

Tuomas Moilanen

# Red Hat CloudFormsin käyttöönotto ja ominaisuudet

Tradenomi

Tietojenkäsittely

Syky 2017



KAJANIN  
AMMATTIKORKEAKOULU  
UNIVERSITY OF APPLIED SCIENCES

## Tiivistelmä

**Tekijä:** Moilanen Tuomas

**Työn nimi:** Red Hat CloudFormsin käyttöönotto ja ominaisuudet

**Tutkintonimike:** Tradenomi, tietojenkäsittely

**Asiasanat:** CloudForms, ManagelQ, pilvihallinta, pilvipalvelu

Tämän opinnäytetyön tarkoituksena oli asentaa hallinta-alusta Red Hat CloudForms Kajaanin ammattikorkeakoulun tietojärjestelmälaboratorion datakeskusympäristöön. Työn teoriaosuudessa tavoitteina oli selvittää IT-organisaatioiden pilviympäristöjen tämänhetkistä tilannetta ja käydä läpi pilvihallinnan merkitystä. Käytännön osuuden tavoitteina oli kuvata lukijalle Red Hat CloudFormsin käyttöönottoprosessi ja keskeiset ominaisuudet.

Opinnäytetyön käytännön osuus aloitettiin tammikuussa 2017. Ennen testiympäristön pystyttämistä tutustuttiin Red Hat CloudFormsin dokumentaatioon yleiskuvan luomiseksi tuotteesta ja asennusprosessin selvittämiseksi. Ensimmäiseen testiympäristöön kuului ainoastaan yksi CloudForms-virtuaalikone, joka mahdollisti tuotteen perusominaisuuksien tutkimisen. Tämän jälkeen pystytettiin opinnäytetyön käytännön osuudessa kuvattu ympäristö. Monimutkaisempi ympäristö oli välttämätön tuotteen kaikkien ominaisuuksien käyttöönottamiseksi ja kattavan kokonais kuvan luomiseksi tuotteen toiminnasta. Testauksessa keskityttiin ominaisuuksiin, jotka ovat asiakas keskeisen käyttöönoton kannalta kaikkein merkityksellisimpiä.

Teoriaosuus kirjoitettiin syksyllä 2017 käyttäen verkosta löydettyjä lähteitä. Tekstiosan alkuun koottiin tietoa pilvipalveluista johdatuksena aiheeseen. Tämän jälkeen kirjoitettiin IT-organisaatioiden siirtymisestä yhä monimutkaisempiin pilviympäristöihin, ja tämän muutoksen taustalla vaikuttavista syistä. Teoriaosuuden loppuun kirjoitettiin lyhyesti hybridipilven käyttöönoton seurauksena syntyvistä haasteista.

Red Hat CloudFormsin käyttöönotto suoritettiin onnistuneesti. Osa ympäristön koneista sijaitsi samoilla virtuaalisilla ESXi hosteilla, joten oikeassa datakeskusympäristössä esiintyviä vaatimuksia korkealle käytettävyydelle ei saavutettu. CloudForms sisältää kaikki eri ympäristöissä olevien virtuaalikoneiden hallintaan tarvittavat perusominaisuudet. Joidenkin ominaisuuksien toteutuksessa ja toiminnassa on kuitenkin eritasoisia ongelmia. Virtuaalikoneiden laskutuksessa ja konsoliyhteyksissä esiintyvien ongelmien vuoksi CloudForms 4.2 ei sovellu asiakkaille myytävien virtuaalikoneiden alustaksi. Versio 4.2 toimii parhaimmillaan IT-organisaatioiden sisäisessä käytössä virtuaalikoneiden hallinnassa ja monitoroinnissa. CloudForms on kuitenkin jatkuvassa kehityksessä, ja osa löydetyistä ongelmista on korjattu tuotteen uusimpiin versioihin.

## **Abstract**

**Author:** Moilanen Tuomas

**Title of the Publication:** The Deployment and Features of Red Hat CloudForms

**Degree Title:** Bachelor of Business Information Technology

**Keywords:** CloudForms, ManagelQ, cloud management, cloud service

The purpose of this thesis was to install multicloud management platform Red Hat CloudForms to the datacenter of the information technology laboratory at Kajaani University of Applied Sciences. The theoretical frame focuses on examining the current situation of IT organizations' cloud environments and the importance of cloud management. In the practical part of this thesis, the goals were to describe the deployment process of Red Hat CloudForms and its main features.

The preparation of the process started in January of 2017. It was necessary to go through the product documentation before installing a test environment. The first test environment comprised of only one CloudForms virtual machine, but it was sufficient for testing purposes. After testing the main functionalities of the product, was time to install a more complex environment that is described in the practical part. Installing a second, bigger environment was essential to creating an overview of all important features and functions. Testing focused on properties that were most important for a customer-centric deployment.

The theoretical part was written using online sources in autumn of 2017. Information about cloud services was written as an introduction to the subject, followed by research information concerning movement to more complex cloud environments and the reasons behind this change. The final paragraphs of theory introduce some challenges that come with hybrid clouds.

Red Hat CloudForms was deployed successfully. The final environment did not fill all the requirements for high-availability, because some of the virtual machines were located on the same virtual ESXi hosts. CloudForms has all the basic properties for virtual machine management on different environments. Some features have problems related to execution and operation. CloudForms 4.2 cannot be used as a platform, where clients can order chargeable virtual machines. This is mainly due to problems in billing and virtual machine console connections. Organizations can use Version 4.2 to manage and monitor their own virtual machines. CloudForms is still in active development and some of the uncovered problems have been resolved on newer versions of the product.

## Sisällys

1	Johdanto .....	1
2	Pilvipalvelut .....	2
2.1	Pilvityypit .....	5
2.2	Pilvimallit .....	6
2.3	Siirtyminen hybridipilveen.....	7
2.4	Pilvihallinta .....	9
3	Red Hat CloudForms .....	12
3.1	Yleistä tietoa .....	12
3.2	Ominaisuudet.....	13
3.3	Red Hat CloudForms Management Engine .....	15
3.4	Vaatimukset .....	15
3.5	Ympäristön suunnittelu.....	16
4	Asennus vSphereen.....	19
4.1	Asennusympäristön kuvaus.....	19
4.2	Asennusprosessi.....	20
4.3	VCenterin määrittäminen provideriksi.....	24
5	Red Hat CloudFormsin ominaisuudet.....	26
5.1	Web-käyttöliittymä ja itsepalveluportaali .....	26
5.2	Virtuaalikoneet .....	26
5.3	Virtuaalikoneiden konsoliyhteydet .....	28
5.4	Käyttäjien hallinta .....	28
5.5	Automatisointi .....	29
5.6	Raportit .....	31
5.7	Laskutus.....	32
5.8	Tietokannan varmuuskopiointi.....	33
6	Red Hat CloudFormsin ongelmat .....	34
7	Versiot.....	36
8	Pohdinta.....	38
	Lähteet.....	40

## Symboliluettelo

Active Directory	Microsoftin luoma suojattu, strukturoitu ja hierarkkinen tiedon tallennuspaikka verkon objekteille.
API	Application programming interface eli ohjelmointirajapinta määrittelee, miten eri ohjelmat voivat tehdä pyyntöjä ja vaihtaa tietoja keskenään.
FQHN	Fully qualified hostname on tietokoneen tunnistamista varten tehty verkkotunnus.
IPAM	IP Address Management koostuu joukosta työkaluja IP-osoiteavaruuden suunnitteluun, hallintaan ja seurantaan tietokoneverkossa.
ISO	CD- ja DVD-levyistä tehtyjen levykuvien tiedostopäätte.
Kontti	Kokonaisuus, joka sisältää sovelluksen ja sen tarvitseman sovel-lusalueen. Konttia voidaan käyttää sitä tukevalla ajoalustalla käyt- töjärjestelmäriippumattomasti.
LDAP	Lightweight Directory Access Protocol on hakemistopalvelujen käyttöön tarkoitettu verkkoprotokolla.
LDAPS	LDAP:n ja Secure Sockets Layer -protokollan yhdistelmä, jota käytetään LDAP-asiakaskoneen ja -palvelimen välisen kommunikaa-tion salaukseen.
NFS	Network File System on hajautettu levyjärjestelmä, jota käytetään hakemistojen ja tiedostojen etäkäyttöön.
NIST	National Institute of Standards and Technology on yhdysvaltalai-nen virasto, jonka tehtävänä on kehittää ja edistää mittaustekniikoita, standardeja ja tekniikkaa.
OVA	Open Virtual Appliance on yksittäinen tiedosto, johon kootaan useita virtuaalikoneeseen liittyviä tiedostoja.
PostgreSQL	Avoimen lähdekoodin tietokannan hallintajärjestelmä.

Quota	Ylläpitäjän asettama raja tietyn resurssin käytölle.
RESTful	Representational state transfer arkkitehtuurimalliin perustuva ohjelmointirajapinta.
Ruby on Rails	Ruby-ohjelmointikielellä kirjoitettu avoimen lähdekoodin ohjelmistokehys.
Samba	Avoimen lähdekoodin ohjelmisto Server Message Block verkkoprotokollan toteuttamiseksi Linux- ja Unix-käyttöjärjestelmissä.
SELinux	Security-Enhanced Linux on Linux-ytimeen kehitetty laajennus, joka rajoittaa ohjelmien toimintaoikeuksia niille kirjoitettujen sääntöjen mukaan.
Snapshot	Virtuaalikoneen tilan tallentamiseen käytetty ominaisuus, joka mahdollistaa tilan palauttamisen jälkikäteen.
SNMP	Simple Network Management Protocol on protokolla, jota käytetään verkossa olevien laitteiden monitorointiin ja hallintaan.
SOAP	Simple Object Access Protocol on tietoliikenneprotokolla, joka toimii useiden eri protokollien yli.
Template	Virtuaalikoneesta tehty alkuperäinen kopio, joka mahdollistaa useiden kloonien luomisen.
URI	Uniform Resource Identifier on merkkijono, jolla tunnistetaan resurssin nimi tai paikka.
VPN	Virtual Private Network on tekniikka, jonka avulla muodostetaan salattu ja todennettu yhteys kahden päätepisteen välille julkisen verkon yli.
WebSocket	Protokolla, joka mahdollistaa vuorovaikutuksen selaimen ja palvelimen välillä.

## 1 Johdanto

Tässä opinnäytetyössä tutustutaan pilvipalveluiden, virtualisointiympäristöjen ja konttien maksulliseen hallinta-alustaan nimeltä Red Hat CloudForms. Tämän tuotteen hallintaominaisuuksista tärkeimmät liittyvät virtuaalikoneisiin ja käyttäjiin. Hallintaominaisuuksien lisäksi CloudForms pyrkii myös tarjoamaan näkyvyyttä hallittaviin ympäristöihin ja tehostamaan ylläpidollisia toimia automaation avulla. Opinnäytetyön teoriaosassa on tietoa pilvipalveluista, organisaatioiden siirtymisestä hybridipilviin ja pilvihallinnasta. Käytännön osuudessa selvitetään CloudForms-ympäristön suunnittelu ja esimerkiympäristön asennus VMware vSphereen sekä käydään läpi tuotteen ominaisuuksia ja toiminnallisuuksia.

Pilvipalvelut tarjoavat tietoteknisiä resursseja verkon yli. Aikaisemmin esimerkiksi asiakkaille sovellusta tarjoava yritys joutui hankkimaan, asentamaan ja ylläpitämään fyysisiä resursseja varmistaakseen sovelluksen toiminnan suurillakin käyttäjämäärillä. Pilvipalvelussa valmiita resursseja varataan palveluntarjoajalta käytön mukaan ja maksukin on yleensä käyttöperusteista. Pilvipalvelut voivat siis tietyissä tilanteissa tarjota ajallisia ja taloudellisia säästöjä. Organisaatiot siirtyvät pilvipalveluiden käyttäjiksi eri nopeuksilla, minkä vuoksi pilvipalveluiden rinnalla käytetään usein perinteisiä virtualisointiympäristöjä. Tämän seurauksena datakeskustoimijat joutuvat työskentelemään sekaympäristöjen kanssa, mikä osaltaan vähentää pilvipalveluihin siirtymisen hyötyjä.

Kilpailun kiristyessä datakeskustoimijat pyrkivät säästöjen lisäksi panostamaan muun muassa asiakaskokemukseen. Useat virtualisointiympäristöt ja pilvipalvelut antavat asiakkaille valinnanvaraa, mutta saattavat olla ylläpidollisesti ja laskutuksellisesti epäkäytännöllisiä. CloudFormsin päätavoitteena on yksinkertaistaa monimutkaisten IT-ympäristöjen hallintaa. Asiakkaat pystyvät kirjautumaan yksillä käyttäjätunnuksilla web-käyttöliittymään ja valitsemaan itsenäisesti, mihin virtualisointiympäristöön tai pilvipalveluun virtuaalikoneet tehdään. CloudFormsin kaltaisia tuotteita on markkinoilla useita, mutta ne eivät ole vielä käytössä suurimmassa osassa datakeskuksista.

CloudForms voi toimia IT-organisaation sisäisessä käytössä tai kaupallisen toiminnan tukena. Opinnäytetyön tavoitteina on suorittaa CloudFormsin käyttöönotto ja tutkia, kuinka hyvin tuotetta voidaan käyttää alustana, jonka kautta IT-organisaation asiakkaat voivat tilata maksullisia virtuaalikoneita. Lisäksi tavoitteena on tutustua CloudFormsin tarjoamiin ylläpitoa helpottaviin ominaisuuksiin ja toiminnallisuuksiin.

## 2 Pilvipalvelut

Pilvipalvelu on hajautettu verkkopalvelu, joka mahdollistaa tietoteknisten resurssien reaaliaikaisen käytön verkon kautta. Käytettäviä resursseja voivat olla esimerkiksi palvelimet, sovellukset ja tallennustila. Itse resurssien lisäksi pilvipalveluihin voidaan katsoa kuuluvaksi myös resursseja tarjoavan datakeskuksen laitteisto ja ohjelmistot. Pilvipalvelussa asiakkaat siis vuokraavat jaettuja resursseja palveluntarjoajalta, joka on etukäteen suorittanut datakeskuksen rakennuksen, ylläpitäjien palkkaamisen ja tietoteknisten resurssien hankinnan sekä varmistanut, että hankitut resurssit toimivat yhdessä. Yhdessä toimivat tietotekniset resurssit voivat tarjota laskentatehoa esimerkiksi asiakkaan sovelluksen toimintaan. Pilvipalvelun päällä toimiva sovellus toimii samalla tavalla kuin se toimisi yksittäisellä palvelimella. Pilvipalvelujen myötä sovellukset eivät tarvitse toimiakseen tiettyä laitteistoa, vaan ne voivat hyödyntää kumulatiivista laskentatehoa. (Armbrust ym. 2009, 4; TSK, 2016; Walker 2010.)

Pilvipalveluille on myös yhdysvaltalainen National Institute of Standards and Technologyn (NIST) antama tarkempi määritelmä, jota pidettiin de facto -standardina jo ennen kuin siitä julkaistiin lopullinen versio. Määritelmän mukaan pilvipalvelu on malli, joka mahdollistaa tarvittaessa helpon pääsyn käsiksi jaettuihin ja muunneltaviin tietoteknisiin resursseihin verkkoyhteyden kautta. Näitä tietoteknisiä resursseja tulisi voida varata ja vapauttaa ilman suurta hallinnallista vaivaa sekä vuorovaikutusta palveluntarjoajan kanssa. (Brown 2011; Mell & Grance 2011, 2.)

NIST määrittelee pilvipalveluille viisi olennaista tunnusmerkkiä:

### 1. Itsepalvelu

Asiakas pystyy halutessaan varaamaan itselleen tietoteknisiä resursseja, kuten tallennustilaa. Varaaminen tehdään itsenäisesti itsepalveluportaalissa ilman asiakkaan ja palveluntarjoajan välistä vuorovaikutusta.

