Haaga-Helia
ammattikorkeakoulu Oy

Valtiokonttorin IT-hallintomalli hybridipilveen

Mika Elola

Opinnäytetyö
Tietojenkäsittelyn Ko.
2020

Tiivistelmä

Haaga-Helia ammattikorkeakoulu Oy

Tekijä(t)
Mika Elola

Koulutusohjelma
Tietojenkäsittely

Raportin/Opinnäytetyön nimi
Valtiokonttorin IT-hallintomalli hybridipilveen

Sivu- ja liitesivumäärä
30+0

Valtiokonttorin tietohallinto on siirtymässä kohti pilveä ja nyt vallitseva tilanne on ns. hybridimalli mikä koostuu sekä konesali – palveluista että pilvipalveluista. Valtiokonttori huomasi tarpeen saada selkeämpää dokumentaatiota aiheesta, jotta he voisivat koostaa selkeän hallintomallin hybridimallia varten, joten lähdin selvittämään miten hybridimallia kannattaa toteuttaa. Vertailin konesalipalvelun hallintomallia pilvipalveluiden hallintomalliin ja ITIL v4 prosessikehykseen, tunnistaakseni hybridimallin vaatimukset mitä ei tule esille kummastakaan vanhasta hallintomallista.

Tutkimus on toteutettu käymällä jo olemassa olevia hallintomalleja läpi kuten myös Valtiokonttorin dokumentaatiota heidän palveluistaan.

Asiasanat
Pilvipalvelut, IT-hallintomalli, On-premises -palvelut, Konesalipalvelut, ITIL v4, Azure

Sisällys

1 Johdanto

Tämä tutkielma käsittelee pilvipalveluiden hallintomallia Valtiokonttorin hybridiympäristössä. Tutkielmassa esitellään myös pilvipalveluita kokonaisuudessaan ja käydään läpi hallintomalleja Microsoftin pilvipalveluiden ja on-premises -palveluiden hyödyntämiseen.

Valtiokonttori on Valtionvarainministeriön alainen virasto, joka vastaa valtion lainanotosta, kassavarojen sijoittamisesta ja valtionvelan riskienhallinnasta.
Valtiokonttori myös hoitaa valtion työntekijöiden tapaturmakorvauksia, sekä kansalaisille mm. rikosvahinkokorvauksia ja hallinnoi valtion myöntämiä lainoja, korkotukia ja valtiontakauksia. (Valtiokonttori, Valtiokonttori pähkinänkuoressa)

Valtion tieto- ja viestintätekniikkakeskus eli Valtori tuottaa kaikille valtionhallinnon virastoille ICT-palveluita, mukaan lukien Valtiokonttorille. Valtori joko tuottaa itse tarvittavan palvelun tai hankkii sen ulkoiselta palveluntuottajalta. (Valtori, Tietoa Valtorista)

Tieto tarjoaa asiakkailleen ohjelmisto- ja ICT-palveluita. Tiedon asiakkaina on isoja yrityksiä ja julkishallintoa. Valtiokonttorille Tiedon kautta on ostettu konesalipalveluita. (Tieto, Tieto yrityksenä)

Microsoft Azure on Microsoftin pilvipalvelualusta. Azureen voi rakentaa, hallita ja julkaista sovelluksia. Pilvipalvelu voidaan mieltää tavaksi vuokrata laskentaresursseja ja tallennustilaa jonkun muun palvelinsalista. (Microsoft Azure 2019a.)

ITIL, eli information technology infrastructure library, on laajasti hyväksytty lähestymistapa IT-palveluhallintaan, ITIL:iä hyödynnetään maailmanlaajuisesti. Se tarjoaa yhtenäisen joukon parhaita käytäntöjä, jotka on kasattu julkiselta ja yksityiseltä puolelta. Axelos on tehnyt kattavaa tutkimusta, jonka mukaan ITIL on olennainen osa yrityksiä. Se mahdollistaa muutoksen ja auttaa organisaatioita ymmärtämään arvoa. ITIL suosittelee, että IT-palvelut sovitetaan yhteen liiketoiminnan tarpeiden kanssa ja että ne tukevat sen keskeisiä prosesseja. (Axelos 2019a.) ITIL –mallin kehitys alkoi 1980-luvulla Englannissa valtionhankkeena, josta se myöhemmin ajautui Axeloksen haltuun, joka nykyään omistaa ITIL tavaramerkin. (Wakaru 2019.)

Tutkimuksessa käydään läpi Valtorin Azure pilviratkaisua ja Tiedon on-premises -palveluita, näitä hallintomalleja vertaamalla toisiinsa ja peilaten niitä ITIL:iä vasten tuotan Valtiokonttorille hallintomallin hybridipilveä varten, joka siis koostuu Azure pilviratkaisusta ja on-

premises -palveluista.

Pilvipalvelut ovat koko ajan kasvava teknologia ja yhä useampi yritys ottaa pilvipalveluita käyttöön, kuitenkaan kaikki eivät halua tai lain nojalla edes voi ottaa puhdasta pilvipalvelumallia käyttöönsä. Tällöin järkevä vaihtoehto onkin toteuttaa hybridimalli, joka hyödyntää pilvipalveluita sekä on-premises -mallia.

Tavoitteena on siis vertailla on-premises -hallintomallia ja sen käytäntöjä Microsoftin Azure-pilvipalveluiden hallintomalleihin ja koostaa näiden avulla Valtiokonttorille hyödyllinen hallintomalli hybridimallia varten. Tärkeätä on tunnistaa selkeät puutoskohdat, eli hallintomallien kohdat, joista ei ole selkeää toimintamallia kummassakaan hallintomallissa tai kohdat, joissa hallintomallit ovat ristiriidassa keskenään.

1.1 Sanasto

Agile, ketterä ohjelmistokehitystapa. On työtapa, joka korostaa suoraa viestintää ja nopeaa muutoksiin reagointia.

AWS, Amazonin tarjoama pilvialusta.

Azure, Microsoftin julkinen pilvipalvelu.

CAB, change-advisory board. Ryhmä tai lautakunta, jonka tarkoitus on ohjata muutoksia läpi prosessin ja varmistaa muutosten tarpeellisuus ja toimivuus.

DevOps, palvelutuotannonmalli, jossa pyritään automatisoimaan ohjelmistokehitys ja siihen liittyvät testaus- ja ylläpidontoiminnot.

IaC, infrastructure as code, tarkoittaa tapaa tallentaa infrastruktuurista tietoja koodiin, jonka avulla voidaan taata, että kehitysympäristö vastaa tuotantoa.

JIRA, on Atlassianin julkaisema tehtävienhallintaohjelmisto. Ohjelmalla voidaan seurata eri työvaiheita, niiden kulkua ja hallita projekteja.

On-premises, yrityksen omissa tiloissa sijaitseva palvelin. Tässä tutkimuksessa on-premises nimitystä käytetään myös konesalipalveluista.

Pipeline, joukko automatisoituja prosesseja, joiden avulla voidaan automaattisesti testata, kasata ja julkaista koodia.

Azure Resource Group, on Azuren Subscriptionin alla sijaitseva ryhmä tai olio, jonka alle on kasattu resursseja mitkä kuuluvat yhteen. Tässä tutkimuksessa käytetään suomennosta resurssiryhmä.

Serverless, on pilvipalvelun malli, jossa ladataan vain esim. metodi tai funktio pilveen, josta sitä kutsuttaessa se allokoi itselleen sopivan palvelimen tai tilan missä sitä ajetaan.

Azure Subscription, voidaan mieltää Azure tenantin alle luoduksi kansioksi. Jokainen kansio voi sisältää useita resursseja ja yhden tenantin alla voi olla useita kansioita.

Azure Tenant, voidaan mieltää organisaatioksi tai sen päätasoksi, joka on yhteistyössä Azuren kanssa. Toisin sanoen tenantti on dedikoitu Azure AD instanssi.

QA-testaus, laadunvalvonta ja ohjelmiston testaustapa, jolla varmistetaan palvelun toimivuutta.

2 Tietoperusta

Tässä kappaleessa avataan hieman pilvipalveluiden eri malleja ja sitä, miten ne eroavat toisistaan.

2.1 Pilvipalvelut

Kun yritys käyttää palvelua tietoliikenneverkon yli ja yritykselle tarjotaan vain sen tarvitsema osa palvelusta, voidaan puhua pilvipalvelusta. Oli se sitten koko palvelu tai vain osa infrastruktuurista. Toisin sanoen pilvipalvelulla tarkoitetaan palvelumallia, jossa tarjotaan asiakkaalle resurssipohjaisesti vain hänen tarvitsemansa osa järjestelmästä. Pilvipalveluiden resursseja tarjotaan muutamalla eri palvelumallilla eli IaaS (Infrastructure as a Service), PaaS (Platform as a service) ja SaaS (Software as a service), asiakkaan kontrollin mukaan laskevassa järjestyksessä. (NIST 2018, 3.)

IaaS pitää sisällään vain pilvialustan, johon asiakas itse kasaa tarvitsemansa palvelut. Palveluilla tässä tarkoitetaan VM/desktop-, tallennustila-palveluita tai verkkokomponentteja. PaaS on kokonaan valmis alusta, johon asiakas voi julkaista valmiin sovelluksen. Asiakas ei voi vaikuttaa palvelimeen, käyttöjärjestelmään tai tallennustilaan. SaaS on valmis sovellus, joka on käytössä pilvessä. Asiakas ei voi vaikuttaa muuhun kuin käyttäjäkohtaisiin asetuksiin sovelluksessa. Tällainen sovellus on esim. Gmail.
(NIST 2018, 9-11.)

Pilvipalveluiden yhtenä isona etuna on-premises -palveluihin verrattuna pidetään niiden skaalautuvuutta eli pilveä hyödynnettäessä ei makseta turhasta kapasiteetista ja voidaan samalla taata palvelun saatavuus myös silloinkin, kun palveluun kohdistuu paljon liikennettä. (Lintilä 26.01.2017)

Pilvipalveluita tarjoavat monet eri toimijat, kuitenkin tässä tutkimuksessa keskitytään Valtiokonttorin käyttämään Microsoftin Azure pilviratkaisuun.

Pilvipalveluista voidaan puhua, kun palvelua käytetään internetin yli. Esimerkiksi sen sijaan että käyttäjä tallentaa tiedostoja tai kuvia henkilökohtaiselle tietokoneelle tai ulkoiseen muistiin, suurin osa käyttäjistä hyödyntää jotain verkon yli tarjottavaa tallennusratkaisua esim. Google Drive. Pilvipalvelualustat, kuten Microsoft Azure, ovat yleensä halvempia, turvallisempia ja vakaampia kuin on-premises palvelimet. Pilven avulla päästään tilanteeseen, jossa palvelun alhaalla olo aika, mahdollinen varkaus tai vahinko ovat lähes ole-

mattomia. Voit skaalata laskenta ja tallennus resursseja, ylös tai alas, melkein reaaliajassa. Pilvipalveluille on myös tyypillistä, että maksat vain käytetyistä resursseista. (Microsoft Azure 2019b.)

