

KEMI-TORNION AMMATTIKORKEAKOULU

Virtualisointi ja pilvipalvelut

Johansson Keijo

Tietotekniikan opinnäytetyö
Ohjelmistosuunnittelu
Insinööri(AMK)

KEMI 2012

TIIVISTELMÄ

Kemi-Tornion ammattikorkeakoulu, Tekniikan ala	
Koulutusohjelma	Tietotekniikka
Opinnäytetyön tekijä	Keijo Johansson
Opinnäytetyön nimi	Virtualisointi ja pilvipalvelut
Työn laji	Opinnäytetyö
päiväys	21.05.2012
sivumäärä	47
Opinnäytetyön ohjaaja	Teppo Aalto

Tämän työn tavoitteena oli perehdyttää lukijaa virtualisoinnin ja pilvipalveluiden perusteisiin. Työssä esitellyt ja käytetyt ohjelmistot ovat avoimen lähdekoodin sovelluksia, joten ne ovat kaikkien käytettävissä ilman hankintamaksuja. Ohjelmistojen lisenssit poikkeavat hiukan toisistaan, joten on suositeltavaa tarkistaa ne kehittäjän kotisivuilta.

Työssä käytiin läpi VDI, eli Virtual Desktop Infrastructure, joka tarkoittaa virtualisoitua työpöytäympäristöä. Käyttäjän tiedot on tallennettu keskitetysti palvelimelle ja niitä hallinnoidaan ja käytetään verkon yli.

Työssä selitettiin tarkemmin myös virtualisoinnissa käytettyä kahta pääperiaatetta, jotka ovat natiivi (native) ja ”isännän alaisuudessa toimiva” (hosted). Natiivin virtualisoinnin avulla ohjelmakoodi voidaan suorittaa suoraan palvelimen prosessorilla. Isännän alaisuudessa vaaditaan virtualisoinnin toimintaan siihen yhteensopiva käyttöjärjestelmä. Valvontaohjelmistojen esittelyyn valittiin kaksi yleisesti käytettyä: KVM, joka on hosted-tyyppinen ja Xen, joka on natiivi. Valvontaohjelmistoista käytetään nimitystä hypervisor.

Pilvipalveluista esiteltiin yhden palvelun tarjoava SaaS-palvelu, palvelu- tai ohjelmistokokonaisuuden tarjoava PaaS-palvelu ja palvelinympäristön tarjoava IaaS-palvelu. Tietoturva-asioissa käytiin läpi asiakkaan ja ylläpitäjän näkökulmasta yleisimmät riskit ja niihin vaikuttavat tekijät. Lopuksi kuvattiin esimerkiasennus Ubuntu IaaS-tyypin UEC-palvelusta.

Asiasanat: pilvipalvelut, virtualisointi, atk-laitteet, tietoturva.

ABSTRACT

Kemi-Tornio University of Applied Sciences, Technology	
Degree Programme	Electrical Engineering
Name	Keijo Johansson
Title	Virtualization and Cloud Services
Type of Study	Bachelor's Thesis
Date	21 May 2012
Pages	47
Instructor	Teppo Aalto

The goal of this work was to brief the reader about the basics of virtualization and cloud services. The software products that are mentioned in this work are open-source software and therefore free and available for everyone. The software licenses are mainly GPLv2 but it is suggested to check them from the developer's website before using.

VDI was also analyzed shortly in this work. VDI stands for Virtual Desktop Infrastructure. It means that the user's data is stored into servers and managed and used via Ethernet.

The two main types of virtualization, native and hosted are also explained. Native means that the virtual machine uses the host computer's cpu directly to run the code. Hosted means that the virtual machine needs a host computer's operating system to work. The two widely used hypervisors KVM (hosted) and Xen (native) are defined briefly. Hypervisor is used to control virtual machines.

SaaS which offers software as a service, PaaS which offers platform as a service and IaaS which offers Infrastructure as a service are explained in the cloud services section. The Information security section is covered by some basic fears about cloud services from the client's and administrator's point of view. In the end, installation of Ubuntu's UEC service was described. The UEC is IaaS type cloud service.

Keywords: cloud services, virtualization, computer hardware, information security.

