erityyppistä, sähköpostia suojaa

kirjesalaisuus kun taasen potilastietoja on varjeltava yksityisyyden suojan vuoksi tarkoin, kuitenkin hoitohenkilöiden pääsy tietoihin on taattava. Asiakkaalla on tarve suojella tietoa yrityksen omilta työntekijöiltä sekä pilvipalvelun tuottajan on suojattava tieto muilta asiakkailta tai omilta mahdollisesti vilpillisiltä työntekijöiltä. Inhimillisistä virheistä tai vilpillisestä toiminnasta syntyneen tietovuodon seurauksena liiketaloudelliset menetykset voivat olla suuria ja aiheuttaa yrityksen omien asiakkaiden luottamukseen suuren särön. Luottamuspulaa vastaan on vaikea taistella ihmiskeinoin, joten teknologiset ratkaisut asiakasympäristöjen eriyttämisessä sekä tiedon salauksessa ovat palveluiden tuottamisessa tärkeitä elementtejä. Yleisen standardin puuttuminen pilvipalveluista tai sen tietoturvallisuudesta on ollut hidaste pilveen siirtymisessä. [4, s. 5.]

Tietoturvallisuutta parannettaessa pitää muistaa, että pilvipalvelun riskit periytyvät muista käytetyistä teknologioista. Sovelluskerroksessa oleva palvelu voi olla altis erilaisille hyökkäystavoille, kuten SQL-injektiolle, sivustossa käytössä olevien skriptien kautta tapahtuville hyökkäyksille (CrossSiteScripting) tai SSL:n haavoittuvuudelle. Virtualisointikerros ja hypervisor-liittymät (OS, ESX, WebSphere, CitrixXen, jne.) ovat alttiita koodivirheille tai haavoittuvuuksille. Fyysisten laitteiden yhteiset resurssit ovat tietoturvan kannalta mahdollinen uhka. Esimerkiksi I/O-kontrolleri on jaettu resurssi, jota kaikki virtuaaliset palvelimet käyttävät. Prosessori ja muisti on varattu yhdelle virtuaalipalvelimelle kerrallaan siellä suoritettavien komentojen käyttöön, mutta kumpikin komponentti kommunikoi I/O-kontrollerin kanssa. Virtualisointitekniikan tai hypervisorin on pystyttävä eriyttämään tarkasti eri asiakkaiden palvelimet täysin toisistaan. Verkkoinfrastruktuurin eriyttäminen asiakaskohtaisesti on välttämätöntä. Yhtä asiakasta kohtaan tehty hyökkäys, joka käyttää TCP/UDP-protokollan haavoittuvuutta, voi kertaantua kaikille verkon isäntäkoneille tai virtuaalipalvelimille. Haavoittuvin teknologia tai sen komponentti on pilvipalveluiden heikoin lenkki ja määrittää palvelun tietoturvatason. [4, s. 8 - 37.]

Yritysten tulisi pilvipalveluita suunnitellessaan/ostaessaan tehdä yhteinen tietoturvariskikartoitus palvelun tuottajan kanssa. Kartoituksessa sekä asiakas että pilvipalveluiden toimittajat tunnistavat ne potentiaaliset riskit, joita palveluun voi kohdistua. Kartoituksessa pitäisi huomioida mahdolliset hyökkäykset, teknologiset uhkakuvat sekä tunnetut että tuntemattomat haavoittuvuudet, joille pilvipalvelu on altis. Tärkeintä analyysissa on, että sen tekemiseen osallistuvat molemmat toimijat, ja he yhdessä päätettävä mahdollisista toimenpiteistä. [11, s. 80.]

Seuraavassa kuvassa esitän, mistä kartoitus koostuu ja kuka on vastuullinen eri analyysin osioiden teosta. Alustan ja teknologian uhkien kartoittamisessa vastuussa on palvelun toimittaja. Sovelluksen haavoittuvuuksien selvittämisessä vastuu on molemmilla, mutta uniikin sovelluksen kohdalla vastuu on asiakkaalla tai asiakkaan ohjelmistotoimittajilla. Hyökkäystapojen arvioinnissa toimittajan merkitys korostuu, koska sillä on paras tietämys, miten ehkäistä hyökkäyksiä. [11, s. 80 -81.]



Kuva 5. Tietoturva-analyysin komponentit [11, s. 80–81.]

Kartoitusta voidaan käyttää apuna kriittisten palveluiden tunnistamiseen ja liiketaloudellisen jatkuvuussuunnitelman pohjaksi. Kartoitus auttaa yleensä luokittelemaan palvelutason ja sen, miten palvelu kestää mahdollisia katkoja. [3, s. 231.]

Palvelun toimittajalla on hyvin vaativa tehtävä palvelun eriyttämisessä asiakkuustasolla ja sen teknologisessa toteuttamisessa. Virtuaalisten palvelimien käyttäessä jaettuja resursseja fyysiseltä isäntäkoneelta resurssien välistä teknistä väylää voidaan käyttää sen sisältämän tiedon tai varmenteen varastamiseen. Englanniksi tästä menetelmästä käytetään termiä covert channel, suomeksi piilotetun väylän hyökkäys. Tällöin yksi virtuaalipalvelin käyttää jotain isäntäkoneen jaettua resurssia, kuten prosessorin toisen asteen välimuistitilaa päästäkseen lukemaan tai kopioimaan siellä olevaa tietoa, joka on

lähtöisin toiselta virtuaaliselta palvelimelta. [12, s. 106 -108.] Uhka voi tuntua vähäiseltä ja teoreettiselta, mutta kyseistä tapaa on käytetty Amazon EC2 -pilvipalvelussa. Kesällä 2015 Worcester Polytechnic Institute:n tutkijat yrittivät päästä käsiksi heidän omassa AWS-instanssissa olevalta palvelimeltaan toisen oman virtuaalikoneen RSA-salausavaimeen. He onnistuivat pääsemään käsiksi tähän avaimeen käyttäen apunaan jaettua prosessorin välimuistia. Verkkoartikkelin kirjoittajat moittivat sitä tapaa, miten Amazon vähätteli tätä löydettyä haavoittuvuutta eikä ”tiedottanut” asiasta. [13.]

Lukiessani alkuperäisen artikkelin, jossa kerrottiin miten ja milloin hyökkäys toteutettiin, en pysty välttämättä samaistumaan moitteisiin. Testit tehtiin aamuyön hiljaisina tunteina, jolloin välimuistitilan tiedot voivat olla hyvin stabiileja eikä ylikirjoittamista tapahdu. Molempien virtuaalipalvelinten on oltava samassa isäntäkoneessa, jotta hyökkäys onnistuisi. Tämä RSA-avaimen varastaminen on vaatinut paljon työtä ja testausta, jotta se onnistui. Tutkijat raportoivat tästä AWS:lle heti testin jälkeen ja käyttivät tietoisesti omia palvelimiaan testissä mutta eivät kokeilleet, onnistuvatko he varastamaan toisen asiakkuuden koneelta tätä avainta. [14.] En voi välttyä tässä kohtaa pohdinnalta, miten realistinen tämä uhka on. RSA-avaimen varastaminen edellyttää todella paljon osaamista ja resursseja onnistuakseen, joten tämä hyökkäystapa on vain harvojen taitajien käsissä. Todennäköisyys avaimen varastamiselle on pieni, sillä pilvipalveluissa on tuhansia fyysisiä palvelimia ja virtuaalisten palvelimen on oltava saman isäntäkoneen välimuistissa. Mahdollisuuden tiedostaminen on tärkeää, mutta siihen on suhtauduttava realistisesti.

Teknisten uhkien lisäksi isäntäkoneen kaikkien kanssa jaetut resurssit voi aiheuttaa taloudellisia riskejä ja uhkia. Asiakkaat odottavat, että he maksavat oman käyttönsä mukaan resursseista, mutta mitä jos heidän palveluunsa kohdistetaan toisista asiakkaista johtuvia rajoituksia tai resursseja väärinkäytetään? Jos isäntäkoneen yhdelle palvelimelle kohdistuu palvelunestohyökkäys, niin pystyykö mahdollisesti alimitoitettu verkko tarjoamaan palvelua muille palvelimille? Jos palvelua ei voida tarjota, miten korvataan siitä mahdollisesti aiheutuneet taloudelliset menetykset ja kuinka ne voidaan näyttää toteen?

Tahallisten rahallisten menetyksien tuottaminen on mahdollinen yritykseen kohdistuva hyökkäyskeino pilvipalveluissa ja siitä käytetään termiä FRC (Fraudulent Resource Consumption). Resurssien vilpillisellä käytöllä halutaan aiheuttaa asiakkaalle taloudellisia menetyksiä. Palvelin voidaan kaapata käyttöjärjestelmän kautta suorittamaan jotain tehtäviä äärettömyyksiin asti. Palvelin voidaan ohjelmoida

suorittamaan tarpeetonta kopioimista/tallentamista levyjen kesken tai replikoimaan eri maantieteellisten kohteiden välillä. Asiakasta laskutetaan lisääntyneestä levytilan käytöstä sekä tietoliikennemaksuista. Lasku voi olla korkea ja aiheutunut palvelun tulvimisesta, mutta tätä ei ole tunnistettu esimerkiksi virustartunnaksi. [4, s. 25 -28.] Asiakkaan tulisi säännöllisesti valvoa ja määrittää peruskäytön rajat, jotta poikkeavuudet havaitaan ajoissa [7].

Yrityksen tiedon pääsyä halutaan kontrolloida tarkemmin sekä sisäisten että ulkoisten käyttäjien kohdalla, tämä tehdään yleensä levyn salauksella. Levyllä olevat tiedot halutaan yleensä salata datan liikkuessa, data pysyessä paikallaan tai varmistuksissa. Salaus ja purkaminen aiheuttavat levylle latenssia luku- ja kirjoitusnopeudessa ja ovat resurssi-intensiivistä toimintaa, johon pitää varautua palvelua mitoitettaessa. Levyt salataan käyttäen erilaisia salausavaimin ja laskentalogiikkaa. Pääsynhallinta salattuun tietoon toteutetaan käyttäjille jaettavilla salausavaimilla. Pilvipalvelussa salaus palauttaa asiakkaan kontrollin levyn käytöstä, jos avaimia ei tarvitse luovuttaa palvelun tarjoajalle. Salausta käytettäessä asiakas pystyy katselmoimaan levyn käyttöä, mutta avoimeksi jää kysymys, mitä tapahtuu, kun palvelua ei enää käytetä. Asiakkaan on sovittava tiedon tuhoamisesta. Tuhoamisen voi tehdä eri tavoilla ja asiakkaan tulisi tietää, miten tuhoaminen tapahtuu, eli poistetaanko silloin tiedostojen pointterit vai poistetaanko levypinnan tasolla LUN tai levyaihiot ja saako levyn tuhoamisesta todistuksen. [15, s. 51 -52.]

Salausavaimien hallinta on haasteellista, sillä kun yhden käyttäjän avaimessa tapahtuu muutoksia, niin kaikki avaimet täytyy muuttaa, ja tämä rasittaa ylläpitoa. Uusimmissa salaustekniikoissa ei enää käytetä pääsynhallintalistoja ja julkisen-yksityisen avaimien yhdistelmiä, vaan pääsynhallintaan käytetään tiedoston attribuutteja eli ABE (Attribute-Based Encryption) -salausta. Salatun levyn jokaiselle tiedostolle on salauksen yhteydessä annettu attribuutit, jotka määrittävät, kuka ja millä oikeuksilla saa purkaa salauksen. Salatun levyn käyttäjillä on jokaisella oma henkilökohtainen avaimensa, jossa on määritetty käyttäjälle annetut oikeudet. Tiedoston ja käyttäjän attribuuttien ollessa samat salaus puretaan. Käyttäjän oikeuksien muuttuessa vain hänen avaimessaan olevat attribuutit muuttuvat eivätkä ne enää vastaa tiedoston attribuutteja, jolloin salausta ei pureta. Kaikkien käyttäjien tai tiedoston avaimia ei tarvitse muuttaa, joten ylläpidon tarve vähenee. Erilaiset SaaS-sovellukset pystyvät nykyään käyttämään salausavaimia käyttäjän tunnistukseen ja helpottavat sovellusten käyttöä. [15, s. 50–68.]

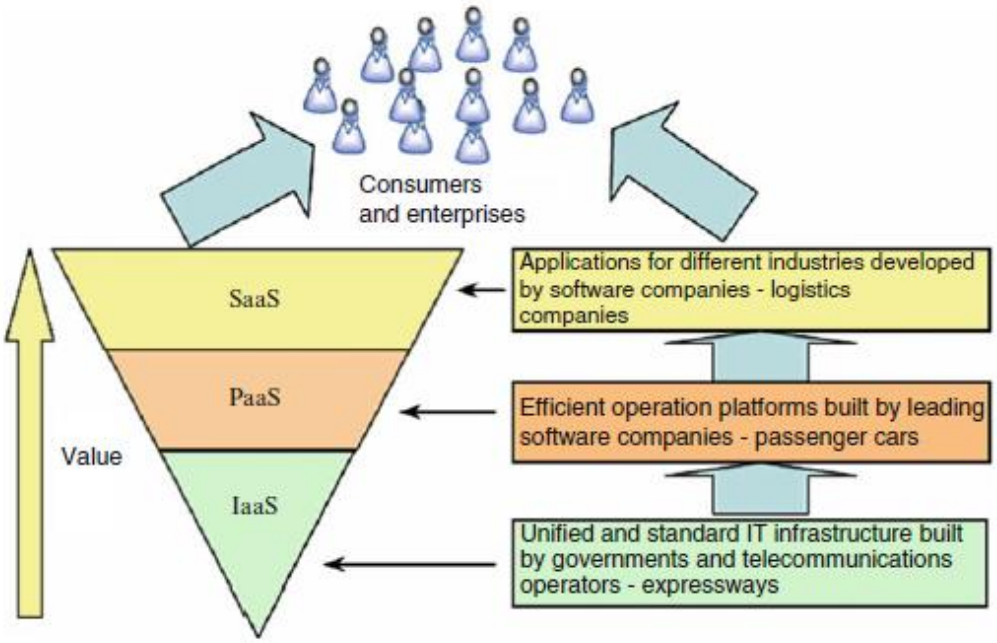
Tiedon sijainti ja liikkuminen eri konesaleissa voi aiheuttaa laillisuusongelmia. Yritys voi olla maantieteellisesti rekisteröity yhteen maahan, mutta sen tieto voi sijaita toisen maan hallinnoimassa levy-yksikössä. Rekisteröidyn maan viranomaiset voivat tarvita pääsyä tähän tietoon esimerkiksi verotarkastuksissa tai tutkiessaan tietoturva- tai talousrikoksia. Tieto voi olla tallennettuna sellaisessa maassa, joka ei hyväksy pääsyä kyseisiltä instansseilta. Tämä voi vaikeuttaa viranomaistoimia. Tietoon pääsy on Euroopan unionin sisällä säänneltyä ja turvattu yhteisellä direktiivillä, mutta jos tieto sijaitsee muissa maanosissa, siihen pääsy voi olla riski. Esimerkiksi Yhdysvaltojen veroviranomainen ei välttämättä saa tietoja Ranskassa olevalta pilvipalvelun toimittajalta. EU:n ”turvasatama”-käytännöt taasen sallivat yksilön tietojen lähettämisen Yhdysvaltojen viranomaisille. Pilvipalvelua koskevaa lainsäädäntöä työstetään useassa maassa, joten tiedon lainsuoja muuttuu vääjäämättä tulevaisuudessa. [16, s. 449–452.]

