LAUREA
AMMATTIKORKEAKOULU
Uuden edellä

ServiceDesk+-palvelun siirto Microsoft Azure -palveluun

Korte, Lauri

2014 Laurea Kerava

Laurea-ammattikorkeakoulu
Kerava

ServiceDesk+-palvelun siirto Microsoft Azure -palveluun

Lauri Korte
Tietojenkäsittelyn koulutusohjelma
Opinnäytetyö
Elokuu, 2014

Laurea-ammattikorkeakoulu **Tiivistelmä**
Laurea Kerava
Tietojenkäsittelyn koulutusohjelma

Lauri Korte

ServiceDesk+-palvelun siirto Microsoft Azure -palveluun

Vuosi 2014 Sivumäärä 40

Opinnäytetyö tehtiin auto- ja konekaupan maahantuontiyritykseen. Tässä opinnäytetyössä tavoitteena oli selvittää, soveltuuko Microsoft Azure -palvelu alustaratkaisuksi yrityksen tietohallinnon toiminnanohjausjärjestelmälle. Samalla opinnäytetyössä pyrittiin löytämään parhaita käytänteitä Azure-palvelun hyödyntämiseen tulevaisuudessa.

Opinnäytetyö toteutettiin projektiluontoisena työnä. Projektille ei määritelty poikkeukselliseti aikataulua. Projektissa oli neljä vaihetta, joista ensimmäinen oli luoda Microsoft Azure -palveluun ympäristö. Toinen oli luoda ja yhdistää Azure-palvelun verkkoympäristö On Premises verkkoon. Kolmannessa vaiheessa luotiin palvelimet Azure-palveluun ja asennettiin ServiceDesk+-palvelu sekä generoitiin asetukset ja tieto. Neljäs vaihe sisälsi palvelun testauksen ja käyttöönoton vaativien muutosten teon.

Opinnäytetyön tavoitteeksi asetettu selvitys soveltuvuudesta toteutui suunnitellun mukaisesti. Palvelua voidaan hyödyntää tietyin reunaehdoin muissakin palveluissa. Microsoft Azure -palveluun siirrettäessä On Premises -ympäristöstä palvelu on huomioitava kasvaneet vaatimukset tietoliikenteen osalta. Yrityksen tietoturvapolitiikka tulee huomioida suunnitteluvaiheessa.

Asiasanat: pilvipalvelu, virtuaalisointi, Azure

Laurea University of Applied Sciences
Laurea Kerava
Business Information Technology

Abstract

Lauri Korte

Utilizing Microsoft Azure for Service Desk+

Year 2014 Pages 40

This *Bachelor's* thesis was carried out for a car and machinery import company. The aim of this thesis was to examine the compatibility of the Microsoft Azure platform solution for an enterprise information management (ERP) system. At the same time, the thesis sought to find the best practices for utilizing the Azure service in the future.

The thesis was carried out as a project for which no schedule was specified. The project had four phases, the goal of the first one being the creating of an environment in the Microsoft Azure service. In the second phase the Azure service network environment was combined with the On Premises network. The third phase consisted of creating servers for the Azure service, installing the ServiceDesk+ service, as well as generating the necessary settings and data. During the fourth step the service was tested and all necessary changes for the deployment of the service were made.

The objective of the thesis, which was to examine the suitability of the service, was achieved. It is possible under certain conditions to utilize the service also in connection with other services. The increased requirements regarding data transport must be considered when transferring the On Premises service to the Microsoft Azure services platform. The company's information security policy must be taken into account already in the planning phase.

Keywords: cloud service, virtualization, Azure

Lyhenneluettelo

VPN	Virtual Private Network
DMZ	Demilitarized Zone
RAID	Reduntant Array of Independent Disks
I/O	Input/Output
NAT	Network Address Translation
DNS	Domain Name System
IP	Internet Protocol
AD	Active Directory
EAS	Enterprise Agreement Subscription
VHD	Virtual Hard Disk
TLS	Transport Layer Security

Sisällys

1 Johdanto

Opinnäytetyön toimeksiantaja on auto- ja konekaupan maahantuontiyritys, jolla on kaksi tytäryhtiötä harjoittamassa vähittäiskauppaa kolmen eri brändin osalta. Opinnäytetyö pohjautuu kehityshankkeeseen ja sen tavoitteena on selvittää, kuinka Microsoft Azure -palvelu soveltuisi yrityksen tietohallinnon toiminnanohjausjärjestelmän hybridi-ympäristön palvelinratkaisuksi DMZ-alueelle. Toiminnanohjausjärjestelmän nykyinen alustaratkaisu on tullut elinkaarensa päähän, joten kevään 2014 aikana on yritykselle löydettävä kustannustehokas alusta toiminnanohjausjärjestelmälle.

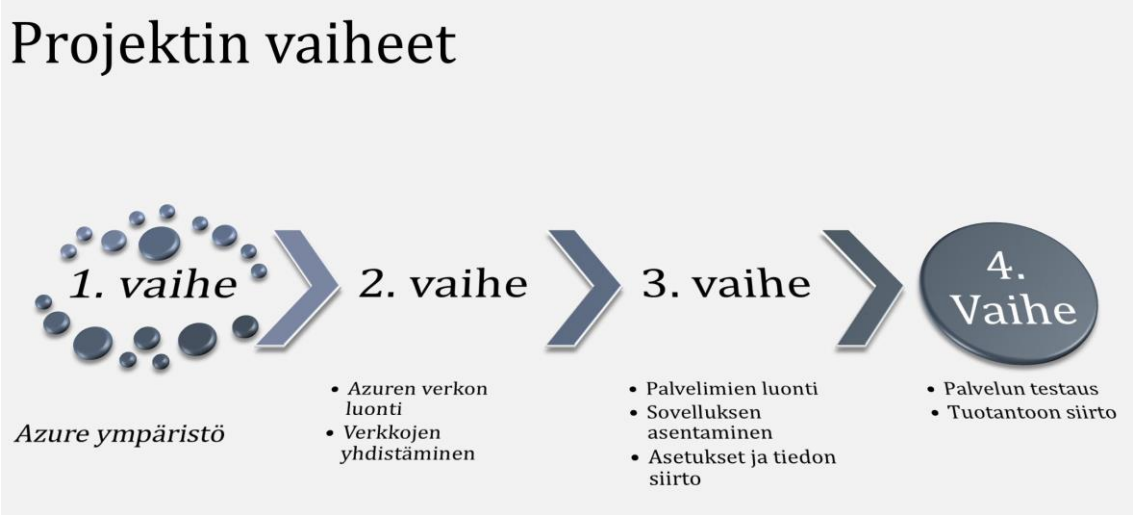
Toteutuksessa hyödynnetään yrityksen On Premises-ympäristöstä tarvittavia palveluita sekä Microsoftin Office365-palvelua sähköpostipalveluiden osalta. Microsoft Azure -palvelu on yritykselle kokonaisarkkitehtuurin kannalta järkevä pilvipalvelu, jota voidaan hyödyntää kehityshankkeessa. Microsoft Azure -palvelu on yritykselle tuttu aiemmista projekteista, jotka on toteutettu sitä hyödyntäen ja julkaistu julkiseen internetiin. Suurimpana erona aiempiin palveluihin verrattuna tulisi tässä toteutuksessa olemaan laajempi integrointi On Premises-ympäristöön ja Microsoftin Office365-palveluun. On Premises-ympäristöstä hyvänä esimerkkinä on sähköposti-palvelu. On Premises ympäristössä oleva sähköpostipalvelu tarvitsee palvelimen, palvelinkäyttöjärjestelmän, sähköpostipalvelinohjelmiston, tietoliikenne ohjaukset ja nimipalvelut. Microsoft Office365 sähköpostipalvelu vaatii toimiakseen yksinkertaisimmillaan vain alkumääritykset.

Tässä opinnäytetyössä pyritään luomaan yrityksen tietohallinnolle käsitys hyvästä käytännöstä Microsoft Azure -palvelun sisäverkon yhdistämisestä yrityksen fyysiseen verkkoon. Työssä myös selvitetään kuinka sinne luodaan sovelluspalvelin ja tietokanta toiminnanohjaus-järjestelmälle. Microsoft Azure -palvelussa luotavan järjestelmän tulee pystyä hyödyntämään yrityksen Active Directoryn Directory Service-palvelua tunnistautumisessa. Active Directory on integroitu toiminnanohjaus-järjestelmään käyttäjätietojenkin osalta, jolloin käyttäjätietoa ei tarvitse ylläpitää kuin Active Directory palvelussa.

Työssä ei tulla syventymään Microsoft Azure -palveluun tehtävään palvelimien konfigurointiin, sillä ne eivät eroa oleellisesti On Premises -ympäristössä olevan fyysisen- ja/tai virtuaalisen palvelimen konfiguroinnista. Työssä ei myöskään käsitellä testaussuunnitelmaa.

2 Projektin esittely

Tässä luvussa esittelen lyhyesti projektin aikataulua ja resursseja sekä toimeksiantajaa. Tietoliikenteen lähtötilanteen, nykyisen ja projektissa toteutettavan ympäristön esittelen tarkemmalla tasolla. Projektilla ei ole selkeää aikataulua poikkeavasta toteutusta johtuen. Projekti vietiin läpi puhtaasti neljän eri vaiheen mukaan, koska se sopi tähän projektiin hyvin (Kuva 1).



Kuva 1: Projektin vaiheet

Toteutus sovittiin tehtäväksi mahdollisuuksien mukaan omien töiden ohessa ja vapaa-ajalla. Toteutukseen ei koettu tarvetta sitoa nimettyjä henkilöresursseja itseni lisäksi.

2.1 Toimeksiantajan esittely

Yritys toimii Suomessa kolmen eri brändin maahantuojana ja Baltiassa yhden brändin maahantuojana. Yrityksellä on yksi tytäryhtiö Suomessa, joka toimii kyseisten brändien jälleenmyyjänä ja jälkimarkkinoinnin edustajana.

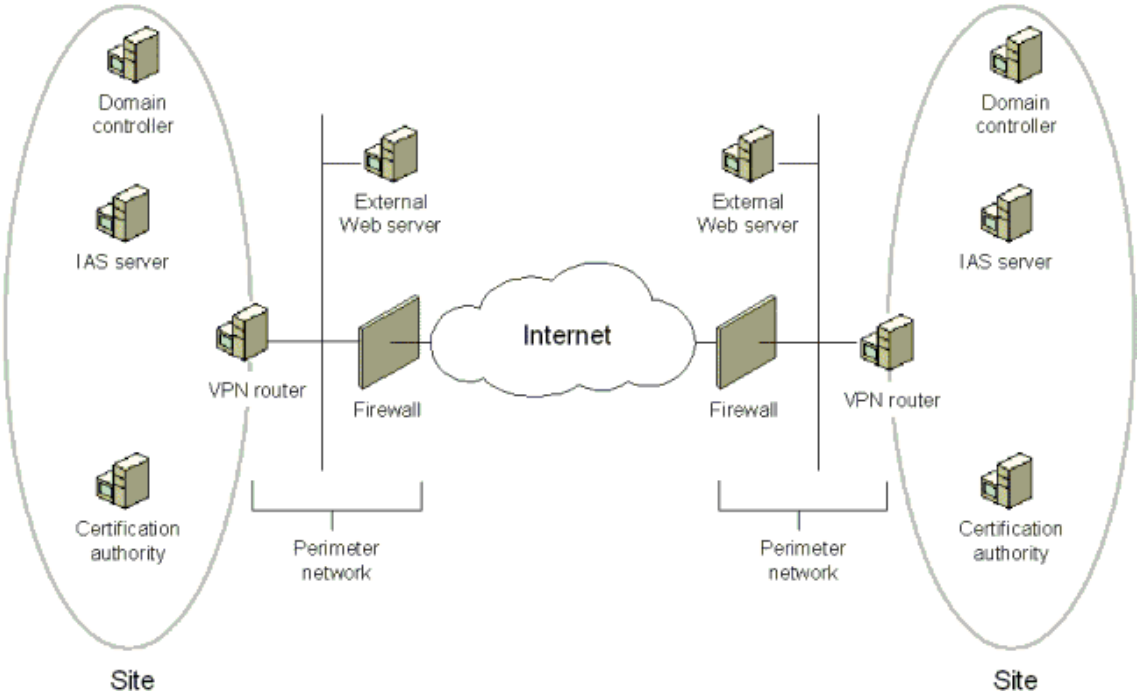
Yritys tarjoaa asiakkailleen palveluita tuotteiden elinkaaren jokaiseen vaiheeseen, joilla on brändin tai brändien edustusoikeus. Yrityksen asiakkaina toimivat koko Suomen alueella brändien myynti- ja jälkimarkkinointia suorittavat organisaatiot. Baltian alueella yrityksen asiakkaana ovat yhden brändin osalta jälleenmyyjä ja jälkimarkkinointi organisaatiot.

2.2 Tietoliikenteen lähtötilanne

Yrityksen verkkoinfrastruktuuri asettaa toteutukselle itsestään jo ison haasteen. Liikennöinti internetiin, tytäryhtiön toimipisteisiin, sisäverkon ulkopuolisille kumppaneille sekä

jälleenmyyjä-verkostolle tapahtuu emoyhtiön tietoliikenteen solmukohdan läpi. Toteutuksessa on tarkoituksena luoda Site-To-Site VPN-verkko yrityksen DMZ-alueen 10.13.x.x osoitteesta emoyhtiön runkoverkon läpi julkisen internetin kautta Microsoft Azure -palveluun.

Site-To-Site VPN-verkolla tarkoitetaan kahta tai useampaa erillistä verkkoaluetta, jotka ovat yhdistetty VPN-reitittimien avulla ja sijaitsevat kunkin yhdistettävän verkon palomuurin takana (Kuva 2). (Microsoft 2005; Wikipedia 2013a.)