SISÄLLYSLUETTELO

TIIVISTELMÄ	I
ABSTRACT	II
SISÄLLYSLUETTELO.....	III
KÄYTETYT MERKIT JA LYHENTEET	IV
1. JOHDANTO	1
2. VIRTUALISOINTI.....	2
2.1. VDI	2
2.2. Hypervisor.....	3
2.3. QEMU	6
2.4. KVM	6
2.5. Xen Hypervisor	6
3. PILVIPALVELUT	8
3.1. SaaS.....	8
3.2. PaaS.....	9
3.3. IaaS	9
3.3.1. OpenStack	10
3.3.2. Eucalyptus	11
4. TIETOTURVA	12
4.1. Tietomurrot	12
4.2. Tietojen säilyvyys	13
5. YKSITYISEN PILVIPALVELUN ASENNUS	14
5.1. Ohjelmistojen valinta	14
5.2. Palvelinkoneen asennus	15
5.2.1. Ensimmäinen testivirtuaalikone	19
5.2.2. Pilvipalvelun asentaminen	28
6. YHTEENVETO	38
7. LÄHDELUETTELO.....	40

KÄYTETYT MERKIT JA LYHENTEET

AMD	Advanced Micro Devices
FTP	File Transfer Protocol
IaaS	Infrastructure as a Service
KVM	Kernel-based Virtual Machine
LTS	Long Term Support
PaaS	Platform as a Service
SaaS	Software as a Service
SCP	Secure Copy
SFTP	SSH File Transfer Protocol
SSH	Secure Shell
UEC	Ubuntu Enterprise Cloud
VDI	Virtual Desktop Infrastructure
VMM	Virtual Machine Manager / virt-manager

1. JOHDANTO

Tässä työssä selvitettiin virtualisoinnin ja pilvipalveluiden mahdollisuuksia yksityisille asiakkaille ja pienyrityksille. Lähtökohtana ohjelmistojen ja palveluiden esittelyille on niiden saatavuus ja hinta. Opinnäytetyöhön ei siksi ole valittu yhtään kaupallista ohjelmistoa. Lisäksi työssä käydään läpi työkaluja ja ohjelmistoja, joita voidaan käyttää apuna, kun virtualisointia tai pilvipalvelua asennetaan.

Työssä kerrotaan myös lyhyesti yleisesti riskinä pidetystä tietoturvasta ja sen eri näkökohdista palveluntarjoajan ja asiakkaan kannalta. Huolta tietoturvassa aiheuttaa palveluiden ja tietojen luovuttaminen pois omasta ylläpidosta.

Lopuksi asennettiin avoimen lähdekoodin käyttöjärjestelmän päälle virtualisoitu yksityinen pilvipalvelu. Pilvipalveluna käytetään Ubuntun IaaS-tyypin UEC-pilvipalvelukokonaisuutta. Asennuksessa käydään läpi tapahtumien eri vaiheet ja vastaanulleet ongelmat sekä esitellään käytettyjä ohjelmistoja ja työkaluja.

2. VIRTUALISOINTI

Virtualisointi on vanha käsite tietotekniikassa, koska se on otettu käyttöön jo 1960-luvulla IBM:n toimesta. IBM:llä oli tavoitteena jakaa suurtietokoneiden laskentateho usealle virtuaalikoneelle, jotta ne pystyivät suorittamaan useita tehtäviä tai sovelluksia yhtäaikaan. Nykypäivänä virtualisoinnilla tarkoitetaan tekniikkaa, jolla tietokoneeseen luodaan jollain metodilla rajapinta, joka eristää isäntäkoneen fyysiset komponentit ohjelmistolta tai järjestelmältä. Isäntäkoneita nimitetään englanninkielisellä termillä ”host” ja sen päällä pyörivää virtualisoitua järjestelmää termillä ”guest”. Virtualisointi mahdollistaa ”guest”-ien yhtäaikaisen ajon riippumatta toisistaan. Periaatteessa virtualisoinnilla pyritään samaan lopputulokseen kuin 60-luvulla, mutta käytännössä käyttöalue on huomattavasti laajempi. /36/

Nykyisissä suorittimissa on ominaisuus, joka mahdollistaa guestien suorittavan ohjelmakoodia suoraan hostin suorittimella. Tätä kutsutaan laitteistokiihdytetyksi virtualisoinniksi, ja osa virtualisointitekniikkaa käyttävistä ohjelmista ja palveluista vaatii sen toimiakseen oikein. Yleensä palvelinkäyttöön suunnitellut suorittimet sisältävät tämän ominaisuuden, mutta se löytyy vain osasta työpöytäkäyttöön tarkoitettusta suorittimesta. Esimerkkeinä ominaisuudesta on AMD:n AMD-V ja Intelin VT. Osassa suorittimia on lisäksi ominaisuus, mikä mahdollistaa, yhdessä emolevyn virtualisointiominaisuuksien kanssa, guestin ohjaavan isäntäkoneen muistia tai I/O-laitteita. Esimerkkeinä AMD:n AMD-Vi (IOMMU) ja Intelin VT-d. /11/ /34/