2.4 Pilvipalveluiden globaalit toimittajat

Yrityksille suunnattuja julkisen pilvipalvelun (public cloud) tuottajia on useita, mutta suurimmat kansainväliset toimijat kesällä 2015 olivat Amazon Web Services (AWS), Microsoft Azure, IBM sekä Google. Julkisen pilvipalvelun toimittajana AWS on kaikkein suurin 29 %:n markkinaosuudellaan ja toisena Microsoft Azure IaaS -palvelullaan 12 %:n markkinaosuudellaan. [17.] AWS:n vuoden 2015 tulos oli 7,88 miljardia dollaria ja tuoton kasvu oli 68 % edellisestä vuodesta [18]. Microsoftin Azure IaaS- ja PaaS-palveluiden tulos oli vastaavasti 6,3 miljardia dollaria vuonna 2015, ja Microsoftista onkin kehittymässä voimakkaampi kilpailija. Yritysten omissa pilviratkaisuissa suurin alustan tarjoaja on tällä hetkellä VMware ja sen vSphere-alusta, joita käyttää 33 % yrityksistä [20]. Yksityisissä pilviratkaisuissa OpenStack-teknologia on saavuttamassa jalansijaa, sillä se tarjoaa lähes ainoana avoimeen lähdekoodiin perustuvaa teknologiaa [7].

Kiinaa ei voida olla huomioimatta, kun puhutaan pilvipalveluiden tuottajista. Kiinassa on tällä hetkellä yli miljardi internet- ja mobiililaajakaistakäyttäjää. Kiinassa on 56 miljoonaa pientä ja keskisuurta yritystä, joista 80 % haluaisi ryhtyä käyttämään ”pay-as-you-go” -mallia. Haasteitakin on, sillä esimerkiksi Bank of Chinan tuotanto pyörii IBM System Z -alustalla (main frame), ja vain pienimmät alueelliset pankit selviytyvät RS/6000-alustalla. Samanaikaisesti palvelutason pitää olla 99,99 %. Vuonna 2012 julkaistun 5-vuotissuunnitelman mukaan pilvipalveluiden on laskettu tuottavan Kiinalle 160 miljardia dollaria vuoteen 2015 mennessä. Pilvipalvelun tarjoaminen näin suuressa mittakaavassa ja halutulla palvelutasolla vaatii suunnattomat resurssit, joten tämä

tehtävä on määrätty valtionhallinnon paikallisille elimille. Paikallishallinto on velvoitettu rakentamaan kansallisen ja paikallisen tason konesaleja pilvipalveluille. PaaS-tasolla Kiinassa on rajoituksia datan säilyttämisestä, mikä sulkee pois ulkomaiset toimijat kuten AWS:in (vuodesta 2012), Microsoft Azuren (2013) ja IBM:n. Ulkomaiset toimijat ovat saavuttaneet vain pienen osuuden markkinoista. Kiinalaiset tuottajat kuten Alibaban Ali-Cloud, Sinan AppEngine, Baidu Frame Computing ovat kasvaneet markkinaosuuksiaan. [21, s. 8 –29.]



Kuva 6. Kiinan suunnitelma pilviorganisaatiosta. [21, s. 29.]

Vuonna 2010 Kiinassa oli viisi kaupunkia, joihin oli keskitetty pilvi-investointeja. Kaupungit olivat Peking, Shanghai, Shenzhen, Hangzhou ja Wuxi. Näistä Wuxin tarina on osoitus siitä, miten pilvipalvelut voivat muuttaa kaupungin suuntaa. Alun perin perinteikkäästä tekstiilien kutojasta ja valmistajasta tuli tekstiilien kysynnän loputtua koodaajien kaupunki. Kaupunkiin rakennettiin yhteistyössä IBM:n kanssa BlueCloud-järjestelmän ohjelmointiin erikoistunut osaamiskeskus. Osaamiskeskus oli tehdas eri SaaS-sovellusten koodaajille. [21, s. 98 -103.]

Alibaban potentiaalista nousua on mielenkiintoista seurata, sillä pilvipalveluista vastaavan yrityksen Aliyun tavoitteena on nousta Amazonin ja Googlen ohitse suurimmaksi pilvipalvelun tuottajaksi kansainvälisellä tasolla. Keinona tämän päämäärän saavuttamiseksi on yhdistää Googlen teknologia ja Amazonin operointikyky

ja samalla kehittää tähän palveluun integroitua tietoseulontaa ja verkosto-ominaisuuksia, joilla saavutetaan laajoja markkina-alueita ja liiketaloudellista kiinnostusta ulkomaita myöten. [21, s. 159.]

2.5 Amazon Web Services -pilviympäristö

Amazon Web Services on pilvipalvelu, joka tuottaa yrityksen tilaaman palvelun asiakasinstanssina ja laskutus perustuu käytettyihin resursseihin. Yrityksen ostaessa Amazon Elastic Compute Cloud (Amazon EC2™) -instanssin siihen tulevat seuraavat palvelut automaattisesti:

- Amazon Machine Image (AMI) -mallista luotu virtuaalinen palvelin. Palvelimella on valittu käyttöjärjestelmä ja palvelun vaatimat ohjelmistot asennettuina.
- Instanssin teholuokan mukaan prosessoreita, muistia, tallennustilaa ja verkkokapasiteettia. Resurssit voidaan määrittää automaattisesti mukautuviksi huippukausien ja hiljaisten aikojen välillä.
- Käyttäjätunnus AWS:n instanssien hallintaan ja operointiin. Käyttäjätunnus on salattu, AWS:ään kirjautuessa tarkistetaan käyttäjän henkilökohtainen avain.
- Pysyvää tallennustilaa AWS:n omasta Elastic Block Store (EBS) -järjestelmästä.
- Palvelu voidaan ostaa toimimaan eri saatavuusvyöhykkeillä, jotka ovat maantieteellisesti rajattuja. Tietoja voidaan tallentaa instanssin sisällä eri alueellisiin keskuksiin. Eri vyöhykkeille sijoitetut instanssit parantavat globaalia saatavuutta palvelulle.
- Asiakastiliin sidottu ”Elastic IP address” eli staattinen IP-osoite, joka voidaan siirtää instanssilta toiselle ilman katkoa. Osoite on vyöhykekohtainen, esimerkiksi eurooppalaiselle verkkokaupan palvelulle on osoite, joka voidaan jakaa joko Saksassa tai Italiassa olevien instanssin käyttöön. Amerikan markkinoilla palvelua pitää suorittaa toisella elastisella IP-osoitteella.
- Ohjelmistollinen palomuuri, mitä kautta sallitaan liikenne, portit tai ryhmät, joilla on pääsy instanssin palveluihin.
- Oma virtuaalinen verkkosegmentti, joka on erillään muiden asiakkaiden tietoliikenteestä. Tarvittaessa tämä segmentti voidaan yhdistää oman yrityksen verkkoon, jolloin se näkyy virtuaalisena yksityisenä pilvenä (VPC).
- Pankki- ja luottokorttitietojen käsittelyn (PCI DSS) mukainen alustapalvelu. [22.]

Perusominaisuuksien lisäksi kokonaisuuteen voidaan yhdistää erilaisia palveluita, kuten relaatiotietokantainstanssit, kuormanjako instanssien välille, välimuistipalvelut nettipalvelimille, jne. EC2-palvelun lisänä tai erikseen voidaan ostaa Amazon S3 -tallennuskapasiteettia, joka on optimoitu erityyppisille datan käyttötavoille. On olemassa S3-tallennuskapasiteettia, joka on optimoitu datalle, jossa ei tapahdu paljon muutoksia. Arkistolevystä maksetaan aina erikseen ja sitä voidaan käyttää esimerkiksi jonkin sisäisen järjestelmän arkistona tai varmistuksena. Tietoja ei synkronoida päivittäin levylle vaan kerran viikossa tai harvemmin. Amazon EC2 -palveluita ja palvelimia voidaan hallita AWS:n oman nettikonsolin, komentorivin tai Windows PowerShellin kautta. [23.]

Amazon EC2 -palvelussa AMI-palvelimien tuetut käyttöjärjestelmät ovat Microsoft Windows -palvelinversiot sekä useat eri Linux- ja Unix-variantit. Suurin osa AWS:n palvelimista toimii Ubuntu Linux- tai Amazon Linux -käyttöjärjestelmillä [24]. Käyttäjät voivat tuoda palvelimiin omia sovelluksiaan, mutta esimerkiksi kaikki Windows-sovellukset eivät ole tuettuja. AWS:n palvelun vahvuus on Amazonin oma ydinosaaminen, ja se tuottaakin menestyksekkäästi erilaisia logistiikan, verkkokaupan tai maksamisen palveluita. Asiakkaat voivat ottaa vähällä vaivalla käyttöön uuden verkkokaupan. Sovelluksiin vain täydennetään yritysten omat tiedot. Palvelua voidaan pyörittää eri saatavuusvyöhykkeisiin sijoitetut AMI-palvelimilla, mikä mahdollistaa korkean saatavuuden. AWS:n luvattu palvelutaso on 99,99 % vuokra-ajasta, toteutumaton palvelu hyvitetään hinnasta. [25.]

Amazon on laajentanut tarjontaansa pois virtuaalisista instansseista. Asiakkaat voivat vuokrata oman alustapalvelimen Amazonin pilvestä. Tässä yhdelle asiakkaalle omistetun fyysisen instanssin sisälle sijoitetaan vain kyseisen asiakkaan virtuaalipalvelimia ja palveluita. Virtuaalipalvelimien välisten piilotetun väylän hyökkäykset voidaan sulkea pois. Omistettu instanssi voi tulla kalliiksi, jos siellä ei ole käytössä tarpeeksi virtuaalipalvelimia. Omistetuissa isäntäkoneissa voidaan ajaa määrättyjä AMI-palvelimia. Vain Ubuntu Linux -palvelimet ovat tuettuja. Omistetuissa instansseissa ei voi pyörittää Microsoft Windows Server- tai Centos AMI -palvelimia. [26.]

Amazon on julkaissut vuonna 2015 17 tietoturvatiedotetta [27]. Tiedotteet koskivat AMI-palvelimien käyttöjärjestelmä haavoittuvaisuuksia. Amazonin omasta alustasta olevia tiedotteita ei ollut. Tiedot alustasta ovat hyvin niukat, joten mahdollisten teknisten riskien arvioiminen voi olla haastavaa.

2.6 Microsoft Azure -ympäristö

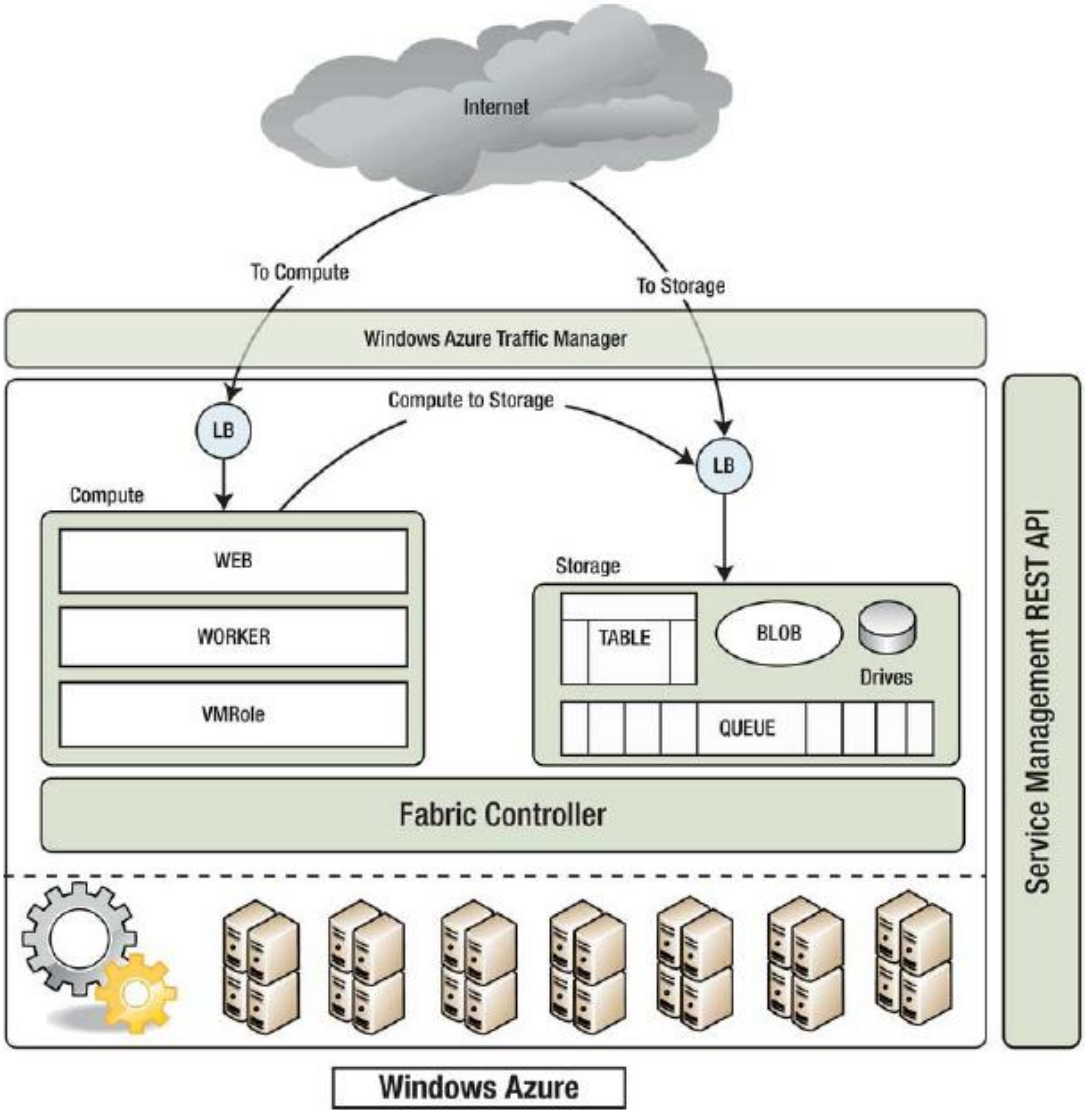
Microsoftin vastaus Amazonille oli julkaista Windows Azure -alusta vuonna 2008 kehittäjien konferenssissa [9, s. 10]. Aluksi Windows Azure miellettiin ”käyttöjärjestelmäksi”, ei palveluksi. Windows Azuren nimi muuttui Microsoft Azureksi 3.4.2014 erotukseksi Windows-käyttöjärjestelmistä [28]. Microsoftin Azure-palvelut pyörivät 6 eri konesalissa kolmessa eri maanosassa. Isäntäkoneissa käyttöjärjestelmänä on Microsoft Windows Server 2008 tai 2012 ja virtuaaliteknologian hypervisor on Hyper-V-tuotteeseen perustuva. [9, s. 11 -14.]