Pilvipalvelun toteutustapoja ovat mm. Private Cloud, Public Cloud ja Hybrid Cloud. Nämä toteutustavat eroavat toisistaan huomattavasti. Yksityisessä pilvessä (Private Cloud) pilvi-infrastruktuuri on rakennettu vain yhden asiakkaan käyttöön ja se voi sijaita joko ulkoisissa palveluntarjoajan tiloissa tai yrityksen omissa tiloissa. Pilven hallintavastuu on joko asiakkaalla tai jollain kolmannella osapuolella. Yksityisessä pilvessä asiakkaat eivät jaa mitään resursseja muiden asiakkaiden kanssa. (NIST 2018, 12.)

Julkinen pilvi (Public Cloud) pilvi-infrastruktuuri sijaitsee pilvipalvelun tarjoajan tiloissa. Nämä ovat yleisesti tunnetuimpia pilvipalveluita eli esim. Azure tai AWS. Samaa palvelualustaa voi käyttää useampikin asiakas. Hybridi pilvi (Hybrid Cloud) on sekoitus näistä kahdesta tai useammasta tavasta toteuttaa pilvipalveluita. Kukin pilvitoteutustapa pysyy silti omana osanaan mutta niiden välille on rakennettu integraatioita, jotka mahdollistavat datan ja sovellusten siirron. Kuitenkin kaikissa näissä toteutustavoissa on samanlaiset pääpiirteet, jotka tekevät niistä pilvipalveluita.

1. Itsepalvelu (On-demand self-service), jonka avulla asiakas itse voi tilata lisää palveluita.

2. Kattava pääsy palveluun (Broad network access): asiakas voi päästä kiinni palveluun mistä vain ja millä vain.

3. Samojen resurssien käyttö (Resource Pooling): useat loppukäyttäjät voivat tietämättään käyttää samoja resursseja (tallennustila, muisti). Multitenant mallin ansiosta

4. Nopea skaalautuvuus (Rapid elasticity): kapasiteettia voidaan nopeasti lisätä tai poistaa, usein myös automaatiolla.

5. Resurssien mittaus (Measured service): pilvipalvelu automaattisesti mittaa käytettyjä resursseja.

(NIST 2018, 13-17.)

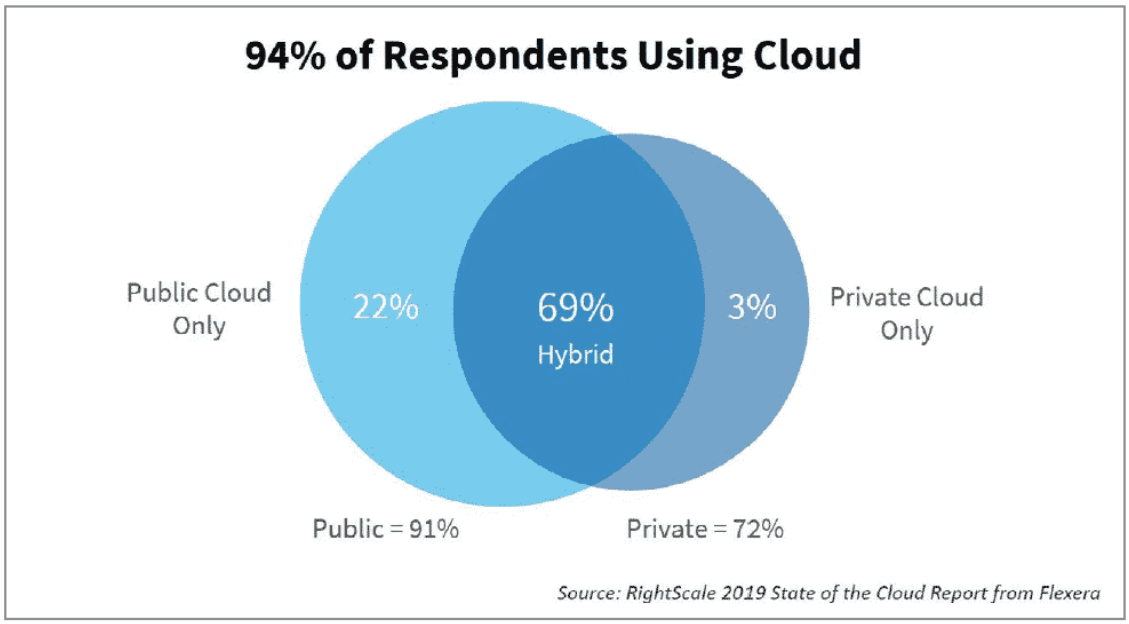
2.1.1 Hybridimalli

Hybridimallissa siis eletään molemmissa ulottuvuuksissa. Eli käytetään pilvipalveluita jossain muodossa on-premises -palveluiden apuna tai rinnalla.

Hybridipilvestä voidaan siis puhua silloin, kun palvelu käyttää kahta eri alustaa. Joko voidaan käyttää julkista ja yksityistä pilveä tai voidaan käyttää julkista- tai yksityistä pilveä ja konesali- tai on-premises -palveluita.

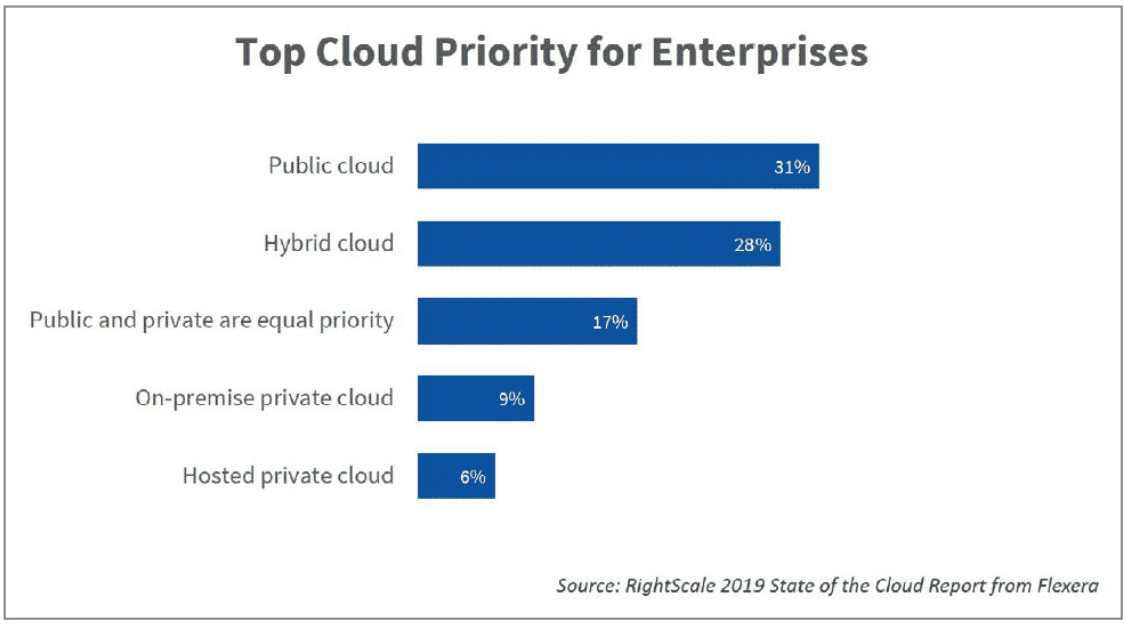
Hybridipilvi tai hybridimalli onkin nouseva trendi ja suosittu tapa toteuttaa pilvistrategiaa.

Flexera on maailmanlaajuinen IT-ratkaisu yritys. Flexeralla on yli 50 000 asiakasta maailmalla ja 30 vuoden historia. Vuonna 2018 Flexera yhdistyi Rightscale yrityksen kanssa, joka myy pilviratkaisuja. RightScale on tehnyt vuosittaisen katsauksen siihen, miten sen asiakkaat ovat hyödyntäneet pilveä ja mitkä ovat asiakkaiden tulevaisuuden näkymät. Vuonna 2019 RightScale ja Flexera tuottivat tämän ”State of the Cloud” -kyselyn yhdessä. (Flexera 2019b.)



Kuva 1. Julkisen-, Hybridi- ja yksityisenpilven prosenttiosuudet (Flexera 2019.)

Flexera toteutti kyselyn yli tuhannen hengen yrityksille, yritysten pilvistrategiasta ja siitä miten yritykset hyödyntävät nyt pilvipalveluita, Kuvassa 1. näkyy jakauma vastanneiden kesken yksityisen-, julkisen- ja hybridipilven välillä. Kyselystä käy myös ilmi, että hybridipilveä hyödyntävien yritysten määrä kasvoi vuodessa 7%. (Flexera 2019a.)



Kuva 2. Yritysten prioriteetit pilvipalveluiden osalta (Flexera 2019a.)

Kuten kuva 2. kertoo Flexeran kyselystä kävi ilmi että yritykset priorisoivat hybridimallia, vaikka ”julkinen pilvi” on 31%:lla kärkisijalla niin yhdistettynä ”hybridipilvi” ja ”julkinen ja yksityinen pilvi ovat yhtä tärkeitä” vievät voiton 45%:lla. (Flexera 2019a.)

Niin sanottu ”pragmaattinen” hybridimalli on todella suosittu tapa toteuttaa pilvistrategiaa. Varsinkin isoilla yrityksillä todennäköisesti on paljon vanhoja legacy-sovelluksia, jotka eivät suoraan käänny pilveen sopiviksi. Vaan nämä sovellukset pitäisi suunnitella ja kirjoittaa alusta asti pilvisopiviksi ”cloud-native” -sovelluksiksi ja tähän kuluisi niin paljon rahaa, että pilvestä saadut rahalliset hyödyt jäisivät todennäköisesti liian pieneksi, että tämä olisi liiketaloudellisesti järkevää. Kun pilven käyttöönoton vaihtoehdot olivat tehdä kaikki legacy-sovellukset uudelleen pilveen sopiviksi tai olla käyttämättä sitä ollenkaan, oli useille yrityksille päätös tehty jo heidän puolestaan.
Pragmaattinen hybridimalli kuitenkin mahdollisti esim. tuon vanhan legacy-sovelluksen pitämisen on-premises -palvelimella, jossa sovellus pyörii ja pilvelle avataan portteja on-premises -palvelimeen. (Cisco)

Tässä mallissa on omat haasteensa, kun tarvitaan selkeät hallintomallit molempiin ratkaisuihin. Toki jokin palvelu voi myös sisältää sellaista dataa, jota ei haluta tai edes voida lain nojalla siirtää pilvipalveluihin.