2.1. VDI

VDI eli Virtual Desktop Infrastructure tarkoittaa virtualisoitua työpöytäjärjestelmää. Järjestelmä voidaan toteuttaa esimerkiksi oppilaitoksiin, jossa henkilöt käyttävät useita eri päätelaitteita. Lisäksi yrityksissä, joissa käytetään paljon laskentatehoa vaativia sovelluksia, voidaan sovellukset ajaa client-server-tyyppisesti. Tällä tarkoitetaan sitä, että laskenta tapahtuu palvelimella eikä käyttäjän päätteellä. Tällöin laskentateho voidaan keskittää tiettyihin laitteisiin. Tämä säästää päätelaitteiden hankintakustannuksia, koska

niiden laskentateho ei ole kriittinen tekijä. Lisäksi ohjelmistojen sijainti palvelimella vähentää massamuistin tarvetta päätelaitteilla, mikä mahdollistaa esimerkiksi älypuhelimien toimivan päätteenä. /26/

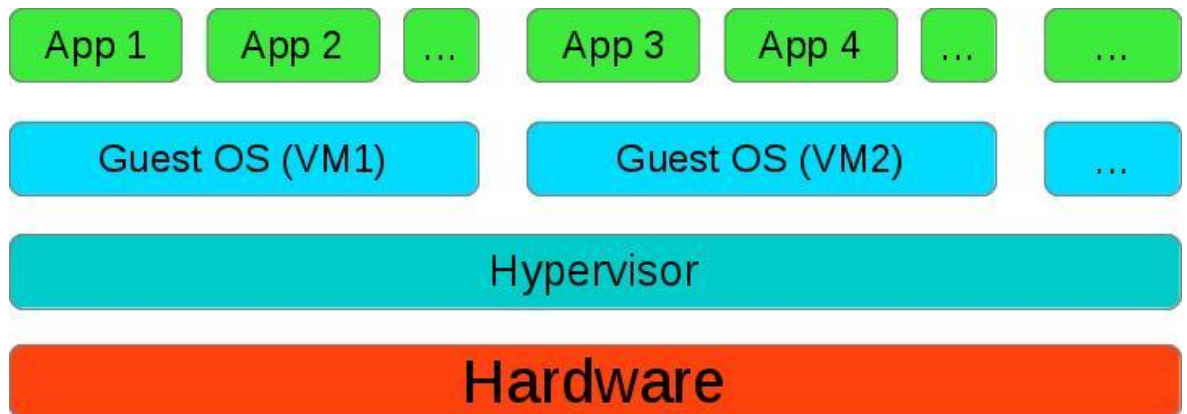
Virtualisoidussa työpöytäympäristössä päätelaitetta kutsutaan normaalisti englanninkielisellä nimellä ”thin client”, joka tarkoittaa riisuttua tietokonetta. Käyttämällä näitä niin sanottuja riisuttuja tietokoneita voidaan säästää energiankulutuksessa ja pidentää olemassa olevien päätelaitteiden käyttöikä. /26/

Virtualisoituja työpöytäympäristöjä on useampaa eri tyyppiä. Virtualisoidut työpöytäympäristöt on jaoteltu niiden yhteydenkäyttötarpeen ja palveluiden sijainnin mukaan. Perinteinen client-server tyyppin virtualisoitu työpöytä vaatii toimiakseen yhteyden palvelimen ja päätelaitteen välillä. Järjestelmää, missä palvelin ylläpitää ja suorittaa päätelaitteen ohjelmistoa, kutsutaan Server-hosted VDI:ksi. Tämä estää siirrettävien päätelaitteiden käytön verkkoyhteyden ulkopuolella. On mahdollista käyttää paikallisesti virtualisoitua käyttöjärjestelmää, joka kopioituu palvelimelle, jos verkkoyhteys on käytettävissä. Tämä virtuaalisen käyttöjärjestelmän kopio voidaan noutaa palvelimelta ja ajaa tarvittaessa toisella päätelaitteella. Tätä tekniikkaa kutsutaan Client-hosted VDI:ksi. Tällöin käyttö onnistuu verkkoyhteyden ulkopuolella, mutta perinteisen thin client - tekniikan etu menetetään, koska päätelaite vaatii laskentatehoa palveluiden suorittamiseen. /1/

2.2. Hypervisor

Hypervisor on nimitys valvontaohjelmistolle, joka kontrolloi isäntäkoneen resursseja ja jakaa niitä virtuaalikoneille. Hypervisor mahdollistaa usean virtuaalikoneen toimia samalla isäntäkoneella riippumatta toisistaan. Hypervisorina on pääsääntöisesti kahta eri tyyppiä (alaotsikot: Tyyppi 1 ja Tyyppi 2). Joskin nykyisillä järjestelmillä täsmällinen jako voidaan sulkea pois, koska erot ovat häilyviä. Hypervisorin päällä pyöriviä virtuaalikoneita kutsutaan nimellä ”guest tai guest OS”. /12/ /21/