### 2. Saatavuus

Pilvipalvelun tarjoamiin ominaisuuksiin tulee päästä käsiksi verkkoyhteyden kautta käyttäen tavanomaisia mekanismeja ja päätelaitteita.



### 3. Resurssien yhteiskäyttö

Palveluntarjoajan tietoteknisiä resursseja voivat käyttää useat asiakkaat. Jaettavia fyysisiä ja virtuaalisia resursseja myönnetään dynaamisesti kysynnän mukaan. Asiakkaalla voi olla mahdollisuus vaikuttaa käyttämiensä resurssien sijaintiin esimerkiksi maa- ja datakeskustasolla.

### 4. Nopea joustavuus

Kapasiteettia voidaan varata ja vapauttaa joustavasti kysynnän mukaan jopa automaattisesti. Asiakkaan näkökulmasta tarjolla olevan kapasiteetin määrä näyttää usein rajattomalta.

### 5. Mitattava palvelu

Resurssien käyttöä voidaan monitoroida, hallita ja optimoida sekä siitä voidaan tehdä raportteja. Resurssien käytön mittaaminen mahdollistaa asiakkaiden laskutuksen. (Mell & Grance 2011, 2.)

Pilvipalvelun käyttöönotolla voi olla monia etuja verrattuna oman infrastruktuurin rakentamiseen ja ylläpitoon. Yksi pilvipalvelujen suurimmista eduista on, että yrityksen ei koskaan tarvitse maksaa ylimääräisistä tietoteknisistä resursseista ja niiden ylläpidosta, vaan maksaminen tapahtuu käytön mukaan. Pilvipalvelut mahdollistavat käytettävissä olevien resurssien määrän nopeat muutokset, sillä uuden laitteiston hankkimisen sijaan esimerkiksi tallennuskapasiteetin lisääminen tapahtuu muutamissa minuuteissa itsepalveluportaalissa. Tämä parantaa työn tuottavuutta ja joustavuutta, sillä esimerkiksi ohjelmistokehitystä ja -testausta varten tarvittavat resurssit saadaan käyttöön ajallisesti ja taloudellisesti järkevästi. Myös mahdollisen valmiin tuotteen tai palvelun loppukäyttäjät hyötyvät, sillä resurssien nopean skaalautuvuuden ansiosta suuretkaan käyttäjämäärät eivät aiheuta käyttökatkoksia. Palveluntarjoajasta riippuen valmis tuote tai palvelu voi olla mahdollista julkaista useilla eri maantieteellisillä alueilla, jolloin käyttäjien verkkoviiveet pienenevät. Jos uudelle palvelulle tai tuotteelle ei löydy käyttäjiä, jäävät taloudelliset tappiot pieniksi, sillä yrityksen omaan infrastruktuuriin ei ole tarvinnut sitoa pääomaa. (Amazon.com.)

Pilvipalvelun käyttöönottoon voi liittyä myös haasteita. Ammattitaidon puutteen ei pitäisi olla esteenä käyttöönotolle. Yrityksen sisäistä ammattitaidon puutetta voidaan kompensoida käyttämällä konsultointipalveluja pilviympäristön suunnitteluun, käyttöönottoon ja

hallintaan. Tietoturva on edelleen yksi tärkeimmistä kynnyskysymyksistä, kun infrastruktuuriin ja sovelluksiin liittyvää vastuuta siirtyy palveluntarjoajalle. Vastuu päivityksistä ja tietoturvan hallinnasta siirtyy toiselle osapuolelle, ja tähän mahdollisesti liittyvät riskit tulee tiedostaa. Pilvipalveluun tai hybridipilveen siirtymisen strategian tulee tukea liiketoimintaa ja selvittää hyväksyttävät tasot muun muassa kustannuksille ja tietoturvalle. Organisaatioiden pitää myös pystyä seuraamaan ja hallitsemaan pilvipalvelun käyttöön liittyviä kustannuksia. Kustannuksien lisäksi haasteiksi voivat muodostua henkilötietojen siirto ja monimutkaisuus. Henkilötietojen siirtoon Euroopan talousalueen ulkopuolelle sekä henkilötietojen käsittelyn tietoturvasuudesta huolehtimiseen liittyy kansainvälisiä säännöksiä, joita tulee noudattaa. Jos otetaan käyttöön useita pilvipalveluita, voi monimutkaisuus heikentää organisaation tuottavuutta, ketteryyttä ja innovointia. Usein työkuormien ja datan pitää pystyä liikkumaan eri ympäristöjen välillä, jotta ketteryys olisi osa hybridipilveä. Toimintojen ja työkalujen lukitseminen tietyn palveluntarjoajan huostaan voi muodostua ongelmaksi. Lisäksi oikeiden palvelutarjousten ja palvelutasojen valitseminen useilta eri pilvipalveluntarjoajilta voi olla hankalaa. (Thorpe 2017; Tietosuojavaltuutetun toimisto 2015.)

## 2.1 Pilvityypit

Erilaisia pilvityyppejä on neljä: yksityinen pilvi (private cloud), julkinen pilvi (public cloud), yhteisöllinen pilvi (community cloud) ja hybridipilvi (hybrid cloud). Yksityinen pilvi on tarkoitettu ainoastaan yhden organisaation käyttöön. Nykyään monien yritysten IT-ympäristöjä voidaan oikeastaan pitää yksityisinä pilvinä, sillä ne on suunniteltu ja rakennettu yhdelle asiakkaalle tiettyjen liiketoimintaan vaikuttavien toimintojen tueksi. Oma organisaatio voi omistaa, hallita ja ylläpitää yksityistä pilveä, mutta nämä asiat voivat olla myös kokonaan tai osittain kolmannen osapuolen vastuulla. Täten pilven resurssit voivat sijaita joko oman organisaation tai kolmannen osapuolen tiloissa. Molemmissa vaihtoehdoissa on omat hyvät ja huonot puolensa. Omassa datakeskuksessa sijaitseva yksityinen pilvi antaa organisaatiolle täyden vallan pilveen tallennettujen tietojen turvallisuuden ja pilven ominaisuuksien osalta. Tällöin palvelut sijaitsevat organisaation sisäisessä verkossa, eikä niitä voida käyttää verkon ulkopuolelta ilman VPN-tunnelin muodostamista organisaation verkkoon. Yksityisen pilven käyttöönotto kolmannen osapuolen datakeskuksessa voi kuitenkin tarjota taloudellisia säästöjä, joustavuutta ja parempaa skaalautuvuutta. (Mell & Grance 2011, 3; Williams 2012.)

Julkisen pilven jaetut tietotekniset resurssit ovat kaikkien käytettävissä julkisen verkon välityksellä. Julkisen pilven omistus, hallinta ja ylläpito ovat palveluntarjoajan roolin omaavan yrityksen tai organisaation vastuulla. Pilveen kuuluvat virtualisoidut palvelimet, verkkolaitteet ja tallennuskapasiteetti sijaitsevat palveluntarjoajan datakeskuksissa. Tunnetuimpia palveluntarjoajia ovat esimerkiksi Amazon, Apple, Microsoft ja Google. Julkisen pilven resursseja ostavat asiakkaat saavat taloudellisia säästöjä maksamalla ainoastaan käyttämistään resursseista. Julkisten pilven ostoa harkitsevien yritysten tulee yleensä ottaa huomioon tietoturva, käyttökatkot ja verkon viiveet. (Mell & Grance 2011, 3; Williams 2012.)

Yhteisöllisen pilven resurssit on tarkoitettu yksinomaan sellaisten ryhmien käyttöön, joilla on tietyt yhteiset tarpeet. Nämä tarpeet voivat liittyä esimerkiksi määräystenmukaisuuteen, käytäntöihin ja turvallisuusvaatimuksiin. Pilvi voi olla yhteisön yhden tai useamman ryhmän omistama, hallitsema ja ylläpitämä, mutta nämä asiat voivat olla myös kokonaan tai osittain kolmannen osapuolen vastuulla. Yhteisöllisen pilven määritelmän kannalta ei ole merkityksellistä, missä pilven resurssit fyysisesti sijaitsevat. (Mell & Grance 2011, 3; Williams 2012.)

Hybridipilvi on kahden tai useamman aikaisemmin mainitun pilvityypin yhdistelmä. Hybridipilvessä yksittäiset pilvet säilyvät omina kokonaisuuksinaan, mutta ne sidotaan toisiinsa

hallinnallisen viitekehyksen avulla. Tällöin saadaan aikaan näennäisesti yhtenäinen pilvi, joka mahdollistaa esimerkiksi pilvien välisen kuormantasauksen. Hybridipilvi voi antaa hyvän kompromissin organisaatioille, jotka tarvitsevat julkisen pilven kustannustehokkuutta ja skaalautuvuutta, mutta haluavat pitää arkaluontoiset tietonsa yksityisessä pilvessä. (Mell & Grance 2011, 3; Williams 2012.)

## 2.2 Pilvimallit

Pilvipalvelut jaetaan tyypillisesti kolmeen eri malliin: SaaS (Software as a Service), IaaS (Infrastructure as a Service) ja PaaS (Platform as a Service). SaaS-mallissa asiakas käyttää palveluntarjoajan pilvi-infrastruktuurissa toimivaa palvelua. Yleensä tarjottava palvelu on sovellus, josta laskutetaan käytön mukaan. Tarjottavaa palvelua voidaan käyttää useilla erilaisilla päätelaitteilla verkkoselaimen avulla. SaaS-mallissa asiakkaan ei tarvitse huolehtia pilvi-infrastruktuurin rakentamisesta, ylläpidosta ja kehittämisestä, vaan asiakas ainoastaan vuokraa käytettävää palvelua. Asiakkaan ei myöskään tarvitse hankkia verkon kautta käytettävää sovellusta varten lisenssejä, eikä huolehtia ohjelmistopäivityksistä. Kääntöpuolena on, että asiakkaalla ei ole päätösvaltaa liittyen sovelluksen ominaisuuksiin ja kehitykseen. (Mell & Grance 2011, 2; Williams 2012.)

PaaS-mallissa asiakas voi ottaa käyttöön tekemiään tai hankkimiaan sovelluksia palveluntarjoajan pilvi-infrastruktuurissa. PaaS-mallia voidaan kuvata kehitysympäristönä, joka mahdollistaa uusien sovellusten nopean suunnittelun, tekemisen, testauksen ja käyttöönoton. Sovellusten tekemiseen pitää yleensä käyttää palveluntarjoajan tukemia ohjelmointikieliä, palveluita ja työkaluja. PaaS-mallissa asiakas ei ole vastuussa pilvi-infrastruktuurin rakentamisesta, ylläpidosta ja kehittämisestä. Asiakkaalla on täysi valta käyttöönotettavaan sovellukseen ja tietyissä tapauksissa mahdollisuus vaikuttaa sovelluksen asennusympäristön konfiguraatioasetuksiin. Käytettävä kehitysympäristö ja sen ominaisuudet voivat kuitenkin asettaa rajoituksia sovelluskehitykselle. (Mell & Grance 2011, 2-3; Williams 2012.)

IaaS-mallissa asiakkaille tarjotaan laskentatehoa, tallennustilaa, verkkoja ja muita resursseja, joita asiakas voi hyödyntää haluamiensa ohjelmistojen ajamiseen. Asiakas ei hallitse tai ylläpidä pilvi-infrastruktuuria, mutta voi vaikuttaa esimerkiksi käyttöjärjestelmiin ja käyttöönotettuihin sovelluksiin. IaaS-mallissa asiakkaan ei itse tarvitse rakentaa infrastruktuuria, vaan tarvittavat resurssit tilataan verkon kautta itsepalveluportaalissa. IaaS-malli on

pilvimalleista kaikkein joustavin ja mahdollistaa käytettävien resurssien määrän ja näin maksettavien kulujen hienosäädön. (Mell & Grance 2011, 3.)

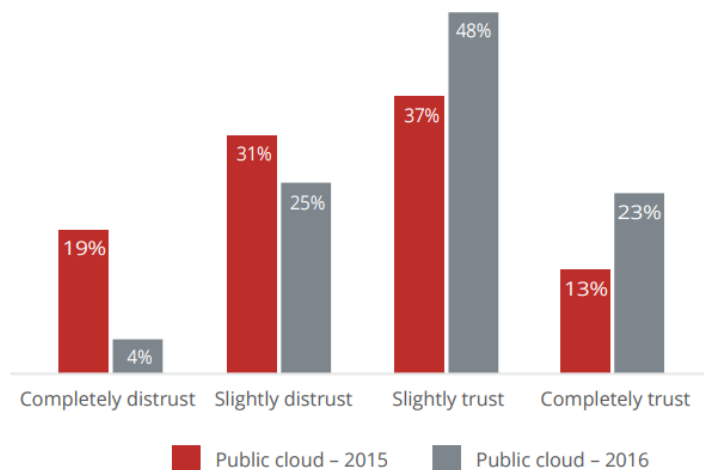
### 2.3 Siirtyminen hybridipilveen

Helmikuussa 2017 Intel Security (nyk. McAfee) julkaisi pilvipalveluiden käyttöönottoon, haasteisiin ja trendeihin liittyvän raportin ”Building Trust in a Cloudy Sky”. Raporttia varten kerättiin tietoa 1400:lta IT-asiantuntijalta eri puolilta maailmaa ottaen huomioon eri alat ja organisaatioiden koot. Kaikki kyselyyn vastanneet asiantuntijat olivat tekemisissä pilvipalvelujen kanssa ja olivat omassa organisaatiossaan vastuussa niihin liittyvästä päätöksenteosta. Tiedon kerääminen suoritettiin syyskuussa 2016. Raportin mukaan 93 prosenttia organisaatioista käytti jotain pilvipalvelua jossain muodossa. Kaikista suurin muutos vuoteen 2015 nähden tapahtui yksityisen ja hybridipilven välisessä suhteessa. Vuonna 2015 ainoastaan yksityistä pilveä käyttävien organisaatioiden osuus oli 51 prosenttia, kun taas hybridipilveä käyttävien organisaatioiden osuus oli 19 prosenttia. Vastaavasti vuonna 2016 yksityisen pilven osuus oli 24 prosenttia ja hybridipilven 57 prosenttia. Siirtyminen yksityisestä pilvestä hybridimalliin on siis ollut voimakasta raporttien kohteina olleissa organisaatioissa. Muutos on vaatinut IT-organisaatiolta ja niiden datakeskuksilta siirtymistä pilvipohjaisiin infrastruktuureihin, joissa virtualisoidun laitteiston osuus on suuri. (McAfee.com 2017, 6, 8.)

Cloudifyn syyskuussa 2017 julkaisema yleiskatsaus kertoo myös osaltaan siirtymisestä monimutkaisempiin IT-ympäristöihin. Yleiskatsaukseen vastasi 700 IT-asiantuntijaa eri alojen organisaatioista, ja yritysten koko vaihteli 50:stä työntekijästä 10 000:een. Yleiskatsaukseen osallistuneista yrityksistä noin puolet hallitsi vähintään kahta eri pilviympäristöä ja 8,6 prosenttia kertoi hallitsevansa vähintään viittä eri pilviympäristöä. Kaikista suosituin kahden eri pilven kombinaatioista oli Amazon Web Services ja Microsoft Azure, joka on suosituin pienissä ja keskisuurissa yrityksissä. Pienemmillä organisaatioilla on matalampi kynnys siirtyä puhtaasti julkisista pilvistä koostuviin ympäristöihin, sillä omaan laitteistoon tehdyt taloudelliset panostukset ovat suhteellisen vähäisiä. Suuremmilla organisaatiolla siirtyminen kestää kauemmin ja hallittavat ympäristöt ovat tällä hetkellä usein yksityisten ja julkisten pilvien muodostamia hybridipilviä. (Cloudify 2017, 3, 9.)