Kuva 2: Site-To-Site VPN -verkko (Microsoft 2005.)

Microsoft Azure -palvelussa sijaitseva virtuaalinen verkko tulisi sijaitsemaan yrityksen DMZ-verkkoalueelle. Virtuaaliset verkot ovat samassa fyysisessä verkossa olevia virtuaalisia toisistaan täysin riippumattomia verkkoja. (Tukiainen 2000, 4.) DMZ-verkkoalueen käyttö mahdollistaa toiminnanohjausjärjestelmän itsepalveluportaalin käytön sekä organisaation että ulkopuolisten jälleenmyyjien henkilöstölle ja muille ulkopuoliselle yhteistyökumppaneille. DMZ-verkkoalue, josta voidaan julkaista palveluita, on eristetty yrityksen sisäverkosta joko suoraan julkiseen internetiin tai ulkopuolisille kumppaneille. DMZ-verkon palvelussa hyödynnettävän tiedon ei tarvitse fyysisesti sijaita samassa verkossa sijaitsevassa tietokantapalvelimessa. Tieto voidaan noutaa esimerkiksi sisäverkon keskitetyltä tietokantapalvelimelta tietoturvallisesti. (Valtiovarainministeriö 2010, 24-25.) DMZ-alueelta laitteet eivät voi muodostaa yhteyttä sisäverkkoon automaattisesti, vaan sallitut yhteydet tehdään palomuurilla esimerkiksi pakettisuodatuksen perusteella. Suodatuksessa voidaan käyttää esimerkiksi seuraavia muuttujia: lähde- ja kohdeosoite, protokolla tai porttinumero. (Oulun seudun ammattiopisto.)

2.3 Nykyinen On Premises -palvelinympäristö

Toiminnanohjausjärjestelmän sovelluspalvelin ja sen SQL-tietokantapalvelin on virtualisoitu yhdelle fyysiselle palvelimelle. Kyseisessä palvelimessa hypervisorina on vmWare esxi-versio. Hypervisor on niin sanottu Isäntäkone, joka toimii alustana suoritettaville virtuaalisille instansseille. Hypervisorilla myös määritetään kunkin virtuaalisen instanssin saamat osuudet isäntäpalvelimen käytettävistä resursseista. Virtuaalipalvelimet on sijoitettu samalle vmWare-isäntäkoneelle siten, että ne sijaitsevat fyysisesti eri RAID-osiolla. Tämän ansiosta saadaan lisää suorituskykyä vähentämällä yhden RAID-osion kirjoitus- ja luku operaatioita.

vmWare-isäntäkoneella on kaksi erillistä RAID5-osiota virtuaalisoituja palvelimia varten ja itse vmWare-isäntäkone ympäristö on asennettu RAID0-osiolle. RAID5-osio sisältää kolme fyysistä kiintolevyä, jotka näkyvät yhtenä levynä. RAID5-osio mahdollistaa yhden levyn rikkoontumisen ilman tiedon menetystä sekä myös niin sanotun hot swapin eli käynnissä vaihtamisen. RAID0-osio puolestaan sisältää kaksi fyysistä kiintolevyä. RAID0-osio kestää myöskin yhden levyn vikaantumisen ilman tiedon menetystä ja hot swapin. Suurin ero RAID0:n ja RAID5:n välillä on RAID5:n parempi suorituskyky sekä se että RAID0:ssa levyt ovat peilikuvia, kun taas RAID5:ssa data on pilkottuna eri levyille. Mikäli RAID5:sta hajoaa kaksi levyä, on sillä sijaitseva tietokin menetetty kokonaan. (Tarkki.)

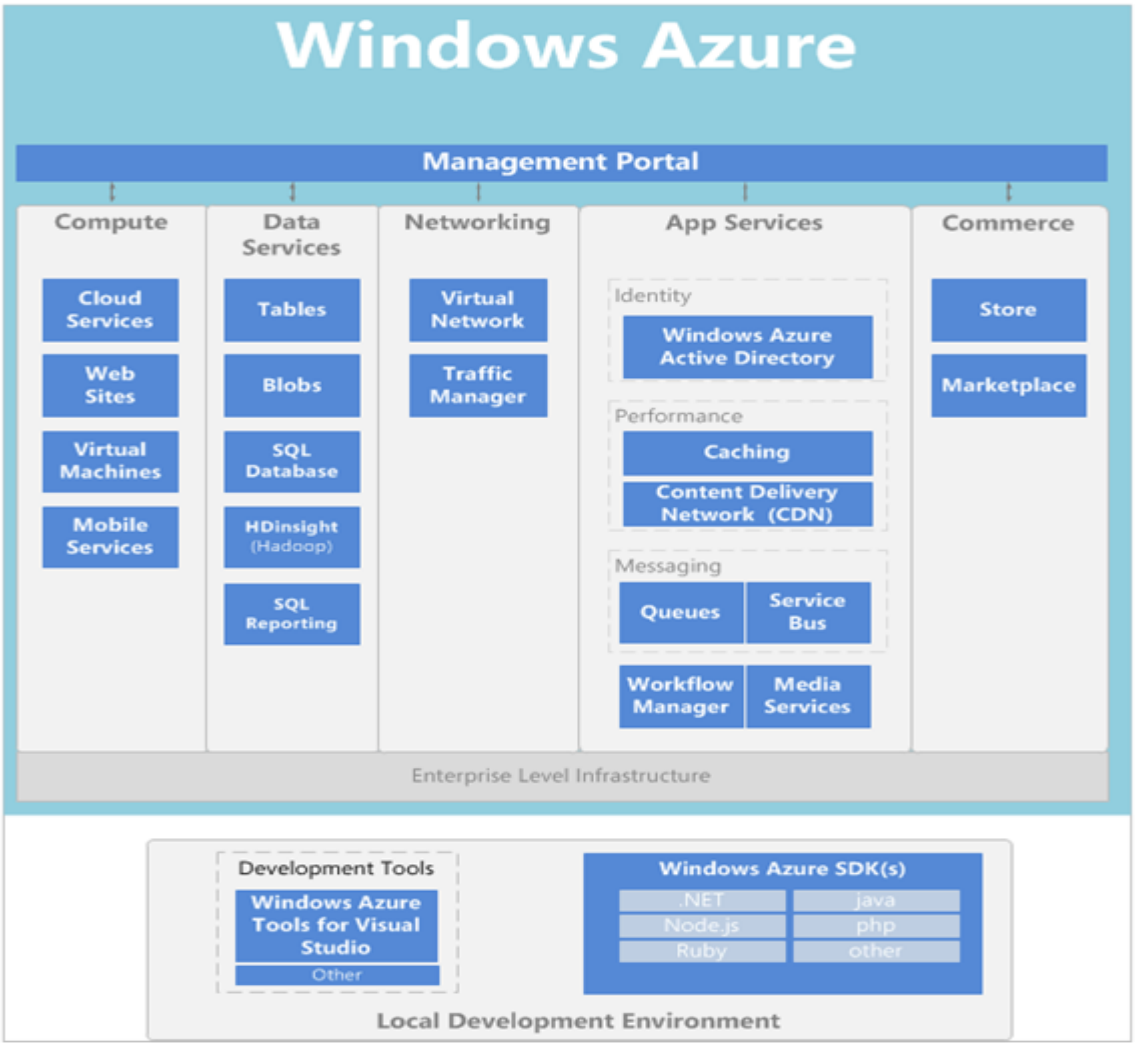
Varsinainen vmWare-palvelin on hankittu yritykseen toiminnanohjausjärjestelmän uusinta projektia varten noin neljä vuotta sitten, joten kyseinen palvelin on elinkaarensa päässä. Toiminnanohjausjärjestelmän siirtäminen kapasiteettipalveluun poistaa tarpeen valvoa alustana toimivaa palvelinta sekä tiedon varmistusta. Microsoft Azure -palvelu on tähän käyttötarkoitukseen kustannustehokkain varmistusatkaisu, mikäli vertaillaan yrityksen nykyisiä palveluntarjoajia, oman fyysisen laitteiston hankintaa ja ylläpitoa sekä palveluiden sisäisiä eroja niin kapasiteetin kuin skaalautuvuuden ja tiedon varmistuksen sekä ominaisuuksien suhteen.

2.4 Microsoft Azure –palvelu ja kilpailijat

Microsoft Azure -palvelu on kattava sovellusalustapalvelu, joka toimii Internetissä niin sanottuna pilvipalveluna (Kuva 3). Pilvipalvelulle itsessään ei ole olemassa yksiselitteistä määritelmää, mutta pilvipalvelun pitää sisältää itsepalveluportaali, jonka avulla voidaan muuttaa tilaukselle kuuluvien resurssien määrää dynaamisesti mahdollisten kuormitushuippujen mukaan. Pilvipalveluissa isäntäpalvelin on palveluntarjoajan hallinnassa, kun taas asiakkaalle allokoitu osa palvelusta on asiakkaan hallittavissa. Pilvipalvelussa asiakas saa infrastruktuurin palveluna (IaaS) dynaamisesti muutettavilla määrityksillä. Pilvipalvelun edullisuus perustuu täysin Hypervisoreina toimivien palvelimien resurssien maksimaalisen

hyödyntämiseen, kun taas perinteisessä hosting-ratkaisussa asiakkaalle on allokoitu tietyillä määrityksillä toteutettu joko virtuaalinen tai fyysinen palvelin. Hosting-ratkaisussa saatavan palvelimen määritykset on muutettavissa, mutta niitä ei pystytä toteuttamaan dynaamisesti ilman palvelukatkosta. (Webopas.)

Microsoft Azure -palvelu skaalautuu erittäin hyvin tarpeiden mukaan mahdollistaen samalla monipuoliset integraatiot muiden niin sanottujen pilvipalveluiden ja sisäverkon palveluiden kanssa. Sisäverkosta Microsoft Azure -palveluun tarjottavia palveluita voivat olla esimerkiksi Active Directory-, DNS-, sähköposti-, verkkolevy- ja verkkosivustopalvelut. Microsoft Azure -palveluun voidaan teoriassa siirtää kaikki niin sanotut On Premises -ympäristön palvelinkoneet ja jo aiemmin virtualisoidut palvelimet. Palvelussa voidaan esimerkiksi ajaa Microsoft SQL-tietokantaa ilman varsinaista Windows SQL -palvelinta. Microsoft Azure –palvelussa on mahdollista hyödyntää suosittujen avoimen lähdekoodin sisällönhallinta ja julkaisujärjestelmiä. (Microsoft 2014b.)



Kuva 3: Windows Azure -palvelu

Microsoft Azure -palvelulle löytyy useita kilpailijoita. Suurimpia kilpailijoita ovat Amazon, IBM ja Google. Eri palveluntarjoajien keskinäinen vertailu on erittäin haastavaa, koska palveluiden sisältö poikkeaa hieman toisistaan niin teknisesti kuin palvelusisällöltään. Vertailtaessa eri palveluntarjoajia keskenään, tulee huomioida mahdollisuus omaan palvelinlaitteistoon. Suurin syy valita Microsoft Azure -palvelu tähän toteutukseen oli luotettu palveluntarjoaja sekä tekniset ratkaisut, joilla toteutus tehdään.

3 Vaatimusmäärittely

Microsoft Azure –palvelun hyödyntäminen asettaa tiettyjä vaatimuksia erityisesti tietoliikenteelle. Yrityksellä tulee olla fyysisessä verkossa julkinen IP-osoite, joka ei ole osoitteen muutoksen takana(NAT). Osoitteen tulisi olla kiinteä, koska sen vaihtuessa yhteys Microsoft Azure -palveluun pitää määritellä uudestaan. Mikäli kyseinen osoite ohjautuu palomuurille, tulee liikenne reitittää palomuurilta VPN-laitteelle. Simonsenin (2012) mukaan VPN-laitteen tulee tukea seuraavia vaatimuksia:

- IKEv1, Internet Key Exchange version 1
  - Protokollalla toteutetaan yhteyksien avausvaiheessa avainten vaihdon vaativat neuvottelut. Ikellä yhdistetään myös ISAKMP:n, IPSec DOI forISAKMP:n ja Oakley Key Determination-protokollat kattavaksi kokonaisuudeksi. (Lapinniemi 2002, 6.)
- IPsec tunnel mode
  - Tunnelimoodissa palomuuri todentaa koko asiakkaan lähettämän paketin todennusotsakkeen mukaan, jonka jälkeen myöntää pääsyn palomuurilla suojattuun verkkoon. Tunnelimoodia käytetään pääsääntöisesti virtuaalisissa yksityisissä verkoissa. (Karvi 2006, 8.)
- NAT-T
  - IPSec-virtuaalisessa yksityisessä verkossa NAT-traversal mahdollistaa kapseloidun suojatun liikenteen NAT:n läpi. NAT on lyhenne sanoista Name Address Translation, joka suoritetaan DNS-palvelussa. NAT:lla tarkoitetaan selkokielisen osoitteen kääntämistä IP-osoitteeksi, esimerkiksi Googlen palvelu löytyy kun selaimen osoiteriville syöttää seuraavan osoitteen: www.google.fi . Käytännössä selain suorittaa nimikyselyn nimipalveluja tarjoavalta palvelimelta, josta se saa vastaukseksi, että kyseinen osoite löytyy seuraavasta IP-osoitteesta 74.125.232.119. Edellä mainittu IP-osoite internet selaimen osoiteriville syötettynä avaa suoraan Googlen palvelun. (Wikipedia 2013b.)

- AES-128
    - Symmetrinen salausmenetelmä, jossa salaus ja salauksen purku suoritetaan samalla salausalgoritmilla ja salausavaimella. (Valtiovarainministeriö 2009.)
- Diffie-Hellman Perfect Forward Secrecy in "Group 2" mode
    - Metodi salausavainten turvalliseen vaihtamiseen tietoverkon aktiivilaitteiden kesken. (Wikipedia 2013c.)