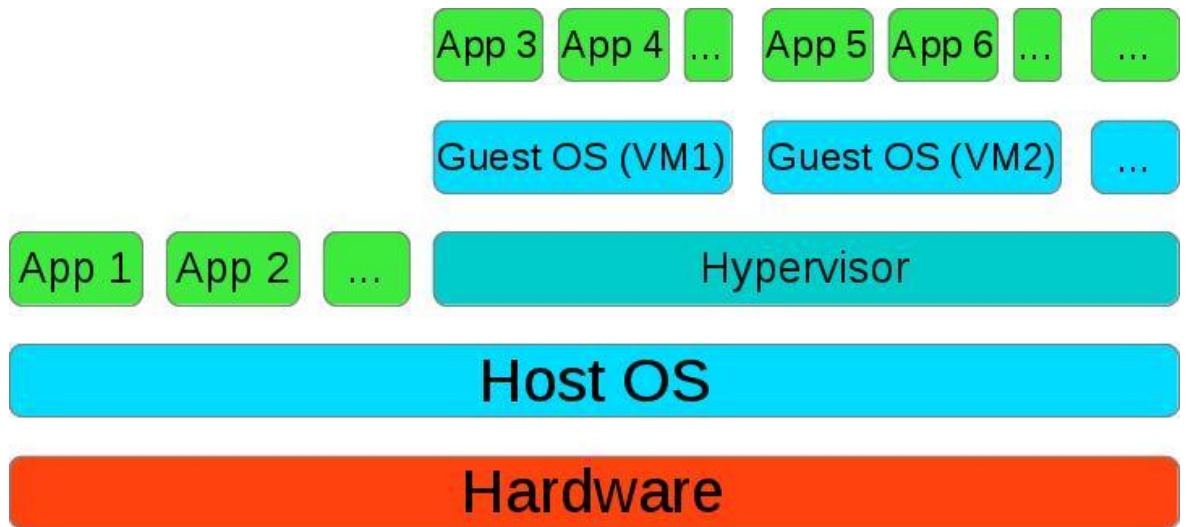
Tyyppi 1



Kuva 1. Tyypin 1 hypervisor

Tyyppi 1 tai yleisemmin kutsuttuna ”bare-metal/native”. Tällä tarkoitetaan, että hypervisor hallitsee suoraan isäntäkoneen laitteistoa, eikä erillisen käyttöjärjestelmän kautta. Kuvassa 1 esitetään hypervisorin arkkitehtuuri. Tyypin 1 hypervisorin toiminta voidaan rinnastaa mikrokerneleiden toimintaan. Hypervisor ei kuitenkaan vastaa mikrokerneleille asetettuja vaatimuksia, joten sitä ei voi sellaiseksi kutsua. Tässä järjestelmässä ei ole tyypin 2 tyyliin Host-käyttöjärjestelmää. Yleisesti tyypin 1 hypervisorin päällä toimii yksi isäntävirtuaalikone (esim. XEN:n tapauksessa Dom0 ja Microsoft Hyper-V:n tapauksessa Parent Partition), joka siltaa lapsivirtuaalikoneiden palvelukutsut eri I/O-laitteisiin itsensä kautta. Toinen vaihtoehto on antaa jokaisen virtuaalikoneen itse hallita omia ajureitaan (esim. VMware ESX) ja niiden kautta käyttää järjestelmän laitteistoa. Näistä kolmesta XEN on ainoa mikä on kehitetty alusta alkaen GNU GPL-lisenssin alaisuuteen ja on tästä syystä ilmainen. VMware ESX on myös GNU GPL-lisenssin alainen palvelinohjelmisto, mutta sen ajoon vaadittavat lisäohjelmistot kuten hallintakonsoli on maksullinen. /4/ , /37/