Organisaatioiden siirtymistä hybridipilviin voidaan selittää monilla eri asioilla. Cloudifyn yleiskatsauksen mukaan yli 38 prosenttia pilveen siirtyneistä yrityksistä pyrkii toimintojen

tehokkuuden lisäämiseen, johon voi liittyä esimerkiksi mahdollisuus tukea vaihtelevia työkuormia. Toiseksi suosituin syy oli innovatiivisuus, joka oli siirtymisen syynä 28:lla prosentilla vastaajista. Tehokkuuden ja innovatiivisuuden lisäämisellä yritykset pyrkivät lisäämään kilpailukykyään ja tarjoamaan parempaa palvelua asiakkailleen. Yritykset pyrkivät myös vastaamaan asiakkaiden tarpeisiin ja yritystoiminnan muutoksiin. Yksi suuri syy siirtymään on myös lisääntynyt luottamus julkisiin pilviin. Kuvassa 1 olevat pylväsdiagrammit kuvaavat Intel Securityn raporttia varten tehtyyn kyselyyn vastanneiden IT-asiantuntijoiden luottamusta julkisiin pilviin. Haastateltavat valitsivat neljästä luottamuksen tasosta sen, joka heidän mielestään kuvasi parhaiten julkisten pilvipalvelujen kykyä pitää organisaatioiden arkaluontoiset tiedot turvassa. Kuvasta voidaan nähdä, että luottamus julkisia pilviä kohtaan lisääntyi vuosien 2015 ja 2016 välillä. Huomattavin muutos tapahtui täydellisen epäluottamuksen määrässä; vuonna 2015 vastaajista 19 prosenttia ei luottanut lainkaan julkisiin pilviin, kun taas vuonna 2016 epäluottamus oli pudonnut neljään prosenttiin. Selvä muutos tapahtui myös täydellisen luottamuksen määrässä. (Cloudify 2017, 22; McAfee.com 2017, 12.)

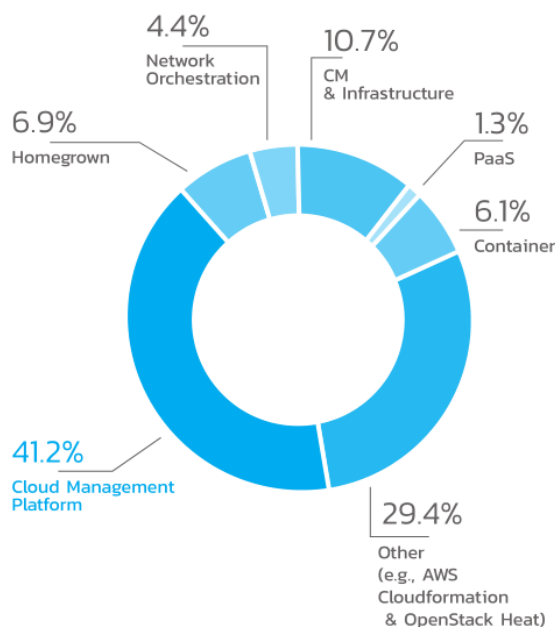


Kuva 1. IT-asiantuntijoiden luottamus julkisiin pilviin maailmanlaajuisesti (McAfee.com 2017, 12).

Lisääntynyt luottamus ja parempi ymmärrys riskeistä näkyvät organisaatioiden arkaluontoisten tietojen siirtämisessä julkisiin pilviin. Organisaatioista 25 prosenttia tallentaa kaikki arkaluontoiset tietonsa johonkin julkiseen pilvipalveluun ja 59 prosenttia tallentaa osan tiedoistaan (McAfee 2017, 12).

## 2.4 Pilvihallinta

Monimutkaisten hybridipilvien hallinta aiheuttaa haasteita, sillä organisaatioiden liiketoimintamallit, tavoitteet ja tarpeet eroavat toisistaan. Organisaatioiden eroavaisuuksien vuoksi käytössä olevat hybridipilvet eroavat toisistaan; organisaation oman laitteiston osuus voi olla suuri tai käytössä voi olla melkein puhtaasti julkisia pilvipalveluja. Eroavaisuuksien vuoksi käytössä olevat hallintaratkaisut eroavat toisistaan, eikä hybridipilvien hallintaan ole olemassa yhtä yleisesti hyväksyttyä ratkaisua. Suurin osa organisaatioista on ottanut käyttöön jonkinlaisen orkestraattorin tai hallinta-alustan, jolla pystytään hallitsemaan työkuormia eri ympäristöjen halki. Kuvassa 2 nähdään käytössä olevien hallintatyökalujen kirjo perinteisestä pilvihallinnasta aina organisaation sisäisiin ratkaisuihin. Hallintatyökalujen tyypeistä suosituin on pilvihallinnan alusta (Cloudify 2017, 16-17).



Kuva 2. Organisaatioissa pilvien hallintaan käytettyjen työkalujen osuudet tyypeittäin (Cloudify 2017, 17).

Hybridipilviä voidaan käyttää esimerkiksi kaupallisten palveluiden ja sovellusten tarjoamiseen, kehitykseen ja testaukseen. Yritysjohdolle tarvitaan tietoa yksittäisten sovellusten ja palveluiden kustannuksista sekä palvelutasoista. Tämä tieto mahdollistaa liiketoiminnan kannalta tärkeiden päätösten tekemisen, ja täten ylläpitäjien pitäisi pystyä tarjoamaan yritysjohdolle tarvittavat tiedot. Ongelmia on tullut erityisesti, kun organisaatioiden sovelluksia on ryhdytty siirtämään julkisiin pilvipalveluihin. Toiminnan tehokkuuden ja loppukäyttäjien mahdollisimman hyvän kokemuksen takaamiseksi organisaatiolla tulee olla mahdollisuus

valvoa sovellusten ja palveluiden suorituskykyä julkisissa pilvipalveluissa. Tällä hetkellä kaikki palveluntarjoajat eivät kuitenkaan tarjoa kattavaa reaaliaikaista monitorointia, asiakkaille ilmoitetut arvot ovat käyttöön perustuvia tai palveluntarjoaja antaa raportteja vain kuukausitasolla. Ongelmista huolimatta siirtyminen osittain tai kokonaan julkiseen pilveen etenee. (Dimensional Research 2016, 2.)

Monimutkaisten hybridipilvien hallinta ja monitorointi voivat onnistua useilla olemassa olevilla hallintaohjelmilla. Käytettävät ohjelmat voivat kuitenkin antaa keskenään ristiriitaista tietoa, lisätä yrityksen kuluja ja vaikeuttaa ylläpitäjien työtä. Viime vuosina markkinoille on ilmestynyt useita kaupallisia tuotteita, kuten pilvihallinnan alustoja, jotka pyrkivät helpottamaan ylläpitoa yhdistämällä useita eri pilviä yhden tuotteen hallintaan. Tällaiset pilvihallinnan alustat tarjoavat näkyvyyttä keräämällä pilvistä yksityiskohtaisia tietoja ja luomalla kerättyistä tiedoista kokonaisvaltaisen kuvan hybridipilvestä. Kerättyjä tietoja voivat olla esimerkiksi virtuaalikoneiden määrä, asennetut käyttöjärjestelmät ja suorituskyky. Pilvihallinnan alustoihin sisältyy myös hallintamahdollisuuksia, ja ne voivat tarjota lisäominaisuuksia aina automaatiosta laskutukseen. Ihanteellisessa tilanteessa yhdellä pilvihallinnan alustalla pystyisi hoitamaan kaikkien yksityisten ja julkisten pilvien monitoroinnin ja hallinnan. Tämä lisäisi ylläpitäjien toiminnan tehokkuutta, sillä koko ympäristön hallintaa varten ei tarvitsisi opetella kuin yhden tuotteen käyttäminen. Yhden hallintapaneelin kautta voisi hoitaa kaikki ylläpidolliset tehtävät ja mahdollisten ongelmatilanteiden selvittämisen. (Dimensional Research 2016, 2-3.)

Hybridipilveen siirtyminen vaikuttaa ylläpitäjien ja yritysjohton väliseen kommunikaatioon. Siirtymän seurauksena määräystenmukaisuuden seurannasta tulee entistä tärkeämpää, ja ylläpitäjien pitää pystyä seuraamaan sekä muuttamaan määräystenmukaisuuteen vaikuttavia asetuksia. Määräystenmukaisuus liittyy hybridipilvessä olevan tiedon turvaamiseen. Hybridipilvessä oleva tietoa pitää pystyä paikantamaan, tiedon yksityisyys tulee varmistaa salauksen avulla ja tiedon häviäminen estää ongelmatilanteissa. Tarvittaessa ylläpitäjien täytyy antaa yritysjohdolle tietoa määräystenmukaisuudesta raporttien muodossa. Uudet pilvihallinnan alustat voivat helpottaa määräystenmukaisuuteen liittyviä toimenpiteitä esimerkiksi automaation muodossa, jolloin ylläpitäjien raporttien luominen helpottuu. Määräystenmukaisuuden toteutumisen seuranta helpottaa myös pilvihallinnan alustan mahdollisesti tarjoama reaaliaikainen tieto hybridipilven toiminnasta. (Dimensional Research 2016, 4.)

Yritysjohto tarvitsee kulujen läpinäkyvyyttä tehdäkseen liiketoiminnan kannalta parempia päätöksiä. Jos yritys tarjoaa asiakkailleen hybridipilvessä olevia palveluita ja sovelluksia,



ovat näiden kehitykseen, käyttöönottoon ja ylläpitoon liittyvät kustannukset päätöksen kannalta oleellisia. Lisäksi palvelun tai sovelluksen arvioitu positiivinen vaikutus yrityksen liiketoimintaan vaikuttaa yritysjohton päätöksiin, ja sitä kautta koko yrityksen toimintaan. Yrityksen palveluiden ja sovellusten kehittäjien tulee keskittää voimavaransa sellaisiin projekteihin, jotka tarjoavat asiakkaille parhaan mahdollisen arvon kustannustehokkaasti. Yksityiskohtaisen tiedon tarjoaminen tuoton tai tappion laskemiseksi on ylläpitäjien vastuulla, mikä lisää tarvetta kokonaisvaltaiselle pilvihallinnan alustalle. Yritysjohton asettamien vaatimusten ja kustannusrajojen perusteella ylläpitäjät voivat tehdä perusteltuja päätöksiä uusien palveluiden ja sovellusten sijoittamisesta. Esimerkiksi sovelluksen kustannusten perusteella voidaan pohtia organisaation yksityisen pilven tai useiden eri julkisten pilvien soveltuvuutta sovelluksen sijoituskohteeksi. (Dimensional Research 2016, 4-5.)

Hybridipilvessä olevien palveluiden ja sovellusten suorituskyvyn yhteydessä puhutaan palvelutasosopimuksista. Palvelutasosopimuksien lisäksi on tärkeää mitata, seurata ja raportoida käyttäjäkokemuksia, kuten sovelluksen käytettävyyttä ja suorituskykyä asiakkaan näkökulmasta. Palvelutasosopimusten ja käyttäjäkokemusten perusteella ylläpitäjät saavat paremman kokonaiskuvan ympäristön toiminnasta ja voivat täten ongelmatilanteissa priorisoida tiettyjä toimintoja. (Dimensional Research 2016, 5.)

## 3 Red Hat CloudForms

### 3.1 Yleistä tietoa

CloudForms on Red Hatin asiakkailleen tarjoama maksullinen hallinta-alusta, joka perustuu avoimen lähdekoodin ManageIQ-projektiin. Tuotteen päätavoitteena on yksinkertaistaa monimutkaisten IT-ympäristöjen hallintaa. CloudForms optimoi virtuaalisten ympäristöjen ja pilvien toimintaa tarjoamalla resurssien hallintaan ja kapasiteetin suunnitteluun liittyviä ominaisuuksia. CloudForms pyrkii myös parantamaan kokonaisvaltaista näkyvyyttä kaikkiin organisaation hallinnassa oleviin ympäristöihin antamalla ylläpitäjille tietoa tapahtumista, resurssien käytöstä ja suorituskyvystä. (Red Hat 2017c.)

Alun perin CloudForms 1.0 oli Red Hatin tuotekokonaisuus, jonka osakokonaisuuksia olivat CloudForms System Engine, CloudForms Cloud Engine ja CloudForms Config Server. Vuonna 2013 Red Hat osti kokonaisuudessaan yksityisyrittäjänä toimineen ManageIQ:n ja päätti CloudFormsin seuraavan version perustuvan ManageIQ:n kehittämään Enterprise Virtualization Manageriin. Tämän seurauksena alkuperäisen CloudFormsin osakokonaisuuksien kehittäminen lopetettiin, ja uuden version ytimenä toimiva Enterprise Virtualization Manager uudelleennimettiin CloudForms Management Engineksi. ManageIQ:n hankkimisen jälkeen Red Hat muodosti avoimen lähdekoodin ManageIQ-projektin, jota varten tehty kehitystyö toimii CloudFormsin perustana. ManageIQ:n luomiseen on käytetty Ruby-ohjelmointikieltä ja sen alustana toimii Ruby on Rails. (McGowan 2016, 10.)

Aikaisemmin CloudForms oli hallinta-alusta perinteisille virtualisointiympäristöille ja IaaS-mallin pilvipalveluille. Version 4.0 myötä saapui tuki myös Docker-konteille kuten Red Hatin PaaS-mallin OpenShift Enterprise tuotteelle. Uusimmat versiot pystyvät perinteisistä virtualisointiympäristöistä hallitsemaan muun muassa VMware vCenteriä, yksityisistä pilvistä OpenStackiä sekä julkisista pilvistä Amazon Web Servicesiä ja Microsoft Azurea. Jokaista pilveä, konttia tai virtualisointiympäristöä hallitaan käyttäen modulaarista alikomponenttia, josta käytetään nimitystä provider. Tämä alikomponentti sisältää toiminnallisuudet yhteyden muodostamiseen sitä vastaavaan pilvi- tai infrastruktuurialustaan ja alustan monitorointiin. Alustan ja providerin välisessä kommunikaatiossa käytetään alustan hallintaan tarkoitettua ohjelmointirajapintaa. (McGowan 2016, 3-5.)

### 3.2 Ominaisuudet

CloudFormsin pääominaisuudet voidaan jakaa neljään eri ryhmään: tiedon tarjoaminen, hallinta, automaatio ja integraatio. Yksi tuotteen päätavoitteista on tarjota ylläpitäjille yksityiskohtaista tietoa hallittavista ympäristöistä, jotta ylläpitoa voidaan suorittaa mahdollisimman tehokkaasti. CloudForms aloittaa tiedon keräämisen välittömästi, kun uusi provider liitetään ympäristöön. Esimerkiksi vCenterin tapauksessa vastaava provider kerää ja ylläpitää tietoa klustereista, tallennuskapasiteetista, virtuaalikoneista ja kaikkien ympäristön objektien välisistä suhteista. Providerista riippuen kerättyyn tietoon saattaa sisältyä myös reaaliaikaista tietoa suorituskyvystä tai tietoa suorituskyvystä jopa edeltävältä ajalta. Reaaliaikaista suorituskvytietoa ja tietoa virtuaalikoneiden toiminnoista käytetään esimerkiksi asiakkaiden laskutuksessa. (McGowan 2016, 7-8.)