Listaus tuetuista ja yhteensopivista VPN-laitteista löytyy liitteestä 1 (Liite 1).

Internet-liittymälle ei ole määritetty mitään vähimmäisvaatimuksia tiedonsiirtonopeuden suhteen. Microsoft Azure -palvelusta tarjottavan palvelun käyttämä tietoliikennekapasiteetti on pois julkisen internetin käyttämiseen varatusta kapasiteetista, joka tulee huomioida suunniteltaessa palvelulle alustaksi Microsoft Azure -palvelua.

Microsoft Azure -palvelun tietoliikenteen hinnoittelu ohjaa suunnittelua hieman. Microsoft Azure -palveluun siirretystä datasta sekä palvelun sisäisestä tietoliikenteestä ei aiheudu kuluja. Kulut syntyvät tietoliikenteen osalta vain Microsoft Azure -palvelusta ulospäin suuntautuvasta liikenteestä. Tässä toteutuksessa tietoliikenne ei suurissakaan määrissä muodosta kuin murto-osan palvelun käytöstä aiheutuvista kuluista. (Microsoft 2014a.)

Omasta fyysisestä verkosta tulee allokoida Microsoft Azure -palvelulle oma verkkoalue. Microsoft Azure -palvelun verkkomäärityksessä voidaan kertoa yrityksen On Premises-ympäristön DNS-palvelimen nimi ja IP-osoite. Mikäli DNS-palvelimen tietoja ei kerrota Microsoft Azure -palvelun verkkomäärityksessä, käyttää Microsoft Azure -palvelu julkista DNS-palvelua. Julkinen DNS-palvelu ei pysty vastaamaan sisäverkkoon kohdistuviin nimi kyselyihin. (Microsoft 2014c.)

4 Toteutus

Toteutuksessa tarvitaan Microsoft ID ja vähintään yksi aktiivinen tilaus Microsoft Azure -palveluun. Microsoft ID:n luominen onnistuu seuraavassa osoitteessa https://manage.windowsazure.com rekisteröitymällä uutena käyttäjänä. Mikäli käytössä on jo jokin Microsoftin tarjoama verkkopalvelu, ei Microsoft ID:tä tarvitse luoda erikseen, vaan kirjautuminen palveluun onnistuu kyseisellä Microsoft ID:llä.

Microsoft Azure -palvelu sisältää useampia vaihtoehtoja tilauksista, joista osa on julkisesti hankittavia ja osa vaatii EAS-sopimuksen (Kuva 4). (Microsoft 2014d; Microsoft 2014e.) Mikäli Microsoft ID:en ei ole liitettynä yhtään aktiivista tilausta, tulee sellainen liittää Microsoft Azure -palvelun hallintaportaalista.

Kuva 4: Microsoft Azure tilauksen vaihtoehdot

4.1 Toteutuksen työjärjestys

Ensimmäisessä vaiheessa toteutusta luodaan Microsoft Azure -palveluun virtuaaliverkko, joka yhdistetään yrityksen fyysiseen verkkoon.

Toisessa vaiheessa Microsoft Azure -palveluun tehdään toiminnanohjausjärjestelmän vaatima virtuaalipalvelin sekä toiminnanohjausjärjestelmän vaatima tietokantapalvelin. Tietokantapalvelin voi tässä toteutuksessa kuitenkin sijaita On Premises -ympäristössä. Microsoft Azure -palvelussa on mahdollista käyttää pelkästään SQL-tietokantaa, joka toimii kuten varsinaisella tietokantapalvelimella oleva SQL-tietokanta. Toinen tapa on tehdä tietokantapalvelimelle oma SQL-tietokanta. Tässä toteutuksessa päädyttiin tekemään Microsoft Azure -palveluun palvelua varten dedikoitu tietokantapalvelin, koska ServiceDesk+-palvelu ei tue Microsoft Azure tietokantaa. (ZOHO Corporation 2012, 3.) Tämä ratkaisu kuormittaa ulospäin suuntautuvaa tietoliikennettä merkittävästi vähemmän. Samalla ratkaisu on suorituskykyisin, koska sovelluspalvelin ja tietokantapalvelin sijaitsevat fyysisesti samassa virtuaaliverkossa, joka sijaitsee fyysisesti samassa palvelinkeskuksessa.

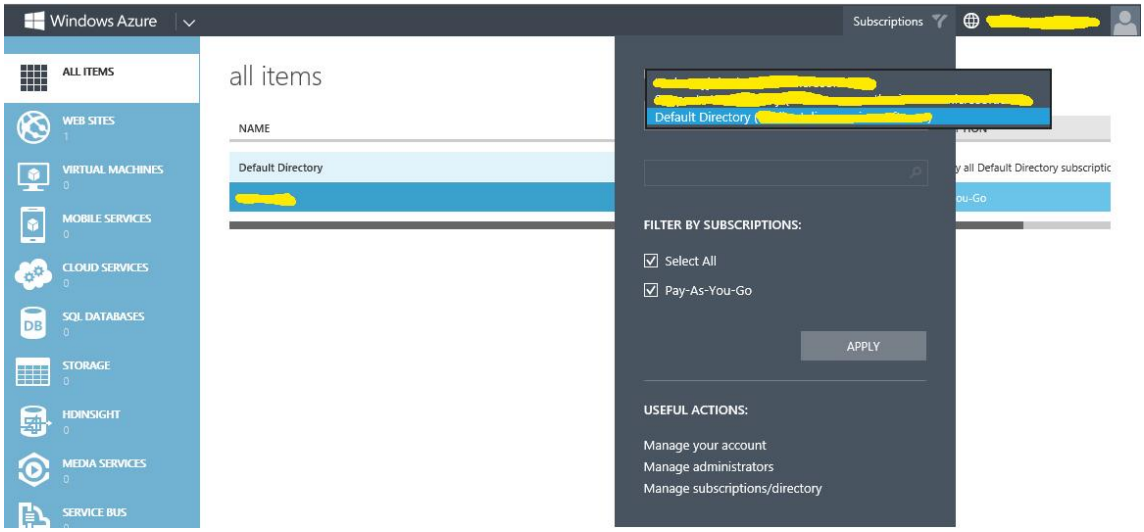
Kolmannessa vaiheessa asennetaan varsinainen toiminnanohjausjärjestelmä hyödyntäen aiemmin Microsoft Azure -palveluun luotuja virtuaalipalvelimia. Asennuksen jälkeen järjestelmälle suoritetaan testaussuunnitelman mukaiset testit. Jos testitulos hyväksytään, jatketaan datan migraatiolla tuotantopalvelusta Microsoft Azure -palveluun luotuun ympäristöön. Datan migraation jälkeen suoritetaan järjestelmälle testaussuunnitelman mukainen laajamittainen testi. Testauksen jälkeen suoritetaan tuloksien analysointi ja tehdään päätös järjestelmän tuotantoon siirtämisestä.

Neljäs vaihe on tuotantoon siirtäminen. Tärkeimpänä vaiheena tuotantoon siirtämisessä on päivittää tuotantokannasta varsinaisen data migraation jälkeen muuttuneet tiedot. Tämän jälkeen tehdään On Premises-ympäristön DNS-palveluun

osoitteen uudelleen ohjaus. Sekä muutetaan ServiceDesk+-palvelun sähköposti määritykset vastaamaan tuotantoympäristöä.

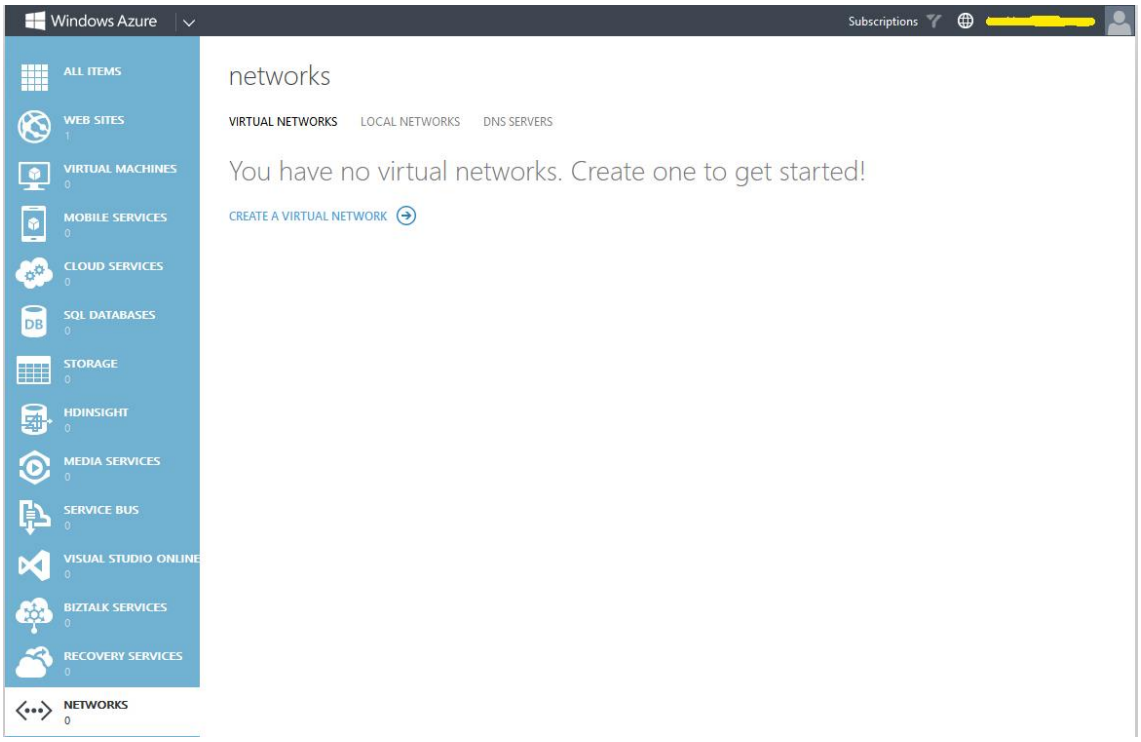
4.2 Virtuaaliverkon luominen ja yhdistäminen yrityksen fyysiseen verkkoon

Virtuaaliverkkoa luotaessa tulee ensimmäiseksi kirjautua Microsoft Azuren -hallintaportaaliin internet-selaimella käyttäen Microsoft ID:tä, johon on liitetty ainakin yksi aktiivinen tilaus. Kirjautumisen jälkeen valitaan tilaus, mikäli tilauksia on aktiivisena useampia (Kuva 5).



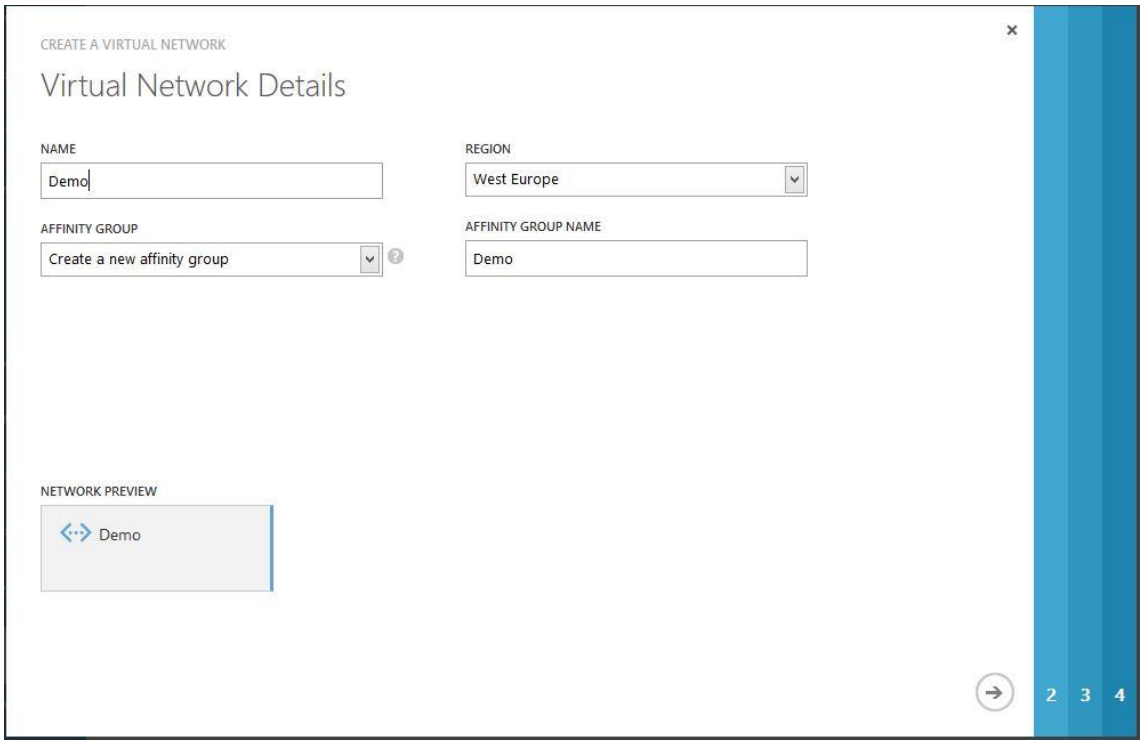
Kuva 5: Microsoft Azure tilauksen valinta

Oikean tilauksen ollessa valittuna aktivoidaan vasemman reunan navigointipalkista ”network”-osio. Tämän jälkeen valitaan keskelle ilmestyvästä osasta ”virtual network”, jonka jälkeen valitaan vielä ”Create a virtual network” (Kuva 6).