Microsoft Azure -palveluun kuuluu asiakkaan omat virtuaaliset palvelimet: ”peruspalvelut” eli DNS, Azure AD -kotihakemisto, reitittimet, kytkimet ja kuormanjakajat (verkkopalvelut), sekä erillinen raportointi- ja laskutusseuranta [9, s. 14]. Kilpailun kiristyessä Microsoft on joutunut laajentamaan palvelintarjontaansa. Syksystä 2015 lähtien Microsoft Azuressa on tuettu ja mallinnettu Linux-käyttöjärjestelmällä olevia palvelimia. Linux Integration Services (LIS) -ajurit voi ladata Microsoftin sivuilta, jos asiakkaat haluavat luoda oman Linux-koneen ja tuoda sen Azure-palveluun. Tuetut käyttöjärjestelmät ovat Centos 6.3, 6.4, CoreOs 494.4, Debian 7.9, 8.2, Oracle Linux 6.4, 7.0, Red Hat Enterprise 6.7, 7.1, Suse Linux Enterprise 11 SP3+, 12, openSuse 13.1 sekä Ubuntu 12.04, 14.04, 15.04, 15.10. [29.]

Windows Azuren tarjontaa voidaan jakaa kolmeen erityyppiseen palveluun: laskentakapasiteettiin, tallennuskapasiteettiin ja palveluiden hallinta. Laskentapalvelu tarkoittaa palvelimen käyttöä. Tässä laskutetaan niistä resursseista, joita käytetään. Asiakas voi laskentapalveluiden puitteissa tilata ja pyörittää kolmen tyyppisiä Windows-palvelimia. Valmiissa Windows-nettipalvelimessa on asennettu IIS-rooli ja siellä voi suorittaa palveluita jotka tarvitsevat toimiakseen php-, c++-, FastCGI-, ASP.NET- ja Java-tukea. Windows-sovelluspalvelimessa voidaan ajaa erilaisia taustapalveluita kuten tiedostojakoja, tulostinpalveluita tai muita palvelinrooleja Windows Server -käyttöjärjestelmästä. Asiakasyritykset voivat tuoda omia palvelimia erillisestä levykuvasta (vhd). [12, s. 14-15.]

Palvelimille on tarjolla kolmea erilaista levytilaa riippuen siitä, mitä dataa halutaan tallentaa. Azuressa voi ostaa levykapasiteettia itsenäisenä palveluna esimerkiksi jatkuvuussuunnitelman varmistuksen tarpeisiin. Blob-tyyppinen levy soveltuu tavallisen datan tallentamiseen, jolloin virtuaalipalvelimet voivat käyttää sitä käyttöjärjestelmä levynä tai tallennusmediana. Jonotyyppinen levy sopii esimerkiksi sanomaliikenteen

tallennustyypiksi tiedolle, joka suoritetaan tietyssä järjestyksessä. Taulukkotyyppiselle levytilalle on hyvä tallentaa kevyttä rakenteellista dataa, esimerkiksi nettisovellukset tallentavat tälle levylle käyttäjän sessioinformaatiota. [12, p. 16 -26.]



Kuva 7. Microsoft Azuren palvelutarjonta, [12, s. 17.]

Ohjelmistokehittäjille sovelluksen ja Azuren hallintaa on helpotettu integroimalla tunnetuimpia ohjelmointivarantoja Azuren käyttöön. Kaikkia Azure-palveluita, kuten levylle tallentamista voidaan kutsua REST API -liittymän komentojen avulla suoraan sovelluksesta. Sovelluspalvelinten ohjelmakoodi voidaan Azuressa tehdä tallentamalla lähdekoodi tietovarantoon kuten GitHubiin ja päivittää sen avulla kaikki sovellukset samaan versioon vaivattomasti. [12, s. 26–27.]

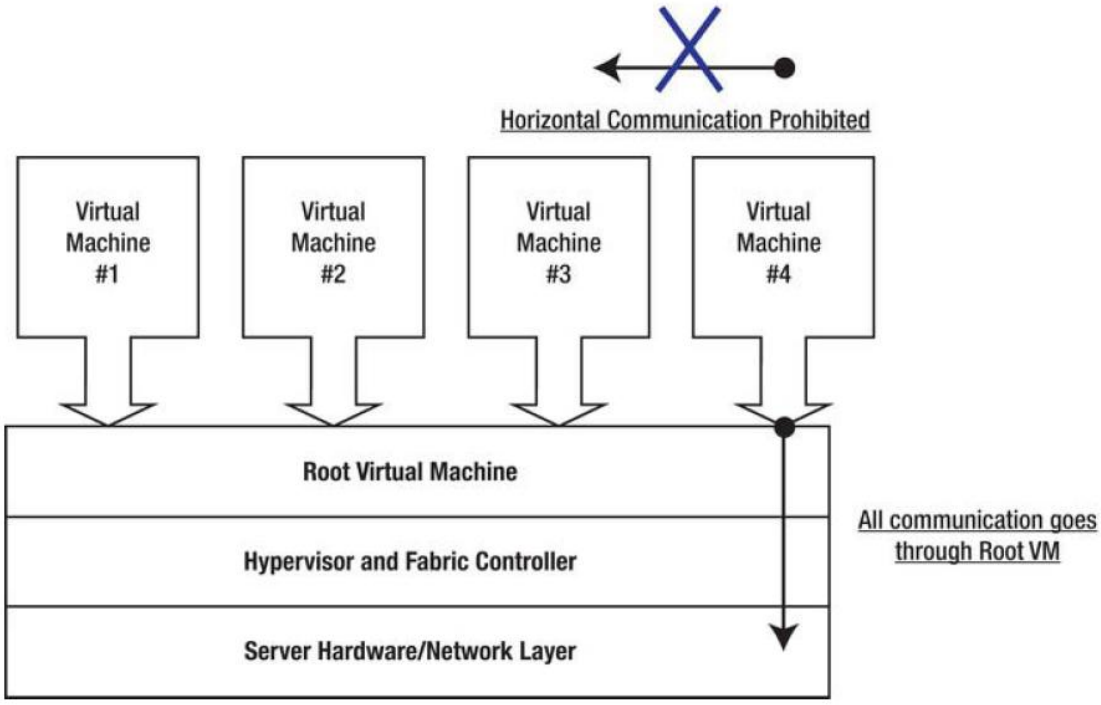
Azure SQL on erillinen palvelu, josta tarjotaan relaatiotietokantapalveluita, mutta sitä voidaan helposti käyttää myös Azuressa olevien sovelluspalvelinten SQL-tarpeisiin. SQL-palvelussa asiakkaan instanssista säilytetään eri konesaleissa kolme replikoitua kantaa, mikä parantaa saavutettavuutta. Yhden instanssin vaurioituessa toinen SQL-palvelin eri konesalissa voi pyörittää instanssia seuraavaksi. [12, s. 497.] Azuren omien tietokantainstanssin lisäksi kantoja voidaan synkronoida asiakkaan omaan infrastruktuuriin tai toiseen maantieteelliseen Azure-instanssiin. Datan siirtoon voidaan käyttää TDS-palvelua, joka tukee useita eri protokollia kuten ODBC, JDBC, ADO.NET, LinQ ja Frameworks. Azuren SQL sisältää myös raportointipalvelinominaisuuden, joka mahdollistaa esimerkiksi TFS:n käytön. Azure SQL -instansseihin voidaan konvertoida tietoja Access-, Oracle-, DB2-kannoista. Yrityksen kannattaa siirtää omassa infrastruktuurissa oleva kanta Azuren SQL-palveluun, jos sovellusta ajetaan Azuresta. Sovelluksen ei enää tarvitse kysellä tietoa verkon ylitse, joten tiedonsiirtomaksut vähenevät. Tiedonsiirtomaksuja voi tulla, jos tietoja replikoidaan eri maantieteellisten konesalien tai etäpisteiden välillä. [12, s. 28 -31.]. Pelkän SQL-palvelun käytössä on rajoitteita, kuten esimerkiksi mahdollisuus käyttää vain SQL-kirjautumista, mikä heikentää tietoturvaa. Azure SQL:ssä ei ole myöskään mahdollista varmistaa kantoja. Kantojen varmistus tehdään ottamalla niistä manuaalinen kopio, joka siirretään yrityksen omaan infraan tallennusta varten. [1, s. 68 -70.]

Azuren sovelluskudos (AppFabric) on ohjelmallinen rajapinta, joka toimii viestikeskuksena pilvipalvelussa olevan sovelluksen ja muun maailman välillä. Se vastaa pilvessä olevan sovelluksen pääsynhallinnasta. AppFab tarjoaa integroinnin asiakkaan omiin sovelluksiin käyttäen luotettua sovellussalausta yhteyden muodostamiseen. Sovelluskudoksen avulla Azuressa pyörivälle sovellukselle voidaan allokoida väliaikaista tilaa sovelluksen tietojen tallennukseen. Täten sovelluksen ei välttämättä tarvitse aina kysellä asiakkaan AD:lta tietoja, vaan se voi tallentaa käyttäjän tilan välimuistiin. Sovellusten kehittäjille tämä ominaisuus luo helpon mahdollisuuden integroida sovellus asiakkaan omassa palvelussa oleviin järjestelmiin. [12, s. 32 -32, s. 486.]

Microsoft Azuren hallintaa ja operointia helpottaa yhteensopivuus Windows PowerShell -ohjelman kanssa. Uusin versio PowerShellin Azure-komentolaajennuksista on 1.0.2. Microsoft Azuren hallinta- ja operointityökalut muuttuvat uudistusten ja kehitystyön tuloksena välillä nopeastikin. Uudistuksista ehkä merkittävin on ollut siirtyminen ”Resource Manager” (RM) -moodiin. RM-mallissa luotuihin palvelimiin ja palveluihin voidaan kohdistaa uusia Azure-funktionaalisuuksia kuten BitLocker-salausta ja Key Vault -avainten hallintaa. Kaikki funktionaalisuudet eivät ole yhteensopivia aikaisempien

luotujen palvelinten kanssa, mikä voi hämmentää käyttäjiä. Hallintasivustoa uudistettiin ja luotiin uusia käsitteitä kuten resurssiryhmä aikaisemman tilitunnisteen tilalle. PowerShellissä otettiin käyttöön RM-komentosarjat erotuksena aikaisempiin ja laajennettiin käytettävyyttä. [30.]

Tietoturvahaasteisiin Azuressa on vastattu usealla eri tavalla. Fyysisten jaettujen resurssien käyttöä on rajoitettu. Virtuaalisten palvelinten välinen komento tai käskyliikenne ei ole sallittu hypervisor- tai sitä ylemmillä tasoilla. Tällä ehkäistään piilotetun väylän käyttöä. Asiakkaan kaikki virtuaaliset palvelimet kommunikoivat vain yhden juuripalvelimen kautta. Juuripalvelin on asiakaskohtainen ja siinä on käytössä oma virtuaalinen palomuuritoiminnallisuutensa. Juuripalvelin luottaa komentojen suorittamisessa vain sen kanssa yhteistyössä toimivaan hypervisoriin. Hypervisor ei luota yhteenkään virtuaaliseen palvelimeen. Hypervisorilla on oma palomuuripalvelu, jossa määritetään sallittu tietoliikenne juuripalvelimelle ja virtuaalipalvelimille. Tämä palomuuri on eri asia kuin Windows-palomuuri. Hypervisor vuorostaan välittää käskyt fyysiselle palvelimelle, huomioitavaa on, että jokaista virtuaalista palvelinta ajetaan omassa prosessoriytimessään. Virtuaalipalvelimet eivät pääse käyttämään hyväksi prosessorin jaettua välimuistitilaa. [12, s. 57.]



Kuva 8. Microsoft Azuren tietoturva-arkkitehtuuri palvelintasolla. [12, s. 58.]

Kaikissa virtuaalisissa palvelimissa sovelluksia ajetaan mahdollisimman alhaisilla oikeustasoilla. Sovelluksessa ja Windowsissa voidaan käyttää esimerkiksi levyjen salausta, Windows-palomuureja, SSL-suojausta jne.