CloudFormsin avulla ylläpitäjät saavat myös yksityiskohtaisempaa tietoa käyttämällä toimintoa nimeltään SmartState-analyysi. SmartState-analyysi suoritetaan yksittäiselle virtuaalikoneelle, instanssille, templatelle tai kontille ilman asennettavaa agenttia, jolloin kohteen taustalla oleva näköistiedosto skannataan. Esimerkiksi Windows-koneilta analyysin avulla voidaan saada tietoon käyttäjät, ryhmät, asennetut korjaustiedostot, sovellukset, Win32 palvelut, kernel ajurit, tiedostojärjestelmän ajurit, osa system 32 tiedostoista ja muutamia rekisteritietoja. Tietojen keräämiseen vaikuttaa käytettävä profiili, jota muokkaamalla voidaan määrittää mitä tietoja halutaan hakea. Ylläpitäjät voivat käyttää kerättyä tietoa virtuaalikoneiden ongelmatilanteiden ratkaisussa. (McGowan 2016, 8.)

Liitetyn providerin resursseihin, kuten hosteihin, klustereihin ja virtuaalikoneisiin, voidaan CloudFormsin web-käyttöliitymän kautta liittää tunnisteita. Tunnisteiden avulla resurssit voidaan jakaa organisaation kannalta loogisiin ryhmiin. Yhdessä käyttäjähallinnan kanssa tunnisteita voidaan käyttää hallitsemaan resurssien näkyvyyttä organisaation osastoille, käyttäjäryhmille tai jopa yksittäisille käyttäjille. Esimerkiksi käyttäjäryhmän tapauksessa ylläpitäjä luo ryhmälle tunnusteen, joka liitetään ainoastaan niihin resursseihin, jotka halutaan näyttää kyseiselle ryhmälle. (McGowan 2016, 8.)

CloudFormsin hallinnallisia ominaisuuksia voidaan käyttää käytänteiden (policy) muodossa. Ylläpitäjien käytettävissä on control-, compliance- ja alert-käytänteitä. Control-käytänteillä suoritetaan ylläpitäjän määrittelemä toiminto tietyn tapahtuman jälkeen tietylle joukolle kohteita. Compliance-käytänteet vastaavat rakenteeltaan ja ominaisuuksiltaan pitkälti control-käytänteitä. Ne on kuitenkin suunniteltu puhtaasti ympäristön tietosuojan varmistamiseen. Compliance-käytänteellä voidaan vahvistaa, että CloudFormsin alaisu-

nessa olevat virtuaalikoneet noudattavat organisaation tietoturvalle asettamia vaatimuksia. Tämä tapahtuu keräämällä ja käymällä läpi konfiguraatitiedostojen tietoja. Virtuaalikoneiden asetuksista voidaan esimerkiksi tarkistaa, onko SELinux otettu pois käytöstä. Compliance-käytänteet voidaan control-käytänteiden tavoin suorittaa automaattisesti, jonka jälkeen kohteena olevien virtuaalikoneiden statukset muuttuvat riippuen siitä, ovatko ne läpäisseet käytänteelle asetetut testit. Käytänteen suorittamisen jälkeen ylläpitäjä näkee web-käyttöliittymästä välittömästi virtuaalikoneet, joiden status on ”noncompliant”. Alert-käytänteiden toiminta perustuu CloudFormsin reaaliajassa keräämään tietoon, jonka perusteella ylläpitäjät voivat saada hälytyksiä sähköpostiinsa. Alert-käytänteeseen määritetään mitä tarkkaillaan, mihin sähköpostiosoitteeseen hälytykset lähetetään, mitä lisätietoja hälytyksiin laitetaan mukaan ja kuinka usein hälytyksiä lähetetään. Alert-käytänteitä voidaan laittaa tarkkailemaan esimerkiksi palveluiden kannalta kriittisiä virtuaalikoneita. Kriittisten virtuaalikoneiden poikkeuksellisen korkea resurssien käyttö voi vaikuttaa palvelun toimintaan negatiivisesti, joten ylläpitäjät voivat reagoida tilanteeseen nopeasti saadessaan hälytyksen automaattisesti. (McGowan 2016, 8-9.)

Ruby-ohjelmointikielellä suoritettava automaatio on CloudFormsin ominaisuus, jonka avulla ylläpitäjät voivat vaikuttaa moniin asioihin. Web-käyttöliittymän kautta tehtävät toiminnot, kuten virtuaalikoneiden luominen, perustuvat valmiiksi luotuihin Ruby-komentosarjoihin. Nämä komentosarjat ovat ylläpitäjien nähtävissä ja muokattavissa web-käyttöliittymässä. Ylläpitäjät voivat myös luoda täysin omia komentosarjojaan, jotka toimivat taustalla web-käyttöliittymään kirjautuneiden käyttäjien tietämättä. Käyttäjien tekemille virtuaalikoneille voidaan esimerkiksi asettaa automaattisesti jokin tunniste. Ylläpitäjät pystyvät luomaan web-käyttöliittymään painikkeita, jotka avaavat valintaikkunoita. Valintaikkuna voivat sisältää tekstikenttiä ja vaikka alasvetovalikoita. Käyttäjien syöttämiä tietoja ja valintoja on mahdollista käyttää automaation Ruby-komentosarjoissa. (McGowan 2016, 9.)

Integraation avulla CloudForms pystyy liittymään moniin työkaluihin ja järjestelmiin. Automaation komentosarjat voivat keskustella RESTful- ja SOAP-ohjelmointirajapintojen kanssa. Myös PowerShell-komentosarjojen ajaminen etänä Windows-palvelimilla on mahdollista. Yksi esimerkki integraatiosta on tilanne, jossa luoduille virtuaalikoneille halutaan hakea IP-osoitteet organisaation omasta IP-osoitteiden hallintaratkaisusta (IPAM). (McGowan 2016, 9-10.)

### 3.3 Red Hat CloudForms Management Engine

Red Hat CloudForms jaetaan asiakkaille virtuaalikoneen levykuvana, jota käytetään CloudForms-virtuaalikoneen tekemiseen haluttuun ympäristöön. Virtuaalikoneesta käytetään nimitystä CloudForms Management Engine, mutta siihen viitataan usein applianceen nimellä käytännöllisyyden vuoksi. Käytännössä CloudForms ladataan Red Hatin sivuilta OVA-tiedostona. Tässä opinnäytetyössä käytetyn Red Hat CloudFormsin versio 4.2 voidaan asentaa seuraaviin ympäristöihin: Red Hat Enterprise Virtualization, VMware vSphere, Red Hat Enterprise Linux OpenStack Platform, Amazon Elastic Compute Cloud, OpenShift Container Platform, Google Compute Engine ja Microsoft Azure. CloudForms 4.2 oli tämän opinnäytetyön käytännön osuuden tekemisen aikana uusin versio, ja uudempi versio 4.5 tuli saataville toukokuussa 2017. Version 4.2 virtuaalikoneen käyttöjärjestelmänä on Red Hat Enterprise Linux 7.3 ja käytettävänä tietokantana on PostgreSQL 9.4. CloudForms 4.2:n Management Enginen versio on 5.7. (McGowan 2016, 10; Red Hat 2017b; Red Hat 2017e.)

### 3.4 Vaatimukset

Red Hat CloudForms appliance tarvitsee vähintään seuraavat resurssit:

- 4 virtuaalista prosessoria
- 8 gigatavua keskusmuistia
- 44 gigatavua levytilaa, ja tietokantakoneelle ylimääräinen levy tietokantaa varten (Red Hat 2017a.)

CloudForms tarvitsee toimiakseen tietokannan, josta käytetään nimitystä Virtual Management Database (VMDB). CloudForms ympäristö voi sisältää useita appliance-koneita, ja tietokanta sijaitsee yleensä sillä apiancella, joka on asetettu ja konfiguroitu tietokantakoneeksi. CloudFormsin alaisuudessa olevista ympäristöistä kerätty tieto tallennetaan tietokantaan. Tietokannan levyn kokoon vaikuttaa neljä asiaa, joita voidaan käyttää levyn kokoa arvioitaessa. Tärkein kokoon vaikuttava tekijä on virtuaalikoneiden yhteenlaskettu määrä. Toinen tekijä on CloudFormsiin liitettyjen pilvi- ja virtualisointiympäristöjen isäntäkoneiden (hosts) määrä. Kolmas tekijä on providerin tai isäntäkoneen perspektiivistä näkyvät yksittäiset tiedon tallennukseen käytettävät elementit, joilla ei kuitenkaan tarkoiteta yksittäisiä virtuaalisia levyjä. Viimeinen vaikuttava tekijä on providereilta kerätyn tiedon

määrä. Providereilla sijaitsevilta instansseilta ja virtuaalikoneilta tietyin väliajoin kerättävät kapasiteetti- ja käyttöastetiedot kasvattavat tietokannan kokoa, mutta tiedon kerääminen ei ole oletuksena päällä. Jos tiedon kerääminen otetaan käyttöön, tulee tietokannan kokoa arvioitaessa ottaa huomioon instanssien yhteenlaskettu määrä ja kerättyjen tietojen tallennusaika. Taulukkoon 1 on koottu esimerkkejä tietokannan koosta yhden ja kahden vuoden jälkeen eri kokoisissa ympäristöissä. Kuvaa voi käyttää apuna tietokannan koon arvioinnissa, mutta siinä ei ole otettu huomioon instanssien kapasiteetti- ja käyttöastetietojen keräämistä. (Red Hat 2017a.)

Virtual Machine Count	Host Count	Storage Count	Estimated VMDB Size in GB	
			1 year	2 year
100	5	50	3.5	5
500	10	100	17	25
5000	50	500	173	251

Taulukko 1. Esimerkkejä CloudFormsin tietokannan koosta eri kokoisissa ympäristöissä (Red Hat 2017a).

CloudForms apliancen asetusten muuttaminen, providereiden liittäminen, automaation tekeminen, monitorointi ja esimerkiksi käyttäjähallinta onnistuvat CloudFormsin web-käyttöliittymässä. Tuettuja selaimia ovat Mozilla Firefox, Internet Explorer ja Google Chrome (Red Hat 2017a).

### 3.5 Ympäristön suunnittelu

CloudForms-ympäristö voidaan jakaa eri alueisiin (regions). Alueisiin jakaminen on aiheellista, jos CloudForms-ekosysteemi on jakautunut maantieteellisesti eri alueille. Tällöin jokainen alue suorittaa tiedon keräämistä hallittavista ympäristöistä itsenäisesti, eikä verkon välityksellä. Jokainen alue on kuvattu VMDB:ssä omana tietokantanaan ja niillä jokaisella on oma ID. Jokaisella alueella on myös oma appliance, joka on asetettu keräämään tietoa ja ylläpitämään tietokantaa. Usean alueen kokonaisuudessa voidaan luoda niin sanottu master-alue. Muilla alueilla olevat tietokanta-apliancet asetetaan replikoimaan keräämänsä tieto master-alueen tietokantaan, jolloin koko CloudForms-ekosysteemistä kerätty tieto kootaan yhteen. Yhteen tietokantaan kerätyn tiedon ansiosta master-alueen apliancella voidaan tehdä raportteja ja kuvaajia koko CloudForms-ekosysteemiin liittyen. Master-tietokannan tietoja ei tulisi muuttaa käsin, eikä sitä voi käyttää SmartState-analyyysien suorittamiseen tai kapasiteetti- ja käyttötietojen keräämiseen. Master apliancella on kuitenkin mahdollisuus suorittaa ylläpidollisia tehtäviä kaikille siihen liitettyissä alueissa

oleville virtuaalikoneille ja instansseille, kuten esimerkiksi virtuaalikoneiden sammuttaminen. Yksittäiset alueet voidaan edelleen jakaa pienempiin alueisiin (zones), joita käytetään verkkoliikenteen jakamiseen ja korkeaan käytettävyyteen. Jokainen pienempi alue sisältää joukon applianceja, jotka ovat erikoistuneet tiedon keräämiseen providereilta. (Red Hat 2017a.)

Red Hat CloudForms applianceet voidaan määrittää suorittamaan eri tehtäviä; tietokanta-, worker- tai ui-kone. Worker-koneet keräävät tietoa providereilta ja hallitsevat niitä tietokantakoneiden sijasta. Ui-koneita voidaan tehdä tarvittaessa, jos web-käyttöliittymään kirjautuvien ylläpitäjien ja käyttäjien määrä on suuri. Appliance-koneiden tehtävät ja suhteet määrää ylläpitäjä muuttamalla koneiden tietokanta-asetuksia ja koneiden rooleja. Tietokanta-asetuksia muutetaan applianceen konfiguroinnin yhteydessä kyseisen virtuaalikoneen komentorivillä, ja koneen rooleja muutetaan web-käyttöliittymän kautta. Jokainen alue sisältää yhden tietokantakoneen. Master-alue koostuu ainoastaan tietokantakoneesta ja mahdollisista siihen liitetyistä ui-koneista. Muut alueet voivat sisältää tietokantakoneen ja ui-koneiden lisäksi useisiin pienempiin alueisiin (zones) jakautuneita worker-koneita. (Red Hat 2017a.)

CloudFormsia voidaan testiympäristössä käyttää yhdellä applianceella. Tuotantoympäristö koostuu minimissään tietokanta-, worker- ja ui-koneesta. Tuotantoympäristö voidaankin rakentaa näiden kolmen koneen varaan, jos CloudForms asennetaan vain yhteen datakeskukseen, hallittavia providereita on vain yksi ja web-käyttöliittymään kirjautuvien henkilöiden määrä on pieni. Ui- ja worker-koneita voidaan tarvittaessa lisätä jälkikäteen, sillä uudet koneet voidaan konfiguroida liittymään olemassa olevan tietokantakoneen ylläpitämään regioniin. Regioniin liittymisen lisäksi uuden koneen pitää hakea CloudForms-ympäristön ensimmäisellä tietokantakoneella luotu salausavain. Uusi kone toimii regioniin liittämisen ja salausavaimen hakemisen jälkeen osana kokonaisuutta. Jos CloudForms-ympäristö halutaan laajentaa toiseen datakeskukseen, tehdään normaalisti uusi region kaikkine appliance koneineen. Uuden regionin liittäminen olemassa olevaan regioniin tapahtuu hakemalla kaikilla uusilla applianceilla ensimmäisellä tietokantakoneella luotu salausavain, ja määrittämällä uuden regionin tietokantakone replikoimaan tietonsa master regionin tietokantakoneelle. Maantieteellisen jakautumisen lisäksi tehtävien appliance koneiden määrään vaikuttaa korkea käytettävyyys. Korkean käytettävyyden klusteri koostuu minimissään kahdesta tietokantakoneesta ja kahdesta normaalista appliancesta. Tietokantakoneista toinen on ensisijainen tietokantakone, joka replikoi tietonsa toissijaiselle tietokantakoneelle. Kahta normaalia appliancea käytetään tietokantakoneiden hallintaan, koska korkean käytettävyyden klusterin tietokantakoneita ei voi hallita web-käyttöliittymän

kautta. Klusterin ansiosta ensisijaisen tietokantakoneen ongelmatilanteet eivät vaikuta ympäristön käytettävyyteen, vaan toissijainen tietokantakone havaitsee ongelmat ja ottaa ensisijaisen koneen tehtävät hoitaakseen automaattisesti.

CloudForms-ympäristön laajuus ja täten käytettävien appliance-koneiden määrä riippuu yrityksen tarpeista. Ennen ympäristön pystyttämistä voidaan pohtia muun muassa seuraavia kysymyksiä:

- Jakautuuko pystytettävä ympäristö maantieteellisesti eri alueille?
- Kuinka paljon käyttäjiä palvelulla tulee olemaan? Tätä tietoa voidaan käyttää, kun päätetään käytettävien ui-koneiden määrä.
- Kuinka monta eri provideria halutaan liittää pystytettyyn ympäristöön? Jokaista provideria kohden tulee olla vähintään yksi worker-kone, mutta koneita saattaa olla tarpeen mukaan jopa neljä.
- Halutaanko pystyttää korkean käytettävyyden klusteri?
- Käytetäänkö ympäristön tietokantakoneina ainoastaan appliance-koneita vai myös ulkoista tietokantaa?
- Varaudutaanko ympäristön laajenemiseen ja käyttäjämäärien kasvamiseen tekeillä ennakkoon ylimääräisiä applianceja?