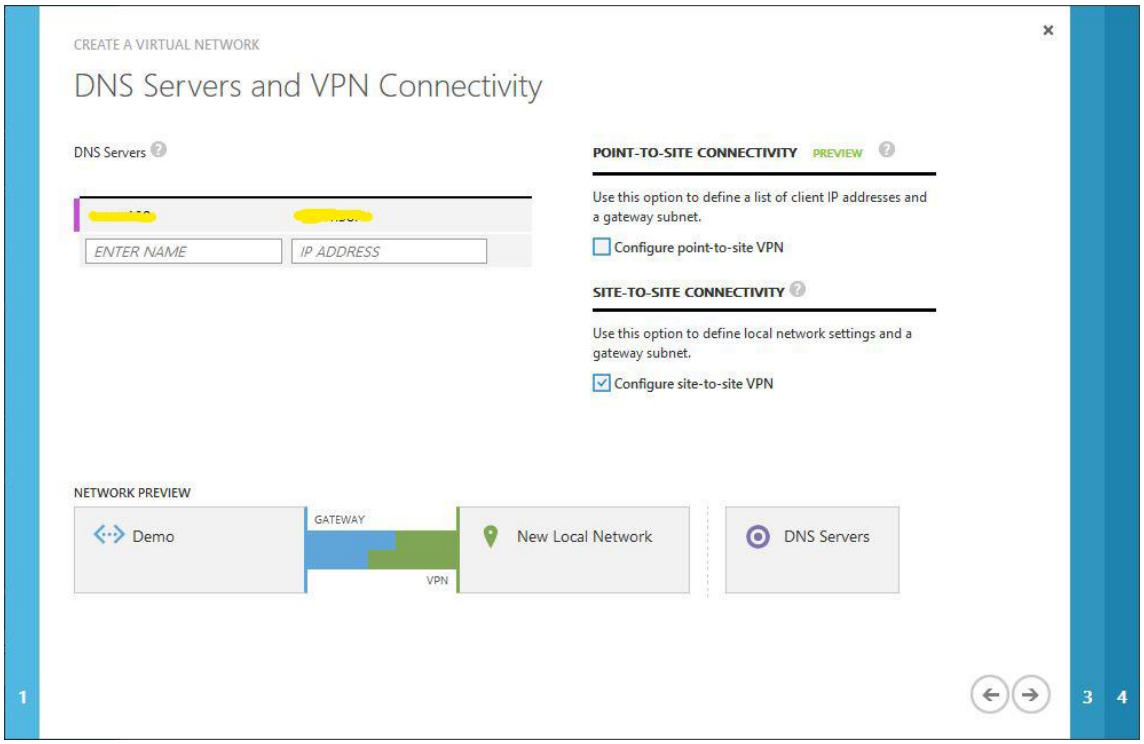
Kuva 6: Microsoft Azure -verkon luomisen aloitus

Seuraavana verkkoa luotaessa syötetään virtuaaliverkolle nimi. Maantieteellinen aluevalinta määrittää mihin palvelinkeskukseen verkko sijoitetaan fyysisesti. Mikäli virtuaalinen verkko sekä verkossa sijaitsevat palvelimet ovat fyysisesti eri maantieteellisillä alueilla, voi seurauksena olla suorituskykyongelmia. Affinity-ryhmän valinnalla voidaan Microsoft Azuressa olevat palvelut sitoa fyysisesti samaan palvelinkeskukseen. Tämä mahdollistaa Microsoft Azuressa olevien palvelujen paremman suorituskyvyn. Mikäli aiemmin ei ole luotu Affinity-ryhmää, tulee se nimetä tässä vaiheessa (Kuva 7).



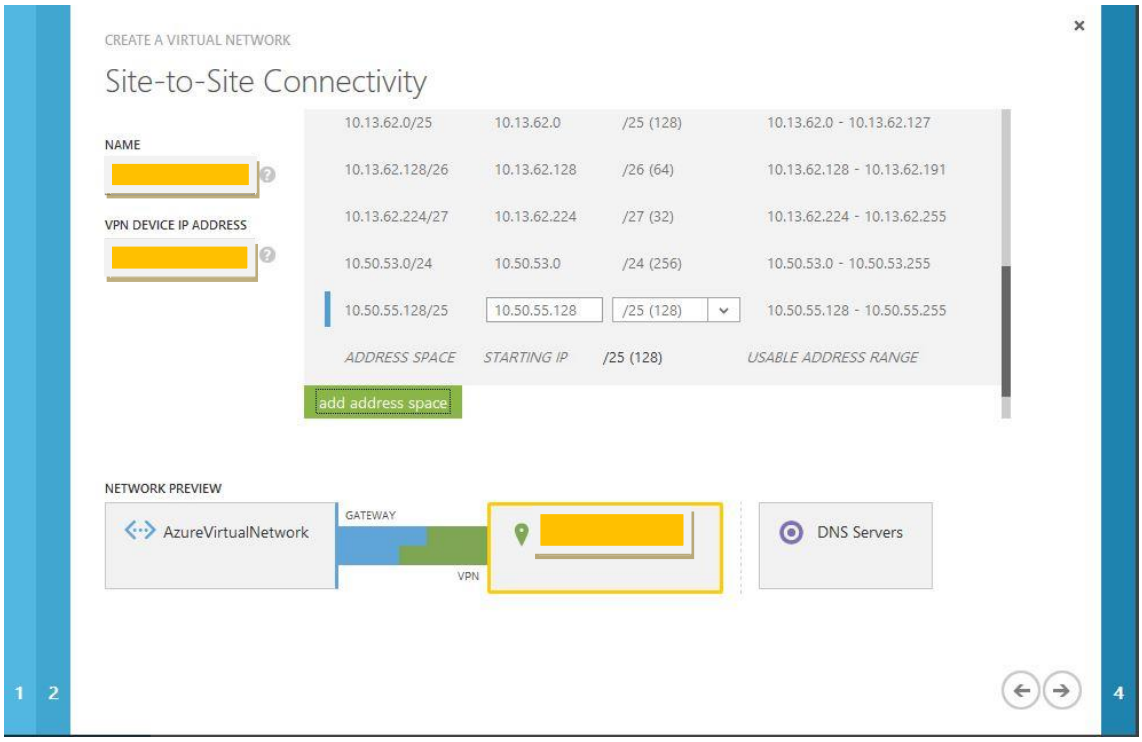
Kuva 7: Microsoft Azure verkon luonti, 1. vaihe

Seuraavaksi määritetään fyysisen verkon DNS-palvelimen nimi ja osoite. Mikäli kohdat jätetään tyhjiksi, palvelu käyttää julkista DNS-palvelua nimikyselyissä ja näin ollen sisäverkon nimikyselyt eivät ole mahdollisia. Tässä vaiheessa otetaan kantaa siihen luodaanko Point-to-Site ja/tai Site-to-Site VPN -yhteys. Tämä toteutus vaatii Site-to-Site VPN -yhteyden luomisen. Molempien hyödyntäminen on tarvittaessa mahdollista (Kuva 8).



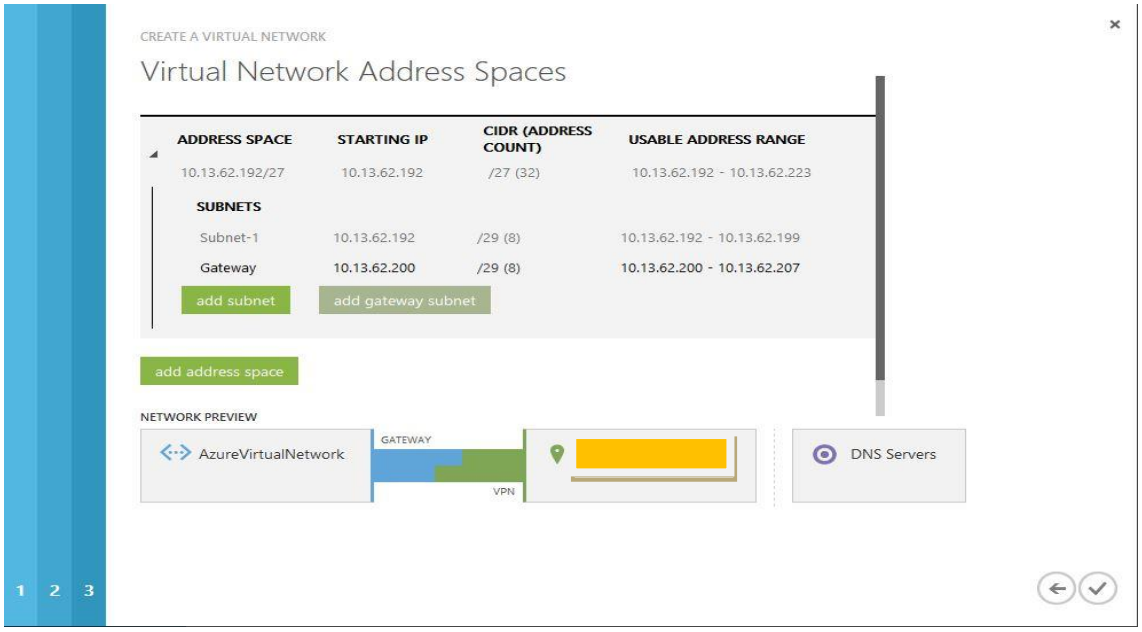
Kuva 8: Microsoft Azure-verkon luonti, 2. vaihe

Kolmannessa vaiheessa määritetään virtuaaliverkolle VPN-nimi ja fyysisen VPN-laitteen osoite. VPN-laitteen osoite ei saa olla nimen muunnoksen takana. Virtuaaliverkon VPN-nimeä käytetään vain Microsoft Azure -palvelun hallintaportaalissa helpottamaan niiden toisistaan erottamista, koska yhdellä tilauksella voi VPN-virtuaaliverkkoja olla useampia kuin yksi. Tässä vaiheessa määritetään myös Microsoft Azure -palveluun luotavan virtuaaliverkon osoiteavaruus sekä ne fyysisen verkon osoiteavaruudet, joilta muodostetaan Site-to-Site VPN -tunneli Microsoft Azure -palveluun luotavaan virtuaaliseen verkkoon (Kuva 9).



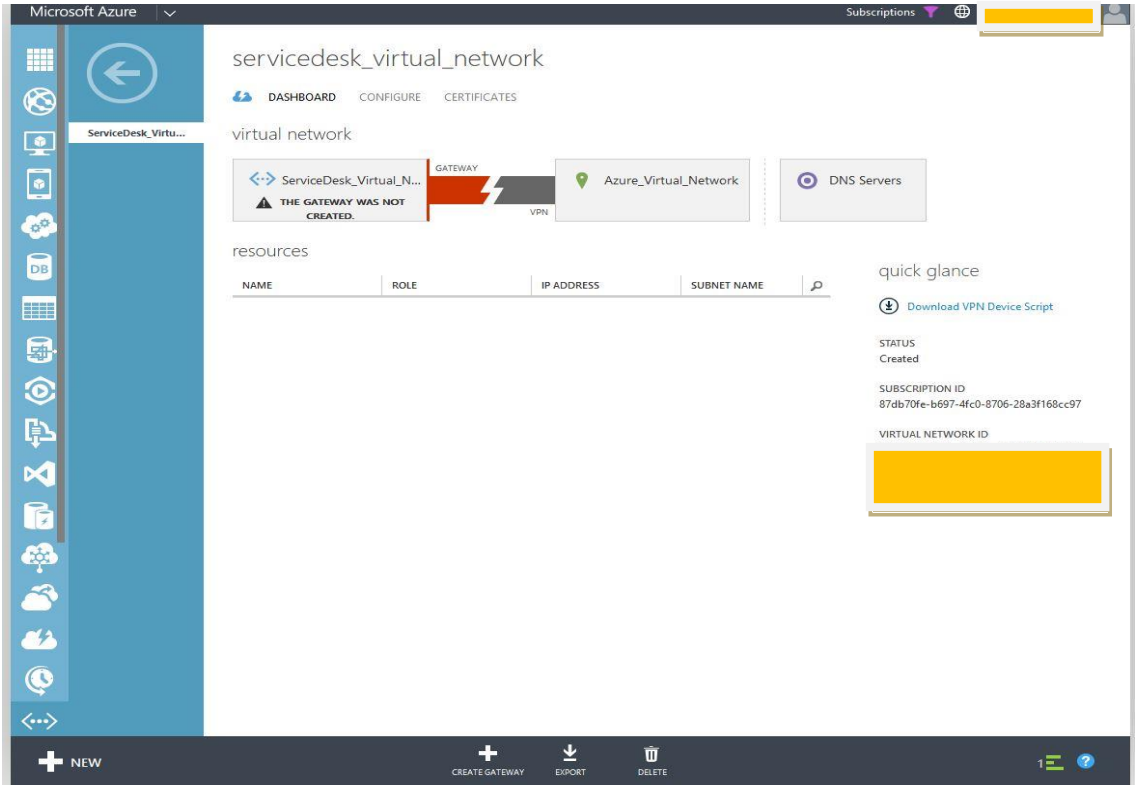
Kuva 9: Virtuaaliverkon luominen, 3. vaihe

Tässä vaiheessa määritetään Microsoft Azure -palveluun luotavan virtuaaliverkon aliverkkot sekä yhdyskäytävä. Valmiiden verkkomäärityksien jälkeen verkon luominen käynnistetään ”Check”-painikkeella (Kuva 10). (Microsoft 2014c).