2.1.2 Full cloud

Pelkästään pilvipalveluihin perustuvassa ratkaisussa koko yrityksen infra ja palvelut ovat pilvessä.

Tällöin päästään tilanteeseen, jossa kaikki on nopeasti skaalattavissa, ylös tai alaspäin. Kuitenkin pelkän pilven hyödyntäminen tuo omat haasteensa ja riskinsä.

Vaikka pilvipalvelun tarjoaja olisi varmentanut ja toisintanut asiakkaan palvelut monelle eri palvelimelle, ei se tarkoita sitä, että käyttäjän päässä tapahtuvia häiriöitä olisi minimoitu. Jos esim. internet-yhteys katkeaa käyttäjän päästä, renderöidään näin yritys täysin pimentoon ja se ei pääse käsiksi omiin palveluihinsa tai dataansa. Jos taas esim. tiedostopalvelin olisi on-premises, voisi yritys edelleen käyttää dataansa ja dokumentteja, jotka ovat tuolla on-premises -palvelimella, eikä internet yhteyden päässä.

Täysin pilvipalveluun nojaava infraratkaisu on toki huomattavasti nopeampi ja halvempi pystyttää kuin perinteinen on-premises, vaikkakin pilviratkaisun käyttö saattaa olla pidemmällä aikavälillä kalliimpaa kuin on-premises -ratkaisu, riippuen paljon resurssien käytön profiilista. Tämän takia pilvi on myös hyvä vaihtoehto vaikka pienille ja uusille start-up-yrityksille, joilla ei ole vielä vakiintunutta käyttäjäkuntaa.

Pilven kapasiteetin skaalautuvuus on myös erinomainen ominaisuus uusien yritysten kannalta. Kun kapasiteettiä voidaan lisätä tai poistaa minuuttien sisällä, ei todennäköisesti olla tilanteessa, jossa palvelu avataan ja käyttäjämäärä ylittääkin odotukset ja palvelu kaatuu, vaan kun todetaan, että käyttäjämäärä alkaa olla kapasiteetin rajoilla voidaan lisätä kapasiteettia ja kun käyttäjämäärä taas laskee, voidaan kapasiteettia myös vähentää. Tällä tavoin voi yritys varmistaa sen, että se ei maksa turhasta palvelinkapasiteetista, ja että yrityksen asiakkaat pääsevät käsiksi palveluun ja loppukäyttäjä on tyytyväinen. (CloudAcademy 2019.)

2.2 On-premises -palvelut

On-premises voidaan mieltää pilvimallin ”vastakohdaksi” ja perinteiseksi tavaksi tehdä asioita, jossa asiakas itse huolehtii kaikesta järjestelmän ylläpidosta aina sen infraan asti, eli asiakas tarvitsee fyysisen palvelimen ja tarvittavat ohjelmistot järjestelmän pyörittämiseksi, ”on premises” eli paikan päällä. (Hewlett Packard Enterprise)

Valtiokonttorin nykyinen malli koostuu on-premises -ratkaisuista ja pilvipalveluista, ja tätä mallia voidaan kutsua hybridimalliksi.

2.3 IT-palvelujen hallintomalli

Hallintomalli kattaa yleensä koko organisaation. Tässä tutkimuksessa hallintomallilla tarkoitetaan IT-hallintomallia. IT-hallintomallilla varmistetaan, että IT-palvelut tuottavat oikeaa arvoa liiketoiminnalle tai auttavat liiketoimintaa. Hallintomallilla tarkoitetaan ohjeita, käytäntöjä ja dokumentteja, joita seuraamalla voidaan toimia sovitulla tavalla ja yhtenäistää prosesseja. (Ellmén 08.11.2019.)

Hallintomalleja löytyy on-premises- ja pilvipalveluihin, mutta kattavaa hybridimalliin soveltuvaa hallintomallia on vaikea löytää valmiina kirjallisuudesta.

Toki jokainen hallintomalli täytyy muokata juuri oman organisaation prosesseihin sopivaksi ja sellaisenaan esim. Microsoftin ”The Cloud Adoption Framework” -hallintomallin toteuttaminen olisi hyvin hankalaa ja vaivalloista.

Hybridihallintomallia lähdettiin siis Valtiokonttorille rakentamaan, vertailemalla on-premises- ja pilvihallintomalleja keskenään. Näiden avulla saatiin kattava kuva Valtiokonttorin prosesseista ja palveluista, joiden avulla voitiin kasata hybridimalliin soveltuva hallintomalli.

3 Hallintomallit ja ITIL

Opinnäytetyötä varten tutustuin Valtorin hallintomalliin heidän tarjoamastaan pilviratkaisusta ja Tiedon hallintomalliin heidän on-premises -palveluaan varten. Tutustuin myös ITIL:iin ja siihen millaisia käytäntöjä ITIL:iin on listattu ja sivuavatko Valtorin ja Tiedon hallintomallit näitä käytäntöjä.

Seuraavissa luvuissa on nostettu esille kustakin hallintomallista ja ITIL:stä kohdat, jotka mielestäni ovat tärkeimmät Valtiokonttorin näkökulmasta ja tuottavat heille eniten arvoa. Jokaisessa luvussa esitellään seuraavat kohdat tai niitä vastaavat kohdat:

1. Häiriö- ja herätteidenhallinta heräte (Event) on palvelun tilan muutos, joka vaikuttaa palvelun saatavuuteen tai toiminnallisuuteen. ITIL määrittää häiriö- ja herätteidenhallinnan seuraavanlaisesti, se on prosessi minkä tarkoitus on monitoroida kaikkia herätteitä läpi palvelun.

2. Verkkoresurssien hallinta kuvaa tapaa, jolla hallinnoidaan verkkoyhteyksiä palveluun ja verkonasetuksia palvelussa.

3. Palveluiden varmistaminen käsittelee sitä, miten palvelu varmuuskopioidaan tai miten voidaan vähentää palvelun alhaalla olo aikaa.

4. Resurssien käyttö ja hallinta antaa tarkemman kuvan siitä, miten palvelun vaatimia resursseja, kuten palvelin tai palomuurin asetuksia voidaan muokata.

5. Identiteetin- ja pääsynhallinta kuvaa prosessin, jolla saadaan tietylle henkilölle pääsy palveluun. Tähän myös kuuluu käyttäjätilien hallinta, eli esim. turhien käyttäjien poisto ja pääsyn epääminen sitä vaadittaessa.

6. Kapasiteetinhallinta käsittää sen, miten esim. palvelimia, niiden muistia tai tallennustilan määrää ja tilaa käsitellään.

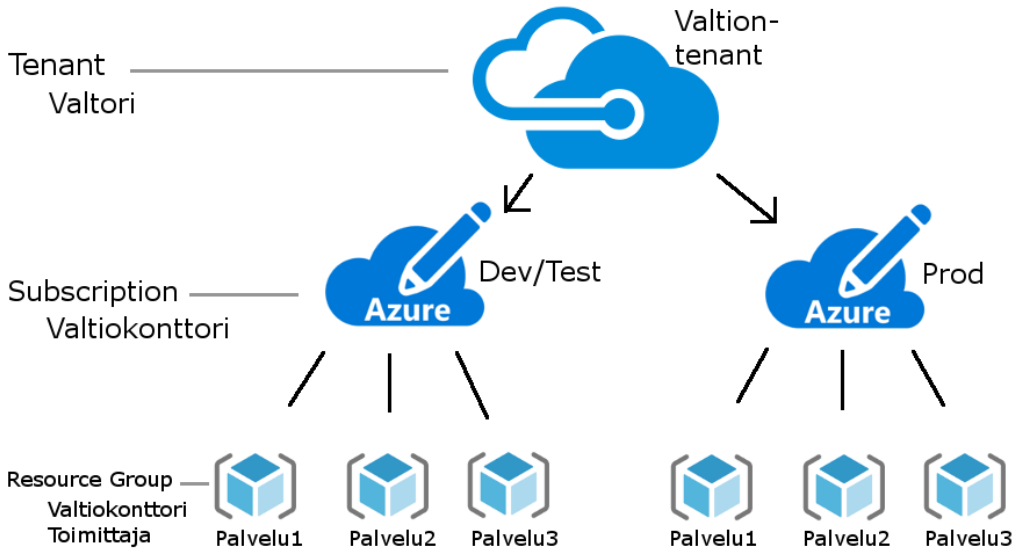
Näiden kohtien lisäksi nostin ITIL:stä esille myös palvelun taloudenhallinnan ja muutoksenohjauksen, muutoksenohjauksella kuvataan prosessi, jonka läpi jokainen muutos palveluun kulkee. Nämä edellä mainitut kohdat ovat erittäin oleellinen osa pilvipalveluita ja erittäin tärkeitä kohtia huomioida, kun pilvipalveluihin siirrytään. Nämä kohdat myös ovat mielestäni kohdat, joissa tapahtuu selkein muutos Valtiokonttorin kannalta ja muutokset näissä kohdissa vaikuttavat työntekijöiden joka päiväiseen tekemiseen.

3.1 Valtorin Pilvipalvelut

Valtori tarjoaa Microsoft Azure -pilvipalvelua Capgeminin kautta, Capgemini on maailmanlaajuinen konsultointi- ja ulkoistuspalveluita tarjoava yritys. Capgemini toimii siis Valtorin

Cloud Solution Provider:nä. (Valtori 2018a, 5) Toisin sanoen Valtori ostaa Azure alustan muualta ja jälleenmyy sitä valtion virastoille.

Valtori tarjoaa kahta eri palvelumallia, pilvipalveluita ja pilvialustaa. Pilvialusta on enemmän ”avaimet käteen” -mallinen toteutus, jossa Valtori hoitaa ainoastaan käyttöönottoon tarvittavat toimenpiteet ja sen jälkeen ylläpito siirtyy asiakkaan kontolle.
Pilvipalvelut-mallissa Valtori valvoo ja ohjaa enemmän asiakasta, ja asiakas itse ei ole pääkäyttäjä vaan Valtori hoitaa edelleen tilaukset ja tilin hallintaa. Pilvipalvelut-malli on myös sidottu käyttämään Valtorin määrittämää hakemistoa eli Valtion AD:ta käyttäjähallintaan. (Valtori 2018a, 7) Kuvassa 3. on kuvattu Valtiokonttorin ja Valtorin arkkitehtuurista rakennetta Azuressa ja kuva avaa Valtorin pilvipalvelu-mallia.



Kuva 3. Valtorin Pilvipalvelu-arkkitehtuuri (Valtori 2018a.)