Tyyppi 2



Kuva 2. Tyypin 2 hypervisor

Tyyppi 2 tai yleisemmin kutsuttuna ”hosted”. Tällä tarkoitetaan, että hypervisor toimii käyttöjärjestelmän alaisuudessa. Hypervisor toimii isäntäkäyttöjärjestelmässä (Host OS) rinnan käyttöjärjestelmien muiden ohjelmistojen kanssa, kuten kuvassa 2 esitetään. Riskinä voi olla huonosti säädetyt ajo-oikeudet, jolloin suoritin hukkaa laskentatehoa käyttöjärjestelmän päällä pyöriviin ohjelmistoihin hypervisorin sijaan. Lisäksi tietoturvaa tämän kaltaisessa järjestelmässä ei pidetä niin hyvänä kuin tyypin 1, koska niin sanottua tartuntapinta-alaa tietoturva-aukoille on enemmän. Tämä vaatii järjestelmän ylläpitäjältä huomiointikykyä, niin isäntäkäyttöjärjestelmän kuin hypervisorin, tietoturvaa kohtaan. Vaikka saastunut virtuaalikone voidaan nopeasti poistaa ja asentaa uudelleen, voi se kuormittaa hypervisoria ja vaikuttaa muiden virtuaalikoneiden toimintaan, jos saastumista ei havaita. Lisäksi vallattua virtuaalikonetta voidaan käyttää hyökkäyksissä muita saman hypervisorin päällä toimivia virtuaalikoneita vastaan. Tämä edellinen riski koskee yhtä lailla tyypin 1 hypervisoria. /4/ , /3/

2.3. QEMU

QEMU on avoimen lähdekoodin prosessori-emulaattori minkä avulla isäntäkoneen suorittimella voidaan suorittaa ohjelmakoodia, joka on alun perin ohjelmoitu käyttämään täysin toista alustaa esimerkiksi ARM:n koodia x86:lla. Lisäksi QEMU mahdollistaa KVM:n kanssa suorittaa virtualisoitavan järjestelmän koodia suoraan palvelimen omalla suorittimella. Tämän avulla virtuaalikoneen suorituskyky on melkein yhtä hyvä mitä natiivisti ajettavalla ohjelmistolla. /28/

2.4. KVM

KVM eli Kernel-based Virtual Machine on Linuxin kerneliin yhdistetty moduuli, joka antaa tuen laitteistokiihdytylle virtualisoinnille. KVM toimii tyypin 2 hypervisorina. KVM:n käyttö laitteistopohjaisella kiihdytyksellä vaatii käyttöönsä, joko Intel-VT tai AMD-V -tekniikan sisältävän suorittimen. KVM ei itsessään sisällä prosessorin emulointia, joten se vaatii lisäksi muunnellun QEMU:n emulaattoriksi, jos halutaan ajaa virtualisoitua järjestelmää, joka käyttää suoraan isäntäkoneen suorittinta ohjelmakoodin suorittamiseen. KVM on keräämässä paljon huomiota ja nykyään moni Linux-jakeluiden ylläpitäjä on mukauttanut käyttöjärjestelmiä jo valmiiksi KVM-yhteensopiviksi. Tästä esimerkkinä Red Hat. Koska KVM toimii tyypin 2 hypervisorina on sen käyttö rinnastettu sen alla toimivaan käyttöjärjestelmään. Tästä syystä käyttökohteet voivat olla esimerkiksi ohjelmistojen tai käyttöjärjestelmien testaus tai lyhytaikaisten projektiympäristöjen ylläpito. /18/

2.5. Xen Hypervisor

Xen Hypervisor tai yleisemmin pelkkä Xen, mikä on tyypin 1 hypervisor. Xen on laajasti käytössä oleva hypervisor, jota käyttää muun muassa Amazon EC2. Xen toimii useissa eri

käyttöjärjestelmissä mukaan lukien Linux, Windows, Solaris ja osassa BSD-pohjaisista. Vaikkakin natiivia virtualisointia pidetään yleensä tehokkaampana, löytyy myös testejä joissa on voitu todentaa tulosten vaihtelevan. Xen:n ollessa Tyypin 1 hypervisor voidaan sitä käyttää esimerkiksi ylläpitämään virtuaalipalvelimia yritysten käyttöön. /19/ /38/

3. PILVIPALVELUT

Pilvipalvelut ovat yleistymässä huimaa vauhtia yritysten käyttöön. On normaalia haluta helpompaa ja halvempaa palveluhallintaa, mitä yleensä pidetään pilvipalveluiden tärkeimpänä ominaisuutena. Yrityksille ja yksityisille on tarjolla laaja valikoima räätälöityjä palveluita. Tämän otsikon alla kerrotaan kolmesta käytetyimmistä palvelutyypistä ja lisäksi kahdesta ilmaisesta ohjelmistokokonaisuudesta millä yksi palvelutyypeistä on mahdollista asentaa omaan palvelinympäristöön. /32/