## 4 Asennus vSphereen

### 4.1 Asennusympäristön kuvaus

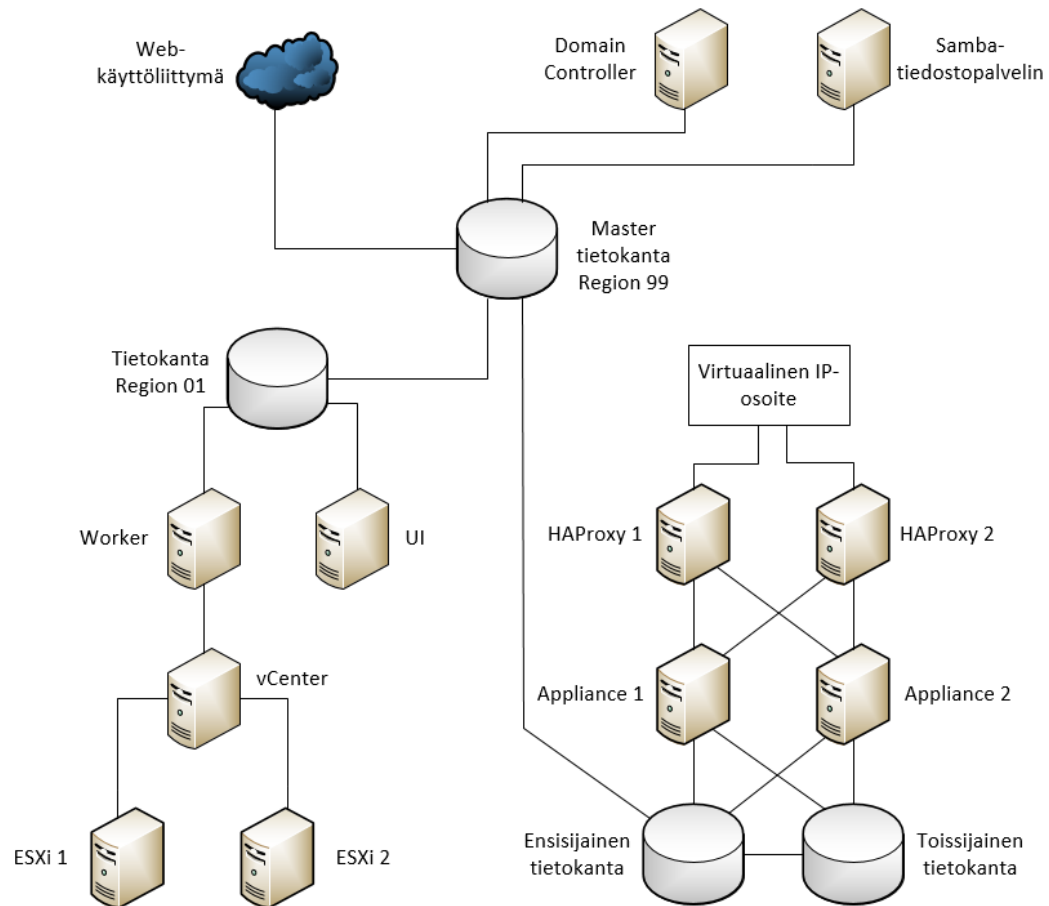
Käytännön osuudessa Red Hat CloudForms asennettiin Kajaanin ammattikorkeakoulun tietojärjestelmälaboratorion VMware-virtualisointiympäristöön, joka koostuu useista ESXi-virtualisointialustoista. Virtuaalikoneiden asentaminen suoritettiin VMware vSphere Clientin kautta. Asennus tehtiin VMware-virtualisointiympäristöön, sillä CloudForms toimii kaikissa tuetuissa asennusympäristöissä samalla tavalla, ja opintojen aikana tutuksi tullut virtualisointiympäristö pystyi tarjoamaan tarvittavat resurssit CloudFormsin virtuaalikoneille. Asennusympäristön sijainti voi olla merkityksellinen esimerkiksi tilanteessa, jossa CloudFormsin halutaan suorittavan skannaus ylläpidettävien ympäristöjen liittämiseksi automaattisesti hallintaan.

Asennettuun ympäristöön tehtiin kaksi aluetta ja korkean käytettävyyden klusteri. Ensimmäiseksi luodulle alueelle annettiin Red Hatin suositusten mukaan ID 99. Luotu alue koostui ainoastaan master-tietokantakoneesta. Toisen alueen ID:ksi annettiin 01 ja luotuun alueeseen yhdistettiin ui ja worker applianceet. Worker applianceen yhdistettiin yksi vCenter provider, joka hallitsi kahta ESXi-virtualisointialustaa.

Korkean käytettävyyden klusteri koostui kahdesta Red Hat Enterprise Linux 7.3.0 -välityspalvelimesta, kahdesta tietokantakoneiden hallintaan käytettävästä CloudForms-virtuaalikoneesta ja kahdesta CloudForms-tietokantakoneesta. Välityspalvelimista toinen oli aktiivisessa tilassa ja toinen valmiustilassa ensimmäisen välityspalvelimen ongelmien varalta. Aktiivinen välityspalvelin välitti virtuaalisen IP-osoitteen kautta tapahtuneet kirjautumiset web-käyttöliittymään molemmille applianceille. Hallintaan käytetyt applianceet kommunikoivat ensisijaisen tietokantakoneen kanssa, joka puolestaan replikoi kaikki tietonsa valmiudessa olevalle tietokantakoneelle. Klusterin applianceille liitettiin myöhemmin yksi vCenter provider. Korkean käytettävyyden klusterin ja vCenterin hallinta onnistuivat ainoastaan virtuaalisen IP-osoitteen kautta. Region 01:llä sijainneen ui applianceen kautta kirjautumalla pystyi vaikuttamaan ainoastaan kyseisen regionin toimintaan. Web-käyttöliittymään kirjautuminen master-tietokantakoneen IP-osoitteella antoi puolestaan kokonaisvaltaisen kuvan koko ympäristöstä.

Active Directoryn käyttäjien ja ryhmien tuomista CloudFormsiin testattiin käyttäjähallintaan liittyen. Tätä varten tehtiin yksi Windows Server 2012 R2 Domain Controller. Lisäksi

master tietokannan varmuuskopioimista varten pystytettiin Samba-tiedostopalvelin. Kuvassa 3 nähdään kaikkien virtuaalikoneiden väliset suhteet testiympäristössä.



Kuva 3. CloudForms-ympäristöä varten asennetut virtuaalikoneet ja niiden väliset suhteet.

## 4.2 Asennusprosessi

Kaikki ympäristön CloudForms apliancet tehtiin samasta OVA-tiedostosta vSphere clientin "Deploy OVF Template" -toiminnolla. Jokaiselle apliancelle määritettiin teon yhteydessä nimi, resource pool ja käytettävä levy. Ainoana poikkeuksena olivat tietokantakoneet, joille tuli määrittää ylimääräinen levy CloudFormsin tietokantaa varten. Domain Controller tehtiin asentamalla Windows Server 2012 R2 ja määrittämällä sille Active Di-

rectory Domain Services- ja DNS Server -roolit. Samba-tiedostopalvelin tehtiin asentamalla Samba Ubuntu 16.04 -palvelimeen. Korkean käytettävyyden klusteri on oma kokonaisuutensa, jonka tekemiseen löytyy ohjeet seuraavan linkin takaa:

[https://access.redhat.com/documentation/en-us/red\\_hat\\_cloudforms/4.2/html-single/configuring\\_high\\_availability/](https://access.redhat.com/documentation/en-us/red_hat_cloudforms/4.2/html-single/configuring_high_availability/)

Appliance-koneiden luomisen jälkeen suoritettiin niiden konfigurointi. Konfiguroinnissa käytettiin hyödyksi konsolia, johon päästiin käsiksi virtuaalikoneen komentoriviltä. Konsoli näytti appliance-asetukset ja listan asetuksista, joita voidaan muokata. Master-tietokantakoneen konfiguroinnin ensimmäisenä vaiheena oli uuden salausavaimen luominen, jonka muut appliance-asetukset tarvitsevat liittyäkseen osaksi ympäristöä. Tämän jälkeen luotiin uusi sisäinen tietokanta (internal database) ylimääräiselle levyille, määritettiin regionin ID ja asetettiin tietokannalle salasana. Tietokannalle määritetyn levyn tuli olla täysin tyhjä, sillä muuten asennus epäonnistui. Jos käytetään ulkoista tietokantaa (external database), tulee kiinnittää huomiota tietokannan määrittämisessä käytettävään konfiguraatitiedostoon. Ongelmien välttämiseksi Red Hat suosittelee käytettävän ulkoisissa tietokannoissa pohjana CloudForms appliance-asetuksia käyttävää standardia postgresql.conf-tiedostoa. Postgresql.conf-tiedoston asetukset tulee määrittää omaan ympäristöön sopivaksi. Esimerkiksi otettaessa huomioon tietokantainstanssiin yhteyden ottavien appliance-koneiden lukumäärää voi olla hyvä muuttaa konfiguraatitiedoston "max\_connections" -asetusta. Koska postgresql.conf kontrolloi kaikkien tietokantojen toimintaa yhden PostgreSQL-instanssin hallinnoimana, ei Red Hat CloudFormsin tietokantoja saa sekoittaa muunlaisten tietokantojen kanssa yhden PostgreSQL-instanssin sisällä.

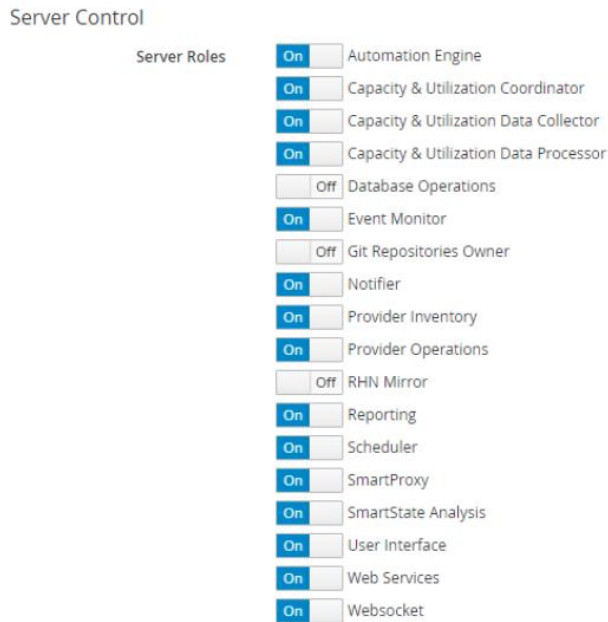
Master-tietokantakoneen minimikonfiguraatioon kuuluivat tietokannan määrittämisen lisäksi myös seuraavat määrittämisasetukset: staattiset verkkoasetukset, fully qualified hostname (FQHN), aikavyöhyke ja aika-asetukset. Konfiguroinnin ja palvelimen prosessien käynnistämisen jälkeen master-tietokantakoneen IP-osoitteella pääsi kirjautumaan web-käyttöliittymään. Kirjautuminen tapahtui oletuskäyttäjätunnuksella admin ja salasanalla smartvm. Web-käyttöliittymässä mentiin kohtaan "Configuration", "Settings:", "CFME Region: Region 99", "Zones", "Zone: Default Zone (current)" ja valittiin palvelimen nimi, jolloin päästiin käsiksi sen hallinta-asetuksiin. Hallinta-asetuksissa palvelimelle määritettiin seuraavat roolit, jotka mahdollistavat raporttien luomisen koko CloudForms-ympäristöstä ja master-koneen hallinnan web-käyttöliittymän kautta: reporting, scheduler, user interface ja web services. Lisäksi tietokannan varmuuskopiointia ja muita ylläpitotoimintoja varten tuli aktivoitaa database operations -rooli. Koneelle asetettavat roolit antavat ylläpitäjille mahdolli-

suuden suorittaa roolien mukaisia toimintoja. Edellä mainitut viisi roolia muodostavat perustan master-tietokantakoneen hallinnalle ja toiminnalle, eikä ylimääräisten roolien aktivoiminen ole yleensä aiheellista. Vaihtoehtoisesti user interface -roolin antamisen sijaan master-tietokantakoneen varten olisi voitu tehdä erillinen ui appliance.

Region 01:n tietokantakoneen konfigurointiprosessi oli sama kuin masterilla lukuun ottamatta seuraavia eroja: ensimmäisenä määritettiin staattiset IP-asetukset, uuden salausavaimen sijaan jo luotu avain haettiin masterilta ja tietokannan luomisen yhteydessä alueen ID:ksi annettiin 01. Roolien osalta valinnan olivat samat, mutta tarvittaessa roolien määrä olisi voitu kasvattaa. Tietyt ominaisuudet, kuten SmartState-analyysi, vaativat ylimääräisiä rooleja. Uuden tietokantakoneen replikointi masterille tapahtui määrittämällä master-tietokantakoneen global copyksi ja toinen kone remote copyksi. Remote copy määritettiin menemällä web-käyttöliittymässä kohtaan "Configuration", "Settings", "CFME: Region" ja "Replication". Tyypiksi valittiin remote, jonka jälkeen muutos tallennettiin. Global copylla tehtiin sama, mutta tyypiksi valittiin global. Tämän jälkeen tuli määrittää remote copylla olevan tietokannan nimi (oletuksena vmdb\_production), Host (koneen IP-osoite tai hostname), Username (oletuksena root), Password (tietokannan salasana) ja Port (oletuksena 5432). Lopuksi yhteyden toiminnan pystyi testaamaan, ja tallentamaan asetukset.

Worker-kone tehtiin samalla tavalla kuin region 01:n tietokantakone lukuun ottamatta toisen levyn lisäämistä. Myös koneen konfigurointi oli lähes samanlainen toimenpide, mutta sisäisen tietokannan luomisen sijaan valittiin vaihtoehto "Join Region in External Database". Worker-kone siis liitettiin aikaisemmin luotuun tietokantaan antamalla tietokantakoneen IP-osoite tai hostname, joka tässä tapauksessa oli region 01:n tietokantakone. Worker-koneelle annettujen roolien määrä on yleensä suurin kaikista ympäristön koneista, sillä se kommunikoi suoraan providereiden kanssa ja tarjoaa suurimman joukon toiminnallisuuksia.

Red Hat suosittelee, että database operations-, event monitor-, reporting-, scheduler-, SmartState Analysis-, user interface-, provider inventory-, provider operations- ja web services -roolit on otettu käyttöön vähintään yhdellä palvelimella jokaisen zonen sisällä. Nämä roolit voivat olla esimerkiksi worker-koneella lukuun ottamatta database operations -roolia. Kuvassa 4 on esimerkki worker-koneen rooleista. Valinnaisten kapasiteetti- ja käyttöastetietojen keräämistä varten tuli aktivoida erityiset roolit. Kuvaan on merkitty myös user interface -rooli, joka kuitenkin annettiin testiympäristössä ui-koneelle.



Kuva 4. Esimerkkilista worker apliancelle annetuista rooleista.

Lopuksi regionin asetuksissa laitettiin päälle kapasiteetti- ja käyttöastetietojen kerääminen klustereille ja datastoreille. Kapasiteetti- ja käyttöastetietojen avulla CloudForms pystyy suorittamaan monitorointia, joka voi auttaa arvioimaan datakeskuksessa olevan kapasiteetin riittävyyttä ja vähentämään käyttökatkoksia. Viimeisenä apliancena asennettiin ui-kone, joka eroaa worker-koneesta ainoastaan roolien osalta. Minimissään aktivoitavat roolit ui-koneelle ovat user interface ja web services.