3.1.1 Häiriö- ja herätteidenhallinta

Palvelun toimittajan ja asiakkaan välisessä palvelusopimuksessa tulee käydä ilmi toimittajan tapa osoittaa palvelulupausten toteutuminen. Tämä voidaan toteuttaa joko asiakkaan käytössä olevalla työkalulla tai seurantaraportin avulla. Jos toimittaja ei tarjoa ylläpitoa tai sen valvontaa tulisi toimittajan ehdottaa sopivia työkaluja. (Valtori 2018a, 13)

Julkisessa pilvessä olevan palvelun valvonnan tasosta päättää lähtökohtaisesti aina asiakas. Päätöksiä tehdessä pitää ottaa huomioon mm. sovelluksen tärkeysluokitus sekä varautumistasosta ja valvonnasta aiheutuvat kulut.

Valtorin tukemissa pilvipalveluissa on sisäänrakennettuja työkaluja, joilla palvelun terveydentilan tai suorituskyvyn valvontaa voidaan toteuttaa. (Valtori 2018a, 14)

3.1.2 Verkkoresurssien hallinta

Valtori pitää huolen kaikista verkkoresursseista ja itse asiakas tai asiakkaan toimittaja ei saa perustaa uusia tai muokata olemassa olevia verkkoresursseja itse.
Asiakas voi lisätä palvelimia ja palveluita jo olemassa oleviin verkkoihin. (Valtori 2018c, 8)

3.1.3 Palveluiden varmistaminen

Palveluiden varmistaminen tulee periaatteessa Azuren puolesta, Valtorilla tähän suositellut oletuspolitiikat tuotantopalveluihin ovat kuvan 4. mukaiset. (Valtori 2018a, 14)

Tyyppi	Aikataulu	Säiltysaika
Päivittäinen (täysi)	7 kertaa viikossa	32 päivää
Kuukausittainen (täysi)	1 kerran kuukaudessa	12 kuukautta
Vuosittainen (täysi)	1 kerran vuodessa	5 vuotta

Kuva 4. Valtorin suositukset tuotantopalvelinten varmistukseen (Valtori 2018a, 15)

Valtorin suosittelema aikaikkuna varmistuksille on klo 24:00-02:00 (Suomen aikaa). Tämä aikaikkuna kannattaa vakioida ja tiedottaa kaikille asianomaisille, jotta vältytään päällekkäisiltä päivityksiltä tai eräajoilta. (Valtori 2018a, 14)

3.1.4 Virtuaalikoneiden käyttöön liittyvät ohjeet ja suositukset

Valtori tarjoaa virtuaalikoneisiin liittyviä ylläpito- ja hallinnointipalveluita kolmella eri mallilla:

1. Valtorin ylläpitämät virtuaalikoneet

   Valtori tarjoaa maksullisia ylläpitopalveluita julkisessa pilvessä ajettaville virtuaalikonetyökuormille, mikäli asiakas on luonut yhteyden VY-verkkoon.

2. Pilvialustan toimittajan ylläpitämät virtuaalikoneet

   Valtori tarjoaa mahdollisuutta ostaa ylläpitopalveluita myös suoraan Valtorin sopimuskumppaneilta.

3. Asiakkaan tai toimittajan ylläpitämät virtuaalikoneet

   Virtuaalikoneita voidaan myös ylläpitää asiakkaan tai asiakkaan valitse-

man toimittajan puolesta. Tällöin asiakas joutuu itse vastaamaan palvelimen tietoturvapäivitysten ja muiden ylläpitoon liittyvien asioiden ajantasaisuudesta.

Mikäli Asiakas on muodostanut yhteyden julkisen pilven verkosta VY-verkkoon, tulee asiakkaan noudattaa VY-verkossa vaadittavia valvonta-, ylläpito- ja tietoturvamalleja. (Valtori 2018a, 15)

3.1.5 Identiteetinhallinta

Valtori käyttää oletushakemistona Valtion Azure AD -hakemistoa, jonne käyttäjät ja ryhmät synkronoidaan Valtion AD-käyttäjähakemistosta. (Valtori 2018b, 8)

Valtori pitää yleisen järjestelmävalvojan roolin vain itsellään ja heidän nimeämillään henkilöillä. Azure active directory global admin -rooli on siis AAD (Azure active directory) -hallinnointiin tarkoitettu rooli. Tämä rooli tuo käyttäjät AAD-tenantiin. Valtorilla on myös joukko muita admin-tason rooleja, joita se ei luovuta asiakkailleen. Näistä löytyy tietoa Valtorin Julkisen pilven hallintomallista. (Valtori 2018b, 10)

Asiakkaalla tai toimittajalla on käytössään asiakkaan pääkäyttäjäryhmä. Tämä ryhmä toimii asiakkaan resurssiryhmissä (Resource group) ”owner”-tason oikeuksilla ja lisäksi omaa ”virtual machine contributor” tyypin oikeudet kaikkiin verkkoresursseihin, joihin asiakas on oikeutettu luomaan uusia virtuaalikoneita. Tämä ryhmä hallinnoi kaikkien resurssiryhmien kaikkia palveluobjekteja ja voi antaa uusille käyttäjille oikeuden hallinnoida niitä. (Valtori 2018b, 12)

Asiakas voi sallia pääkäyttäjäryhmän ulkopuolisille työntekijöilleen ja toimittajilleen pääsyn hallinnoimaan resurssiryhmiä. Tällaisessa tilanteessa seurataan Valtorin normaalia käytäntöä ulkoisten tunnusten tilaamiseen. Asiakas itse määrittää, mitä resurssiryhmiä ja palveluobjekteja toimittaja pystyy muokkaamaan. Jos asiakas tarvitsee tukea toimittajan käyttöoikeuksien asettamisessa, Valtori voi auttaa asiakasta oikean käyttöoikeustason määrittämisessä ja asettamisessa. (Valtori 2018b, 13)

3.1.6 Kapasiteetinhallinta

Valtori esittää kaksi eri vaihtoehtoa kapasiteetin kasvattamiseen: vertikaalinen- ja horisontaalinen skaalaaminen.

Vertikaalinen skaalaaminen tarkoittaa palveluinstanssin koon muuttamista eli yleensä siis muistin, prosessointitehon tai muiden ominaisuuksien lisäämistä tai vähentämistä.

Vertikaalinen skaalaaminen toimii paremmin ylöspäin kuin alaspäin, eli on helpompaa lisätä muistia kuin poistaa sitä. Joskus palveluobjektin palvelutason laskeminen tai sen resurssien vähentäminen voi vaatia koko palvelun uudelleen rakentamista. Siksi Valtori suositteleekin ”aloita pienestä ja kasvata tarvittaessa” -logiikkaa. (Valtori 2018c, 14)

Horisontaalinen skaalaaminen taas muuttaa aktiivisten palveluinstanssien lukumäärää. Horisontaalinen skaalaaminen on usein tehokkain tapa optimoida kustannuksia. Usein horisontaalista skaalaamista voidaan tehdä automaattisesti työkuorman perusteella.
Myös palveluiden sammuttaminen määräajaksi (esim. kehityspalvelimen sammuttaminen virka-ajan ulkopuolella) voi säästää huomattavasti kustannuksissa. (Valtori 2018c, 14)

Valtori suosittelee, että horisontaalinen skaalautuminen ja sammuttaminen määräajaksi tulisi ottaa huomioon jokaisen palvelun kohdalla. Toimittaja on velvollinen käymään läpi asiakkaan kanssa skaalautumisen mahdollisuudet kunkin palvelun kohdalta ja tästä aiheutuvat mahdolliset kustannukset. (Valtori 2018c, 15)

3.2 Tiedon On-premises -palvelut

Tieto Oyj toimittaa Valtiokonttorille konesalipalveluita.

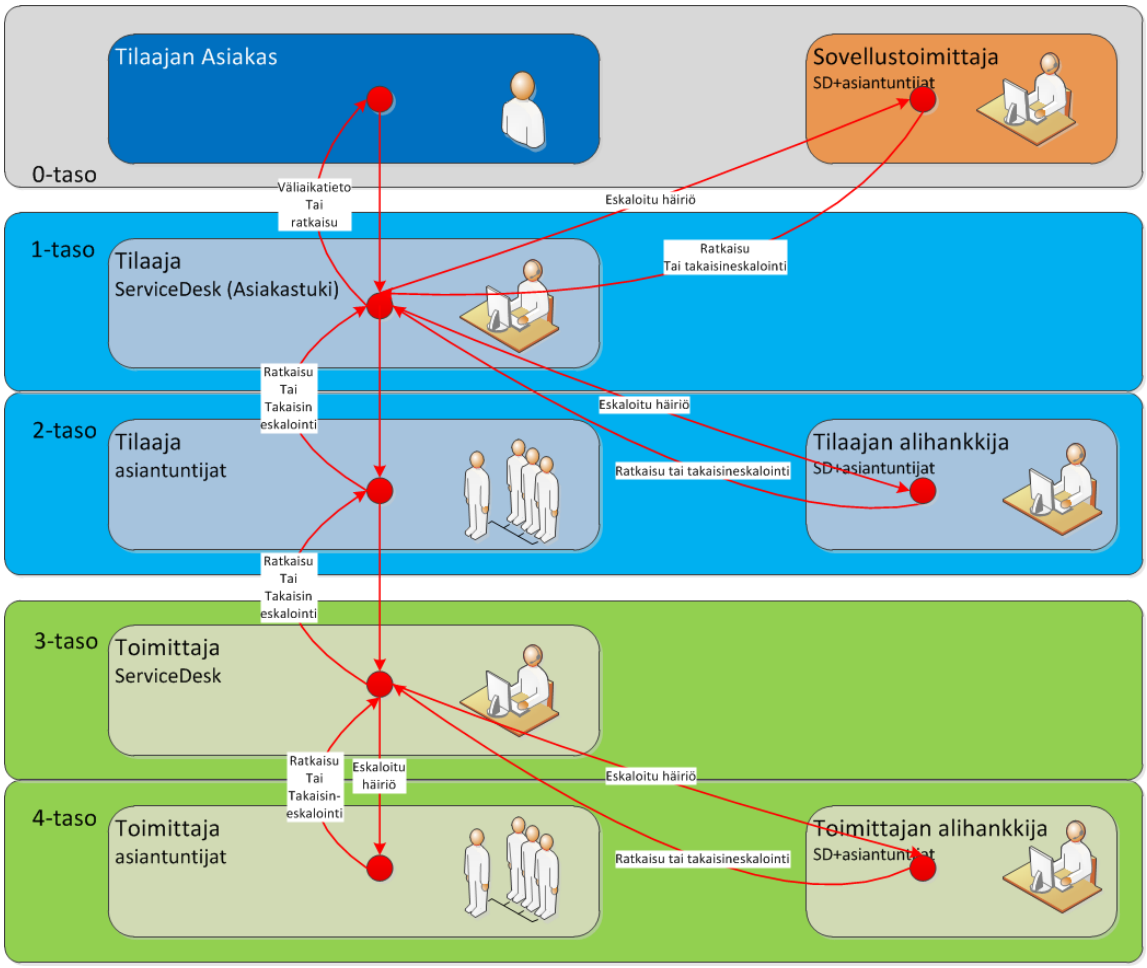
3.2.1 Häiriö- ja herätteidenhallinta

Herätteet (Events) hoidetaan toimittajan valvontavälineitä hyödyntäen. Infran perusvalvonta kuuluu palvelun hintaan, mutta tarjolla on myös lisävalvontoja sekä infraan että sovelluksiin. Perusvalvonta sisältää seuraavat komponentit:

- Palvelinalusta
- Palvelimen käyttöjärjestelmä
- Palvelimen middleware-tuote: kuten Jboss, DB2 jne
- Verkkokomponentit

Tieto Watch Dashboard hoitaa siis palvelimen valvonnan ja seuraa, että palvelin on pystyssä ja vastaa kyselyihin. Valvontavälineet tuottavat herätteet valvomolle. Valvomo toimii ohjeiden mukaisesti. Ellei kohde toivu, tekee valvomo herätteestä asianmukaisen häiriöilmoituksen. (Tieto 2015, 5)

Alla oleva kuva avaa häiriöhallintaa ja sitä, miten häiriö eskaloidaan eteenpäin vastuuketjussa.