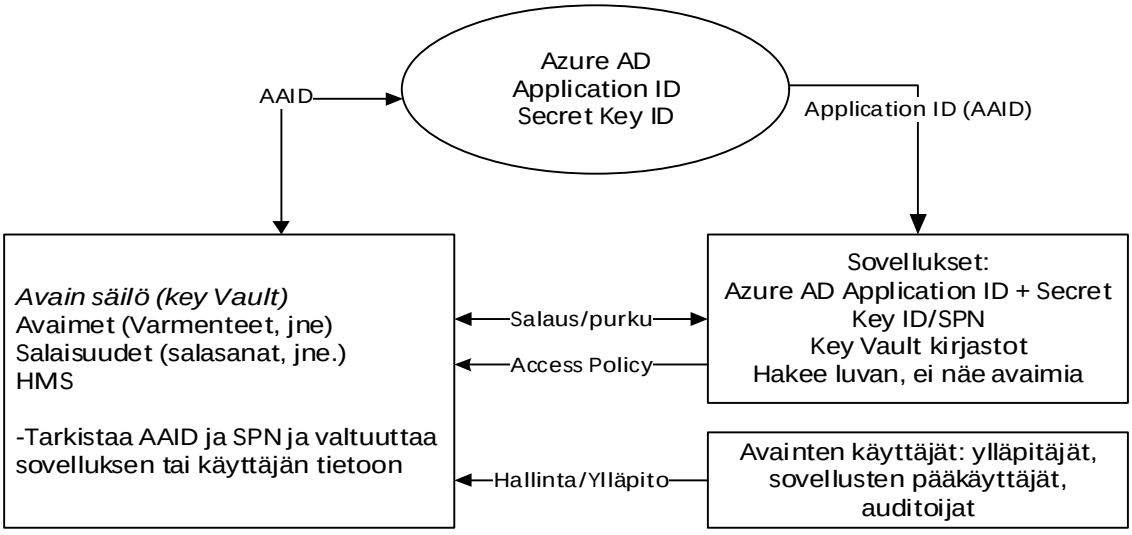
Microsoft Azuressa olevat Linux- ja Windows-palvelimien käyttöjärjestelmä- ja datalevyt voidaan salata joko DM-Crypt- (Linux) tai BitLocker (Windows) -ohjelmilla. Salausavaimet tai käytetyt salaisuudet voidaan tallentaa Microsoft Azure Key Vault -palveluun. Levyjen salausta voidaan käyttää kolmessa erityyppisessä IaaS-palvelimessa:

- Asiakkaan omista levykuvista tehdyt palvelimet, joissa on käytetty asiakkaan omia avaimia.
- RM-mallilla tehty uusi palvelin.
- RM-mallilla tehdyssä palvelimessa, joka on jo olemassa. [31.]

Jos palvelin ei ole mikään yllämainituista eli sitä käytetään osana SaaS-palvelua, tai jos ostetaan vain levytilaa tai kyseessä on klassisen mallin mukaan tehty IaaS-palvelin, niin silloin ym. salausohjelmia ei voi käyttää. Palvelin ja levyt on suojattava silloin käyttäen kolmannen osapuolen tuotteita. [32.]

Key Vault -avaintenhallintapalvelu on käytössä vasta uusien RM-mallin Azure-portaalin tehtyjen palvelinten kanssa. Key Vault -palvelua voi operoida vain PowerShell-komentojen kautta. Jokainen Key Vault -säilö on sidottu yhteen Azure-alueeseen, ja käytettävän palvelun ja säilön on sijaittava samalla alueella, jotta operointi on mahdollista. Avainsäilöön ei tallenneta tietoja tai tiedostoja salattavaksi, vaan siellä säilytetään avaimia ja salaisuuksia. Säilö on varmentaja, joka päättää, voiko sovellus salata tai purkaa tietoa. Sovelluksen, jolle oikeus salaukseen halutaan antaa, pitää olla rekisteröity Azure AD -oletushakemistoon. Azuren AD:ssa sovellukselle luodaan yksilöllinen ID-tunniste (Azure AD Application ID AAID) sekä salaisuusavain (Secret key ID). Luonnin yhteydessä sovellus linkitetään AD:n URI -yksikön haltijaksi. [33.] Sovellus voidaan ohjelmoida .NET-kirjaston avulla käyttämään näitä URI-, AAID- ja salausavaimia ja avainsäilöä automaattisesti tiedostoja luettaessa tai ladattaessa [34]. Kun sovellus salaa tai purkaa tietoa, se kutsuu Azuren Key Vault -säilöä ja kysyy lupaa salauksen purkamiseen. Avainsäilön hyväksyessä sovellus ID:n ja salaisuusavaimen voidaan salaus/purkaminen suorittaa. Avainsäilöä käytettäessä tietoturva paranee, sillä avaimia tai salaisuuksia ei näe tai voi operoida kuin asiakas itse, mikä sulkee pois vilpilliset ylläpitäjät. Tieto ei liiku levyltä mihinkään ilman valtuutusta, joka haetaan keskitetystä

järjestelmästä. Käyttäjät eivät tarvitse avaimia, sovellukseen kirjautumisen yhteydessä heidän tunnuksensa sulautetaan sovelluksen identiteettiin. [33.]



Kuva 9. Key Vault -toiminnan periaatteet

Avaimia hallitaan ylläpitäjien ja roolien kautta. Avainten hallintaa ja sovellusten sallimista hallitsevat avainsäilön omat ylläpitäjät. Heidän tehtäviinsä kuuluu luoda sovellukselle säilöön oma avain/salaisuus. He antavat sovellukselle oikeuden käyttää säilöä toimintojen tarkistamiseen. He voivat poistaa sovelluksen oikeudet ja avaimet. Sovelluksen pääkäyttäjät voivat nähdä omat avaimensa säilössä, mutta eivät voi muuttaa niitä. Auditoijat voivat taasen lukea salauksesta kertyneitä lokeja. [33.]

Salaus tehdään Azuren levytyypeissä eri tavoin. Blob-levyissä salaus tehdään käyttäen ns. kirjekuorisalausta. Ensin tieto salataan satunnaisella symmetrisellä avaimella. Sen jälkeen symmetrinen avain salataan epäsymmetrisellä avaimella. Epäsymmetrinen salausavain tallennetaan esimerkiksi Key Vault -palveluun. Kun suojattua tietoa ladataan blob-levylle, samalle blobille tallentuvat salattu symmetrinen avain ja sen metadata. Tiedon purkamisessa puretaan ensin symmetrisen avaimen epäsymmetrinen salaus Key Vaultin avulla. Symmetrisellä avaimella puretaan itse salaus tiedostolta/levyltä. Tämä nopeuttaa levyn käsittelyä, sillä symmetrinen salaus on nopeampaa, ja epäsymmetrinen salaus on tehty vain salausavaimelle ja vain tämä pitää purkaa. [35.]

3 Azure SharePointin käytännön toteutus

Azure-palvelu sisältää valmiit virtuaalikoneet Microsoft SharePoint Server 2013 -farmiin. Vaihtoehdot ovat korkean käytettävyyden farmi ja yksittäinen SharePoint 2013 -palvelin. Microsoft suosittaa, että valmista farmia käytetään sovelluksen testaamiseen tai vikasietoisena varmistuksena yrityksen omalle farmille. Julkaisemattomasta uudesta SharePoint 2016 -sovelluksesta on olemassa testiversiot, joissa löytyvät niin ikään korkean käytettävyyden ja yksittäisen palvelimen mallipohjat. [36.] Työssäni valitsin toteuttamistavaksi yksittäisten palvelinten luomisen valmiista konemallista ja sen jälkeen SharePoint-farmin asentamisen manuaalisesti.

3.1 Microsoft Azuren toteutus

Microsoft Azuren portaalissa olen käyttänyt ”Resource Managerilla” (RM) toteutettuja virtuaalisia palvelimia. Kaikki luodut palvelimet on tehty käyttäen RM-palvelinmalleja, jotta niihin voitaisiin kokeilla mm. Key Vault -toimintoja ja salausta.

Käytännön toteutuksessa loin ensimmäiseksi omalla sähköpostitunnuksellani Microsoft Azureen palvelutilin, jossa käyttöalueena on Pohjois-Eurooppa. Tilaustapana oli ilmainen 30 päivän lisenssi, jonka aikana voin käyttää 170 euroa pilvipalveluihin. Rahalla voi ostaa palvelimille resursseja kuten laskentatunteja, enintään neljä prosessoriydintä, levytilaa, verkkopalveluita jne. Kirjautumisen jälkeen loin uuden oman resurssiryhmän, jolle annoin nimeksi KPMT2. Resurssiryhmän alle rakennettiin pilvipalvelun muut komponentit kuten virtuaaliset verkot, palvelimet, palvelut sekä levytilan hallinnoimiseen käytettävä asiakastili. Palvelinten levyinä käytettiin standardi-SAS-levyjä eikä oletuksena luotuja SSD-levyjä.

SharePoint 2013 -sovellus vaatii taustalle aktiivihakemistopalvelimen sekä SQL-palvelimen. Nämä palvelimet luotiin käyttäen Azure PowerShell -skriptejä. Halusin käyttää skriptejä, jotta voin arvioida niiden käytettävyyttä automatisoinnissa. Aktiivihakemistopalvelin toteutettiin valmiista Windows Server 2012 R2 -palvelinmallista. PowerShell-skriptissä määritellään aluksi useita muuttujia. Muuttujien alkuperäisiä ominaisuuksia lisätään eri set- tai get- käskyillä (cmdlet) tai yhdistelemällä muuttujia. Muuttujia operoidaan, kunnes siihen on liitetty kaikki halutut ominaisuudet. Esimerkiksi aluksi luodaan muuttuja nimeltään virtuaalinen palvelin. Tähän muuttujaan lisätään tieto levytilasta, teholuokan tieto, mistä käyttöjärjestelmästä tai sovellusmallista palvelin

luodaan jne. Lopuksi palvelin luodaan komennolla ”New-AzureRmVM ja komennon vaadittavat parametrit olivat resurssiryhmä, alue minne palvelin luodaan sekä luotavan palvelimen nimi. Palvelinten luomisessa käytetyt skriptit löytyvät liitteestä 1. Alla on osa komennoista, joilla muuttujia käsitellään.

```
$Interface = New-AzureRmNetworkInterface -Name $InterfaceName
-ResourceGroupName $ResourceGroupName -Location $Location -SubnetId
$VNet.Subnets[0].Id -PublicIpAddressId $PIp.Id

$Credential = Get-Credential

$VirtualMachine = New-AzureRmVMConfig -VMName $VMName -VMSize
$VMSize

$VirtualMachine = Set-AzureRmVMOperatingSystem -VM $VirtualMachine
-Windows -ComputerName $ComputerName -Credential $Credential
-ProvisionVMAgent -EnableAutoUpdate

$VirtualMachine = Add-AzureRmVMNetworkInterface -VM $VirtualMachine
-Id $Interface.Id

New-AzureRmVM -ResourceGroupName $ResourceGroupName -Location
"North Europe" -VM $VirtualMachine
```

AD-palvelimelle rakensin uuden aktiivihakemiston metsän nimeltään kpmt2.azure.local ja nostin palvelimen kpmt2dc1 toimialueen ohjauskoneeksi. Toimialueeseen liitettiin kaikki muut luodut palvelimet. DC-palvelimen Azure-portaalissa määritetyt DNS-asetukset piti muuttaa käyttämään yksilöityä DNS-palvelinta eli itseään. Muutos mahdollisti sisäisen DNS-alueen mainostamisen ja toimialueen käytön. Azureen ja internetiin se käytti julkisia DNS-asetuksia.

SQL-palvelin luotiin käyttäen samaa PowerShell-skriptiä, mutta käyttöjärjestelmän mallina oli Windows Server 2012, johon oli esiasennettu Microsoft SQL Server 2012. Vanhassa Azuren PowerShell-komennoissa pystyi luotavan palvelimen liittämään toimialueelle määrittelemällä komennossa add-azureprovisioningconfig domain-muuttujan arvon. Uudessa PowerShellissä tämä komento ei ollut käytettävissä vaan toimialueeseen liittäminen olisi vaatinut JSON-lisäosan käyttämistä GitHub-koodilähteestä. Minulla ei ollut tarvittavia taitoja tähän, joten palvelin luotiin työryhmään ja liitettiin manuaalisesti toimialueelle. Palvelimelle lisättiin levy, jolle SQL-tietokannat määritettiin tallentumaan.

Kolmannen palvelimen kohdalla käytin luomiseen sekä skriptiä että portaalin graafista käyttöliittymää. Olin tehnyt kaksi palvelinta aikaisemmin ja tässä kohtaa kokeilulisenssin neljän prosessoriytimen rajoitus tuli vastaan. Pystyisin luomaan SharePoint-palvelimen käyttäen vain yhtä prosessoria. Tämä ei täytä SharePoint 2013:n teknisiä vaatimuksia.

AD- ja SQL-palvelimien käytössä oli kolme ydintä, joten käytössäni oli vain yksi prosessoriydin ja tavallisessa A1-luokan palvelimessa oli vain 1,5 GB muistia. Loin SharePoint-palvelimen skriptin avulla, mutta siinä eivät tehot riittäneet SharePoint 2013 -palvelun käyttöön. Tuhosin luodun palvelimen ja loin uuden palvelimen portaalin kautta käyttäen SharePoint 2013:n valmiiksi asennettua mallia. Valitsin palvelimen kohdalla teholuokaksi D1, jossa on yksi prosessoriydin mutta onneksi 3,5 GB muistia. Toinen vaihtoehto olisi ollut, että tuhoan aikaisemmat palvelimet ja luon tilalle yhden palvelimen. Uudessa palvelimessa minun olisi pitänyt ajaa sekä aktiivihakemistopalveluita että SQL-palvelinta samalla palvelimessa. Tämä ei ole Microsoftin suositusten mukaista. Loin siis SharePointista D1-tason palvelimen. Taulukossa 1 on esitetty palvelinten nimet, teholuokat sekä käyttöjärjestelmät.