Kaikkien näiden toimenpiteiden jälkeen kaikkien appliance-koneiden tietoturvan tasoa nostettiin seuraavien Red Hatin ohjeiden mukaan:

[https://access.redhat.com/documentation/en-us/red\\_hat\\_cloudforms/4.2/html-single/appliance\\_hardening\\_guide/](https://access.redhat.com/documentation/en-us/red_hat_cloudforms/4.2/html-single/appliance_hardening_guide/)

Jos CloudFormsin web-käyttöliittymän kirjautuminen laitetaan näkyviin julkiseen verkkoon, ei Red Hatin ohje riitä suojaamaan vaarassa olevia koneita. Julkiseen verkkoon näkyvät palvelimet ja tarvittaessa myös muut palvelimet voidaan tehdä redundanteiksi erilaisille hyökkäyksille käyttäen RHEL:lle tai yleisesti Linux-palvelimille tarkoitettuja tietoturvaohjeita. Tietoturvan tason nostamisen lisäksi tuli vielä laittaa päälle master-tietokantakoneen ja korkean käytettävyyden klusterin välinen replikointi, tietokannan ajastettu varmuuskopiointi, valinnainen SmartState-analyysi sekä määrittää vCenter provideriksi.

### 4.3 VCenterin määrittäminen provideriksi

Opinnäytetyön käytännön osuudessa CloudForms-ympäristöön liitettiin yksi vCenter provider. Liitettynä providerina käytettiin pilvipalvelun sijaan perinteistä virtualisointialustaa, sillä vCenter antoi paremmat mahdollisuudet muun muassa liitetyn providerin resurssien ja virtuaalikoneiden verkotuksen tutkimiseen. Lisäksi CloudForms tarjoaa suunnilleen samat ominaisuudet ja toiminnallisuudet providerista riippumatta.

VCenterin liittäminen region 01:een tapahtui kyseisen alueen worker-koneen web-käyttöliittymässä. Web-käyttöliittymässä tuli vasemman reunan valikosta valita "Compute", "Infrastructure", "Providers", "Configuration" ja "Add a New Infrastructure Provider". Tämän jälkeen tuli kuvan 5 mukaan täyttää liitettävän vCenterin tiedot, varmistaa yhteyden toimivuus ja tallentaa lomakkeen tiedot.

[Infrastructure Providers](#) > [Add New Infrastructure Provider](#)

#### Add New Infrastructure Provider

Name	<input type="text" value="vCenter"/>
Type	<input type="text" value="VMware vCenter"/>
Zone	<input type="text" value="default"/>

---

Endpoints

Hostname (or IPv4 or IPv6 address)	<input type="text" value="192.168.204.201"/>
Username	<input type="text" value="administrator@vsphere.local"/>
Password	<input type="password" value="....."/>
Confirm Password	<input type="password" value="....."/>

Validation Required

Kuva 5. VCenterin liittämiseksi CloudFormsin providereiden listaan tarvittavat tiedot.

Tietojen tallentamisen jälkeen vCenter ilmestyi infrastruktuuri-providereiden listaan. Liitetyn ympäristön tiedot haettiin valitsemalla liitetty vCenter provider ja valitsemalla sen konfiguraatioasetuksista "Refresh Relationships and Power States". Tietojen hakeminen edellytti providerin API:n autentikointia. Onnistuneen autentikoinnin jälkeen haettuihin tietoihin sisältyivät muun muassa liitettyjen ESXi hostien yhteenlasketut resurssit, klusterit, datastoret ja virtuaalikoneet. Haetut tiedot ilmestyivät providerin yhteenveto-välilehdelle.

Tämän jälkeen CloudForms alkoi automaattisesti seurata liitetyn providerin tapahtumia ja päivittää ympäristössä tapahtuneet muutokset web-käyttöliittymän arvoihin.

Kaikkien toiminnallisuuksien käyttöön saamiseksi tuli suorittaa vielä vCenterin ESXi hostien autentikointi. Tämä tapahtui valitsemalla vCenter providerin yhteenveto-välilehdellä "Hosts", "Check All", "Configuration" ja "Edit Selected items". Tämän jälkeen annettiin ESXi hostien kirjautumistunnukset, varmistettiin yhteyksien toimivuus ja tallennettiin tehdyt muutokset.

## 5 Red Hat CloudFormsin ominaisuudet

### 5.1 Web-käyttöliittymä ja itsepalveluportaali

CloudFormsin käyttäjille voidaan antaa tilanteesta ja tarpeista riippuen mahdollisuudet kirjautua joko web-käyttöliittymään tai itsepalveluportaaliin. Käyttäjälle näkyvä web-käyttöliittymä on samatyylinen kuin ylläpitäjillä, mutta toiminnallisuuksien määrältään huomattavasti rajoitetumpi. Itsepalveluportaali toimii sillä periaatteella, että ylläpitäjä tekee palveluita (Service Catalog Item) joita käyttäjät voivat tilata portaalissa. Palveluun voi sisältyä yksi tai useampi virtuaalikone. Itsepalveluportaalin hyvänä puolena on, että ylläpitäjällä on täysi valta siihen mitä vaihtoehtoja käyttäjälle näkyy palvelun tilaamisen yhteydessä. Käyttäjälle voidaan antaa esimerkiksi mahdollisuus ainoastaan palvelun nimen muuttamiseen. Tämän lisäksi itsepalveluportaali on käyttöliittymältään hyvin yksinkertainen ja sitä on helppo käyttää. Portaalin hyödyllisyys ei kuitenkaan ole täysin selvää, sillä nämä asiat voidaan saavuttaa myös web-käyttöliittymässä. Ylläpitäjä voi rajata tai lisätä käyttäjän web-käyttöliittymässä näkyvien asioiden määrää sekä muokata virtuaalikoneen luomisdialogissa näkyviä valintoja. Itsepalveluportaalin kautta tehtyjen virtuaalikoneiden prosessoreiden ja muistin määrän muuttaminen ei onnistu jälkikäteen ilman Red Hat Satellite integraatiota.

### 5.2 Virtuaalikoneet

Virtuaalikoneiden tekeminen onnistuu vCenteriin kloonaamalla olemassa olevia koneita tai templatien avulla. Jos halutaan tehdä virtuaalikone esimerkiksi OpenStack-ympäristöön, kyseisen providerin tulee olla liitettynä CloudFormsiin ja sisältää käytettävä template. Virtuaalikoneen tekeminen ISO:sta onnistuu ainoastaan Red Hat Virtualization Manager providerille. Koneiden luominen onnistuu myös asiakkaiden omista templateista, mutta templatien siirtäminen käytettävään virtualisointiympäristöön tulee tapahtua CloudFormsin ylläpitäjän toimesta. Tämän lisäksi templatelle tulee laittaa oikeanlainen tunniste, jotta asiakas näkee sen. Asiakkaat eivät myöskään voi tehdä virtuaalikoneita omista OVA-tiedostoistaan, vaan virtuaalikone pitää tehdä halutulle providerille ylläpitäjän toimesta.

Web-käyttöliittymään kirjautuneet perustason käyttäjät voivat oletusasetuksilla tehdä itsenäisesti ainoastaan yksittäisiä virtuaalikoneita. Jos samalla aikaa luotavia koneita on



enemmän kuin yksi, niiden luominen ei käynnisty ennen ylläpitäjän hyväksyntää. Administrator- ja super administrator -rooleja omaavat ylläpitäjät voivat muokata, poistaa ja kieltää pyyntöjä virtuaalikoneiden tekemiseksi.

Virtuaalikoneiden poistamisen voi suorittaa kahdella tavalla: Laittamalla koneelle LifeCycle-tunnisteryhmässä olevan tunniste nimeltään "Fully retire VM and remove from Provider" tai käyttämällä painiketta "Remove selected items". Tunnistetta käyttämällä kone poistuu kokonaan, ja painikkeella kone siirtyy tilanteesta riippuen archived tai orphaned tilaan. Archived tilassa virtuaalikoneeseen ei ole enää liitettyä hostia eikä datastorea. Orphaned tilassa kone poistuu providerin, kuten vCenterin, listauksesta, mutta sen tiedot säilyvät massamuistissa. Jos halutaan, että käyttäjä ei voi poistaa virtuaalikoneita lopullisesti voidaan käyttäjäryhmän roolia muokkaamalla tämä estää. Käyttäjäryhmän roolin asetuksia muokkaamalla voidaan vaikuttaa kaikkiin asioihin mitä ryhmään kuuluvat käyttäjät voivat tehdä web-käyttöliittymässään. Käytännön osuutta varten tehdyssä ympäristössä ei kuitenkaan tarvinnut estää käyttäjien koneiden poistamista, sillä luotuihin virtuaalikoneisiin kiinnitettiin automaattisesti tunniste. Koneen käyttötiedot ja tunniste kiinniloaika säilyvät tietokannassa, jolloin laskutus oli mahdollista suorittaa jälkikäteen.

Virtuaalikoneiden snapshotien ottaminen ja hallinta onnistuvat CloudFormsin web-käyttöliittymän kautta yhtä hyvin kuin vCenterissä. Testaamisvaiheessa huomattiin, että käyttäjä pystyi tekemään snapshotteja niin paljon kuin käyttäjien virtuaalikoneille varatuilla levyillä riitti tilaa. Tämä toiminta estettiin tekemällä policy, jossa ylläpitäjä pystyi määrittämään käyttäjän snapshotteille maksimimäärän. Snapshottien ottaminen tai näkyminen oltaisiin voitu myös estää kokonaan asiakkaalta.

Oletusasetuksilla käyttäjä voi virtuaalikonetta luodessaan valita muun muassa virtuaalikoneen sijoituspaikan, muistin määrän, prosessorien määrän, verkon, koneen luomisen ajankohdan sekä ajankohdan, jolloin kone poistuu käytöstä. Virtuaalikoneen muistin, prosessoreiden, prosessoriydinten ja levyjen määrää voidaan muokata jälkikäteen. Yksittäisille käyttäjille voidaan määrittää quodat virtuaalikoneiden kaikkiin resursseihin liittyen. Ylläpitäjällä on mahdollisuus muokata virtuaalikoneen tekemisessä käytettävää dialogia, mutta muokkaaminen rajoittuu dialogin välilehtien näkyvyyteen sekä välilehdillä olevien kenttien näkyvyyteen ja arvoihin. Periaatteessa kenttien tyyppiä on myös mahdollista muuttaa eli dialogissa olevasta tekstilaatikosta voidaan tehdä esimerkiksi alasvetovalikko. Tällaisen toteuttaminen vaatii kuitenkin ManageIQ:n mukana tulevien koodien muokkaamista. Tämä voi aiheuttaa ongelmia siinä tapauksessa, jos ManageIQ päivittyy ja muokatut skriptit häviävät.

VCenter providerille tehtävän virtuaalikoneen verkon vaihto onnistuu koneen luomisen yhteydessä, mutta ei jälkeenkään. Käytännössä virtuaalikoneen luomisen yhteydessä näkyvät verkot ovat ESXi hosteihin liitettyjen virtuaalisten kytkimien (vSwitch) ja hajautettujen kytkimien (distributed switch) porttiryhmiä. Myöskään virtuaalikoneiden verkkokorttien lisääminen ja poisto eivät onnistu web-käyttöliittymän kautta.

### 5.3 Virtuaalikoneiden konsoliyhteydet

CloudFormsin versio 4.2 sisältää kaksi tapaa jolla käyttäjät voivat ottaa konsoliyhteyden virtuaalikoneisiinsa: HTML5-konsoli ja Cockpit. VCenterin HTML5-konsolia varten tulee ainostaan määrittää ylläpitäjän web-käyttöliittymässä käytettävän konsolin tyypiksi VNC, määrittää vCenter providerille konsoliyhteyksien portit ja sallia gdbserver ESXi hostien palomuurien asetuksissa. vCenter providerille määritettävät konsoliyhteyksien portit riippuvat yhtäaikaisten yhteyksien määrästä, koska jokainen käyttäjän avaama konsoliyhteys käyttää eri porttia. Alla sadan käyttäjän ympäristössä portit voivat olla esimerkiksi 5800-5900. Gdbserverin salliminen avaa ESXi hostin palomuurin portteja, jotta hostilla oleviin virtuaalikoneisiin voidaan avata konsoliyhteyksiä. HTML5-konsolissa käyttäjän selain ottaa yhteyden CloudForms appliancella olevaan WebSocketiin, jonka jälkeen kommunikointi suoritetaan ESXi:n palomuurin läpi kohdekoneeseen. Cockpitin toiminta vaatii ainostaan, että se on asennettu kohdekoneelle. Se mahdollistaa konsoliyhteyden lisäksi esimerkiksi virtuaalikoneen monitoroinnin ja käynnissä olevien palveluiden hallinnan.

### 5.4 Käyttäjien hallinta

CloudForms-käyttäjiä voidaan tehdä paikallisesti web-käyttöliittymässä tai käyttäjät voidaan hakea LDAP- tai LDAPS-protokollalla Active Directorystä (AD). CloudFormsiin voidaan liittää useita AD-toimialueita käyttämällä Trusted forests -asetusta. Paikallisesti määritettyjen käyttäjien tiedot tallennetaan CloudFormsin tietokantaan. AD:hen määritettyjen käyttäjien ryhmä pitää liittää CloudFormsissa tehtyyn ryhmään, jotta ryhmän jäsenet pääsevät kirjautumaan web-käyttöliittymään. CloudFormsissa tehdyllä ryhmällä tulee olla täysin sama nimi kuin liitettävällä AD:n ryhmällä.

Jokaisella käyttäjällä pitää olla CloudForms-ryhmä ja jokaiselle ryhmälle pitää määrittää CloudForms-rooli sekä tenant. Tenantilla tarkoitetaan tässä yhteydessä organisaatioyk-

sikköä tai projektia, jolle voidaan määrittää rajoituksia ja sääntöjä. Ryhmän rooli määrittelee, mitä ryhmän käyttäjät näkevät web-käyttöliittymässä ja mitä ominaisuuksia he voivat käyttää. Rooleilla voidaan esimerkiksi estää käyttäjiä näkemästä automatisointiin tarkoitettua valikkoa ja ominaisuuksia. Roolilla voidaan myös määrittää näkeekö käyttäjä tenantin sisällä vain käyttäjän omistamat, ryhmän sisäiset vai koko tenantin virtuaalikoneet. CloudFormsin valmiita rooleja ei voi muokata, mutta uusien roolien luominen on mahdollista. Ryhmällä voi olla vain yksi rooli ja yksi tenant, mutta tenantissa voi olla useita ryhmiä. Tenantille voidaan määrittää maksimi quota-arvot virtuaalisten prosessorien lukumäärälle, muistille, tallennuskapasiteetille sekä virtuaalikoneiden ja templatejen lukumäärälle.

Käyttäjien oikeuksia CloudFormsiin liitettyihin resursseihin hallinnoidaan tunnisteiden avulla. Esimerkiksi antamalla virtuaalikoneen templatelle oma tunniste, voidaan rajoittaa templatien näkyvyyttä vain käyttäjille, joilla on omalla käyttäjätulillaan sama tunniste. Tunnisteet periytyvät tenantilta ryhmille ja ryhmiltä käyttäjille. Antamalla templatella oleva tunniste tenantille, saa jokainen tenantin sisällä oleva käyttäjä oikeuden nähdä kyseisen templatien. Tunnisteiden käytössä tulee olla huolellinen, sillä useiden tunnistryhmien kanssa CloudFormsin resurssien näkyvyydestä voi tulla monimutkaista.