Pilvipalveluiden vahvuutena on niiden skaalautuvuus usean eri palvelinkoneen välillä, koska sama sovellus voidaan suorittaa usealla eri palvelinkoneella. Vanhassa mallissa palvelinkoneilla on yleensä ollut jokin täsmennetty tehtävä tai sovellus mitä ne ylläpitävät. Tämän vuoksi osa palvelinkoneista on ollut jatkuvasti sovelluksesta riippuen, joko rasiitettuna tai levossa. Tällaisissa tapauksissa palvelinlaitteistoa ylläpitävän ryhmän täytyy jatkuvasti ottaa huomioon laitteistojen resurssit ja niiden riittävyys asiakkaiden määrän, tai kuormituksen lisääntyessä. Fyysisissä palvelimissa, joissa ajetaan useaa virtualisoitua palvelinta, voidaan taakka jakaa esimerkiksi siirtämällä osa korkeaa laskentatehoa vaativaa ohjelmistoa toisen fyysisen koneen virtuaalipalvelimeen. Tämä säästää muun muassa energiaa ja rahaa, koska fyysisiä palvelinkoneita voi olla normaalia vähemmän. /14/

3.1. SaaS

SaaS eli Software as a Service tarkoittaa pilvipalvelun muotoa, missä asiakkaalle tarjotaan jotain ohjelmistoa palveluna. Palveluntarjoaja on vastuussa ohjelmiston toimivuudesta ja päivityksestä, joten käyttäjä tai tilaaja säästää siihen vaadittavat resurssit. Esimerkiksi DropBox-palvelu, joka tarjoaa käyttäjälle rajallisen tallennustilan pilvipalvelussaan. Käyttäjä voi luoda yhteyden melkein mistä laitteesta tahansa - käyttäen joko nettiselainta tai tietokoneen tiedostonhallintaohjelmistoon asennettua laajennusta. Lisätyt tai päivitettyt tiedostot siirtyvät haluttaessa automaattisesti kaikkiin käyttäjän päätelaitteisiin. On helppoa mieltää perinteisiä palveluita, kuten sähköpostit ynnä muut sellaiset, SaaS-tyypin

pilvipalveluiksi. Näissäkin käyttäjä tilaa palvelun (rekisteröityy järjestelmään) toiselta osapuolelta, eikä ole itse vastuussa sen ylläpidosta. SaaS-palvelu eroaa näistä sillä, että sen tarjoama sisältö on tilaajan päätettävissä. Tilaaja voi määrittää palvelun näkyvyyden ja käytettävyyden tarpeidensa mukaan. Lukuisia MMORPG-pelejä (esim. World of Warcraft) voidaan luokitella SaaS-tyypin palveluiksi. /9/ , /35/

3.2. PaaS

Platform as a Service tarjoaa asiakkaalle ohjelmistokokonaisuuksia. Lähes kaikki nykyiset palveluntarjoajat ovat keskittäneet tarjonnan ohjelmistokehitykseen. On tarjolla valmiita kokoonpanoja eri ohjelmointikoodeille tai alustoja ohjelmien testaamiseen. Yrityksille, jotka haluavat käyttöönsä vain tiettyjä ohjelmistoja, on tämän tyyppin pilvipalvelu oiva valinta, koska silloin yritys ei tarvitse IT-tukea ylläpitämään laitteistoa tai päivittämään ohjelmistoa. Laitteiston ylläpito on tässäkin tapauksessa palveluntarjoajan vastuulla. /20/

Huono puoli PaaS-palveluissa on niiden räätälöiminen asiakkaan tarpeiden mukaan. Palvelun ylläpitäjät myyvät samaa ohjelmistokokonaisuutta kaikille asiakkaille, koska eri ohjelmistokokonaisuudet vaatisivat eri järjestelmien ylläpitoa. Eri kokonaisuuksien tarjoaminen ei ole mahdotonta, mutta ei myöskään taloudellisesti niin kannattavaa. Tilaaja tekee kompromissin haluamastaan palvelusisällöstä palveluntarjoajan valinnan mukaan. /20/ , /35/

3.3. IaaS

Infrastructure as a Service on pilvipalvelutyyppi, missä asiakkaalle tarjotaan virtualisoitu palvelinympäristö. Asiakkaan on mahdollista luoda ja poistaa virtuaalisia palvelinkoneita nopeasti tarpeidensa mukaan. Tässäkään palvelutyyppissä tilaajan ei tarvitse itse ylläpitää palvelinympäristön laitteistoa. Palvelu myydään asiakkaalle määräaikaisena ja hinnoittelu

tapahtuu käytön, ei kiinteän taksan mukaan. Käyttö määritellään käytetyn ajan, tiedonsiirtomäärien ja käyttäjien suhteen. /35/