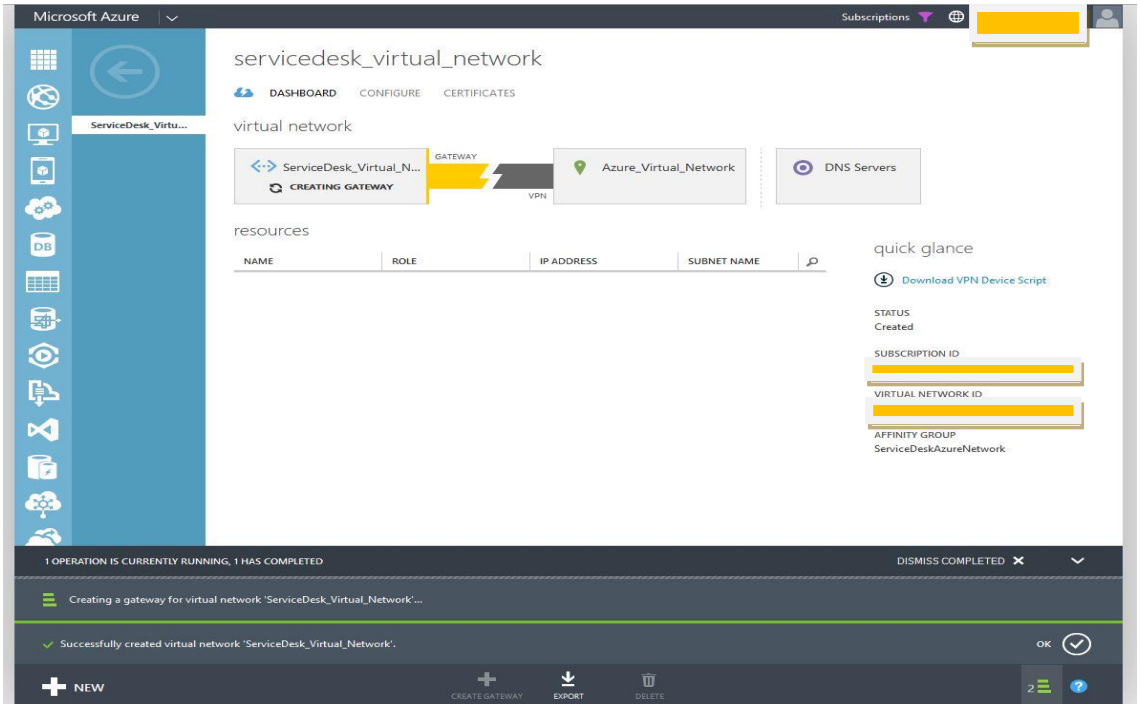


Kuva 10: Virtuaaliverkon luominen, 4. vaihe

Kun virtuaalinen verkko on luotu Microsoft Azure -palveluun onnistuneesti, tulee sen sisäinen yhdyskäytävän luominen käynnistää (Kuva 11), jonka jälkeen virtuaalinen verkko on valmis ja toteutuksessa voidaan siirtyä palomuurille tehtäviin konfiguraatioihin (Kuva 12).



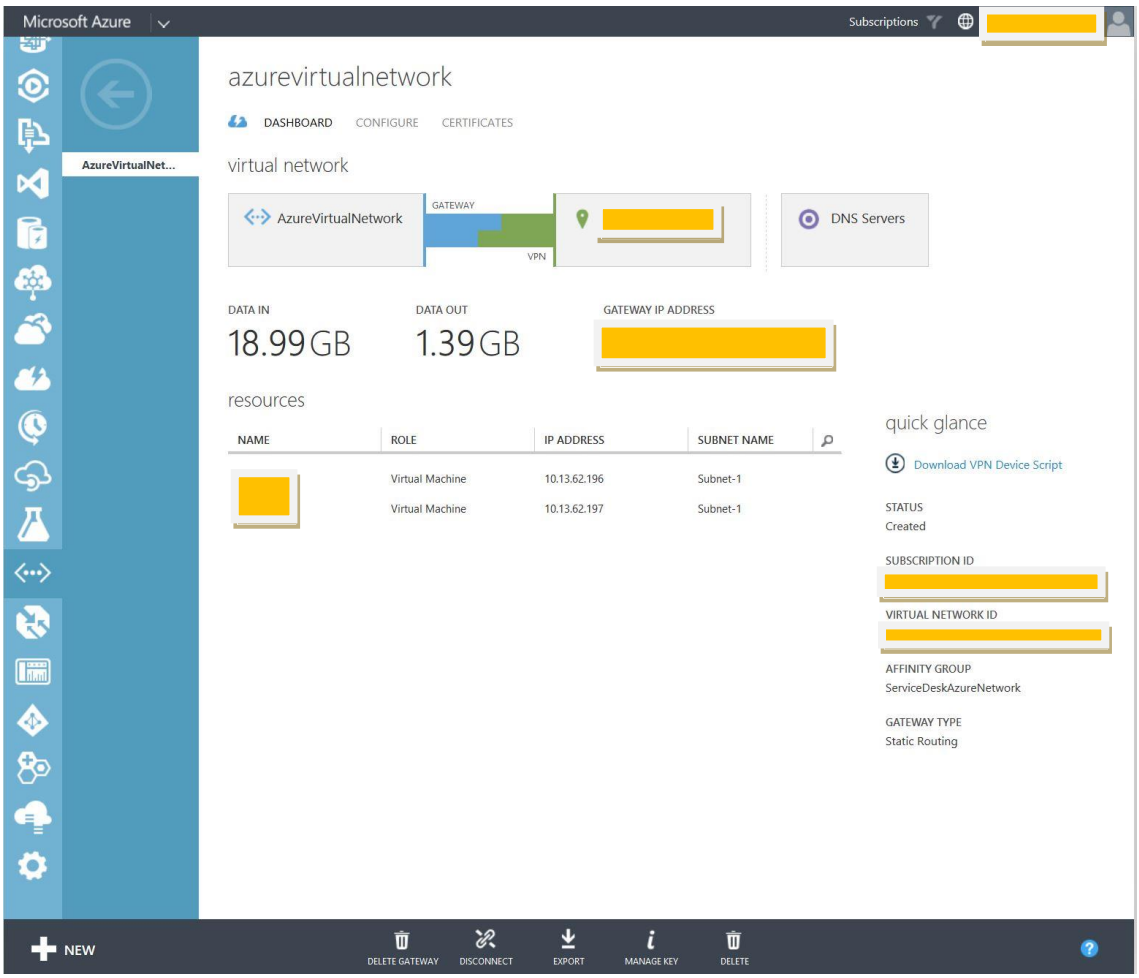
Kuva 11: Yhdyskäytävän luomisen käynnistäminen



Kuva 12: Virtuaaliverkko valmiina

Seuraavaksi toteutuksessa tilataan palomuuri- ja reititysmuutokset emoyhtiön tietohallinnolta muutoslomakkeella (Liite 2). Lomakkeella on kysytty käytetyistä salausmenetelmistä tietoja, jotka löytyvät helposti Microsoft Azure -palvelun hallintatyökalusta ladattavasta skripti-tiedostosta (Liite 3).

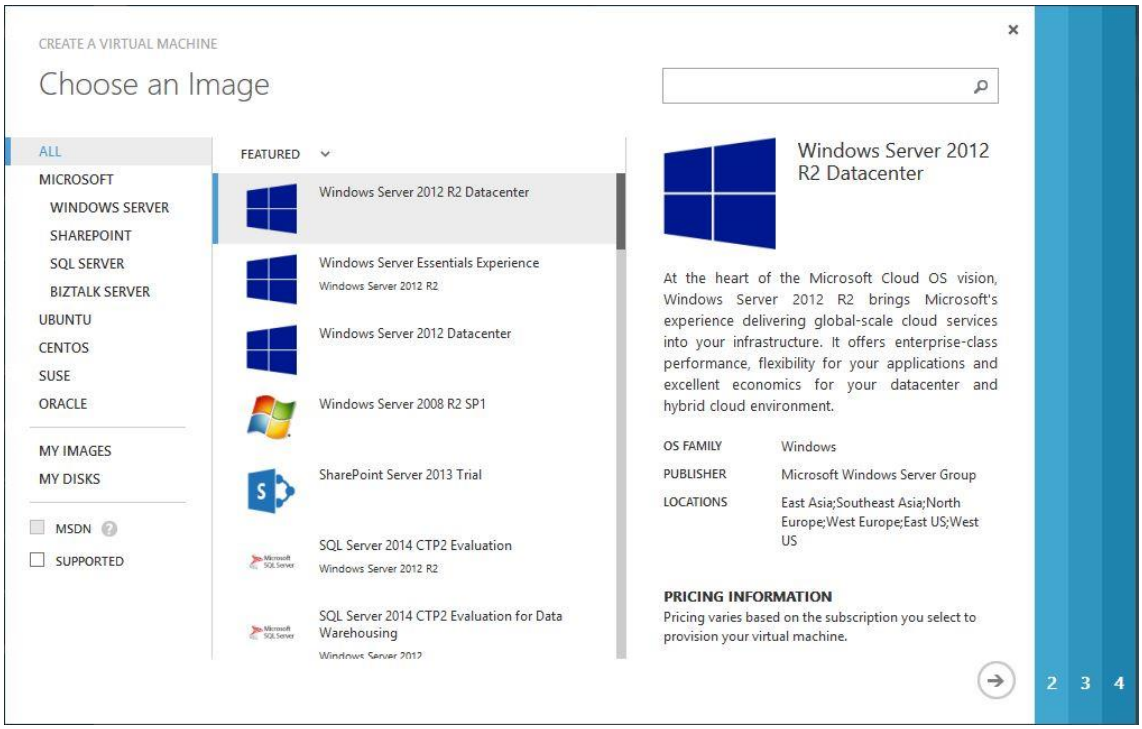
Microsoft Azure -palvelun hallintatyökaluilla saa helposti perustiedot Azure-palveluun tehdystä virtuaaliverkosta ja gatewaystä sekä niiden käytöstä (Kuva 13).



Kuva 13: Azure-verkon status

4.3 Virtuaalipalvelimien luominen

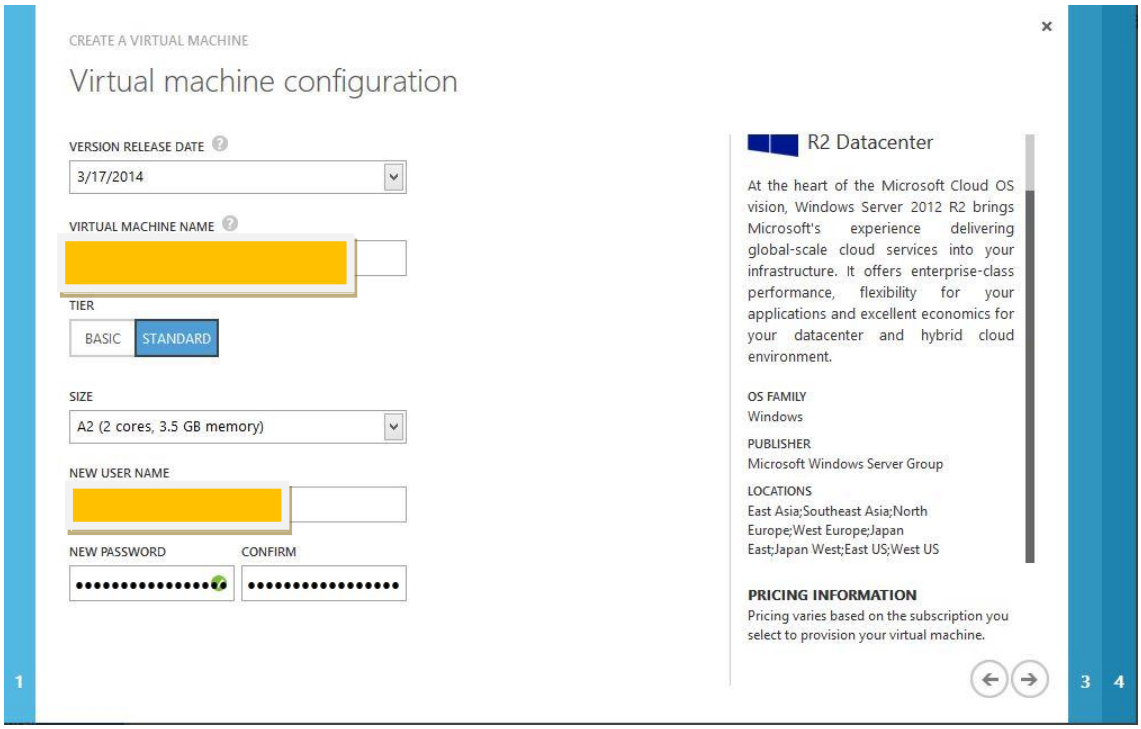
Microsoft Azure -palveluun on mahdollista tehdä virtuaalipalvelin usealla eri tavalla. Yksinkertaisin ja samalla helpoin tapa tehdä palvelin on valita galleriasta haluttu käyttöjärjestelmä ja käyttää valmista image-tasoista palvelinkäyttöjärjestelmää (Kuva 14).