Asiakkaiden laskutus voidaan konfiguroida perustumaan tunnisteisiin. Tällöin tunnisteeseen liitetään tietty hinnasto, jolloin tietokantaan alkaa tallentua laskutustietoa kyseisellä tunnisteella merkitystä kohteesta. Eri hinnastojen avulla saadaan määritettyä virtuaalikoneille eri resurssitasoja. Asiakkaita laskutettaessa laskutushinnaston määrittelevän tunnisteen lisäksi laskutuskohteelle on annettava asiakkaalle itselleen luotu asiakas-tunniste. Tällöin laskutustiedosta on helppo eritellä vain se aika, jolloin asiakkaan tunniste on ollut laskutuskohteella, ja sen perusteella kerätä laskutukseen käytettävät tiedot.

## 5.5 Automatisointi

CloudFormsin automaatio-ominaisuus sisältää Ruby-kielellä kirjoitettuja valmiita komentosarjoja, jotka vaikuttavat CloudFormsin toimintaan, kuten virtuaalikoneiden luomisprosessiin. Nämä toimintaan vaikuttavat komentosarjat ovat ylläpitäjien nähtävissä ja muokattavissa. Myös kokonaan omien komentosarjojen tekeminen on mahdollista ja niitä voidaan liittää esimerkiksi web-käyttöliittymän painikkeeseen tai asettaa suoritettavaksi tietyn tapahtuman sattuessa. Valmiiden komentosarjojen toimintaa selittävä dokumentaatio on kuitenkin puutteellista. Tämä tekee niiden muokkaamisesta, ja itse tehtyjen komentosarjojen sovittamisesta vaikeaa. Ruby-kielellä suoritettava automaatio on haasteellista,

mutta voi oikein käytettynä helpottaa ylläpitäjien työtä ja mahdollistaa uusien toiminnallisuuksien tarjoamisen käyttäjille. Esimerkkinä käytännön osuudessa luotiin CloudFormsin web-käyttöliittymään painike, jonka kautta pystyttiin muuttamaan vCenter providerilla olevan virtuaalikoneen levyn kokoa. CloudForms ei oletuksena anna käyttäjien muuttaa virtuaalikoneen levykokoa koneen tekemisen jälkeen, vaan sallii ainoastaan kokonaisten levyjen lisäämisen. Esimerkkitoteutuksessa käyttäjä pystyi syöttämään painikkeen kautta avautuvaan valintaikkunaan virtuaalikoneelleen uuden levykoon tietyltä väliltä. Toiminnan hyväksymisen jälkeen tehty komentosarja käynnisti levykoon kasvattamisen kommunikoimalla vCenterin kanssa. Automaation avulla levykoon kasvattamisesta pystyttiin tekemään uusi toimiva ominaisuus.

Automaattisia toimintoja voidaan suorittaa komentosarjojen lisäksi hallintakäytänteillä (control policy). Hallintakäytänteillä muokataan ja hallitaan CloudFormsin toimintaa eri tapahtumien sattuessa. Uuden käytänteen tekeminen koostuu neljän osan määrittämisestä: laajuus, ehto, tapahtuma ja toimenpide. Hallintakäytänteen laajuus määrittää, mihin kohteisiin kyseinen käytäntö vaikuttaa. Toimenpide voidaan rajoittaa koskemaan esimerkiksi tiettyjä virtuaalikoneita tai tietyllä tunnisteella merkityjä objekteja. Ehdolla voidaan edelleen rajata kohteita joihin käytäntö vaikuttaa. Käytänteeseen ennalta määritetyt tapahtumat käynnistävät ehtojen tarkistamisen, jonka perusteella päätetään toimenpiteen suorittamisesta. Yhteen hallintakäytänteeseen voidaan määrittää useita tapahtumia, ja jokainen tapahtuma voi käynnistää eri toimenpiteen. Yksi tapahtuma voi käynnistää myös useita eri toimenpiteitä, jotka voidaan suorittaa yhtä aikaa tai tietyssä järjestyksessä. Hallintakäytänteistä voidaan tehdä ryhmiä, joita voidaan liittää osaksi CloudFormsin objekteja.

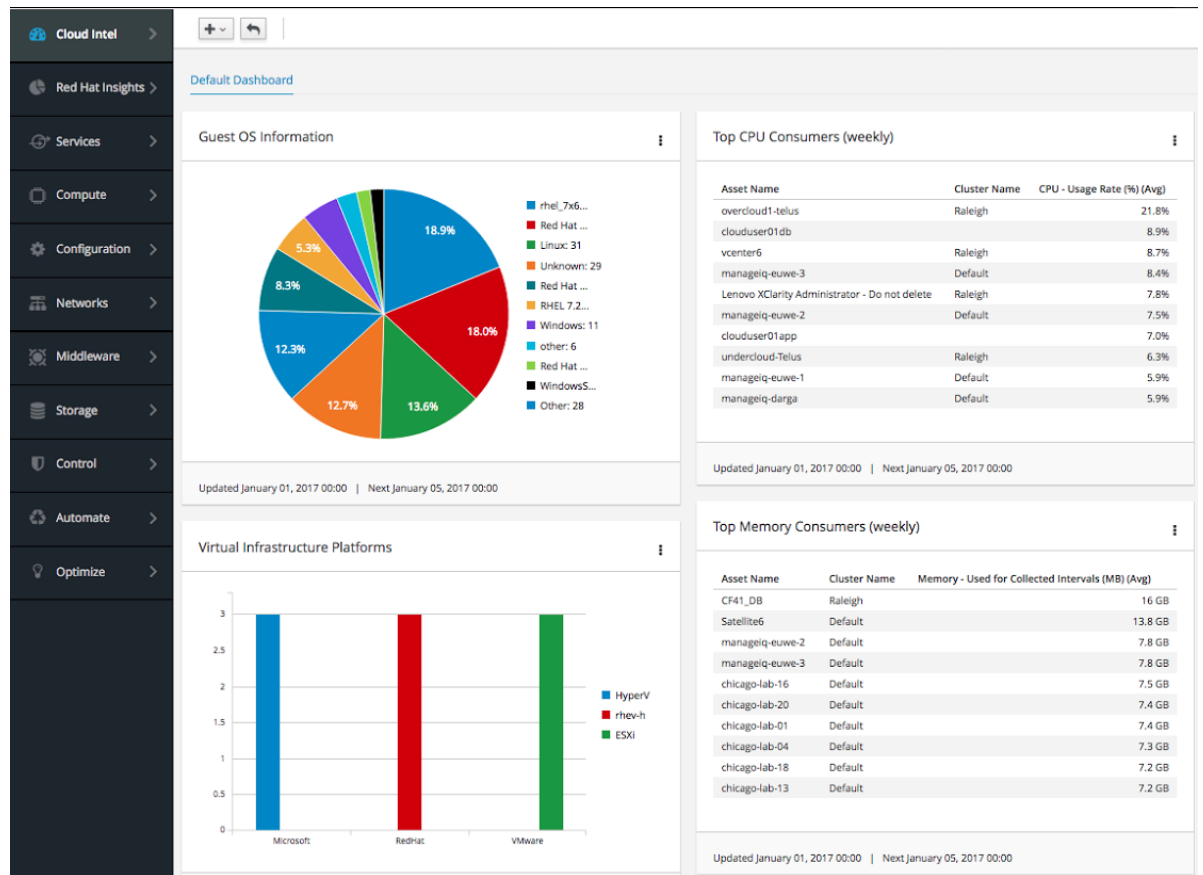
Hallintakäytänteillä myös rajataan käyttäjien toimia. Esimerkiksi käytäntö voidaan rajata koskemaan tietyn käyttäjän virtuaalikoneita, ja näiden virtuaalikoneiden snapshotien suurinta mahdollista määrää. Virtuaalikoneiden snapshotien ottamisen yhteydessä hallintakäytäntö voi tarkistaa aikaisemmin otettujen snapshotien määrän, jota verrataan ylläpitäjän määrittämään arvoon. Vertaamisen perusteella tehdään päätös toiminnan hyväksymisestä tai hylkäämisestä. Hallintakäytänteeseen määritetty toimenpide voi olla myös ylläpitäjän tekemän Ruby-komentosarjan suorittaminen.

Hallintakäytänteiden lisäksi hälytyskäytänteillä (alert policy) on mahdollista lähettää ylläpitäjille hälytyksiä tiettyjen tapahtumien yhteydessä tai asetettujen raja-arvojen ylittyessä. Hälytyksiä voidaan lähettää sähköpostin tai SNMP-protokollan välityksellä. Hälytyksiä voidaan liittää ryhmiin, jotka voidaan määrittää tarkkailemaan koko ympäristöä tai pienempiä kokonaisuuksia. Määräystenmukaisuutta tarkkailevat käytänteet (compliance policy) vas-

taavat rakenteeltaan ja ominaisuuksiltaan hallintakäytänteitä. Niitä voidaan käyttää ympäristön tietosuojan varmistamiseen. Tällaisilla käytänteillä tarkistetaan kohteena olevien objektien määräystenmukaisuutta ja tarvittaessa merkataan objektit, jotka eivät ole läpäisseet testejä.

## 5.6 Raportit

CloudFormsissa voidaan luoda raportteja lukuisista eri tiedoista, kuten esimerkiksi virtuaalikoneiden resurssien käytöstä. Näiden raporttien luonti voidaan suorittaa kerran tietynä ajankohtana tai niitä voidaan generoida joka tunti, päivä, viikko tai kuukausi. Valmiit raportit voidaan myös lähettää sähköpostilla eteenpäin. Ylläpitäjien lisäksi perustason käyttäjät voivat luoda omia raporttejaan. Esimerkiksi asiakkaat voivat luoda raportteja virtuaalikoneidensa kuluista. Raporttien näkyvyyttä ja generointia voidaan estää tai rajoittaa perustason käyttäjiltä niin, että he näkevät vain heille kuuluvaa tietoa raporteissaan. Raporteista voidaan tehdä myös erilaisia kuvaajia, joita voidaan esittää ylläpitäjän tai käyttäjän web-käyttöliittymän etusivulla. Kuvassa 6 on esimerkki ylläpitäjän web-käyttöliittymän etusivusto, joka sisältää raporttien pohjalta luotuja kuvaajia ja taulukoita muun muassa virtuaalikoneiden käyttöjärjestelmien osuuksista ja virtuaalikoneiden muistin käytöstä.



Kuva 6. Ylläpitäjän web-käyttöliittymän etusivun kuvaajia ja taulukoita (Schabell 2017).

## 5.7 Laskutus

CloudFormsin laskutusominaisuudella voidaan luoda hinnastoja prosessorin, keskusmuistin, verkon ja massamuistin käytölle tai käyttäjälle varattujen resurssien määrälle. Resurssien hinnastoihin perustuva laskutus voidaan kohdentaa jopa yksittäiseen käyttäjään käyttäjätunnukselle asetetun tunnisteiden perusteella. Jokaiselle laskutettavalle kohteelle määritetään, miltä aikaväliltä hinta määräytyy. Resurssien käytön laskutus voidaan tehdä tunnin, viikon tai kuukauden perusteella. Prosessorien käytön laskutus perustuu kellotajuuteen, verkon laskutus siirretyn tiedon määrään ja muistin laskutus käytössä olevan muistin määrään. Kaikkien laskutettavien resurssien eri käyttöasteille voidaan määrittää joko kiinteä tai kertoimeen perustuva summa. Asiakas voi virtuaalikoneita tehdessään varata virtuaalikoneen käyttöön tietyn määrän ytimiä ja muistia, jolloin virtuaalikone saa käyttöönsä varatut resurssit myös resurssipulan aikana. Tämäkin voidaan ottaa laskutuksessa

huomioon. Esimerkiksi asiakkaan virtuaalikoneelle varatulle neljälle ensimmäiselle ytimelle voidaan määrittää yhden euron tuntihinta, jonka jälkeen jokaiselle lisäytimelle määritetään täysin omat hintansa.

## 5.8 Tietokannan varmuuskopiointi

CloudForms VMDB:n varmuuskopiointi voidaan suorittaa säännöllisesti tai kerran NFS-jakoon tai Samba-tiedostopalvelimelle. Varmuuskopiointi on mahdollista suorittaa tunneittain, päivittäin, viikoittain tai kuukausittain. Jos käytössä on Samba-tiedostopalvelin, tulee varmuuskopioinnin määrittämisen yhteydessä antaa varmuuskopiolle nimi, tiedostopalvelimelle tehdyn jaetun kansion nimi, jaetun kansion sijainnin kertova URI-tunniste, tiedostopalvelimen käyttäjätunnukset ja varmuuskopioinnin aika-asetukset. NFS-jakoon tehtäessä riittävät ainoastaan varmuuskopion nimi, URI-tunniste ja aika-asetukset.

Tietokannan palauttaminen varmuuskopiosta vaatii, että varmuuskopion tiedosto tallennetaan tietokanta-appliancella kansioon tmp nimellä evm\_db.backup. Palauttaminen suoritetaan kirjautumalla koneelle root-käyttäjänä, pysäyttämällä palvelimen prosessit, suorittamalla tietokannan palauttaminen ja lopuksi käynnistämällä palvelimen prosessit.

## 6 Red Hat CloudFormsin ongelmat

Käytännön osuuden testauksen aikana havaittiin CloudForms version 4.2 toiminnassa muutamia ongelmia. Yksi suurimmista ongelmista liittyy vCenteriin tehtyjen virtuaalikoneiden verkotukseen. Super administrator -käyttäjä näkee virtuaalikonetta tehdessään kaikki VMware-ympäristön virtuaalisten kytkimien ja hajautettujen kytkimien porttiryhmät, jolle voidaan määrittää VMwaren puolella oma virtuaalisen lähiverkon ID. Virtuaalikoneelle tulee valita porttiryhmä, jotta se saa verkkoyhteyden muihin virtuaalikoneisiin ja Internetiin. CloudFormsin perustason käyttäjät eivät oletusasetuksilla näe yhtään porttiryhmää. Yksittäisiin porttiryhmiin ja virtuaalisiin kytkimiin ei ole mahdollista liittää asiakkaiden tunnisteita. Ylläpitäjän web-käyttöliittymässä kokonaisille hajautetuille kytkimille voi liittää tunnisteita, mutta tunnisteeet häviävät web-käyttöliittymästä ohjelmavirheen vuoksi. Liitetyt tunnisteeet kuitenkin toimivat, eikä tunnisteeiden näkymättömyys vaikuta CloudFormsin toimintaan. Porttiryhmät saa käyttäjille näkyväksi myös lisäämällä käyttäjien tunnisteeet ESXi hosteille, jolloin kaikki hosteihin liitettyjen virtuaalisten- ja hajautettujen kytkimien porttiryhmät näkyvät käyttäjille. Kyvyttömyys vaikuttaa täydellisesti virtuaalikoneiden verkotukseen muodostuu ongelmaksi, jos asiakkaiden virtuaalikoneet halutaan ryhmitellä omiin virtuaalisiin lähiverkkoihinsa.

CloudFormsin verkotusongelman voi osittain kiertää virtuaalikoneen luomisen yhteydessä käytettävällä Ruby-komentosarjalla, joka liittää asiakkaan virtuaalikoneet automaattisesti tiettyyn porttiryhmään. Automaation rajoitusten vuoksi tämä ratkaisu toimii vain, jos asiakkaalla on käytössään ainoastaan yksi porttiryhmä. Useiden porttiryhmien tapauksessa virtuaalikoneiden siirrot verkosta toiseen täytyy tehdä VMwaren kautta ylläpitäjän toimesta.

Toinen ongelma liittyy perustason käyttäjien quota-rajoihin. Testeissä käyttäjä pystyi ylittämään hänelle asetettu quota-rajat, mikäli yhtä aikaa tehtäviä virtuaalikoneita oli useita. Quota-rajan tarkistus tapahtuu heti virtuaalikoneen luomisen alussa ja se ei ota huomioon yhtä aikaa tekeillä olevia virtuaalikoneita. Tämän seurauksena käyttäjä voi tehdä kerralla useita virtuaalikoneita, jotka yksittäin tehtynä alittavat asetettu rajat, mutta yhdessä ylittävät ne.