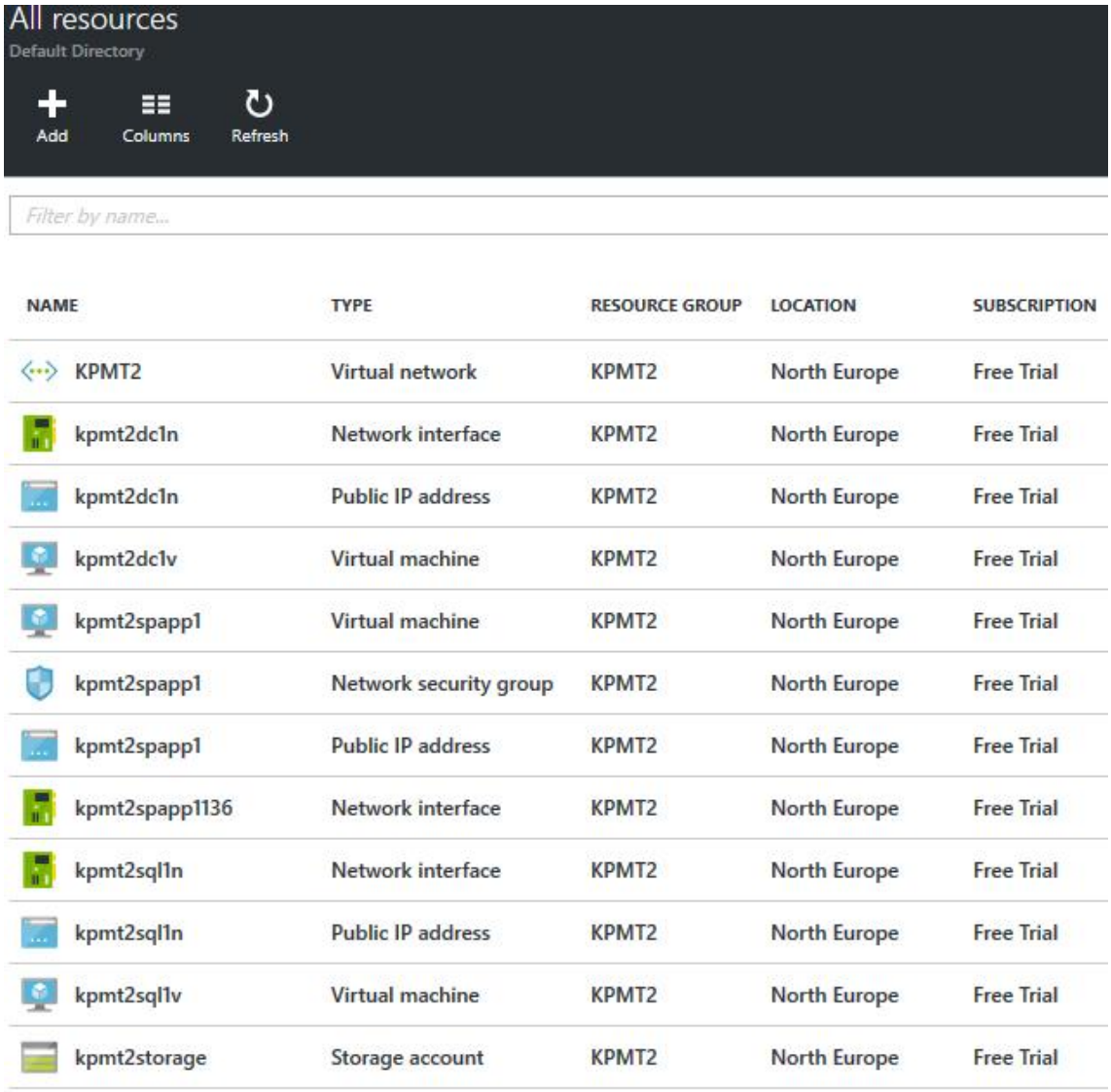
Taulukko 1. SharePoint 2013 -farmin palvelimet

Palvelimen nimi	**Teholuokka**	**CPU lkm**	**Muisti GB**	**Käyttöjärjestelmä**
kpmt2dc1	A1	1	1,75	Windows 2012 R2 Datacenter
kpmt2sql1	A2	2	3,5	Windows 2012 R2 Datacenter sekä SQL Server 2012 R2 SP2
kpmt2spapp1	D1	1	3,5	Windows 2012 Datacenter sekä SharePoint Server 2013

Erot graafisen ja skriptin välillä luoduilla palvelimilla olivat vähäiset. Skriptillä luoduissa palvelimissa voitiin määrittää eri nimet virtuaaliselle palvelimelle kuin mitä Windows-käyttöjärjestelmässä oli. Verkkokortin nimi pystyttiin määrittelemään helpommin tunnistettavaksi kuin portaalin kautta, jossa nimeksi tuli satunnaisia numeroita. Graafisesti luoduille palvelimille tulee oletuksena verkon tietoturvaryhmä (Security Group). Ryhmän avulla sallitaan tietoliikenne virtuaaliselle palvelimelle. Tämä palomuuri pystyy muokkaamaan hypervisor-tason sääntöjä. Onnekkaaksi yhteensattumaksi voi siis sanoa, että tein SharePoint-palvelimen portaalin kautta sillä kyseiselle palvelimelle piti sallia http-liikenne internetistä. PowerShellin kautta operoiminen palautti kontrollia takaisin käyttäjälle. Esimerkiksi loin levyhallintatilin uudestaan PowerShellin kautta, koska Azuren satunnaisesti arpoma nimi oli minulle liian haastava muistaa. Haasteellisuus oli toinen PowerShellin skriptien ominaisuus, niiden syntaksin ymmärtäminen oli aluksi hankalaa. Minulta kului lähes 1,5 päivää uuden virtuaalipalvelimen luovan skriptin kirjoittamiseen. Esimerkkejä löytyi kyllä internetistä mutta vasta useamman kokeilun ja erehdyksen kautta onnistuin. Yritys, joka tilaa paljon tai säännöllisesti palvelimia Azuresta hyötyy PowerShellin käytöstä. Aika joka kestää komennon suorittamiseen on lähes sama sekä PowerShellillä kuin hallintaportaalin

kautta. PowerShellillä palvelimen luonti on kuitenkin suoraviivaisempaa ja vähentää inhimillisiä virheitä, jos skripti automatisoidaan. Hallintaportaalin kautta joutuu kuitenkin useamman kerran hyväksymään asetuksia, kun PowerShellissä se tehdään enterin painalluksella.

Kuvassa 10 näkyvät kaikki resurssit, jotka luotiin KPMT2-resurssiryhmän alle.



Kuva 10. KPMT2-resurssiryhmä

DC- ja SQL-palvelimissa otettiin käyttöön sekä käyttöjärjestelmä- että datalevyjen salaus, salausavainten säilytykseen käytettiin Key Vault -palvelua. SharePoint-palvelimelle salausta ei otettu käyttöön, koska sillä oli pulaa resursseista. Aluksi luotiin uusi avainsäilö kpmt2holvi seuraavalla komennolla:

```
New-AzureRmKeyVault -VaultName kpmt2holvi -ResourceGroupName kpmt2
-Location "North Europe"
```

Palvelimille luotiin Azuren AD:n oman hakemiston alle kaksi uutta web-sovellusta, kummallekin salattavalle palvelimelle omansa. Molempien palvelimien Bitlocker-sovellukselle tuli oma Azure AD Application ID ja salausavain. PowerShellissä määritettiin resurssiryhmä, saatu AAID ja Secure KeyID muuttujiksi. Seuraavaksi avainsäilöön sallittiin lukuoikeus avaimiin tälle sovellukselle. Tämä pääsynhallinta pitää erikseen suorittaa. Normaalisti se on evätty. Lopuksi määritettiin, että suoritetaan BitLocker-asennus ja salaus automaattisella käynnistyksellä palvelimelle. Alla on esitetty osa käytetyistä komennoista. Komennot ovat täydellisinä liitteessä 2.

```
Set-AzureRmKeyVaultAccessPolicy -VaultName $KeyVaultName
-ServicePrincipalName $aadClientID -PermissionsToKeys all
-PermissionsToSecrets all -ResourceGroupName $rgname
```

```
Set-AzureRmKeyVaultAccessPolicy -VaultName $KeyVaultName
-ResourceGroupName $rgname -EnabledForDiskEncryption
```

```
Set-AzureRmVMDiskEncryptionExtension -ResourceGroupName $rgname
-VMName $vmName -AadClientID $aadClientID -AadClientSecret
$aadClientSecret -DiskEncryptionKeyVaultUrl
$diskEncryptionKeyVaultUrl -DiskEncryptionKeyVaultId
$KeyVaultResourceId
```

Salaus onnistui DC-palvelimella. Kaikki levyt saivat statuksen salattu. SQL-palvelimen kohdalla kryptaus epäonnistui ensimmäisellä kerralla. Ongelmana oli Windows-päivitysten automaattinen asennus. Palvelin oli päivän aikana löytänyt yhden Windows-päivityksen, ja asennuksen valmistuminen odotti uudelleenkäynnistystä. Olin sammuttanut palvelimelta kaikki ohjelmat ennen päivitystä, mutta en ymmärtänyt käynnistää palvelinta uudestaan asennuksen loppuun viemiseksi. Komennon alkaessa suorittaa BitLocker-asennusta ja uudelleen käynnistymistä BitLocker-asennus epäonnistui. Windows-päivitys asentui kyllä, mutta BitLocker ei asentunut. Kirjautuessani palvelimelle uudestaan BitLocker odotti uudelleen käynnistystä, jotta C:-levyn salaus voitaisiin suorittaa. Virheilmoitus jatkui ja jatkui, vaikka käynnistin palvelimen uudelleen useasti. Käynnistyksen yhteydessä tuli tapahtumien hallintaan virhe että BitLocker-ajuria ei löydy eikä sitä voida käynnistää. Lopulta tilanteen korjasi se, että ajoin uudestaan tuon PowerShell-komennon, jolloin palvelin käynnistyi oikein ja BitLocker asentui. Käyttöjärjestelmä- ja tiedostolevyn salaus suoritettiin onnistuneesti. Lopputuloksena kahden palvelimen levyt oli salattu, alla käytetty komento ja sen tulokset:

```
Get-AzureRmVm|Format-Table @{Label="MachineName";
Expression={$_.Name}}, @{Label="OsVolumeEncrypted";
```

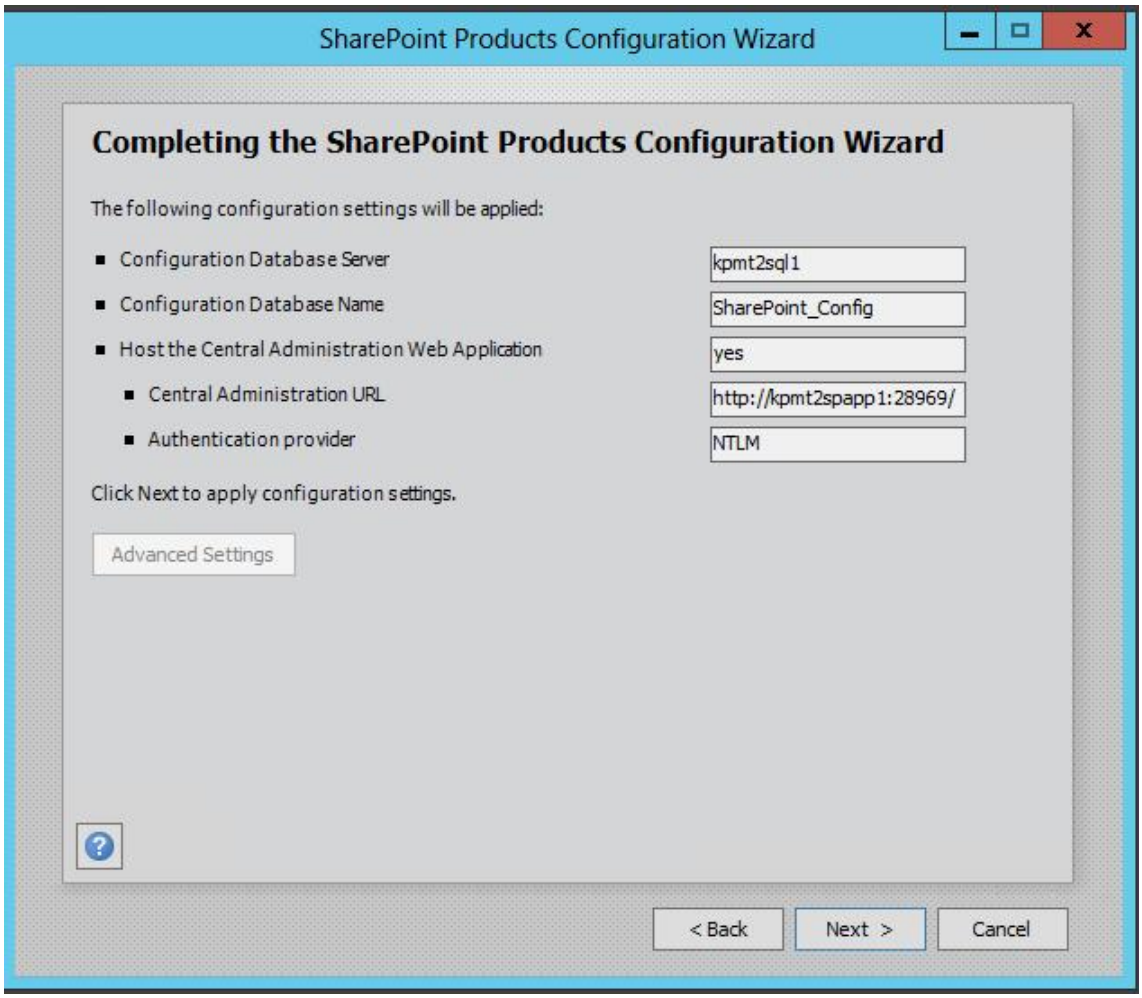
```
Expression=$osVolEncrypted}, @{Label="DataVolumesEncrypted";
Expression=$dataVolEncrypted}

MachineName          OsVolumeEncrypted    DataVolumesEncrypted
kpmt2dc1v            True                 True
kpmt2spapp1          False                False
kpmt2sql1v           True                 True
```

3.2 SharePoint 2013 -farmin toteutus

SharePoint toteutusta varten luotiin toimialueelle kolme palvelutiliä, kpmt2_spfarm, kpmt2_spserviceapp ja kpmt2_sphaku. Tilejä käytetään SharePoint-farmin palveluiden suorittamiseen. Kaikki tilit rekisteröitiin SharePointiin hallituiksi tileiksi, jolloin niillä on suoritusoikeudet sovelluksiin. Farmi luotiin käyttäen tiliä kpmt2_spfarm ja tällä tunnuksella suoritetaan palveluita kuten käyttäjäprofiilin synkronointi ja osaa farmin ajastuksista. Tunnuksella kpmt2_spserviceapp ajetaan verkkosovelluksen käytössä olevia palveluita kuten IIS-sovelluspoolia ja Excel-palveluita. Haun indeksointiin käytetään tunnusta kpmt2_sphaku. Hakutoimintoihin käytettävällä tunnuksella ei saa olla verkkosovellukseen enempää kuin lukuoikeudet. Suoritusoikeudet impersonoivat käyttäjän oikeudet väärin ja voivat näyttää liikaa tuloksia haussa.