Kuva 14: Image-tason käyttöjärjestelmät galleriasta

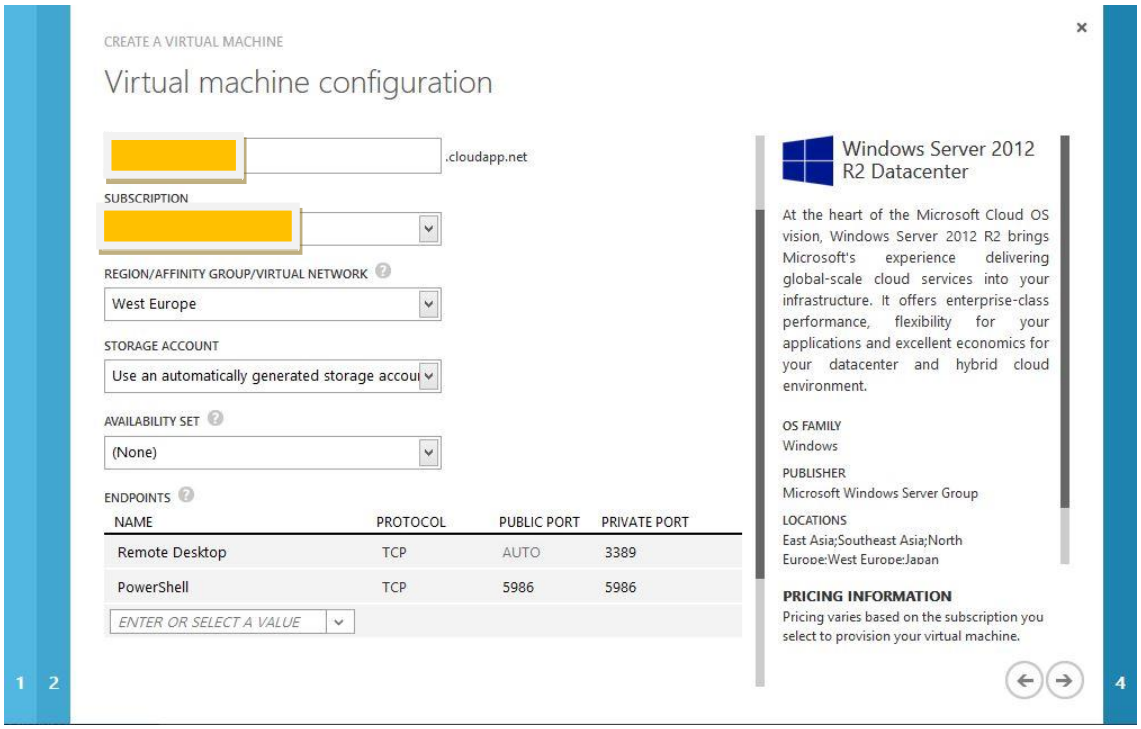
Hieman työläämpi vaihtoehto on oman olemassa olevan palvelimen hyödyntäminen. Mikäli palveluun halutaan siirtää jo olemassa oleva palvelin, tulee sen käyttöjärjestelmän levyosio konvertoida VHD-tiedostoksi. Konvertoinnin jälkeen VHD-tiedosto ladataan Microsoft Azure -palveluun ja lisätään gallerian omiin imageihin. Konvertoimalla voidaan Microsoft Azure -palveluun tuoda myös käytössä olevia data-levyosioita. (Crotty 2013.)

Tässä toteutuksessa päädyttiin käyttämään galleriasta valmista palvelinkäyttöjärjestelmää Windows Server 2012 molemmilla virtuaalipalvelimella. Päätöksen jälkeen seuraavassa vaiheessa valitaan mahdollinen versio käyttöjärjestelmästä, annetaan palvelimelle nimi ja valitaan palvelimen taso sekä palvelimen teho ja koko. Palvelimelle tulevan paikallisen järjestelmänvalvojatilin käyttäjätunnus sekä salasana ovat muutettavissa jälkikäteen. (Kuva 15).



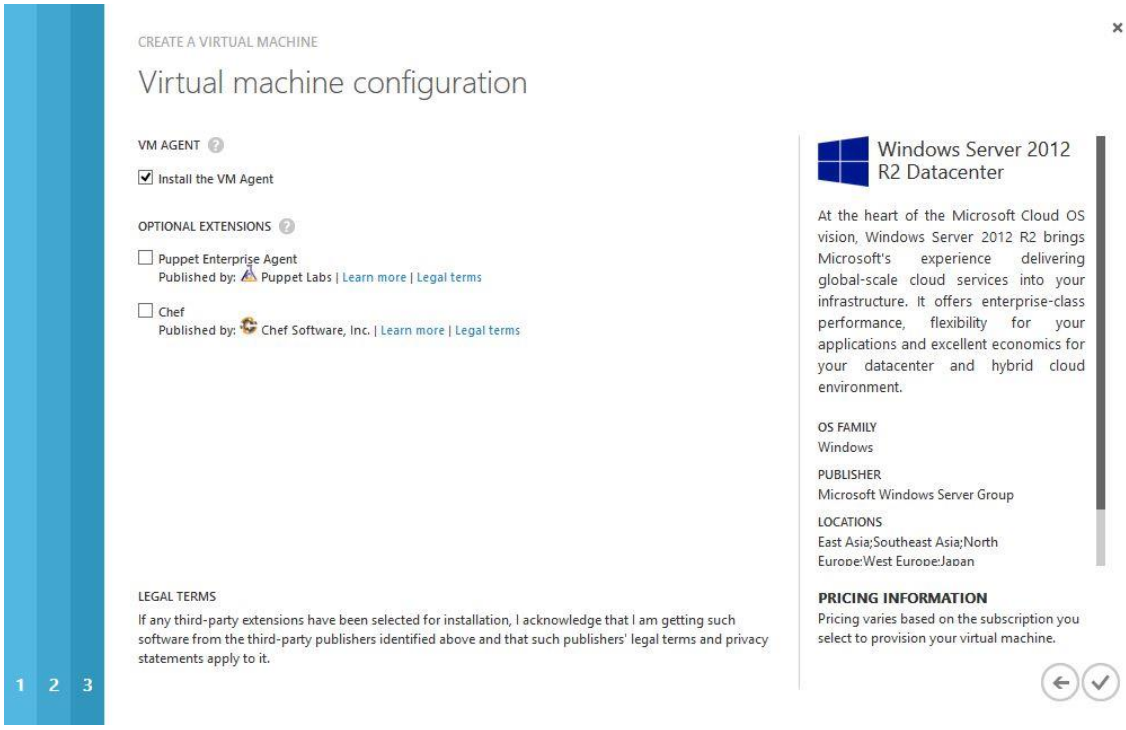
Kuva 15: Ensimmäinen palvelinmääritys

Edellisen vaiheen jälkeen palvelimelle määritetään Microsoft Azure -tilaus, johon kyseisestä palvelimesta syntyvät kulut ohjataan. Palvelimelle valitaan myös sijainti ja Microsoft Azuren Storage Account sekä mahdollinen saatavuusmääritys. Tässä vaiheessa voidaan määritellä sallitut ja tarvittavat etäyhteys- ja hallintaprotokollat, sekä niiden käyttämät portit. (Kuva 16).



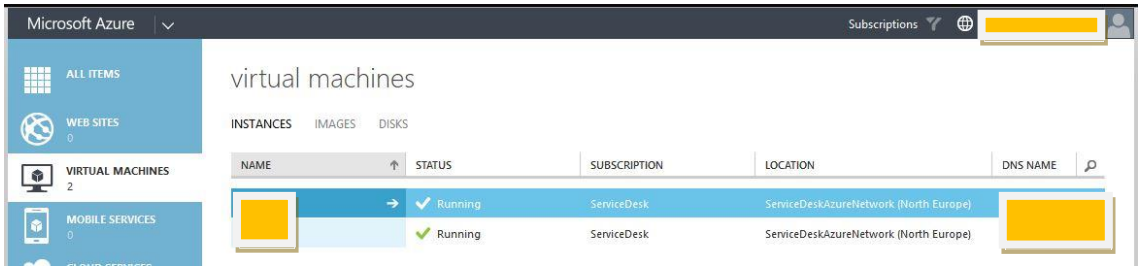
Kuva 16: Toinen palvelinmääritys

Kolmannessa vaiheessa valitaan vain mahdolliset palvelimelle asennettavat niin sanotut hallinta-agentit. (Kuva 17).

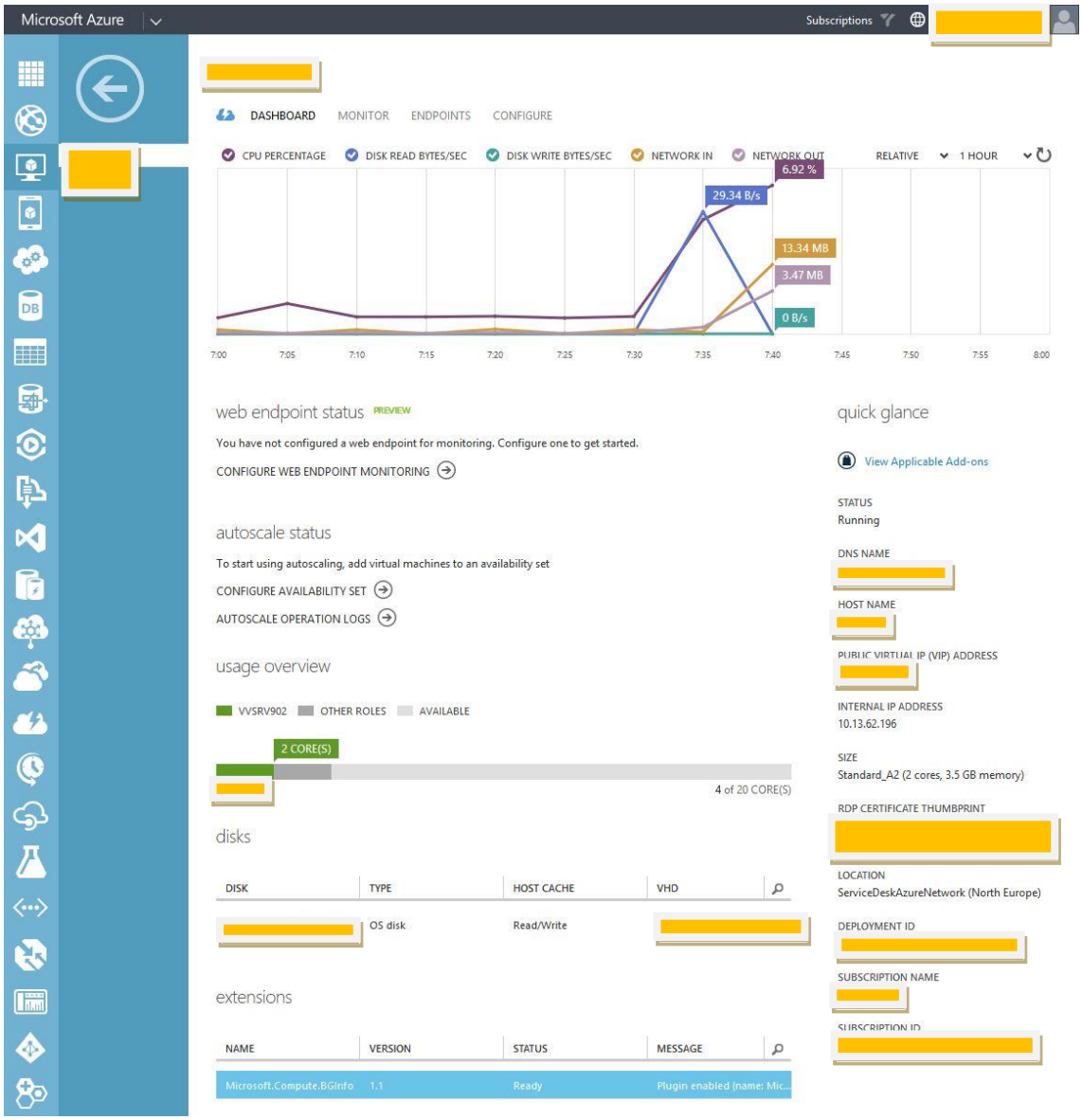


Kuva 17: Kolmas palvelinmääritys

Tämän jälkeen palvelin generoidaan ja käynnistetään automaattisesti. Palvelimen käynnistettyä sille tehdään aivan normaalit päivitykset ja konfiguroinnit, jotka tehtäisiin niin fyysiselle kuin muulla tavalla virtualisoidulle palvelinkäyttöjärjestelmälle. Microsoft Azure -palvelussa olevien palvelinten hallinta tapahtuu etätyöpöytä-asiakassovelluksen avulla, koska siinä ei ole esimerkiksi vmWare-virtualisointitekniikasta tuttua konsoli-istuntoa käytettävissä. Microsoft Azure -palvelun hallinta-portaalissa näkyy kummankin palvelimen status (Kuva 18). Haluttaessa voidaan myös tutkia tarkemmin palvelimen tietoja valitsemalla palvelin (Kuva 19).



Kuva 18: Palvelin hallinta



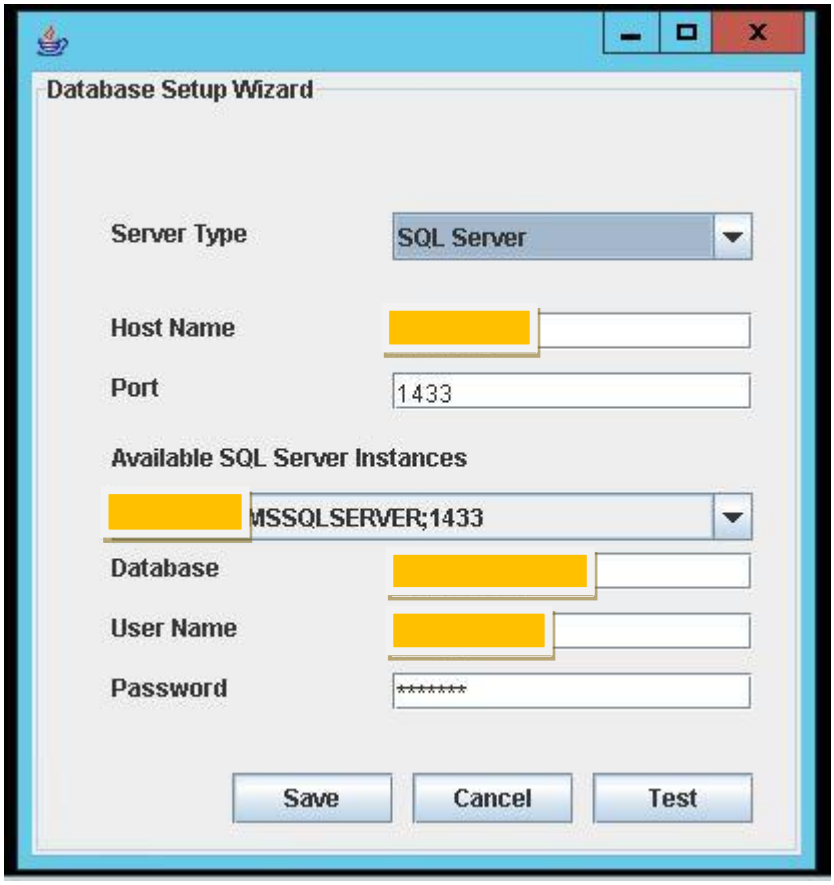
Kuva 19: Palvelimen tiedot

4.4 Toiminnanohjausjärjestelmän asentaminen

Toiminnanohjausjärjestelmän asentaminen aloitetaan luomalla Windows Azure -palveluun luotuun tietokantapalvelimeen järjestelmä ja sovellustunnus sekä tietokanta. Tunnusta luotaessa on huomioitava, että sille myönnettävät oikeudet ovat riittävät tietokannan skema-päivityksiin.