3.3.1. OpenStack

OpenStack on NASA:n ja Rackspace Hosting:n kehittämä avoimeen lähdekoodiin perustuva ohjelmistokokonaisuus, jolla voidaan toteuttaa IaaS-tyypin pilvipalvelu. Tällä hetkellä OpenStack:llä on yli 140 suurta asiakasta ja yhteistyökumppania. OpenStack:n uskotaan nousevan kilpailijansa Eucalyptuksen ohii käyttömäärältään. Esimerkiksi Canonical on vaihtanut kehittämälleen UEC-pilvipalvelualustalle OpenStack:n Eucalyptuksen tilalle. Asiakkaan kannalta huomattavia eroja ei näiden kahden välillä ole, koska ne muistuttavat paljolti toisiaan. OpenStack on palvelukokonaisuus, joka on jaettu useampaan komponenttiin/moduuliin. /17/ , /24/ , /31/

Komponentit ovat (tärkeimmät alleviivattuna):

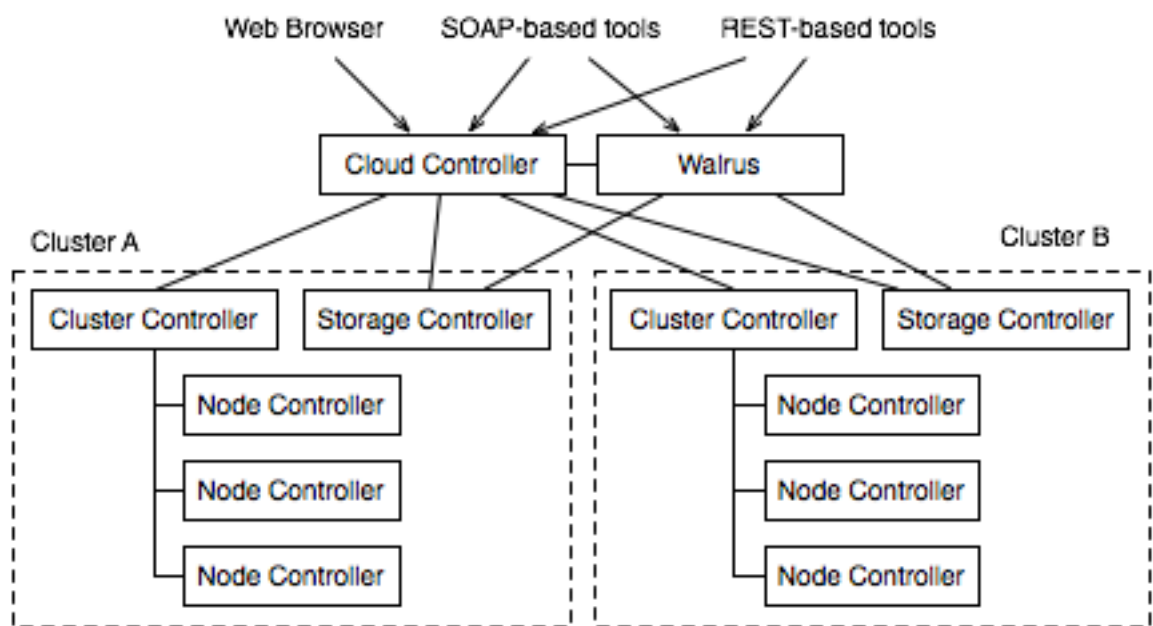
- Glance
- Horizon
- Keystone
- Nova
- Quantum
- Swift.

Glance tarjoaa palvelulle työkalut levykuvien tai ns. instanssien käsittelyyn ja rekisteröintiin. Glance toimii REST-arkkitehtuuriin perustuvalla rajapinnalla. Horizon tarjoaa palvelulle web-käyttöliittymän, josta käyttäjä voi hallinnoida palvelun muita komponentteja. Horizonin kehitys alkoi erillisenä työkaluna, mutta nykyään se on liitetty mukaan kokonaisuuteen. Keystone on työkalu, joka huolehtii käyttäjien toimintaoikeuksien varmentamisen, eli se toimii autentikointipalveluna. Nova toimii palvelun aivoina, eli sen vastuulla on tarkkailla resursseja ja jakaa tehtäviä. Swift toimii tiedostojen arkistojana, minkä vastuulla on toimittaa ja varmentaa tiedostojen sijainnit järjestelmään. Swift ei toimi niinkään reaaliaikaisena tiedostontallennusjärjestelmänä vaan pikemminkin sen tehtävänä

on tallentaa enimmäkseen pitkäaikaistiedostoja, kuten virtuaalikoneiden levykuvia, sähköposteja ynnä muita sellaisia, järjestelmään. Quantum:n tehtävänä on luoda verkkoyhteydet virtuaalisien verkkosovittimien väleille. Quantum:n ominaisuudet olivat ennen osana Nova-moduulia. Nykyään Quantum on erillinen komponentti mitä Nova hallitsee. Palvelun jakaminen komponentteihin mahdollistaa järjestelmän skaalautumisen, joka vähentää palvelimien hankintakustannuksia. /23/