SharePoint-farmin toteutusta varten luodulle SQL-palvelimelle (kpmt2sql1) lisättiin toimialueen pääkäyttäjä SQL-hallinnoijiin, SharePoint-tunnusten lisäys ja oikeuksien myöntäminen tapahtuivat täysin automaattisesti ja oikealla tasolla. Työssäni olen joutunut myöntämään erikseen esimerkiksi valvontaa suorittavan palvelutilin oikeuksia SQL:ään ja näiden saaminen oikein on välillä ollut haastavaa. SharePoint-farmin ja keskitetyn hallinnan sivuston rakentaminen epäonnistui kolmesti, koska SharePoint-palvelimella oli liian vähän prosessoritehoja käytössä. Epäonnistuneetkin yritykset loivat yleensä WSS_Content- ja spconfig-kannat, mutta muita kantoja ei onnistuttu luomaan. Onnistunut farmi saatiin lopulta rakennetuksi seuraavin määrityksin



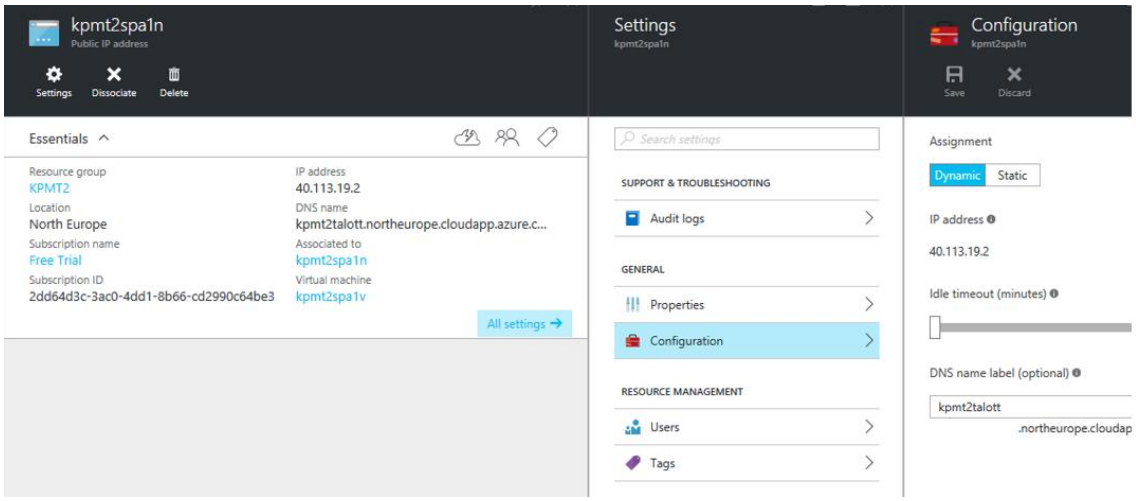
Kuva 11. SharePoint-määritykset.

Otin käyttöön kaikki palvelusovellukset, mutta realistisesti tätäkin olisi voinut rajoittaa. Näin lyhyen kokeilun ajalta ei tarvita välttämättä käytettävyystietoja tai Access-sovelluspalvelua.

SharePoint farmissa on käytössä kaksi verkkosovellusta: SharePoint - 80 ja keskitetty hallinta. SharePoint 80 -sovelluksessa julkaistaan ylimmän tason sivustokokoelma nimeltään http://kpmt2spapp1 käyttäen http-protokollaa. Azuren ulkoisen käytön mahdollistamiseksi sivustolle määritettiin vaihtoehtoinen yhdistämistapa (AAM). Vaihtoehtoinen osoite on http://kpmt2talott.northeurope.cloudapp.azure.com ja käyttäjille kohdentuvat SharePointin internetvyöhykkeen asetukset. Internetvyöhykkeen autentikointitapa on NTML, ja alla kuva SharePoint-asetuksista.

Kuva 12. Vaihtoehtoinen yhdistämisosoite.

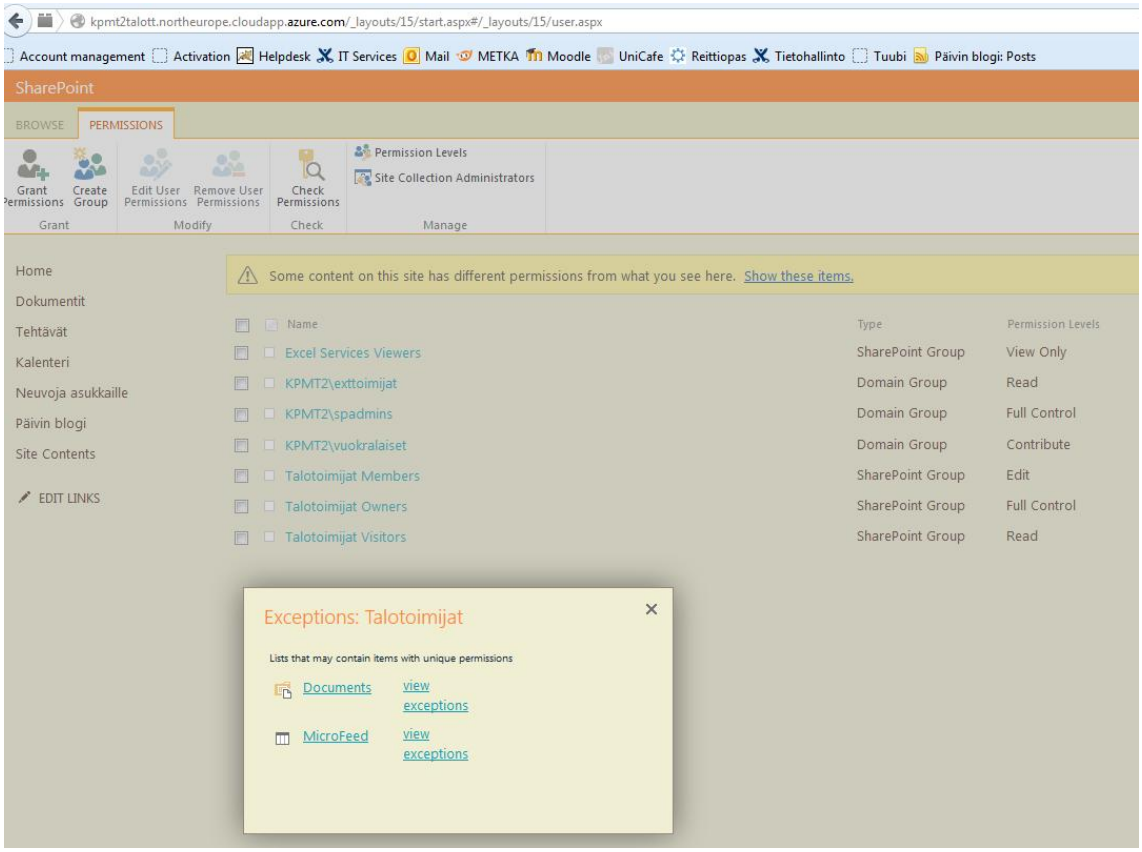
Azure-portaalissa pitää sallia http-liikenne tälle virtuaalipalvelimelle. Tämä asetus tehdään palvelimen verkon tietoturvaryhmän asetuksissa eli tässä muokattiin hypervisor-tason palomuuria. Vaihtoehtoinen yhdistämisosoite pitää lisätä Azuren hallinnassa palvelimen julkisen IP-osoitteen määrityksiin kohtaan DNS label. Tällöin sivusto oli löydettävissä Azure DNS -palvelun kautta.



Kuva 13. Julkisen IP-osoitteen sitominen sivuston osoitteeseen

Sivustolle kpmt2talott luotiin perussivusto, johon lisättiin eri verkkoelementtejä. Sivuston testausta varten toimialueelle luotiin seitsemän uutta käyttäjätunnusta, joista neljä on vuokralaisia, kolme vuokranantajan tai sidosryhmän edustajia. Pääsynhallinnassa käyttäjät tunnistautuvat toimialuetta vastaan. Käyttäjien hallinta ei tapahdu SharePointin omien ryhmien avulla eikä yksittäisinä käyttäjinä vaan AD-ryhmien kautta. Ryhmiä luotiin kolme: spadmins, vuokralaiset ja ulkoiset. Ylläpitäjät-ryhmään liitettiin kaksi sivuston ylläpitäjää, tälle ryhmälle annettiin sivustokokoelma tasolla täydet oikeudet. Vuokralaiset-ryhmään liitettiin muut vuokralaiset ja oikeustasoksi valittiin sivustokokoelmatasolla sisällöntuottajat. Muokkausoikeudet valittiin, jotta he voivat tarvittaessa kommentoida etusivun uutisia ja päivittää hyödyllisiä vinkkejä wikiin.

Ryhmällä ei ole oikeuksia lisätä käyttäjiä tai oikeuksia. Ulkoisia käyttäjiä varten luotuun ryhmään exttoimijat lisättiin ulkoiset jäsenet lukuoikeuksin sivustokokoelmaan.



Kuva 14. Oikeustasot SharePoint-sivulla

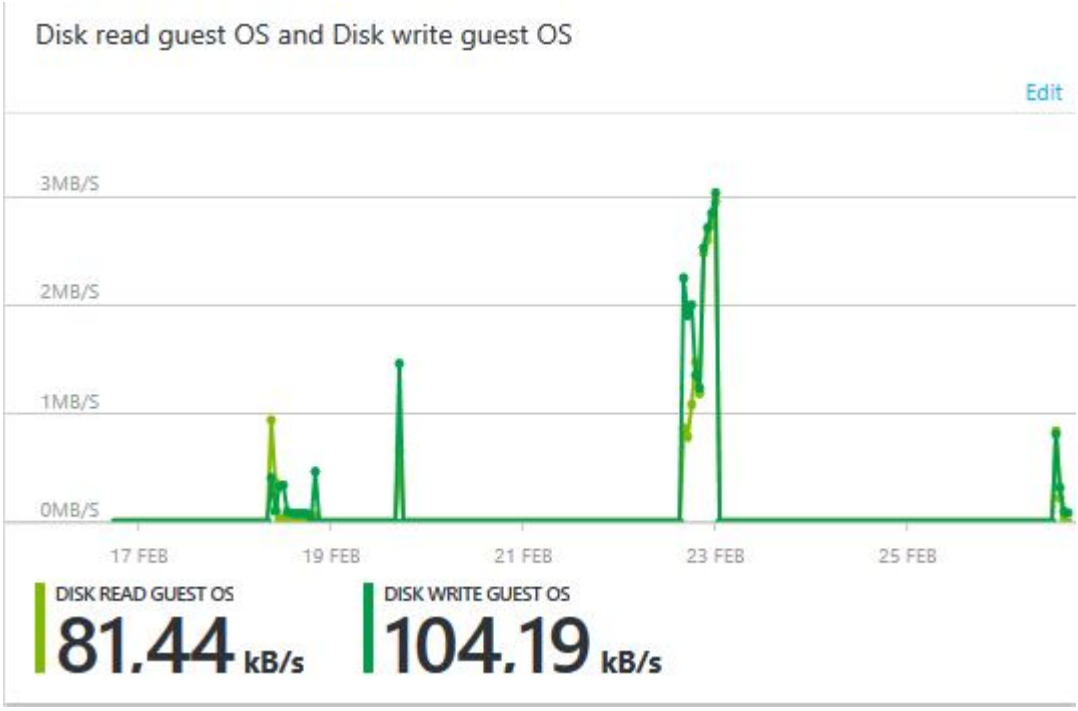
Sivustolle luotiin eri elementtejä eli wikisivut, blogisivusto, tiedostokirjasto, linkkipalsta ja yleisiä tehtäviä ja RSS syötteiden tilaus sallittiin kaikkiin elementteihin. Tiedostokirjastoon luotiin alihakemisto, johon määriteltiin erilliset oikeudet. Kansiosta poistettiin periytyvyys, muut käyttäjäryhmät poistettiin. Vain pääkäyttäjät pääsevät lukemaan ja muokkaamaan kansion sisältöä.

4 Tulosten tarkastelu

Microsoft Azuren toteutus onnistui mielestäni hyvin. Epäonnistumiset kuuluvat kokeiluihin, eikä ilman voi oppia. Tämä kokeilu hälvensi vastenmielisyyttäni PowerShell-operointia kohtaan, jatkossa toivottavasti käytän tätä työkalua enemmänkin. Hallintaportaalin visuaalinen ilme oli helppotajuinen, valikoiden selailu tapahtui jouhevasti, mutta toisinaan hitaasti. Osa sivun elementeistä kuten monitorointi-ikkuna ei

päivittynyt aina. On toki asioita, jotka ovat helpompia tehdä graafisesti kuin etsiä PowerShell-komentoja. Microsoftin kehittäessä Azure-portaalia uskon sen olevan mainio työkalu palvelinten hallintaan. Lisätään mukaan PowerShell-hallinta, niin käyttökokemus on loistava. Uskoakseni näitä isoja muutoksia, kuten RM-mallin lanseeraus ei tapahdu usein. Muutoksiin sopeutuminen voi kyllä viedä aikaa ainakin PowerShellin puolella. Useiden komentojen jääminen pois käytöstä vaikeuttaa skriptien suorittamista. Skriptejä tosin käyttää melko vähän ihmisiä, joten heiltä varmaan löytyy intoja ja taitoa muokata komennot uusiksi. Positiivisena pidän myös sitä, että Microsoftin omat Azure-blogit ja tukisivut ovat hyvin informatiivisia ja ajan tasalla, joten apuja löytyy tarvittaessa. Azuren valmiit palvelimet antavat loistavan tavan tutustua uusiin palvelinten käyttöjärjestelmiin ja sovelluksiin, siinä varmaan piilee Azuren suurin lumo ja hyöty.