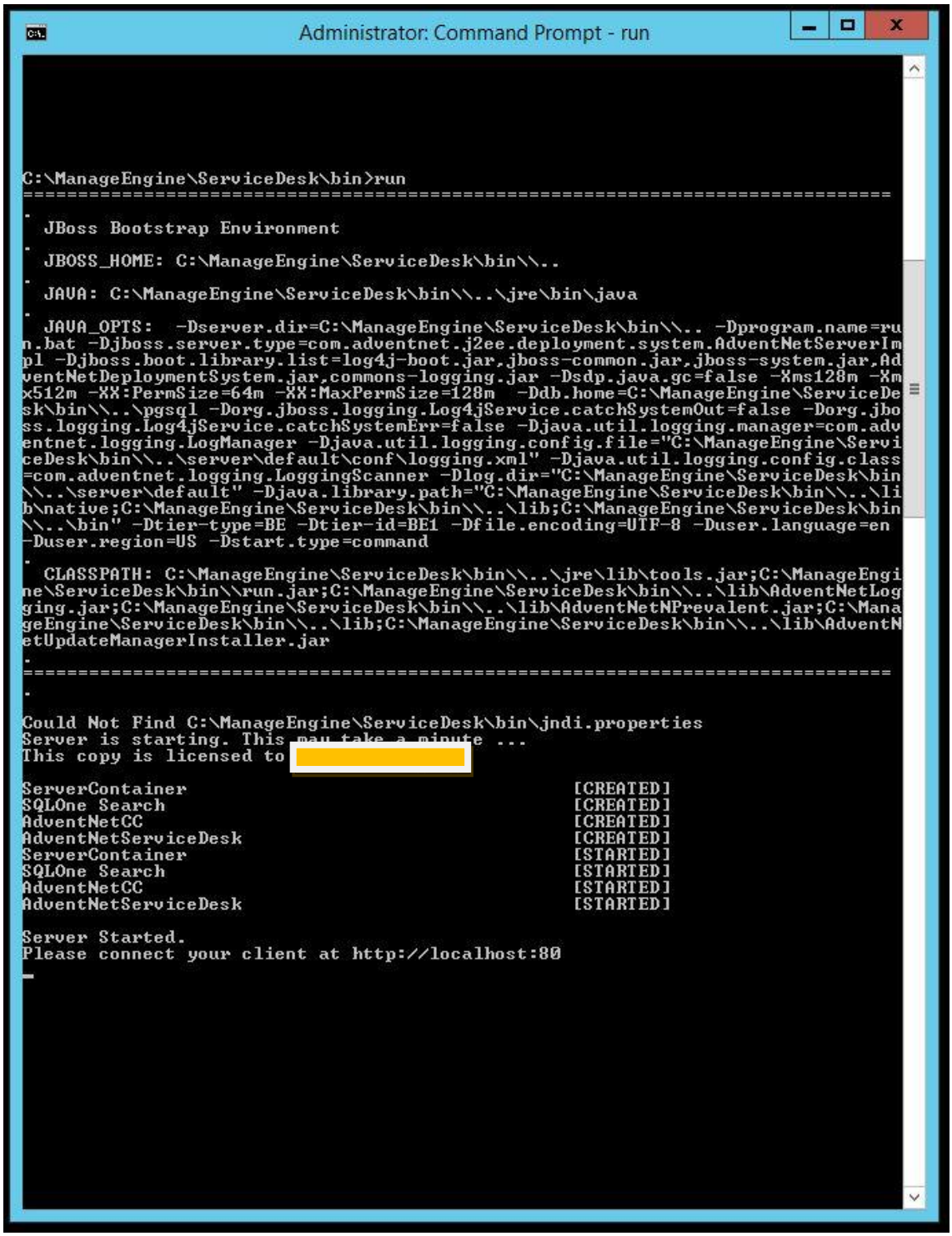
Tämän jälkeen otetaan etäyhteys toiminnanohjausjärjestelmää varten luodulle palvelimelle. Toiminnanohjausjärjestelmän asennus käynnistetään, jonka jälkeen ohjatussa asennuksessa valitaan palvelun asennus siihen integroidulla MySql-tietokannalla oletustunnuksin. Aiemmin luotua tietokantapalvelinta ja sovellustunnusta ei tässä vaiheessa pysty hyödyntämään palvelun ohjatun asennuksen puutteen vuoksi. Kun asennusohjelma on asentanut palvelun, se

kysyy, käynnistetäänkö palvelu. Tässä vaiheessa on tärkeää olla käynnistämättä palvelua, koska ensimmäinen käynnistyskerran yhteydessä palvelu tarkastaa määritetyn tietokantapalvelun ja tietokannan. Mikäli se ei löydä niitä, se aloittaa tietokantapalvelun ja tietokannan luomisen ja tässä toteutuksessa ei ole tarkoitus hyödyntää palveluun integroitua MySQL-palvelua ja tietokantaa. Tässä vaiheessa tulee käynnistää komentokehoite korotetuin oikeuksin ja käynnistää asennushakemiston ”bin”-kansiosta changedbserver.bat-tiedosto komentosarja. Kyseisen tiedoston suorittaminen avaa sovelluksen graafisen käyttöliittymän, jossa kerrotaan aiemmin luotu tietokantapalvelin, tietokanta ja käyttäjätunnus sekä salasana (Kuva 20).



Kuva 20: Tietokantamääritykset

Tämän jälkeen suoritetaan vielä ”bin”-kansiosta run.bat-tiedosto, joka käynnistää palvelun manuaalisesti. Ensimmäisellä kerralla palvelu myös huomioi tietokannan olevan tyhjä, jolloin se rakentaa tietokannan ja luo tarvittavat alkutiedot tietokantaan (Kuva 21).



Kuva 21: Manuaalinen käynnistys

Asennus on nyt valmiina ensimmäistä käyttökertaa varten. Ensimmäisellä käyttökerralla järjestelmään kirjaudutaan paikallisilla tunnuksilla. Onnistuneen kirjautumisen jälkeen ei tarvitse tehdä muita konfiguraatioita järjestelmään, vaan asetukset ja järjestelmässä oleva data palautetaan tuotantojärjestelmästä otetusta varmistuksesta. Konfiguraatio tiedon ja

datan varmistus sekä palautus suoritetaan toiminnanohjausjärjestelmän omilla työkaluilla (Kuva 22).

Kuva 22: Datan palautus

Asetusten ja datan palautuksen jälkeen toiminnanohjausjärjestelmälle suoritetaan testaussuunnitelman mukainen perustoimintojen testaus.

Hyväksytyn testituloksen jälkeen voidaan toiminnanohjausjärjestelmän konfiguraatiota muuttaa luettavan sähköpostilaatikon osalta. Aiemmin toiminnanohjausjärjestelmä on lukenut servicedesk@xxx.fi osoitetta yrityksen On Premises -ympäristössä sijaitsevalta Lotus Domino -sähköpostipalvelimelta. Yrityksessä on aiemmin siirrytty käyttämään Microsoft Office365 -palvelua. On Premises -ympäristön sähköposti-palvelin on yrityksessä vain muutamia sovelluksia varten, joita ei ole vielä muutettu käyttämään Microsoft Office365 -palvelua. Suurin haaste vanhojen sovellusten muuttamisessa käyttämään Office365-palvelua on se, että sovellusten pitää tukea TLS-salausprotokollaa sovellusten välisessä tietoliikenteessä. Toiminnanohjausjärjestelmä on tukenut jo kyseistä protokollaa Microsoft Office365:n käytön aloituksesta asti, mutta yrityksen tietohallinto ei ole katsonut tarpeelliseksi muuttaa ServiceDesk+-palvelun sähköposti-palvelun sijaintia. Siirto onkin Microsoftin suositusten mukaan järkevintä toteuttaa osana laajamittaista toiminnanohjausjärjestelmän alustapalvelun kehityshanketta. (Cameron 2012; Microsoft 2012.)

Ennen tuotannonohjausjärjestelmän siirtämistä tuotantokäyttöön Microsoft Azure -palvelussa, siinä käytetään testausta varten tehtyjä sähköpostilaatikoita. Mikäli järjestelmä lukisi tuotannossa olevan palvelun sähköpostilaatikkoa, generoisi se väärään järjestelmään sisältöä asiakkailta tulleista viesteistä. Näin ollen asiakaspalvelu häiriintyisi pahasti, koska asiantuntijat eivät saisi tietoa asiakkaiden ongelmista tietoa tai vastauksia asiakkailta tai kolmansilta osapuolilta.

5 Testaus ja evaluointi

Asennuksen ja konfiguraatiomuutosten jälkeen toiminnanohjausjärjestelmälle suoritetaan kattava toiminnallisuuksien testaus erillisen testaussuunnitelman mukaan. Mikäli kyseisessä testauksessa ei havaita yhtään kriittistä tai vakavaksi määriteltyä ongelmaa voidaan aloittaa toteutuksen tuotantoon siirtäminen. Tuotantoon siirtäminen toteutetaan suunnitellusti viikonloppun aikana erikseen tiedotettavana huoltotyönä palveluaikojen ulkopuolella. Tämä mahdollistaa asiakaspalvelun katkeamattomuuden palveluajalla sekä takaa tarpeeksi suuren aikaikkunan ennalta odottamattomien ongelmien mahdollisesti vaatimalle takaisinvedolle.

Tuotantoon siirrossa palautetaan toiminnanohjausjärjestelmään nykyhetken data tuotantoympäristössä olevasta toiminnanohjausjärjestelmästä. Uudessa toiminnanohjausjärjestelmässä muutetaan konfiguraatioita sähköpostin osalta sekä tehdään tarvittavat DNS-muutokset On Premises -ympäristön DNS-palveluun. Samalla muutetaan sähköpostin ohjaus On Premises -ympäristöstä suoraan Microsoft Office365 -palveluun. Muutosten jälkeen toiminnanohjausjärjestelmälle suoritetaan uudestaan kattava toiminnallisuuksien testaus erillisen testaussuunnitelman mukaan. Mikäli testaustuloksessa ei ole edelleenkään yhtään kriittistä tai vakavaa ongelmaa, voidaan siirto hyväksyä ja jättää muutokset voimaan. Tämän jälkeen vanhat järjestelmät ajetaan alas, mutta niitä ei poisteta, vaan ne pidetään varalla kahden viikon ajan mahdollista takaisinvetoa varten.

6 Johtopäätökset

Opinnäytetyön toimeksiantona oli selvittää kuinka Microsoft Azure -palvelu soveltuisi yrityksen tietohallinnon toiminnanohjausjärjestelmän alustapalveluksi. Toteutuksessa suurimman haasteen muodosti hieman yllättäen tietoliikenteen ja sen asetusten määrittäminen yrityksen fyysisen verkon ja Microsoft Azure -palvelun virtuaalisen verkon välille emoyhtiön keskitetyn internet-liittymän läpi. Toteutusta testattaessa palvelun suorituskyvyssä ei havaittu merkittävää eroa On Premises -ympäristöstä tarjottavaan palveluun. Suorituskykyä mitattiin Internet Explorer 11:sta kehittäjätyökaluilla selaimen vasteaikoja ja latausaikoja vertailemalla. Integraatiot muihin ulkoisiin järjestelmiin onnistuivat aivan kuin On Premises -ympäristössä. On Premises -ympäristön puolelta muodostuneet parhaat käytänteet sovelutuvat suoraan Microsoft Azure -palveluun hyödynnettäväksi.

Vastaavia toteutuksia suunniteltaessa tietoliikenne ja sen suunnittelu tulee ottaa erityisen hyvin huomioon. Tietoliikenne oli toteutuksessa ainoa vaihe, jossa ei voinut hyödyntää jo olemassa olevia hyväksi todettuja käytänteitä. Microsoft Azure -palvelu soveltuu mielestäni niin pienille kuin suurillekin yrityksille pilvipalvelualustaksi sen monipuolisten kyvykkyyksien

ja ominaisuuksien sekä erittäin hyvän skaalautuvuuden takia. Tietoliikenne ja sen toiminta aiheuttavat suurimman yksittäisen riskin palvelukatkoksille. Puolen vuoden aikana palvelussa on ollut yksi käyttökatkos, joka johtui emoyhtiön tietoliikenne häiriöstä. Itse palvelussa ei ole ollut teknisiä ongelmia. Tietoliikenteen kahdentaminen pienentää riskiä mahdollisille palvelukatkoille.

Myös yrityksen tietoturvapolitiikka tulee ottaa huomioon toteutusta suunniteltaessa. Yrityksen tieto sijaitsee tässä toteutuksessa fyysisesti kahdessa eri lokaatiossa. Ensisijainen lokaatio on Dublin ja toissijainen lokaatio on Amsterdam.