Kuva 5. Häiriöilmoituksenketju (Tieto 2015, 9)

Kuten kuvassa 5. nähdään häiriöilmoitukset menevät tilaajan asiakastuen kautta tilaajan omaan toiminnanohjausjärjestelmään (1-taso). Tilaajan asiakastuki eskaloi tiketit tilaajan asiantuntijoiden työjonoihin (2-taso).
Tilaajan asiantuntijat eskaloivat tarvittaessa häiriötiketin toimittajan servicedeskiin, eli Tiedolle (3-taso). (Tieto 2015, 9)

3.2.2 Verkkoresurssien hallinta

Verkkojen hallinta on käytännössä Tiedon omien infrastruktuuriohjeiden noudattamista. Asiakkaan hallinnassa on käytännössä valita verkkorakenteen arkkitehtuuri, jos sekään, ja järjestelmän suojelemiseksi pystytetyn palomuurin sääntöjen palvelukohtaisten muutosten pyytäminen. (Tieto 2015, 23)

Toimittaja siis hallitsee ja tekee tarvittavat muutokset verkkoihin. Asiakas tekee tarvittavasta verkkomuutoksesta tiketin.

3.2.3 Tietoturva ja palveluidenvarmistaminen

Toimittaja (Tieto) seuraa tietoturvan tilannetta ja raportoi löytämistään poikkeamista. Tilaaja seuraa omalla tahollaan poikkeamia ja saa myös herätteitä asiakkailtaan. (Tieto 2015, 28)

Turvallisuuden ohjausryhmä koostuu edustajista tilaajalta sekä toimittajalta. Ohjausryhmä kokoontuu säännöllisesti ja käy läpi asialistan mukaan tietoturva-asioita. Ohjausryhmä on päättänyt vuosittain katselmoitavat tietoturvakohteet. Katselmointi tapahtuu joko dokumenttien tarkastamisena, haastatteluna tai auditointina. (Tieto 2015, 29)

3.2.4 Resurssien käyttö ja hallinta

Kaikki palvelinresurssit ovat Tiedon hallinnassa. Niihin voidaan tehdä muutoksia palvelupyyntö/muutospyyntö-lomakkeella. (Tieto 2015, 17)

Käytännössä resurssien palvelupyynnössä määritellään "konekokonaisuus" eli virtuaalikoneen prosessori- ja muistimäärä sekä tarvittava levytila. Toimitusaika muutokselle tyypillisimmillään on muutamista päivistä viikkoon. (Tieto 2015, 19)

3.2.5 Identiteetin- ja pääsynhallinta

Tuotanto-oikeuksien myöntämismenettelyhierarkia tilaajan ja toimittajan välillä:

1. Tietoturvaselvitettyjen tilaajan tai toimittajan henkilöiden tuotanto-oikeudet. Kun menettely on kerran hyväksytty Turvallisuuden ohjausryhmässä, oikeuksia voivat myöntää niin tilaaja kuin toimittaja.
2. Jos tarvitaan muita menettelyitä, ne käsitellään ensin turvallisuuden ohjausryhmässä ja sen esityksestä tarvittaessa taktisessa ohjausryhmässä.

Pääsy tuotantoympäristöihin ja työvälineisiin sallitaan vain tietoturvaselvitetyille nimetyille henkilöille. (Tieto 2015, 30)

Pääsy tuotantoympäristöihin voidaan evätä, poistamalla käyttäjän oikeudet palvelimelta. Valtiokonttorin palvelusta vastaavalla henkilöllä on admin-oikeudet palvelimelle, joten hän voi suorittaa poiston, tai Tiedolta nimetty henkilö, jolla on riittävät oikeudet käyttäjän poistoon. (Tieto 2015, 31)

3.2.6 Kapasiteetinhallinta

Kapasiteettia seurataan kapasiteettikokouksessa, toimittaja nimittää omasta puolestaan kapasiteetinhallinnasta vastaavan. Tilaaja toimittaa kolmen kuukauden välein ennusteen kapasiteettitarpeista toimittajalle. Toimittaja puolestaan kerää kapasiteetin käytöstä trendiraportteja, jotka toimitetaan tilaajalle joka kuukausi. Toimittaja myös muodostaa arvion kapasiteettitarpeista ja käynnistää tarvittaessa hankintaprosessin. (Tieto 2015, 36)

3.3 ITIL 4

ITIL 4 on uusin versio ITIL:stä joka on suunnattu DevOps ja Agile pohjaisiin prosesseihin. Tässä tutkimuksessa on käytetty ITIL Foundation, ITIL 4 Edition versiota.

3.3.1 Häiriö- ja herätteidenhallinta

Herätteeksi voidaan lukea jokainen tunnistettava tai erottuva tapahtuma, jolla on selkeä vaikutus joko palvelun infrastruktuuriin tai siihen, miten palvelu toimii. (Axelos 2019, 121)

Kun tiketti on luotu joko automaatiolla tai käyttäjän puolesta, se osoitetaan oikealle tasolle, joka lähtee sitä ratkomaan. Helpoimmista ongelmista loppukäyttäjä voi itse selvitä, seuraamalla ”self-help” -ohjeita. Haastavimpiin ja äärimäisissä tapauksissa voidaan tiketin ratkaisemiseksi joutua turvautumaan ”Disaster recovery” (katastrofista palautumis) suunnitelmaan. (Axelos 2019, 122)

Herätteistä ja häiriöistä on hyvä pitää lokia ja kirjaa. Kun laitetaan ylös dataa häiriöistä, voidaan uusiutuvien häiriöiden ja herätteiden ratkomista nopeuttaa huomattavasti. Myös mahdolliset ”work aroundit” on hyvä kirjata ylös. (Axelos 2019, 123)

3.3.2 Palveluiden ja resurssien hallinta

ITIL määrittää resurssien ja palvelualustan hallinnan seuraavanlaisesti: tarkoitus on valvoa yrityksen käyttämää infrastruktuuria ja palvelualustaa. Tarkoitus on myös kartoittaa tarjolla olevia ratkaisuja niin talon sisältä kuin ulkopuoleltakin.
Yksi tarkoitus on myös säädellä teknologioita, joita tarvitaan tukemaan prosesseja, jotka tuottavat arvoa yritykselle ja sen sidosryhmille. (Axelos 2019, 117)

3.3.3 Muutoksenohjaus

Muutoksenohjauksen tarkoitus on taata mahdollisimman korkea onnistumisprosentti palveluiden muutoksissa varmistamalla, että muutokseen liittyvät riskit on arvioitu, antamalla muutokselle vihreää valoa ja hallita muutoksen aikataulua. (Axelos 2019, 118)

Muutoksenohjauksen on löydettävä tasapaino hyödyllisten muutosten, jotka tarjoavat lisäarvoa ja tarpeen suojella käyttäjiä muutosten kielteisiltä vaikutuksilta välillä. Muutokset pitää arvioida ja hyväksyä ennen kuin ne julkaistaan. Kuitenkaan arviointi ei saa turhaan hidastaa julkaisua. (Axelos 2019, 119)

On olemassa kolmea eri tyyppistä muutosta, joista jokaista käsitellään eri tavalla.
Vakiomuutos, ovat vähäriskisiä ennalta jo hyväksyttyjä muutoksia. Usein nämä syntyvät palvelupyynnöistä.
Normaalit muutokset ovat muutoksia, jotka pitää aikatauluttaa, arvioida ja hyväksyä prosessin mukaisesti. Muutoksen tyyppi määrää sen tarvitseman arvioinnin ja hyväksynnän laajuuden. Normaaleja muutoksia voi olla useaa eri tyyppiä: matalariskisiä, jolloin arviointi ja hyväksyntä voi olla lähes kokonaan automatisoitu tai korkeariskisiä, jolloin arviointi voi olla hyvinkin kattavaa ja hyväksynnän antaa esim. johtoryhmä.
Hätämuutokset ovat muutoksia, jotka pitää implementoida niin nopeasti kuin mahdollista, jotta voidaan varmistua joko palvelun toimivuudesta tai turvallisuudesta. Hätämuutokset eivät yleensä ole osana muutosaikataulua. Niihin kuitenkin pitäisi soveltaa samoja arvioinnin ja hyväksymisen tapoja kuin normaalimuutoksiin, kuitenkin niin että edetään nopeasti kohti julkaisua. (Axelos 2019, 119-120)

3.3.4 Tietoturva ja riskienhallinta

Tärkeä osa tietoturvan- ja riskienhallintaa on turvata sitä tietoa, jota yritys tarvitsee toimiakseen. Tämä pitää sisällään riskien tunnistamisen ja hallitsemisen, niin tiedon luottamuksellisuuden, eheyden kuin saatavuuden osalta, kuin myös käyttäjien autentikaation ja kiistämättömyyden saralta. (Axelos 2019, 83)

Tarvittava tietoturva koostuu käytettävistä politiikoista, prosesseista, riskien hallinnasta ja valvonnasta. Näiden on oltava oikeassa tasapainossa ennaltaehkäisyn, havaitsemisen ja toipumisen välillä. Tärkeää on myös löytää hyvä tasapaino käytettävyyden ja tietoturvallisuuden välillä. Lisäksi on tärkeää myös jättää tilaa innovoinnille. (Axelos 2019, 83)

Tietoturva on riippuvainen käyttäjistä. Käyttäjät, jotka ovat saaneet tarpeeksi koulutusta ja ovat tarkkaavaisia tietoturvan suhteen ovat iso apu yrityksen tietoturvassa, kun taas huonosti koulutetut ja huonosti motivoituneet käyttäjät muodostavat ison tietoturvariskin. (Axelos 2019, 84)

Riskienhallinta on erittäin tärkeää yrityksen jatkuvan kestävyyden ja asiakkaille arvon luonnin kannalta. Ilman hallittujen riskien ottamista yritys ei voi saavuttaa tarjolla olevia hyötyjä ja maksimaalista kasvua. Riskit yleensä mielletäänkin vain ja ainoastaan uhkiin, mutta riskit myös voivat liittyä mahdollisuuksiin. Siksipä riskien välttely voi olla riski itsessään, kun ohitetaan samalla jokainen mahdollisuus. (Axelos 2019, 97)

3.3.5 Pääsynhallinta

ITIL määrittää pääsynhallinnan prosessina, joka joko antaa pääsyn tai rajoittaa sitä, tietyltä henkilöltä tai ryhmältä. (Greycampus 2019)

ITIL 4v ei käsittele pääsynhallintaa enää omana käytäntönään vaan se on osana Tietoturvan hallintaa, ”Information security management”.