Olin positiivisesti yllättänyt, että levyjen salaus onnistui verrattain vaivattomasti. Mielipiteeseeni ei vaikuta se, että salauksesta toinen epäonnistui aluksi. Levyn salaus ei näkynyt nousuna prosessorin kuormituksessa, arvot olivat samat sekä ennen että salauksen jälkeen. Salauksen kuormitusta levyn operoinnissa ei voinut järkevästi mitata, sillä pidin palvelimet sammutettuina säästääkseni ilmaisen tilauksen saldoa. SQL-palvelimen levyn valvonnasta voi jotain huomioita tehdä. Salaus tehtiin 23.2.2016, josta aiheutui piikki luku- ja kirjoitusoperaatioissa. Levyn kirjoitus- ja lukunopeudet eivät kuitenkaan muuttuneet huomattavasti salausta ennen tai sen jälkeen.



Kuva 15. SQL-palvelimen levyn valvonta

Kvantitatiiviset mittauksen latenssin eroista olisi pitänyt suunnitella etukäteen, mitä valitettavasti en tehnyt. Ennen salausta lukunopeutta olisi voinut testata esimerkiksi xcopy-komennolla kopioimalla levyjen sisällä tiedostoja. Azure-valvonnasta olisi seurattu haluttujen latenssista kertovien muuttujien tasoa. Salauksen jälkeen sama testi olisi tehty uudestaan. Kuormituksen erot olisi voitu havainnoida testin avulla. Suuntaa antavia johtopäätöksiä voi väljästi tulkita, eli tässä ympäristössä salaus ei hidastanut levyn kirjoitus- tai lukunopeutta. Salauksen vaikutusta voitaisiin tutkia tekemällä tiedostopalvelin, jossa on paljon usein toistuvia levytapahtumia. Levyn nopeuden muutos ennen ja jälkeen voisi antaa enemmän tuloksia. Tätä ei kuitenkaan haluttu tämän työn parissa testata, joten jätetään sen tutkiminen toiseen kertaan.

Pohtiessani, onko SharePoint-ympäristö sopiva pienen yhdistyksen viestintäkanavaksi, niin vastaus on kyllä ja ei. Teknologisilta mahdollisuuksilta se soveltuu hyvin, mutta taloudellisesti se on lähes mahdoton. Uuden SharePoint 2016 -järjestelmän normaalin yhden palvelimen farmissa prosessoriydinten määrä on minimissään 10. Laskin palvelintasolla, että kustannukset kuukaudessa olisivat vähintään 120 €. Vuodessa hinta tulisi olemaan yli 1400 €. Realistisesti ajatellen sivujen käyttö on vähäistä, mutta samalla niiden pitäisi olla päällä koko ajan. Yhdistyksen näkökulmasta hinta on liian korkea, jotta se toteutettaisiin.

Viimeisimmässä Azuren uutiskirjeessä Microsoft on varannut kolmen vuoden ajalle miljardi dollaria vapaaehtoisjärjestöjen käyttöön. Avustusten tarkoitus on helpottaa järjestöjen Azuren käyttämistä. Vaihtoehtoja tarkasteltaessa yksi olisi nettisivun ylläpitäminen Azuressa sivustojen kautta. Tarjolla on ilmaisia verkkosivuja käyttöön, mutta niissä on vähän levytilaa eikä niihin voisi luoda mitään SQL-kirjautumista. Nettisivu jaetulla nettipalvelimen IIS:ssä pääsynhallinnan kanssa maksaisi n. 8 € kuukaudessa. Oman nettipalvelimen hinta olisi n. 47 € kuukaudessa. Jaetulla nettipalvelimelle olevat sivut riittäisivät yhdistyksen tarpeisiin ja olisivat samalla kustannustehokas ratkaisu. SharePoint Online -palvelu on yksi vaihtoehto, siinä olisi mahdollista uutena ominaisuutena käyttää työnkulkuja ja ulkoista jakamista. Hinta peruspalvelulle olisi yhtä käyttäjää kohden n. 5 € kuukaudessa. Käyttäjien määrän ollessa alle 10 tämä voisi olla tutkimisen arvoinen mahdollisuus.

SharePointin käytettävyyttä ja oikeuksien todennusta testasin kirjautumalla sivuille eri tunnuksilla ja tarkistin heidän oikeutensa sivustolle. Testatessani sivustoa pääkäyttäjän oikeuksilla näin kaikki kansiot, muokkasin tiedostoja sekä sivuja ja poistin käyttäjien oikeuksia. Haku löysi muilta salatut asiakirjat ja näytti ne haun tuloksissa. Käyttäessäni

muokkausoikeuksilla olevaa tunnusta en nähnyt salattua kansiota. Pystyin kommentoimaan blogeja ja suorittamaan tehtäviä ja muokkaamaan tiedostoja. Hakutuloksissa ei löytynyt dokumenttia, joka sijaitsi salatussa kansiossa. Käyttäjä ei pystynyt muokkaamaan sivuston oikeuksia. Ulkoisen käyttäjän oikeuksilla pystyin vain lukemaan sivuja eikä haku löytänyt salattuja dokumentteja. Indeksointi ja hakusovellus toimivat oikein näyttäen vain käyttäjän oikeuksilla luettavaksi sallitut dokumentit. Olin todella tyytyväinen siihen, että Azuressa voi julkaista sivuston näin helposti. Vaihtoehtoinen yhdistämistapa ja julkiseen IP-osoitteeseen sidottu sivu oli toimiva ratkaisu internetin käyttäjille. SharePoint-sivusto toimi ilman teknisiä virheitä, vaikka sille oli allokoitu yksi ydin. Alun vaikeuksien jälkeen en saanut virheitä vaikka sivut olivat hitaita.

SharePoint sopii kyllä yhdistyksille, mutta yrityksille se on erinomainen Azure-pilvipalvelussakin. SharePointin päivittäminen ja yksilöidyt sovellusratkaisut (wsp-paketit) on helppo ottaa käyttöön, Azuressa on nimittäin mahdollista käyttää TFS-palvelua ohjelmien versionhallintaan ja jakeluun. TFS:n käyttö on mahdollista ainakin WAWS kautta. Olen työssäni hiukan seurannut mitä TFS:llä voi tehdä. Esimerkiksi yrityksellä on Azuressa yli 10 SharePoint-palvelinta, he voivat jaella uuden päivitetyn wsp-paketin kaikille palvelimille TFS:n kautta ja samalla päivittyy tietoa, mikä version palvelimelle on asennettu.

5 Yhteenveto

Kohtasin insinöörityötä tehdessäni haasteita, kaikki asiat eivät onnistuneet ensimmäisellä kerralla. Haasteet eivät kuitenkaan estäneet lopputulokseen pääsemistä, sain luoduksi talotoimikunnallemme SharePoint-sivuston. Lähdin pois mukavuusalueeltani käyttäessäni Azure PowerShelliä aina pystyessäni. Käyttäessäni PowerShelliä enemmän opin arvostamaan sen ominaisuuksia. Azuren voimakkaan kehitystyön tuloksena sieltä löytyy palveluita kuten Key Vault ja uusia kiinnostavia palveluita on tulossa.

Ilokseni huomasin, että tietoturvahaasteiden tutkiminen on yleistynyt paljon. Tutkijayhteisöt järjestävät vuosittaisia seminaareja aiheesta ja siitä kirjoitetaan enemmän. Henkilökohtaisesti haluan tutustua tähän aiheeseen paremmin jatkossa, teknologiaan liittyvien kysymysten syvempi ymmärtäminen kiinnostaa. Sovellusten pääsynhallinnan tiukentaminen on näkyvissä jo nyt, esimerkiksi OKTA lupaa SSO:n

käyttöön myös pilvessä yrityksen tunnuksilla. Ohjelma lupaa paljon, mutta pystyykö se toteuttamaan lupauksen, se jää nähtäväksi.

Pilvipalveluihin, olivat ne sitten julkisia, yksityisiä tai muita, on syytä suhtautua positiivisella varauksella. Yksityiset ihmiset käyttävät mielellään pilviratkaisuja, ja yritysten on vaikeampia päästä pilven reunalle. Mikään viisasten kivi pilvipalvelut eivät ole, vaan käyttö on syytä suunnitella hyvin. IT-osastojen työ muuttuu vääjäämättä pilvipalveluiden yleistyessä, palvelutason seuranta ja palveluiden mitoitus ovat uusia tehtäviä, joissa käytetään vanhoja oppeja. Ostetun pilvipalvelun suorituskykyä on syytä valvoa, ei saa silmät suljettuina uskoa automaattista resurssien joustavuutta. Vanhat kvantitatiiviset suorituskykymittarit valvovat pilvessäkin hyvin, kunhan niitä itse valvoo valvontaa.

Pilvipalvelut ovat kypsymässä ja niiden kehitys jatkuu yhä kiristyvässä kilpailussa AWS:n, Microsoftin ja muiden toimijoiden välillä. Tulevaisuus tuo vääjäämättä uusia teknologisia haasteita ja innovaatioita. Vierivä kivi ei sammaloidu ja mielenkiinnolla seuraan, mitä uutta pilvipalveluista löytyy 10 vuoden kuluttua.

Lähteet

1 Chambers James. 2013. Windows Azure Web Sites. Indianapolis: Wiley & Sons.

2 Salo Immo. 2010. Cloud computing palvelut verkossa. Jyväskylä: Docendo.

3 Chorafas Dimitris. 2011. Cloud computing strategies. Boca Raton: Taylor & Francis Group, CRC press.

4 Soares, Fernandes, Gomes, Freire, Inãcio. 2014.Cloud Security: State of the Art teoksessa , Nepal Surya & Pathan Mukaddim (toim.) Security, Privacy and Trust in Cloud Systems. Heidelberg: Springer.

5 RightScale. 2015 State of the cloud report. Verkkodokumentti. <http://assets.rightscale.com/uploads/pdfs/RightScale-2015-State-of-the-Cloud-Report.pdf>. Luettu 9.2.2016.

6 RightScale. 2015 State of the cloud report. Verkkodokumentti. <http://assets.rightscale.com/uploads/pdfs/RightScale-2016-State-of-the-Cloud-Report.pdf>. Luettu 19.2.2016.

7 Lahav, Susan. 2016. Security: the reason to move to cloud. Verkkodokumentti. <http://www.itproportal.com/2016/01/13/security-the-reason-to-move-to-the-cloud/>. 13.1.2016. Luettu 8.2.2016.

8 Coles, Cameron. 2016. Five suprising truths from the cloud security alliances latest survey. Verkkodokumentti. <https://blog.cloudsecurityalliance.org/>. 8.2.2016. Luettu 8.2.2016.

9 Redkar, Tejaswi & Guidici Tony. 2011. Windows Azure Platform, 2nd ed. New York: Apress.

10 Wang, Xi & Xun, Xu teoksessa Li, Weidong & Mehnen Jörn (toim.). 2013. Cloud manufacturing. London: Springer.

11 Almorsy Mohamed, Ibrahim Amani & John Grundy. 2014. Adaptive Security Management in SaaS applications teoksessa Nepal, Surya & Pathan, Mukaddim (toim): Security, Privacy and Trust in Cloud Systems. Heidelberg: Springer.

12 Caron, Eddy, Desprez Frédéric & Rouzaud-Cornabas Jonathan. 2014 Smart Resource Allocation to Improve Cloud Security teoksessa Nepal, Surya & Pathan, Mukaddim (toim): Security, Privacy and Trust in Cloud Systems. Heidelberg: Springer.

13 Schwartz Mathew. 2015. Amazon downplays cloud breach threat. Verkkodokumentti <http://www.bankinfosecurity.com/crypto-keys-stolen-from-amazon-cloud-a-8581/op-1>. 12.10.2016. Luettu 8.2.2016.

14 Inci, Mehmet Sinan, Gülmezoglu Berk, Irazoqui Gorka, Eisenbarth Thomas & Sunar Berk. 2015. Verkkodokumentti. <https://eprint.iacr.org/2015/898.pdf>. Luettu 8.2.2016.

15 Thilakanathan, Danan, Chen, Shiping, Nepal Surya & Rafael Calvo. 2014. Secure Data Sharing in the Cloud teoksessa Nepal, Surya & Pathan, Mukaddim (toim): Security, Privacy and Trust in Cloud Systems. Heidelberg: Springer.

16 Kertesz Attila & Varadi Szilvia. 2014. Legal Aspects of Data Protection in Cloud Federations teoksessa Nepal, Surya & Pathan, Mukaddim (toim): Security, Privacy and Trust in Cloud Systems. Heidelberg: Springer.

17 Babcock Charles. Amazon, Microsoft, IBM and Google capture cloud market. Verkkodokumentti. <http://www.informationweek.com/cloud/amazon-microsoft-ibm-google-capture-cloud-market/d/d-id/1321484>. 28.7.2015. Luettu 9.2.2016.

18 Amazon Web Services records $2.4B in Q4 Revenue and roughly $8B in revenue for 2015. Verkkodokumentti. <http://cloud-computing-today.com/2016/01/29/1074342>. 29.1.2016. Luettu 5.2.2016.

19 Microsoft's earnings report underscores nascent success of Nadella's cloud-first strategy. Verkkodokumentti. <http://cloud-computing-today.com/2016/02/01/microsofts-earnings-report-underscores-nascent-success-of-nadellas-cloud-first-strategy/>. 1.2.2016. Luettu 5.2.2016.

20 VMware named a leader in Forrester waves. Verkkodokumentti. <http://www.vmware.com/radius/forrester-wave-announcement/>. 2.2.2016. Luettu 5.2.2016.

21 Zhu, Jinzy. 2014. China cloud rising. Heidelberg: Springer.

22 What is Amazon EC2? 2015. Verkkodokumentti. <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/concepts.html>. Luettu 9.2.2016.

23 Overview of Amazon Web Services. Verkkodokumentti. <https://aws.amazon.com/whitepapers/overview-of-amazon-web-services/>. 31.12.2015. Luettu 9.2.2016.

24 Arpit Verma. Ubuntu Linux is the most popular operating system in cloud. Verkkodokumentti. <http://fossbytes.com/ubuntu-linux-is-the-most-popular-operating-system-in-cloud/>. 30.8.2015. Luettu 9.2.2016.