Toteutusta tehdessäni syvensin omaa osaamistani tietoliikenteen suunnittelusta ja määrittelystä sekä terminologiasta. Azure-palvelusta itselläni oli projektia aloittaessa hyvä osaaminen, mutta pystyin koko projektin ajan syventämään omaa asiantuntijuuttani Azure-palvelusta koulutustasolle asti. Toteutuksen vaiheita suunniteltaessa keskustelin Microsoftin Azure -palvelun ratkaisuarkkitehdin kanssa. Hänen neuvojen ja parhaiden käytäntöjen mukaan laadittu suunnitelma mahdollisti toimivan ympäristön toteutuksen ilman ongelmia. Tietoliikenteen suunnitteluun panostaisin toteutusta uudelleen tehtäessä huomattavasti aiempaa enemmän.

Lähteet

Cameron, S. 2012. Is My Office 365 E-mail Secure?. Viitattu 24.2.2014. http://blog.quitecloudy.com/2012/05/is-my-office-365-e-mail-secure-part-2.html

Crotty, B. 2013. Moving a System or Drive to Windows Azure. Viitattu 13.2.2014. http://blog.credera.com/technology-insights/microsoft-solutions/moving-system-drive-windows-azure/

Microsoft. 2005. Components of Windows Server 2003 Site-to-Site VPNs. Viitattu 18.2.2014. http://technet.microsoft.com/en-us/library/cc775818(v=ws.10).aspx

Microsoft 2012. Tietoa Transport Layer Security (TLS) -salauksesta FOPE-palvelussa. Viitattu 24.2.2014. http://technet.microsoft.com/fi-fi/library/ff715256.aspx

Microsoft. 2014a. Data Transfers Pricing Details. Viitattu 30.1.2014. http://www.windowsazure.com/en-us/pricing/details/data-transfers/

Microsoft. 2014b. What Is Azure?. Viitattu 28.1.2014 http://msdn.microsoft.com/en-us/library/windowsazure/dd163896.aspx/

Microsoft. 2014c. Virtual Networks. Viitattu 2.2.2014. http://www.windowsazure.com/en-us/documentation/articles/virtual-networks-create-site-to-site-cross-premises-connectivity/

Microsoft. 2014d. How to buy Azure. Viitattu 12.2.2014. http://www.windowsazure.com/en-us/pricing/purchase-options/

Microsoft. 2014e. Licensing Azure for the Enterprise. Viitattu 12.2.2014. http://www.windowsazure.com/en-us/pricing/enterprise-agreement/

Microsoft. 2014f. Create a Virtual Machine Running Windows Server. Viitattu 13.2.2014. http://www.windowsazure.com/en-us/documentation/articles/virtual-machines-windows-tutorial/

Karvi, T. 2006. Verkkojen tietoturva. Viitattu 18.2.2014. http://www.cs.helsinki.fi/u/karvi/vkurssi06-28.pdf

Lapinniemi, T. 2002. Suojatut tietoyhteydet: FreeS/WAN VPN. Viitattu 8.7.2014. http://www2.it.lut.fi/kurssit/01-02/010628000/semmat/freeswan_vpn.pdf

Oulun seudun ammattiopisto. Palomuuri tekniikoita. Viitattu 18.2.2014. http://www.okol.org/verkkokurssit/datanomi/tietojarjestelmien_kehittaminen/tietoturvajarjestelmat/palomuurit/palomuuritekniikoita.htm

Simonsen, M. 2012. How to connect your on-premise network to Windows Azure using Windows Server as a VPN gateway. Viitattu 30.1.2014. http://morgansimonsen.wordpress.com/2012/10/24/how-to-connect-your-on-premise-network-to-windows-azure-using-windows-server-as-a-vpn-gateway-2/

Tarkki. Raid-luentomateriaali. Viitattu 24.2.2014. http://www.cs.uta.fi/tarkki/suoritus/luennot/raid.html

Tukiainen, K. 2000. Lähiverkot. Viitattu 11.3.2013. http://www2.it.lut.fi/kurssit/04-05/010626000/seminaarit/VLAN_Kimmo_Tukiainen_seminaari.pdf

Valtiovarainministeriö. 2009. Vahtiohje - Terminologiat, teknologiat ja tekniset suositukset. Viitattu 19.2.2014.
https://www.vahtiohje.fi/web/guest/terminologiat-teknologiat-ja-tekniset-suositukset;jsessionid=27AB602A4B922EC5EB4E7E3F27B3B726BAF0FC51D5E413339E371C1068BCF777C53B74E3B5E413E8CA61F9?p_p_id=56_INSTANCE_3paB&p_p_lifecycle=0&p_p_state=exclusive&p_p_mode=view&p_p_col_id=column-1&p_p_col_count=1&_56_INSTANCE_3paB_struts_action=%2Fjournal_content%2Fview&_56_INSTANCE_3paB_groupId=10128&_56_INSTANCE_3paB_articleId=27410&_56_INSTANCE_3paB_viewMode=print

Valtiovarainministeriö. 2010. Sisäverkko-ohje. Viitattu 18.2.2014.
http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20101203Sisaeve/Sisaeverkko-ohje.pdf

Webopas. Pilvipalvelu. Viitattu 17.2.2014.
http://www.webopas.net/pilvipalvelu.html

Wikipedia. 2013a. VPN. Viitattu 17.2.2014.
http://fi.wikipedia.org/wiki/VPN

Wikipedia. 2013b. NAT travelsal. Viitattu 18.2.2014.
http://en.wikipedia.org/wiki/NAT_traversal

Wikipedia. 2013c. Diffie–Hellman key exchange. Viitattu 18.2.2014.
http://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange

ZOHO Corporation. 2012. Manage Engine ServiceDesk Plus Installation Guide. Viitattu 18.7.2014.
http://www.manageengine.com/products/service-desk/help/ManageEngine_ServiceDeskPlus_Help_InstallationGuide.pdf

Kuvat

Liitteet

Liite 1: Tuetut VPN-laitteet

http://msdn.microsoft.com/en-us/library/windowsazure/jj156075.aspx Luettu 18.2.2014
Known compatible VPN devices

We have worked with VPN device vendors to jointly qualify specific VPN device families. The section below provides a list of all device families known to work with our virtual network gateway. All devices that are members of the listed device families are known to work unless exceptions are mentioned.

Note

For VPN device support, please contact your device manufacturer.

Vendor	Device family	Minimum OS version	Configuration template for static routing (policy-based)	Configuration template for dynamic routing (route-based) [Preview]
Cisco	ASA	8.3	Cisco ASA templates	Not compatible
Cisco	ASR	IOS 15.1 (static) IOS 15.2 (dynamic)	Cisco ASR templates	Cisco ASR templates
Cisco	ISR	IOS 15.0 (static) IOS 15.1 (dynamic)	Cisco ISR templates	Cisco ISR templates
Juniper	SRX	JunOS 10.2 (static) JunOS 11.4 (dynamic)	Juniper SRX templates	Juniper SRX templates
Juniper	J-Series	JunOS 10.4r9 (static) JunOS 11.4 (dynamic)	Juniper J-series templates	Juniper J-series templates
Juniper	ISG	ScreenOS 6.3 (static and dynamic)	Juniper ISG templates	Juniper ISG templates
Juniper	SSG	ScreenOS 6.2 (static and dynamic)	Juniper SSG templates	Juniper SSG templates

Watchguard	All	Fireware XTM v11.x	Configuration instructions	Not compatible
F5	BIG-IP series	N/A	Configuration instructions	Not compatible
Citrix	CloudBridge MPX appliance or VPX virtual appliance	N/A	Integration instructions	Not compatible
Microsoft	Routing and Remote Access Service	Windows Server 2012	Not compatible	Routing and Remote Access Service templates

Liite 2: Lan-2-Lan -tilauslomake

XXX Lan2Lan VPN Connection Request Form v2.0				Order Date:	27032014
Totally new Lan2Lan VPN connection setup	x				
Modification to existing Lan2Lan VPN connection setup					

IKE negotiation (Phase 1) (needed if totally new Lan2Lan-connection)							
Parameter name	Parameter setting (The preferred setting is bolded)						
IKE Mode	Main						
Supported data encryptions	x	AES-256		AES-128		3DES	
Supported hash algorithms	x	SHA1		MD5			
Diffie-Hellman Group		5	x	2		7	
Lifetime measurements		Time 14400s	x	Time 28 800s		Other time (pls specify)	

IPSec negotiation (Phase 2) (needed if totally new Lan2Lan-connection)							
Supported data encryptions	x	AES-256		AES-128		3DES	
Supported hash algorithms	x	SHA1		MD5			
Diffie-Hellman Group (PFS)		5	x	2		No PFS	
Lifetime measurements		Time 28800 s	x	Other time (3600s)			
Authentication Header	x	ESP					

XXX (VPN maintained by XXX)		Address:	Katu 12
Company:	XXX Oy	City:	00100 Helsinki
First name:	Last name:	Phone:	123456
Matti	Meikäläinen	E-mail address:	osoite@osoite.fi

XXXXXX Technical Contact information			
Company:	XXX Oyj		
Technical Contact			
First name:	Last name:	Phone:	E-mail address:
XXX	XXX	123456	osoite@osoite.fi

*** _ ***VPN gateway parameters	
VPN GW model	PA 5020 (VSYS VPN)
IP-address:	xxx.xxx.xxx.xxx

XXX Tunneled networks		
Network*	Subnet mask*	Add/Remove
10.13.0.0	255.255.192.0	Add
10.50.53.0	255.255.255.0	Add

Firewall rules for tunneled traffic should be ordered separately.

Customer B (partner of Customer A)		Address:	Katu 12
Company:	XXX Oy	City:	00100 Helsinki
First name:	Last name:	Phone:	123456
Lauri	Korte	E-mail address:	osoite@osoite.fi

Customer B Technical Contact information			
Company:	XXX Oy		
Technical Contact			
First name:	Last name:	Phone:	E-mail address:
Lauri	Korte	123456	osoite@osoite.fi

Customer B VPN gateway parameters	
VPN GW model	Azure
IP-address:	xxx.xxx.xxx.x

Customer B Tunneled networks		
Network*	Subnet mask*	Add/Remove
10.13.62.192	4	Add

Preshared Key will be agreed separately btw specialists (eg. by e-mail or SMS).

Return address / Service requests: osoite@osoite.fi

Liite 3: VPN Device –skripti

```
! Microsoft Corporation
! Windows Azure Virtual Network

! This configuration template applies to Cisco ASA 5500 Series Adaptive Security Appliances
running ASA Software 8.3.
! It configures an IPSec VPN tunnel connecting your on-premise VPN device with the Azure
gateway.

! ------------------------------------------------------------------------------------------------
----
! ACL and NAT rules
!
! Proper ACL and NAT rules are needed for permitting cross-premise network traffic.
! You should also allow inbound UDP/ESP traffic for the interface which will be used for the
IPSec tunnel.
object-group network azure-networks
 network-object 10.13.62.192 255.255.255.224
 exit
object-group network onprem-networks
 network-object 10.13.0.0 255.255.224.0
 network-object 10.13.32.0 255.255.240.0
 network-object 10.13.48.0 255.255.248.0
 network-object 10.13.56.0 255.255.252.0
 network-object 10.13.60.0 255.255.254.0
 network-object 10.13.62.0 255.255.255.128
 network-object 10.13.62.128 255.255.255.192
 network-object 10.13.62.224 255.255.255.224
 network-object 10.50.53.0 255.255.255.0
 network-object 10.50.55.128 255.255.255.128
 exit
access-list azure-vpn-acl extended permit ip object-group onprem-networks object-group az-
ure-networks
nat (inside,outside) source static onprem-networks onprem-networks destination static azure-
networks azure-networks

! ------------------------------------------------------------------------------------------------
----
! Internet Key Exchange (IKE) configuration
!
! This section specifies the authentication, encryption, hashing, Diffie-Hellman, and lifetime
parameters for the Phase
! 1 negotiation and the main mode security association. We have picked an arbitrary policy #
"10" as an example. If
! that happens to conflict with an existing policy, you may choose to use a different policy #.
crypto isakmp enable outside
crypto isakmp policy 10
 authentication pre-share
 encryption aes-256
 hash sha
 group 2
 lifetime 28800
 exit

! ------------------------------------------------------------------------------------------------
----
! IPSec configuration
!
```

```
! This section specifies encryption, authentication, and lifetime properties for the Phase 2
negotiation and the quick
! mode security association.
crypto ipsec transform-set azure-ipsec-proposal-set esp-aes-256 esp-sha-hmac
crypto ipsec security-association lifetime seconds 3600
crypto ipsec security-association lifetime kilobytes 102400000

! ------------------------------------------------------------------------------------------------------
----
! Crypto map configuration
!
! This section defines a crypto map that binds the cross-premise network traffic to the
! IPSec transform set and remote peer. We have picked an arbitrary ID # "10" as an example.
If
! that happens to conflict with an existing crypto map, you may choose to use a different ID
#.
crypto map azure-crypto-map 10 match address azure-vpn-acl
crypto map azure-crypto-map 10 set peer xxx.xxx.xxx.xxx
crypto map azure-crypto-map 10 set transform-set azure-ipsec-proposal-set
crypto map azure-crypto-map interface outside

! ------------------------------------------------------------------------------------------------------
----
! Tunnel configuration
!
! This section defines an IPSec site-to-site tunnel connecting to the Azure gateway and speci-
fies the pre-shared key
! value used for Phase 1 authentication.
tunnel-group xxx.xxx.xxx.xxx type ipsec-l2l
tunnel-group xxx.xxx.xxx.xxx ipsec-attributes
 pre-shared-key xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
 exit

! ------------------------------------------------------------------------------------------------------
----
! TCPMSS clamping
!
! Adjust the TCPMSS value properly to avoid fragmentation
sysopt connection tcpmss 1350
exit
```