Pääsynhallinta prosessi lähtee usein käyntiin joko käyttäjän luomana tikettinä, kun hän tarvitsee pääsyä tai sen rajoittamista tai vaihtoehtoisesti osana esim. ”off-boarding” prosessia. Usein pääsynhallintaa kannattaa toteuttaa ”vähimmät oikeudet” periaatteella, jolla siis rajoitetaan käyttäjän pääsy vain tiedostoihin ja dataan, joita hän oikeasti tarvitsee. Tällä lähestymistavalla voidaan taata parempi tietoturva. Pääsynhallinnan luomia ryhmiä kannattaa aika ajoin auditoida ja tarkastella, jotta voidaan varmistua ryhmien eheydestä ja siitä että toteutetaan ”vähimmät oikeudet” periaatetta. (Invensislearning 2018)

3.3.6 Kapasiteetin ja suorituskyvyn hallinta

Kapasiteetin ja suorituskyvyn hallinnan tarkoitus on taata, että palvelu suoriutuu ja toimii sovitulla ja odotetulla tasolla ja tavalla. Yleensä tarkoitus on siis optimoida palvelun suorituskykyä ja palveluun liittyviä resursseja kuten infrastruktuuria, sovelluksia ja kolmannen osapuolen palveluita. (Axelos 2019, 117)

Kapasiteetin ja suorituskyvyn hallinta koostuu kahdesta osasta, analyysista ja suunnittelusta. Analyysi pitää sisällään nykyisen suorituskyvyn mittausta ja kapasiteetin ja suorituskyvyn mallintamista. Suunnittelu koostuu analyysista, kysynnän ennustuksesta ja resurssien suunnittelusta ja suorituskyvyn parannussuunnitelmasta. (Axelos 2019, 117)

Palvelun suorituskyky onkin iso osa asiakas- ja käyttäjätyytyväisyyttä ja luo heille myös lisäarvoa palvelua käytettäessä. (Axelos 2019, 117)

3.3.7 Palvelun taloudenhallinta

Palvelun taloudenhallinta keskittyy tukemaan organisaation strategioita ja suunnitelmia palvelun hallinnan kannalta, varmistamalla, että organisaation varoja ja sijoituksia käytetään tehokkaasti. (Axelos 2019, 100)

Palvelun taloudenhallinta tukee päätöksentekoa siinä, mihin suunnataan organisaation varoja. Se myös tarjoaa läpinäkyvyyttä budjetointiin, kustannuslaskentaan ja palveluihin liittyviin kirjanpidon toimintoihin. (Axelos 2019, 100)

Tapa, jolla IT-budjetointia tehdään, tulee muuttumaan huomattavasti pilviteknologioiden myötä. Vanhassa on-premises -palveluihin perustuvassa tavassa IT-budjetti oli hyvinkin ”staattinen” ja ennustettavissa. IT-budjetti yleensä laskutettiin pääomamenoista (Capital expenditure). Nyt kuitenkin pilvipalveluiden yleistyessä ja ”as a Service” -mallisten palveluiden lisääntyessä vaihtuukin tuo kertaluontoinen maksu ”subscription based” -tyyliseksi, jolloin järkevämpää on budjetoida IT suoraan juokseviin kuluihin (Operational expenditure). Tämä tulee eteen, jos pilvipalveluita skaalataan esim. automaattisesti, jolloin täytyy voida ennustaa käyttöpiikit ja huomioida esim. kiireisimmät kuukaudet budjetoinnissa. (Axelos 2019, 102)

4 Tulokset

Valtiokonttorin hybridipilvi-ratkaisu pohjaa DevOps-tyyliseen ajatteluun, joten julkaisun ja testauksen helppous ja nopeus ovat avainasemassa. Siksi suurimmat eroavaisuudet on-premises- ja pilvihallintomalliin löytyvätkin muutoksenhallinnasta ja resurssienhallinnasta, kuitenkin tunnistettiin selkeitä eroavaisuuksia myös muista alla esitellyistä kohdista.

Suurimmilta osilta voidaan käyttää jo Valtorin luomia käytäntöjä esim. käyttäjien luontiin ja pääsynhallintaan.

4.1 Hybridihallintomalli

Valtiokonttori päätyi toteuttamaan hybridimallia, koska Valtiokonttori koki tarpeen muuttaa vanhaa kankeahkoa julkaisu- ja kehitystapaansa. Pilvipalvelut tarjosivat hyvän tavan toteuttaa ketterää ja nopeaa tapaa mukautua nouseviin tarpeisiin. Pilvipalvelun helppous testaamisen ja julkaisun puolesta nopeuttivat julkaisuprosessia huomattavasti. Vaikka operatiiviset kustannukset ja niissä säästäminen eivät olleet etusijalla, oli kulujen laskeminen silti hyvä kannuste muutokselle. (Ellmén 08.11.2019.)

Pilvipalveluista valikoitui Microsoftin Azure, koska käytännössä Azure ja AWS ovat tällä hetkellä ainoat järkevät vaihtoehdot pilvipalveluista niiden kypsyyden takia. Hetken aikaa Valtiokonttorilla toteutettiin multicloudia Azuren ja AWS:n kanssa, mutta todettiin, että henkilöstömäärä ei yksinkertaisesti riitä multicloud-strategiaan ja myös AWS koettiin hankalammaksi, kun suurin osa työntekijöistä oli tottunut Windows- ja Microsoft-ympäristöihin. (Ellmén 08.11.2019.)

Kaikkea dataa ja palveluita ei kuitenkaan voida tai kannata siirtää pilvipalveluihin, joten osa infrastruktuurista koostuu edelleen Tiedon konesalipalveluista. Valtiokonttori tunnistaa seuraavat kohdat, kun tehdään päätös toteuttaa palvelu on-premises -mallilla.
Palvelu on ns. legacy-palvelu, joka ei välttämättä toimi mutkattomasti pilvessä ilman, että sen toimintaa pitäisi uudelleen suunnitella ja rakentaa. Tästä aiheutuvat kustannukset ovat usein niin suuret, että palvelun migraatio pilveen toisi niin minimaalista hyötyä, että sitä ei tehdä. Toinen tärkeä pohdittava asia on palvelun tai järjestelmän kriittisyys ja sen huoltovarmuus. Jos palvelu on ainoastaan saatavilla internetin yli, miten sen toimivuus voidaan varmistaa, jos pääsy internettiin on estynyt syystä tai toisesta. (Ellmén 08.11.2019.)

4.1.1 Herätteidenhallinta

Herätteiden hallintaan hybridimallissa kannattaa käyttää pilvessä tarjolla olevia ratkaisuja. Azure tarjoaa esim. Azure Monitor palvelun, joka kerää palvelun metriikkaa, suoriutumisdataa ja muita lokeja. Metriikan avulla voidaan halutessaan asettaa hälytyssäännöt, joilla voidaan esim. nostaa ongelmat tai herätteet valvovan tahon tietoisuuteen. (Microsoft Azure 2019c.)

Jokaisen palvelun ja sovelluksen kohdalla on erikseen sovittava, kuka on valvovataho. Valtiokonttorilla ei ole resursseja tarjota 24/7-valvontaa, joten jos palvelu tarvitsee ympärivuorokautisen valvonnan, täytyy toimittajan tarjota tämä palvelu.

On-premises -puolella kannattaa seurata palveluntarjoajan ohjeita herätteidenhallinnasta. Yleensä palvelun tarjoajat tarjoavat näitä palveluja samalla. Esimerkiksi Tiedolla Control-Desk -valvomo, tarkkailee palvelun tilaa toimittajan omilla valvontavälineillä. Infran perusvalvonta kuuluu Tiedolla palveluun.

4.1.2 Tapahtumienhallinta

Tapahtuma (Incident) on spontaani häiriötilanne, joka vaikuttaa joko palvelunlaatuun tai palvelun saatavuuteen.
Tapahtumat voivat nousta joko herätteiden hallinnan kautta tai käyttäjien, asiakkaiden tai henkilökunnan, tekeminä tiketteinä.

Hybridimallissa tärkeää on tunnistaa, mikä osa palvelusta aiheuttaa tapahtuman. Ilman hyvää herätteiden hallintaa ja tarkkoja lokeja tämä voi olla haastavaa. Kun jokin heräte havaitaan, siitä nostettu tiketti voidaan integraation avulla välittää suoraan toimittajalle esim. JIRA:n välityksellä, tai toimittajan johonkin omaan tikettijärjestelmään.

Tärkeää tapahtumienhallinnan kannalta on saada riittäviä lokitietoja ja dataa palveluista, sillä jos palvelu tarjoaa tapahtumasta riittämätöntä dataa voi tapahtuman alkulähdettä olla hankala selvittää.

Tapahtumista on myös hyvä kerätä tietoa tulevia häiriötä varten, jotta nämä saadaan korjattua mahdollisimman nopeasti.

4.1.3 Muutoksenhallinta

Valtiokonttorin syyt siirtyä pilveen tukevat muutoksenhallinnan muutosta klassisesta CAB-tyylisestä muutoksenhallinnasta uuteen agilea ja devops -ajattelua tukevaan malliin, jota voidaan kutsua muutoksenohjaukseksi

Perinteisessä muutoksenhallintaprosessissa valitettavan usein muutosprosessi pysähtyi ja jäi odottamaan CAB:in hyväksyntää, kunnes QA-testaus oli tehty. Uudessa muutoksenohjaukseen perustuvassa tavassa painotetaan, että QA-testaus ja koodin laatu ja toimivuus ovat osa prosessia eli varmistetaan muutoksen toimivuus ja laatu useaan otteeseen.

Muutoksenhallinta pilvipalveluissa voi olla siis lähes automatisoitua, kun voidaan hyödyntää DevOps CI/CD-pipelinejä. CI/CD eli Continuous integration, continuous delivery. CI:llä tarkoitetaan työtapaa, jossa ohjelmoijat yhdistävät eli integroivat koodinsa muiden ohjelmoijien kanssa. Usein tähän työtapaan kuuluu myös uuden koodin yksikkötestaaminen. CD:llä taas tarkoitetaan työtapaa, jossa julkaisusykli on todella nopea. Kuvassa 6. on avattu CI/CD-pipelinen toimintaa ja sen osat.