25 Kitchens Sheryl. 2015. Verkkodokumentti. <http://searchaws.techtarget.com/feature/Amazon-Elastic-Compute-Cloud-features-explained>. Luettu 9.2.2016.

26 Tung, Liam. 2015. Now Amazon customers can rent dedicated AWS physical Servers. Verkkodokumentti. <http://www.zdnet.com/article/now-amazon-customers-can-rent-dedicated-aws-physical-Servers/> 24.11.2015. Luettu 11.2.2016.

27 AWS Security Bulletins. 2015. Verkkodokumentti. <http://aws.amazon.com/security/security-bulletins/>. Luettu 8.2.2016.

28 Steven Martin. 2014. Upcoming Name change for Windows Azure. Verkkodokumentti. <https://azure.microsoft.com/en-us/blog/upcoming-name-change-for-Windows-azure/>. 25.3.2014. Luettu 5.2.2016.

29 Zarkos Stephen. 2015. Verkkodokumentti. < https://azure.microsoft.com/en-us/documentation/articles/virtual-machines-linux-endorsed-distributions/ >.12.8.2015.Luettu 5.2.2016.

30 Cross, D. 2015. Explore Azure Disk Encryption with Azure PowerShell. Verkkodokumentti. < http://blogs.msdn.com/b/azuresecurity/archive/2015/11/17/explore-azure-disk-encryption-with-azure-PowerShell.aspx >. 16.11.2015. Luettu 15.2.2016.

31 Shinder Thomas. 2015. Azure Disk Encryption for Linux and Windows machines - Public preview now available. Verkkodokumentti < http://blogs.msdn.com/b/azuresecurity/archive/2015/11/17/azure-disk-encryption-for-linux-and-Windows-virtual-machines-public-preview.aspx >. 16.11.2015. Luettu 15.2.2016.

32 The 100 Coolest Cloud computing vendors of 2016. Verkkodokumentti. <http://www.crn.com/news/cloud/300079585/the-100-coolest-cloud-computing-vendors-of-2016.htm> 3.2.2016. Luettu 8.2.2016.

33 Plastina Dan. 2015. Azure Key Vault Step by Step. Verkkodokumentti. <http://blogs.technet.com/b/kv/archive/2015/06/02/azure-key-vault-step-by-step.aspx > 12.11.2015. Luettu 15.2.2016.

34 Client-side encryption for Microsoft Azure Storage - Preview. Verkkodokumentti. <http://blogs.msdn.com/b/Windowsazurestorage/archive/2015/04/28/client-side-encryption-for-microsoft-azure-storage-preview.aspx> 28.4.2015. Luettu 8.2.2016.

35 Keir Gordon. 2015. Storing data securely in Azure Blob Storage with Azure Encryption Extensions. Verkkodokumentti. < http://blogs.msdn.com/b/partnercatalystteam/archive/2015/06/17/storing-data-securely-in-azure-blob-storage-with-azure-encryption-extensions.aspx > 17.6.2015. Luettu 15.2.2016.

36 Microsoft Azure Architectures for SharePoint 2013. 2016. Verkkodokumentti. <https://technet.microsoft.com/library/dn635309%28v=office.15%29.aspx >. 4.2.2016. Luettu 8.2.2016.

Palvelinten luomiseen käytetyt PowerShell-komennot

Skriptitiedosto 1 (azureperus.ps1)

```
$ResourceGroupName = "KPMT2"
$Location = "North Europe"

$InterfaceName = "kpmt2dc1n"
$Subnet1Name = "Default"
$VNetAddressPrefix = "10.0.0.0/16"
$VNetSubnetAddressPrefix = "10.0.0.0/24"

$VMName = "kpmt2dc1v"
$ComputerName = "kpmt2dc1"
$VMSize = "Standard_A1"
$OSDiskName = $VMName + "OSDisk"
$storageAccount = get-AzureRmStorageAccount

$PIp = New-AzureRmPublicIpAddress -Name $InterfaceName
-ResourceGroupName $ResourceGroupName -Location $Location
-AllocationMethod Dynamic
$VNet = get-AzureRmVirtualNetwork
$Interface = New-AzureRmNetworkInterface -Name $InterfaceName
-ResourceGroupName $ResourceGroupName -Location $Location -SubnetId
$VNet.Subnets[0].Id -PublicIpAddressId $PIp.Id

$Credential = Get-Credential
$VirtualMachine = New-AzureRmVMConfig -VMName $VMName -VMSize $VMSize
$VirtualMachine = Set-AzureRmVMOperatingSystem -VM $VirtualMachine
-Windows -ComputerName $ComputerName -Credential $Credential
-ProvisionVMAgent -EnableAutoUpdate
$VirtualMachine = Set-AzureRmVMSourceImage -VM $VirtualMachine
-PublisherName MicrosoftWindowsServer -Offer WindowsServer
-Skus 2012-R2-Datacenter -Version "latest"
$VirtualMachine = Add-AzureRmVMNetworkInterface -VM $VirtualMachine
-Id $Interface.Id
$OSDiskUri = $StorageAccount.PrimaryEndpoints.Blob.ToString() +
"vhds/" + $OSDiskName + ".vhd"
```

```
$VirtualMachine = Set-AzureRmVMOSDisk -VM $VirtualMachine -Name
$OSDiskName -VhdUri $OSDiskUri -CreateOption FromImage

New-AzureRmVM -ResourceGroupName $ResourceGroupName -Location "North
Europe" -VM $VirtualMachine
```

Skriptitiedosto kpmt2sql1.ps1

```
$ResourceGroupName = "KPMT2"
$Location = "North Europe"

$InterfaceName = "kpmt2sql1n"
$Subnet1Name = "Default"
$VNetAddressPrefix = "10.0.0.0/16"
$VNetSubnetAddressPrefix = "10.0.0.0/24"

$VMName = "kpmt2sql1v"
$ComputerName = "kpmt2sql1"
$VMSize = "Standard_A2"
$OSDiskName = $VMName + "OSDisk"
$storageAccount = get-AzureRmStorageAccount

$PIp = New-AzureRmPublicIpAddress -Name $InterfaceName
-ResourceGroupName $ResourceGroupName -Location $Location
-AllocationMethod Dynamic
$VNet = get-AzureRmVirtualNetwork
$Interface = New-AzureRmNetworkInterface -Name $InterfaceName
-ResourceGroupName $ResourceGroupName -Location $Location -SubnetId
$VNet.Subnets[0].Id -PublicIpAddressId $PIp.Id

$Credential = Get-Credential
$VirtualMachine = New-AzureRmVMConfig -VMName $VMName -VMSize $VMSize
$VirtualMachine = Set-AzureRmVMOperatingSystem -VM $VirtualMachine
-Windows -ComputerName $ComputerName -Credential $Credential
-ProvisionVMAgent -EnableAutoUpdate
$VirtualMachine= Set-AzureRmVMSourceImage -VM $VirtualMachine
```

```
-PublisherName "MicrosoftSQLServer" -Offer "SQL2012sp2-ws2012r2" -skus
Standard -version "11.0.5569"
$VirtualMachine = Add-AzureRmVMNetworkInterface -VM $VirtualMachine
-Id $Interface.Id
$OSDiskUri = $StorageAccount.PrimaryEndpoints.Blob.ToString() +
"vhds/" + $OSDiskName + ".vhd"
$VirtualMachine = Set-AzureRmVMOSDisk -VM $VirtualMachine -Name
$OSDiskName -VhdUri $OSDiskUri -CreateOption FromImage

New-AzureRmVM -ResourceGroupName $ResourceGroupName -Location "North
Europe" -VM $VirtualMachine
```

Palvelinten levyjen salaukseen (Key Vault) käytetyt komennot

DC- ja SQL- palvelinten levyjen salaukseen käytetyt komennot.

```
New-AzureRmKeyVault -VaultName kpmt2holvi -ResourceGroupName kpmt2
-Location "North Europe"

$rgName ="kpmt2"
$vmName = "kpmt2dc1v"
$aadClientID = "1d67f870-437f-48d3-b683-3edf15a2e0fc"
$aadClientSecret = "1LSiF+plUoD8eL8qaE1tv36rac+IzoSrm1CM3NHMeqk="
$KeyVaultName = "kpmt2holvi"
$KeyVault = Get-AzureRmKeyVault -VaultName $KeyVaultName
-ResourceGroupName $rgname
$diskEncryptionKeyVaultUrl = $KeyVault.VaultUri
$KeyVaultResourceId = $KeyVault.ResourceId
Set-AzureRmKeyVaultAccessPolicy -VaultName $KeyVaultName
-ServicePrincipalName $aadClientID -PermissionsToKeys all
-PermissionsToSecrets all -ResourceGroupName $rgname
Set-AzureRmKeyVaultAccessPolicy -VaultName $KeyVaultName
-ResourceGroupName $rgname -EnabledForDiskEncryption
Set-AzureRmVMDiskEncryptionExtension -ResourceGroupName $rgname
-VMName $vmName -AadClientID $aadClientID -AadClientSecret
$aadClientSecret -DiskEncryptionKeyVaultUrl $diskEncryptionKeyVaultUrl
-DiskEncryptionKeyVaultId $KeyVaultResourceId

Enable AzureDiskEncryption on the VM
This cmdlet prepares the VM and enables encryption which may reboot
the machine and takes 10-15 minutes to finish.
Please save your work on the VM before confirming. Do you want to
continue?

[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): y

RequestId  IsSuccessStatusCode   StatusCode ReasonPhrase
True       OK                   OK

Get-AzureRmVMDiskEncryptionStatus -ResourceGroupName $rgname -VMName
$vmname
```

```
OsVolumeEncrypted          : True

OsVolumeEncryptionSettings : {
  "diskEncryptionKey":{
    "secretUrl": "https://kpmt2holvi.vault.azure.net/secrets/6F415A84-
3B79-48EB-96E9-5000D76BC413/932e97bbf49d4fe584d483ae14b4eb01",

   "sourceVault": {"id": "/subscriptions/2dd64d3c-3ac0-4dd1-8b66-
cd2990c64be3/resourceGroups/kpmt2/providers/Microsoft.KeyVault/vaults/
kpmt2holvi"}
                        },
   "keyEncryptionKey": null
                              }

DataVolumesEncrypted       : True

$osVolEncrypted = {(Get-AzureRmVMDiskEncryptionStatus
-ResourceGroupName $_.ResourceGroupName -VMName
$_.Name).OsVolumeEncrypted}
$dataVolEncrypted= {(Get-AzureRmVMDiskEncryptionStatus
-ResourceGroupName $_.ResourceGroupName -VMName
$_.Name).DataVolumesEncrypted}

Get-AzureRmVm | Format-Table @{Label="MachineName";
Expression={$_.Name}}, @{Label="OsVolumeEncrypted";
Expression=$osVolEncrypted}, @{Label="DataVolumesEncrypted";
Expression=$dataVolEncrypted}

MachineName           OsVolumeEncrypted     DataVolumesEncrypted
kpmt2dc1v             True                  True
kpmt2spapp1           False                 False
kpmt2sql1v            True                  True
```

SQL-palvelimelle salausta varten suoritetut komennot:

```
$rgName ="kpmt2"
$vmName = "kpmt2sql1v"
$aadClientID = "5239f468-874f-457b-bdbf-415cf635da8c"
```

```
$aadClientSecret = "/6xd4JPs0vdAWf4J64n0DQjSqidfEvYmIRPKY2HbZjQ="
$KeyVaultName = "kpmt2holvi"
$KeyVault = Get-AzureRmKeyVault -VaultName $KeyVaultName
-ResourceGroupName $rgname
$diskEncryptionKeyVaultUrl = $KeyVault.VaultUri
$KeyVaultResourceId = $KeyVault.ResourceId
Set-AzureRmKeyVaultAccessPolicy -VaultName $KeyVaultName
-ServicePrincipalName $aadClientID -PermissionsToKeys all
-PermissionsToSecrets all -ResourceGroupName $rgname
Set-AzureRmKeyVaultAccessPolicy -VaultName $KeyVaultName
-ResourceGroupName $rgname -EnabledForDiskEncryption
Set-AzureRmVMDiskEncryptionExtension -ResourceGroupName $rgname
-VMName $vmName -AadClientID $aadClientID -AadClientSecret
$aadClientSecret -DiskEncryptionKeyVaultUrl $diskEncryptionKeyVaultUrl
-DiskEncryptionKeyVaultId $KeyVaultResourceId

Enable AzureDiskEncryption on the VM

This cmdlet prepares the VM and enables encryption which may reboot
the machine and takes 10-15 minutes to finish.
Please save your work on the VM before confirming. Do you want to
continue?
[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): y
Set-AzureRmVMDiskEncryptionExtension : Long running operation failed
with status 'Failed'.
StartTime: 22.2.2016 17:35:08
EndTime: 22.2.2016 18:38:43
OperationID: 67f3ac05-1857-4e26-92b9-f0c0295b7b8e
Status: Failed
ErrorCode: VMExtensionProvisioningError
ErrorMessage: VM has reported a failure when processing extension
'AzureDiskEncryption'. Error message: "Failed to configure bitlocker
as expected. Exception: Installing bitlocker package failed with 87,
InnerException: , stack trace:at
Microsoft.Cis.Security.BitLocker.BitlockerIaasVMExtension.BitlockerPre
p.EnableBitlockerOptionalFeature(Boolean& rebootRequired)at
Microsoft.Cis.Security.BitLocker.BitlockerIaasVMExtension.BitlockerOpe
rations.PrepareMachineForBitlocker(Boolean& rebootInitiated)at
Microsoft.Cis.Security.BitLocker.BitlockerIaasVMExtension.BitlockerExt
```

```
ension.PrepareMachineForBitlocker(Boolean&rebootInitiated)at
Microsoft.Cis.Security.BitLocker.BitlockerIaasVMExtension.BitlockerExt
ension.OnEnable()".
At line:1 char:1
+ Set-AzureRmVMDiskEncryptionExtension -ResourceGroupName $rgname
-VMName $vmName  ...
+ CategoryInfo          : CloseError: (:)
[Set-AzureRmVMDiskEncryptionExtension], ComputeCloudException
    + FullyQualifiedErrorId :
Microsoft.Azure.Commands.Compute.Extension.AzureDiskEncryption.SetAzur
eDiskEncryptionExtensionCommand
```