Virtuaalikoneiden laskutusta varten tehdyt raportit laskevat virtuaalikoneiden päälläoloajaksi automaattisesti 24 tuntia, vaikka koneet olisivat olleet päällä vähemmän aikaa. Myös alle vuorokauden käynnissä ollut ja poistettu kone laskutetaan 24 tunnin mukaan. Toinen laskutukseen liittyvä virhe näyttää virtuaalikoneen viikoittaiselle ja kuukausittaiselle laskulle eri summaa, vaikka kone olisi ollut päällä vain muutaman päivän. Nämä



kaksi ongelmaa on kuitenkin korjattu CloudForms Management Enginen versioon 5.8.0.10. (Red Hat 2017f; Red Hat 2017g.)

Yksi suuri ongelma liittyy myös virtuaalikoneiden konsoliyhteyksiin. Kaikilla selaimilla muodostetut konsoliyhteydet virtuaalikoneisiin katkeilevat sattumanvaraisesti. Konsoliyhteyden ongelmat johtuvat Apache-palvelinohjelma. Apachen ongelmien vuoksi käyttäjän selain ei saa yhteyttä CloudForms appliancen WebSocketiin, mikä aiheuttaa yhteyden ajoittaisen vuotamisen. Tällöin yhteys jää auki appliancella, mikä voi suurien käyttäjämäärien tapauksessa aiheuttaa koko web-käyttöliittymän toiminnan loppumisen. Ongelmien vuoksi yhteyden muodostamiseksi uudelleen selainnäkyä pitää päivittää muutaman minuutin välein. Tämä ongelma ratkennee tulevaisuudessa CloudFormsin ja Apachen päivityksen yhteydessä.

## 7 Versiot

CloudFormsin merkittäville versioille tarjotaan julkaisun jälkeen tukea kolmen vuoden ajan. Tämä kolmivuotinen tukijakso jakautuu kahteen vaiheeseen: Production1 ja Production2. Kuvassa 7 on kuvattuna, mihin tukitoimiin asiakkaat ovat oikeutettuja näiden kahden vaiheen aikana (Red Hat 2017d).

Description	Life Cycle Phase	
	Production 1	Production 2
Access to previously released content through the Red Hat Customer Portal	Yes	Yes
Self Help through the Red Hat Customer Portal	Yes	Yes
Technical Support <sup>1</sup>	Unlimited	Unlimited
Asynchronous Security Errata (RHSA)	Yes	Yes
Asynchronous Bug Fix Errata (RHBA) <sup>2</sup>	Yes	Yes
Minor Releases	Yes	No
Software Enhancements	Yes	No

1. Technical Support depends on the service level included in your Red Hat CloudForms subscription agreement.

2. Red Hat may choose, as an intermediate measure, to address serious issues that have an important impact to customer business with a hotfix while a Red Hat Bug Fix Advisory is created and verified.

Kuva 7. CloudFormsin kahden tukivaiheen tiedot (Red Hat 2017d).

Kuvassa 8 esitellään CloudFormsin aikaisempien versioiden aikataulut. Taulukko sisältää versioiden julkaisupäivämäärän sekä päivämäärät tukivaiheiden loppumiselle.

### Life Cycle Dates

Red Hat CloudForms Release	General Availability	End of Production, Phase 1	End of Production, Phase 2
4	December 8, 2015	December 8, 2017	December 1, 2019
3	November 05, 2013	February 28, 2016	February 28, 2017
2**	April 10, 2013	April 10, 2015	April 10, 2016
1	June 06, 2012	August 01, 2013	n/a

Kuva 8. CloudFormsin merkittävien versioiden elinkaarten aikataulut (Red Hat 2017d).

Selkeät suunnitelmat ja aikataulut eri versioiden tukemiselle antavat kuvan, että Red Hat on valmis seisomaan tuotteensa takana ja haluaa tukea asiakkaitaan tuotteen elinkaaren ajan. Aikaisempina vuosina CloudFormsin uusia versioita on julkaistu noin puolen vuoden välein. Uusin merkittävä versio on 4.5, joka julkaistiin toukokuussa 2017. Tähän mennessä uuden version ominaisuuksien esittelyssä on keskitytty parantuneeseen Ansible-integraatioon. Uudessa versiossa Ansiblea voidaan hyödyntää esimerkiksi käyttäjien itsepalveluportaalin playbookeista tehtävien palveluiden muodossa. Playbookeja voidaan hyödyntää myös virtuaalikoneiden automaattiseen konfigurointiin ylläpitäjän määrittämien

käytänteiden mukaisesti. Ansiblen tärkeys tulee varmaan kasvamaan tulevaisuudessa, jotta ylläpitäjillä on entistä paremmat mahdollisuudet suorittaa automaatiota CloudForms-ympäristön toiminnassa. Uusien ominaisuuksien tuominen CloudFormsiin kertoo halusta viedä tuotetta eteenpäin ja tehdä siitä entistä monipuolisempi. Muutenkin tuotteen tulevaisuus näyttää melko hyvältä eikä merkkejä kehityksen loppumisesta ole. (Kernel 2017.)

## 8 Pohdinta

Opinnäytteen päätarkoituksena oli kuvata Red Hat CloudForms ympäristön käyttöönottoprosessi ja ominaisuudet. Lisäksi tavoitteena oli tutkia alustan mahdollisuutta toimia portaalina maksullisten virtuaalikoneiden tilaamisessa. CloudFormsin käyttöönotto suoritettiin onnistuneesti, ja kaikki tärkeimmät ominaisuudet pystyttiin testaamaan. Koska jokaisella IT-organisaatiolla on käytössään oman liiketoiminnan ja vaatimusten kannalta tärkeimmät virtualisointialustat ja pilvipalvelut, CloudForms-ympäristön käyttöönottoprosessi voi olla aina erilainen. Datakeskusten, liitettävien providereiden ja käyttäjien määrät vaikuttavat asennettävien appliance-koneiden määrään. Käytännön osuudessa pystytettyyn ympäristöön pyrittiin kokoamaan kaikki perustoiminnallisuuksien testauksen kannalta oleelliset koneet. Lopullisessa käyttöönottoprosessissa ei ollut suurempia ongelmia lukuun ottamatta virtualisoidun asennusympäristön asettamia haasteita. Asennusprosessi on kuitenkin aina suunniteltava tarkoin, sillä huomioon otettavia asioita on paljon. Red Hatin tarjoama dokumentaatio on melko kattavaa, sillä kyseessä on yrityksen tarjoama maksullinen tuote. Dokumentaatio vaatii kuitenkin perehtymistä, sillä se on sirpaleista eikä välttämättä muodosta yhtä selkeää ohjetta ympäristön käyttöönotolle. Tämän vuoksi ympäristön suunnittelulle ja käyttöönotolle tulee varata runsaasti aikaa. Taidollisesti ympäristön asennus vaatii tietoutta Linux-palvelimista, verkotuksesta, palvelimien tietoturvasta, korkeasta käytettävyydestä ja käyttäjähallinnan tapauksessa Windows-palvelimista.

CloudForms sisältää melko kattavat ominaisuudet ylläpidolle ja automaatiolle. Ominaisuuksien toteutus olisi kuitenkin voinut olla parempi esimerkiksi käyttäjähallinnan tapauksessa. Eniten aikaa vei ominaisuuksien ongelmien selvittäminen. Ongelmien sattua vika yritettiin etsiä ensin omasta ympäristöstä. Yleensä ongelmaksi paljastui kuitenkin CloudFormsin virheellinen toiminta. Red Hatilla on ohjelmavirheiden seuraamiseen tehty Bugzilla-sivusto, josta CloudFormsin ongelmista löysi tietoa ja keskustelua. Tuotteen kaikkia ominaisuuksia ei käyty läpi tässä opinnäytetyössä. Näihin ominaisuuksiin sisältyvät esimerkiksi kapasiteetin suunnittelu ja diagnostiikka.

CloudFormsin versio 4.2 ei sovellu asiakkaille tarjottavien maksullisten virtuaalikoneiden alustaksi johtuen lähinnä laskutuksen ja konsolilyhteyksien virheellisestä toiminnasta. Ongelmista johtuen tuotteen kaikki hyödyt kokonaisvaltaisena hallinta-alustana eivät toteudu. Versio 4.2 soveltuu parhaiten sellaisten organisaatioiden sisäiseen käyttöön, jotka haluavat hallita ja monitoroida useissa eri CloudFormsin tukemissa ympäristöissä sijaitsevia virtuaalikoneitaan.

Paremmen kuvan saamiseksi tuotteesta mahdollisuutena olisi ollut esimerkiksi jonkin pilvipalvelu-providerin liittäminen, tässä opinnäytetyössä mainitsemattomien ominaisuuksien tutkiminen ja tuotteen päivittäminen uuteen versioon. Lisäksi olisi ollut mielenkiintoista verrata Red Hatin CloudFormsia muiden toimijoiden vastaavanlaisiin tuotteisiin.

Ongelmista huolimatta tuotteen käyttöönotto tarjosi yhden näkökulman siihen, millaista monimutkaisten IT-ympäristöjen hallinta voi olla nykypäivänä. Yksi pilvi, virtualisointialusta tai konttiratkaisu ei välttämättä vastaa kaikkiin organisaation johdon, ylläpitäjien ja asiakkaiden vaatimuksiin, minkä vuoksi sekaympäristöt ovat yleisiä. Hallinta-alustojen tuntemisesta voikin olla tällä hetkellä hyötyä työelämän ylläpitotehtävissä. Teoriaosuuden kokoamisen yhteydessä sain uutta tietoa yritysten hybridipilveen siirtymisen voimakkuudesta ja lisääntyneestä luottamuksesta julkisiin pilviin. En ole opiskelujeni aikana tutustunut CloudFormsin kaltaisiin tuotteisiin, joten käyttöönotto oli kokonaisuutena erittäin mielenkiintoista.

## Lähteet

- Amazon.com. What is Cloud Computing? Amazon Web Services:n verkkosivu. Viitattu 12.9.2017. <https://aws.amazon.com/what-is-cloud-computing/>
- Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R. H., Konwinski, A., ... & Zaharia, M. (2009). *Above the clouds: A berkeley view of cloud computing* (Vol. 17). Technical Report UCB/EECS-2009-28, EECS Department, University of California, Berkeley. Viitattu 9.9.2017. <https://www2.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html>
- Brown, E. 2011. Final Version of NIST Cloud Computing Definition Published. National Institute of Standards and Technology 25.10.2011. Viitattu 11.9.2017. <https://www.nist.gov/news-events/news/2011/10/final-version-nist-cloud-computing-definition-published>
- Cloudify. 2017. 2017: State of Enterprise Multi-Cloud. Cloudify:n julkaisema yleiskatsaus. Viitattu 4.10.2017. <http://cloudify.co/2017-state-of-enterprise-multi-cloud-report/>
- Dimensional Research. 2016. Hybrid Clouds: What the business is asking for and IT should be providing. Dimensional Research:n julkaisema tutkimus. Viitattu 17.10.2017. <http://www.melillo.com/Public/Pages/Solutions/pdf/4AA6-6701ENW.pdf>
- Kernel, S. 2017. Red Hat delivers cloud control and insight with Ansible integration. eWeek 3.5.2017. Viitattu 17.11.2017. <http://www.eweek.com/enterprise-apps/red-hat-delivers-cloud-control-and-insight-with-ansible-integration>
- McAfee.com. 2017. Building Trust in a Cloudy Sky. Intel Security:n (nyk. McAfee) julkaisema raportti. Viitattu 4.10.2017. <https://www.mcafee.com/us/solutions/lp/cloud-security-report.html>
- McGowan, P. 2016. *Mastering CloudForms Automation: An Essential Guide for Cloud Administrators*. O'Reilly Media, Inc. Viitattu 25.20.2017. <https://www.safaribooksonline.com/library/view/mastering-cloudforms-automation/9781491957219/>
- Mell, P., & Grance, T. (2011). The NIST definition of cloud computing. National Institute of Standards and Technology syyskuu 2011. Viitattu 11.9.2017. <http://nvl-pubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>

- Red Hat. 2017a. Red Hat CloudForms 4.2 Deployment planning guide. Red Hat:n verkkosivu. Viitattu 25.10.2017. [https://access.redhat.com/documentation/en-us/red\\_hat\\_cloudforms/4.2/html-single/deployment\\_planning\\_guide/](https://access.redhat.com/documentation/en-us/red_hat_cloudforms/4.2/html-single/deployment_planning_guide/)
- Red Hat. 2017b. Red Hat CloudForms 4.2 Support matrix. Red Hat:n verkkosivu. Viitattu 25.10.2017. [https://access.redhat.com/documentation/en-us/red\\_hat\\_cloudforms/4.2/html/support\\_matrix/](https://access.redhat.com/documentation/en-us/red_hat_cloudforms/4.2/html/support_matrix/)
- Red Hat. 2017c. Red Hat CloudForms. Red Hat:n verkkosivu. Viitattu 24.10.2017. <https://www.redhat.com/en/technologies/management/cloudforms>
- Red Hat. 2017d. Red Hat CloudForms Life Cycle. Red Hatin verkkosivu. Viitattu 17.11.2017. <https://access.redhat.com/support/policy/updates/cloudforms>
- Red Hat. 2017e. Product Documentation for Red Hat CloudForms. Red Hat:n verkkosivu. Viitattu 25.10.2017. <https://access.redhat.com/documentation/en/red-hat-cloud-forms?version=4.2/>
- Red Hat. 2017f. Bug 1390773. Red Hatin tuotteissa ilmenneiden ohjelmavirheiden seuraamiseen tarkoitettu sivusto. Viitattu 17.11.2017. [https://bugzilla.redhat.com/show\\_bug.cgi?id=1390773](https://bugzilla.redhat.com/show_bug.cgi?id=1390773)
- Red Hat. 2017g. Bug 1402072. Red Hatin tuotteissa ilmenneiden ohjelmavirheiden seuraamiseen tarkoitettu sivusto. Viitattu 17.11.2017. [https://bugzilla.redhat.com/show\\_bug.cgi?id=1402072](https://bugzilla.redhat.com/show_bug.cgi?id=1402072)
- Schabell, E. 2017. 3 Steps to Cloud Operations Happiness with CloudForms. Viitattu 26.11.2017. <https://www.javacodegeeks.com/2017/01/3-steps-cloud-operations-happiness-cloudforms.html>
- Tietosuojavaltuutetun toimisto. 2015. Pilvipalvelut. Viitattu 26.11.2017. <http://www.tietosuojafi.fi/index/useinkysyttya/pilvipalvelut.html>
- Thorpe, E. 2017. 5 obstacles holding your hybrid cloud strategy back. CloudPro:n julkaisema artikkeli. Viitattu 5.10.2017. <http://www.cloudpro.co.uk/cloud-essentials/hybrid-cloud/7074/5-obstacles-holding-your-hybrid-cloud-strategy-back>
- TSK. 2016. Tietotekniikan termitalkoot: pilvipalvelu; etäresurssipalvelu. Viitattu 9.9.2017. <http://www.tsk.fi/tsk/termitalkoot/>

Walker, G. 2010. Cloud computing fundamentals. A different way to deliver computing resources. IBM 17.12.2010. Viitattu 14.9.2017. <https://www.ibm.com/developer-works/cloud/library/cl-cloudintro/index.html>

Williams, B. 2012. The Economics of Cloud Computing: An Overview For Decision Makers. Cisco 30.7.2012. Viitattu 15.9.2017. <http://www.ciscopress.com/articles/article.asp?p=1925617>