Kuva 6. CI/CD-pipeline (Redhat, What is CI/CD?)

Tätä CI/CD-mallia hyödyntämällä toimittaja saa muutospyynnön ja alkaa tehdä muutosta sovellukseen, jonka jälkeen toimittaja tekee vaaditut testaukset muutokselle ja kun testit ovat kunnossa voidaan muutos julkaista automaattisesti pipelinen avulla.

IT-johtoryhmän päätöksellä voidaan antaa ylläpito-oikeudet myös toimittajille Azuren Production ja Development Resource Group:eihin, jolloin voidaan muutoksen hallintaa siirtää enemmän toimittajan vastuulle. Muutoin mahdolliset muutokset palveluiden infrastruktuuriin ja itse sovelluksiin on toteutettava Valtiokonttorin tai Valtorin puolesta.

4.1.4 Tietoturva ja palveluidenvarmistaminen

Tietoturvaa pilvessä voidaan hoitaa ja vahvistaa monella eri tapaa Azuren tarjoamia työkaluja hyödyntäen.

Yleisellä tasolla Azure tarjoaa mahdollisuuden tarkkailla jokaisen subscriptionin tietoturvan tilaa Security Dashboardilla, joka tarjoaa reaaliaikaista dataa ja katsauksen mahdollisiin tietoturvauhkiin.

Pilven käyttöönotossa pitää pohtia sovelluksen kriittisyyttä. Tämä asettaa sovellukselle tiettyjä vaatimuksia niin saatavuuden kuin tietoturvan osalta.

Tietoturvassa tulee kiinnittää huomiota myös tunnuksiin, joilla päästään kirjautumaan pilvialustan hallinnointiportaaliin. Azure-portaali on saavutettavissa kaikkialta, joten kuka tahansa, joka saa tunnuksen haltuunsa, pääsee kirjautumaan portaaliin sisälle, jos kirjautumista ei ole suojattu vahvalla tunnistuksella.

Hybridipilvessä hajautettu datamalli antaa lisättyä turvaa, kun pidetään esim. sensitiivinen data pois pilvestä, voidaan välttää julkiseen-pilveen liittyviä tietoturva uhkia ja samalla kuitenkin hyötyä pilvestä. Eriytetyt ympäristöt, jotka luovat hybridipilven, kommunikoivat kontainereiden tai salattujen API:en kautta. Tämä malli mahdollistaa kriittisen ja sensitiivisen datan käsittelyn privaatissa -pilvessä tai on-premisessä ja ei-niin-tärkeän datan käsittelyn julkisessa pilvessä, jolloin minimoidaan julkisen pilven riskejä datavuodoista.
Tällä hajautetulla datamallilla voidaan siis minimoida niitä riskejä, jotka nousevat, kun sensitiivistä dataa viedään ulkopuolisille palvelimille.

Hybridimallissa on myös hyvä toteuttaa tietoturvakatselmuksia aika-ajoin. Katselmuksen kohteet on hyvä määrittää tietoturvallisuuden ohjausryhmässä.

Azure tarjoaa työkalut palveluiden varmentamiseen. Arvioida tarpeellinen varmuuskopioinnin tiheys ja asettaa tarpeelliselle aikajaksolle. Azure tarjoaa erilaisia palveluita riippuen sovelluksen tyypistä ja siitä mitä halutaan varmentaa.

On-premises -palveluntoimittaja seuraa tilannetta omalta taholtaan ja raportoi löytämistään poikkeamista palvelusopimuksen mukaisesti. Myös palvelun varmentaminen pitää rajata palvelusopimuksessa.

4.1.5 Resurssienhallinta

Valtiokonttori voi perustaa lisää resurssiryhmiä, *Resource Group,* tarpeen tullessa. Toistaiseksi resurssiryhmiä on perustettu pääsääntöisesti jokaista palvelua kohden development- ja production-, ja mahdollisesti vielä test/QA-subscription:ien alle.

Jokaisella palvelulla on siis vähintään kaksi subscription:ia.
Development subscription on tarkoitettu kehittäjille. Tässä resurssiryhmässä on todennäköisesti niin Valtiokonttorin kuin myös toimittajan puolesta admineja, jotka voivat tehdä muutoksia resurssiryhmään. Täällä tapahtuu siis palvelun kehitys.

Production subscription:in alla on julkaistu versio palvelusta. Tähän resurssiryhmään pusketaan development-resurssiryhmästä palvelun uusin versio CI/CD-pipelinejen avulla. Automaation ansiosta production:in puolella ei tarvita niin kattavaa pääsyä, joten vain muutamalla Valtiokonttorin avainhenkilöllä tarvitsee olla pääsy näihin resurssiryhmiin.

Resurssiryhmien sisäiset komponentit on alustavasti kasattu Valtiokonttorin toimesta kunkin palvelun tarpeiden ja pilvipalvelun tyypin mukaisesti. Valtiokonttori hallinnoi näitä komponentteja toimittajan kanssa, jos toimittaja on erikseen hyväksytty admin-oikeuksin resurssiryhmään voi toimittaja myös tehdä muutoksia komponentteihin. Muutoin tekee toimittaja muutospyynnön Valtiokonttorin palvelusta vastaavalle taholle.

Valtori rajoittaa VY-verkkoon suuntautuvien verkkokomponenttien muokkausta. Nämä muutokset pitää aina tehdä Valtorin kautta. Vnet:in sisäisiä muutoksia voi Valtiokonttori tehdä ilman erityistoimenpiteitä. Valtorin asiakas saa siis oikeudet esim. uusien palvelinten lisäämiseen jo olemassa oleviin verkkoihin, mutta verkkojen, yhteyskäytävien ja palomuurien hallintaoikeutta asiakas ei saa.

On-premises -verkkoresurssien määritys tapahtuu melkeinpä kokonaan toimittajan puolesta. Heidän käsissään on hoitaa pyydetyt avaukset kyseiselle palvelimelle.

4.1.6 Identiteetin- ja pääsynhallinta

Identiteetinhallintaan käytetään olemassa olevaa Valtorin tarjoamaa ratkaisua.
Siis jokainen käyttäjätili tilataan Valtorin järjestelmän kautta. Azure AD synkronoi itsensä paikallisen AD:n kanssa ja hakee käyttäjät ja ryhmät sieltä.

Hybridimallissa identiteetin ja pääsyn hallinta kannattaa hoitaa ”single sign-on” -tyylisesti, eli käyttäjä kirjautuu kerran sisään ja enempää käyttäjätunnusten näpsyttelyä ei tarvita. Helpoin tapa hoitaa SSO-kirjautuminen, kun Valtiokonttorilta löytyy on-premises -aktiivihakemisto käyttäjiä varten, hoituu Azuren Azure AD Connectin avulla. Azure AD Connect synkkaa käyttäjän salasanan on-premises -AD:n ja pilven Azure AD:n kanssa. Tämä tar-

koittaa, että käyttäjä siis pääsee kirjautumaan suoraan Azureen jo olemassa olevilla tunnuksillaan. Tässä kannattaa käyttää hyvien tapojen mukaista ”vähimmät oikeudet”-ajattelumallia käyttäjien roolituksessa, jos joku käyttäjätunnus vuotaa, vahinko on minimoitu. On myös hyvä esim. jokaiselle admin-roolin omaavalle henkilölle asettaa MFA-tunnistus, jolloin sisäänkirjautuminen varmennetaan esim. mobiilin kautta.

4.1.7 Kapasiteetinhallinta

Kapasiteetin hallinnassa täytyy ottaa huomioon vaihtuminen staattisesta menoerästä ”pay as you go” -malliksi. Tämä tarkoittaa sitä, että pilvipalvelun budjetin ennustaminen pitkällä aikavälillä voi olla todella haastavaa. On-premises -mallissa tehtiin päätöksiä ennustusten perusteella todella pitkällä tähtäimellä ja kapasiteetin lisääminen on pitkä prosessi. Pilvessä taas kapasiteettiä voidaan lisätä muutamalla klikkauksella. Tämän takia ”ylivarautuminen” ja kapasiteetin ylimitoitus ovat turhia varotoimenpiteitä pilvessä.

Pilvessä kannattaa myös hyödyntää sen alaspäin skaalautuvuutta, varsinkin kun Valtiokonttorilla on paljon palveluita, joihin kohdistuva liikenne tapahtuu suurimmaksi osaksi vain virka-aikaan klo. 8:00 – 16:00. Tällöin kannattaa pohtia voidaanko palvelu toteuttaa, kokonaan on/off-periaatteella, jolloin se sulkisi itsensä virka-ajan ulkopuolella ja lähtisi taas automaattisesti käyntiin aamulla. Tai vastaavasti voidaan palvelua ajaa minimiasetuksilla virka-ajan ulkopuolella ja nostaa sen kapasiteettia virka-aikaan, jolloin voidaan taata palvelun responsiivisuus ja sen sulava käyttö.

Hybridipilvessä onkin tärkeää seurata pilvenkapasiteettia ja pitää siitä tarkkaa seurantaa, jotta voidaan nähdä, mitä resursseja on käytössä ja mitkä niistä ovat tarpeellisia. Valtiokonttorin pitääkin siis pitää kirjaa siitä mitä kapasiteettia on käytössä, myös toimittajien mahdollisista testaus palvelimista.

4.1.8 Palvelun taloudenhallinta

Pilvipalveluiden myötä myös IT-palveluiden budjetointi tulee muuttumaan. Siinä missä on-premises -palveluissa maksettiin staattisesta palvelusta, niin pilven skaalautuvuus tulee tekemään budjetoinnista haastavampaa.

Skaalautuvuus tuo mukanaan mahdollisia yllättäviäkin kuluja, jos esim. ei pidetä tarkkaa lokia kapasiteetista ja toimittaja nostelee testipalvelimia pystyyn useita ja ei muista näitä poistaa tai sammuttaa. Vaikka yksittäisen palvelimen hinta voikin olla matala, kun jokainen palvelu ja jokainen toimittaja tekee muutaman testipalvelimen, alkaa hinta nousta jo tuntuviin summiin.

On myös hyvä huomioida, että CAPEX (capital expenditure, pääomameno) tyylistä laskutusta ja budjetointia voidaan käyttää hybridipilvessä siihen osaan palvelua, joka vielä pyörii on-premises -puolella. Pilvipalveluihin yleisesti käytetään OPEX (operative expenditure, juoksevatkulut) -tyylistä laskutusta.

5 Johtopäätökset ja suositukset

Tässä osiossa esitetään mahdollisia toimenpiteitä tulevaisuuden varalta ja vaihtoehtoisia toimintamalleja. Tämä osio pohjautuu tämän hetkisiin toteutus vaihtoehtoihin, joita Microsoft Azure:ssa on tarjolla.

5.1 Herätteiden ja tapahtumien hallinta

Herätteiden hallinnassa kannattaa miettiä automatisointia mahdollisimman pitkälle. Valtiokonttori käyttää JIRA:aa projektin hallintaan ja muutospyyntöihin toimittajien suuntaan, joten tässä olisi hyvä mahdollisuus integroida esim. Azure Monitor lähettämään tikettejä suoraan JIRA:aan, josta toimittajat itse nostavat automaatiolla luodut tiketit backlogista työn alle.

5.2 Tietoturva ja palveluidenvarmistaminen

Tietoturvapuolella kannattaa pyrkiä saamaan Valtorilta pääsy Security Dashboardiin, jotta päästään tutkailemaan oikeasti palveluiden tilaa. Tietoturva ja tietoturvauhat ovat koko ajan kehittyviä, joten kannattaa seurata Azuren suosituksia sitä mukaan, kun ne muuttuvat ja päivittyvät.

Palveluiden varmistamisessa kannattaa keskittyä sovellusten kriittisyyden tunnistamiseen ja pohtia niiden replikointi tapaa. IaC (infrastructure as code) on tapa tallentaa infrasta ja jokaisesta resurssiryhmästä ”snapshot” JSON-tiedostoon, jonka avulla voidaan automaatiolla palauttaa infrastruktuuri. Tällä tavoin voidaan palauttaa palvelu toimivaan tilaan, jos palvelu kaatuu tai tapahtuu joitain ei haluttuja muutoksia. Snapshot ei kuitenkaan pidä sisällään mitään muuta kuin tiedon infrastruktuurin ja sen komponenttien konfiguraatioista eli data pitää kuitenkin erikseen varmentaa.

5.3 Identiteetinhallinta

Identiteetinhallinta tuskin tulee pahemmin muuttumaan niin kauan, kun Valtiokonttori on Valtorin AD:n alla.

Single sign-on -tyylistä lähestymistapaa varmasti koitetaan ottaa enemmän käyttöön. SSO:n yleistyessä kannattaa ”vähimmät oikeudet” -politiikkaa valvoa tarkemmin.

5.4 Kapasiteetinhallinta

Valtiokonttorin kannattaa yrittää tunnistaa vielä enemmän palveluita, joissa on mahdollista hyödyntää automaattista sulkemista niinä aikoina, kun palvelua ei tarvita. Melkein kaikissa Valtiokonttorin palveluissa käyttöpiikit ovat 8:00 – 16:00 aikavälillä. On myös hyvä tunnistaa serverless-mahdollisuudet, jotka voivat säästää vielä enemmän, kun voidaan asettaa vaan funktioita pilveen, jotka vasta kutsuttaessa allokoivat itsellensä sopivan palvelimen.

5.5 Muutoksenhallinta

Muutoksenhallintaa voidaan viedä vielä enemmän kohti DevOpsia, jolloin tuotannon puolen Production resurssiryhmiin ei tarvitsisi juurikaan tehdä manuaalisia muutoksia, vaan kaikki tarpeellinen tulisi automaation kautta. Kun julkaisu on hyväksytty testien avulla, voidaan se suoraan viedä pipelinejen avulla tuotantoon ja myös mahdolliset infrastruktuurin muutokset voidaan viedä tuotannon puolelle IaC (infrastructure as code) -tyylisesti.

6 Projektin Retrospektiivi

Projekti kokonaisuudessaan oli mielestäni onnistunut ja lopputulos on hyväksytty toimeksiantajalla. Projektin alussa minua huoletti aikataulun tiukkuus. Tiesin, että projektissa on mukana riskejä juurikin aikataulun puolesta. Toimeksiantajan puolella oli kova kiire ja avainhenkilöiltä ajan saaminen palaveriin oli paikoitellen todella haastavaa, onneksi kuitenkin joustavat lounaat ja erittäin positiivinen asenne projektia kohtaan auttoivat ajan löytämisessä niinäkin päivinä, kun kalentereissa oli jo valmiiksi päällekkäisiä buukkauksia.

Valtiokonttorilla oli alusta asti selkeä näkemys projektin lopputuotoksesta tai ainakin projektin scopesta ja siitä, että hybridihallintomallin tulee käsitellä prosesseja hyvin yleisellä tasolla. Tämä auttoi minua suuresti ja valoi minuun luottamusta, että projekti oli tehtävissä tiukallakin aikataululla, kun projektin scope oli niin selkeä.

Pilvipalveluista itselläni ei hirveästi ollut aikaisempaa kokemusta, jotain perus pohjatietoa ja muutama oma testiserveri Azuressa. Näinkin juuri siksi projektin hyvänä oppimismahdollisuutena. Projektin edetessä oma osaamiseni Azuresta ja pilvipalveluiden maailmasta karttui huimasti, kuten myös tietous IT-palvelutuotannosta ja siihen sisältyvistä prosesseista. Ilman selkeää kuvaa pilvipalveluiden mahdollisuuksista ja niiden toiminnasta olisikin hybridihallintomallin koostaminen todella haastavaa. Tässä myös piili yksi projektin riskeistä, jos en ehdi sisäistämään joko Valtiokonttorin tarpeita pilvessä tai pilven tarjoamia mahdollisuuksia olisi hallintomallin kasaaminen ollut lähes mahdotonta. Kuitenkin aikaisempi kokemukseni Valtiokonttorin IT-palvelutuotannossa oli tässä isona apuna, jonka ansiosta omasin jo kattavan läpileikkauksen Valtiokonttorin palveluista.

Jälkeenpäin projektia miettiessäni olisin voinut olla vielä tehokkaampi Valtiokonttorin asiantuntijoiden kanssa ja käyttää heidän tietämystään paremmin hyödyksi. Nyt välillä kokoukset menivät prosessien turhaksi pilkkomiseksi ja jonkin yksittäisen Azuren ominaisuuden läpikäymiseksi. Tämä on ymmärrettävää ja varmasti Valtiokonttorille hyödyllistä, kun voidaan keskustella vaihtoehtoja läpi ja saada prosesseihin ”ulkopuolisen” näkökulmaa. Minun ja projektin kannalta nämä olivat ehkä hieman turhia kiertoteitä, mutta myös näiltä kiertoteiltä löytyi tiedon murusia, joita seuraamalla osasin esittää lisää kysymyksiä mitkä avasivat Valtiokonttorin pilvistrategiaa minulle tarpeellisella tavalla.

7 Lähdeluettelo

Axelos 2019a. Best Practice, What is ITIL? Luettavissa: https://www.axelos.com/best-practice-solutions/itil/what-is-itil.
Luettu: 27.11.2019

Axelos 2019b. ITIL v4 Foundation. TSO, London

Cisco. After some sputtering, hybrid cloud adoption gathers steam. Luettavissa: https://www.cisco.com/c/en/us/solutions/cloud/hybrid-cloud/adoption.html.
Luettu: 09.11.2019

CloudAcademy 2019. Cloud Migration Risks Benefits. Luettavissa: https://cloudacademy.com/blog/cloud-migration-benefits-risks.
Luettu: 14.11.2019

Ellmén, P. 08.11.2019. Apulaisjohtaja IT-palvelutuotanto, Valtiokonttori. Keskustelu. Helsinki

Flexera 2019a. Cloud Computing Trends: 2019 State of the Cloud Survey. Luettavissa: https://www.flexera.com/blog/cloud/2019/02/cloud-computing-trends-2019-state-of-the-cloud-survey.
Luettu: 12.11.2019

Flexera 2019b. Meet Flexera. Luettavissa: https://www.flexera.com/about-us/our-story.html.
Luettu: 13.01.2020

Greycampus. ITIL Foundation. Luettavissa: https://www.greycampus.com/open-campus/itil-foundation/access-management. Luettu: 11.11.2019

Hewlett Packard Enterprise. On-Premises Data Centres vs. Cloud Computing. Luettavissa: https://www.hpe.com/fi/en/what-is/on-premises-vs-cloud.html.
Luettu: 27.09.2019

Invensislearning. What is ITIL Access Management? Luettavissa: https://www.invensis-learning.com/resources/itil/what-is-itil-access-management. Luettu: 20.11.2019

Microsoft Azure 2019a. What is Azure? Luettavissa: https://docs.microsoft.com/fi-fi/learn/modules/welcome-to-azure/2-what-is-azure.
Luettu: 27.11.2019

Microsoft Azure 2019b. Overview. Luettavissa: https://azure.microsoft.com/en-gb/overview.
Luettu: 2.9.2019

Microsoft Azure 2019c. Azure Monitor. Luettavissa: https://docs.microsoft.com/fi-fi/azure/azure-monitor/platform/data-platform. Luettu: 20.11.2019

NIST 2018. NIST Special Publication 500-322, Evaluation of Cloud Computing Services Based on NIST SP 800-145. Luettavissa: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-322.pdf.
Luettu: 13.11.2019

Redhat. What is CI/CD? Luettavissa: https://www.redhat.com/en/topics/devops/what-is-ci-cd. Luettu: 01.12.2019

Lintilä, R. 26.01.2017. Serverless – mitä se tarkoittaa ja miksi siitä pitäisi kiinnostua? Luettavissa: https://www.solita.fi/blogit/serverless-mita-se-tarkoittaa-ja-miksi-siita-pitaisi-kiinnostua. Luettu: 2.9.2019

TechTarget 2019. Hybrid Cloud. Luettavissa: https://searchcloudcomputing.techtarget.com/definition/hybrid-cloud. Luettu: 9.9.2019

Tieto. Tieto yrityksenä. Luettavissa: https://www.tieto.com/fi/meista/tieto-yrityksena.
Luettu: 05.11.2019

Tieto 2015. Toimintamalli, versio 2H. Luettavissa: Tiedon sisäistä dokumentaatiota.

Valtiokonttori. Valtiokonttori pähkinänkuoressa. Luettavissa: https://www.valtiokonttori.fi/tietoa-valtiokonttorista/valtiokonttori-pahkinankuoressa.
Luettu: 10.11.2019

Valtori. Tietoa Valtorista. Luettavissa: https://valtori.fi/tietoa-valtorista. Luettu: 10.11.2019

Valtori 2018a. Valtorin Pilvipalvelu Toimintamalli, versio 3.4. Luettavissa: Valtorin sisäistä dokumentaatiota.

Valtori 2018b. Julkisen pilven identiteetinhallinta, versio 1.1. Luettavissa: Valtorin sisäistä dokumentaatiota.

Valtori 2018c. Julkisen pilven palveluiden suunnitteluperiaatteet, versio 1.2. Luettavissa: Valtorin sisäistä dokumentaatiota.

Wakaru 2019. Parhaat käytännöt, ITIL. Luettavissa: https://www.wakaru.fi/valmennus/parhaat-kaytannot/palvelujohtaminen/itil. Luettu: 13.01.2020