3.3.2. Eucalyptus

Eucalyptus muodostuu sanoista ”Elastic Utility Computing Architecture”. Eucalyptus on laajasti käytössä oleva ohjelmistokokonaisuus, mikä luo IaaS-tyypin pilvipalvelun, mutta on nyt kiihtyvällä tahdilla korvautumassa OpenStack:lla. /5/ , /25/ , /33/



Kuva 3. Eucalyptuksen arkkitehtuuri /5/ , /33/

Yllä kuvassa 3 esitetään Eucalyptuksen arkkitehtuuri, jossa kuvataan eri komponenttien vaikutusalueet ja näkyvyydet. Tämän opinnäytetyön toteutusosassa tullaan kertomaan tarkemmin eri komponenttien tehtävät. Myös tämä IaaS-palvelukokonaisuus on modulaarinen, eli palveluita voidaan jakaa käytön mukaan eri palvelimille, jonka avulla säästetään palvelimien hankintakustannuksissa. /5/ , /33/

4. TIETOTURVA

Pilvipalveluissa on yleisesti ollut pelko tietomurroista ja tietojen säilyvyydestä. On aina arveluttavaa säilyttää tietoja palvelimella, jota hallitsee toinen osapuoli. Lisäksi pilvipalveluissa harvoin tiedetään missä palvelimet sijaitsevat fyysisesti tai kuka niitä hoitaa. Asiakas voi esimerkiksi tilata SaaS-, tai PaaS-palvelun yritykseltä, joka toimii asiakkaana kolmannen osapuolen IaaS-palvelussa. /22/

4.1. Tietomurrot

Tietomurtoihin kannattaa olla aina varautuneena. On järkevää ajatella ylläpidettyä järjestelmää aina turvattomana, sekä pyrkiä hakemaan siihen parannuksia. Ylläpitäjä voi vaikuttaa tietomurtoihin pitämällä palvelimien ohjelmistot päivitettyinä ja oikein säädetyinä. Avoimen lähdekoodin ohjelmistossa on suuri etu siinä, että kun jostain ohjelmistosta havaitaan haavoittuvuus on siihen yleensä korjaus nopeasti saatavilla. Palvelimen ylläpitäjällä on hyvä suorittaa koehyökkäyksiä omaan ympäristöönsä, jotta mahdolliset aukot havaitaan ja korjataan. Isommat yritykset voivat myös kerätä tietoa mahdollisista riskeistä ulkopuolisten henkilöiden avulla. Tähän voidaan käyttää vaikka avoimia nettilomakkeita kotisivuilla tai käyttämällä www-hakukoneita yhdessä yrityksen nimen ja jonkin avainsanan kanssa. Avainsanoiksi voidaan mieltää jokin tietomurtoon tai hakkerointiin liittyvä sana. Tämän haun avulla voi mahdollisesti paljastua keskustelupalstoja tai muita sosiaalisia medioita missä henkilö(t) ovat jakaneet tietoa aukoista. /27/

Sovelluksia, jotka käyttävät salasanoja yksilön varmentamiseen voidaan käyttää salatun yhteyden läpi. Hyvä esimerkki on perinteisen FTP-yhteyden luominen, jossa salasana näkyy protokollassa tekstimuodossa. Vaihtoehtona FTP:lle on uudemmat salatut protokollat, kuten SCP ja SFTP. Jos palvelimissa on tarkoitus säilyttää arkaluontoisia tietoja, kuten asiakkaiden luottotietoja tai muuta vastaavaa, on hyvä miettiä mahdollisuuksia tietojen salaukseen. On lisäksi hyvä sääntö pitää yhtä verkkoyhteyttä

vaativaa prosessia (MySQL, Apache jne.) virtuaalikonetta kohden, jotta mahdollisen tietomurron sattuessa on sen vaikutusalue pienempi. /10/

Useasti pienelle yritykselle on helpompaa ja halvempaa vuokrata palvelin tai ostaa palvelu asiaan vihkiytyneeltä palveluntarjoajalta kuin itse hankkia konesali ja palkata ja kouluttaa sitä ylläpitävä IT-ryhmä. Asiakkaana on järkevää ottaa selville palveluntarjoajan käyttämästä tekniikasta ja sen heikkouksista, ja tehdä sen pohjalta vertailua eri palveluntarjoajien kesken. Palveluntarjoajilla on mahdollista kehittää tietoturvaansa sille tasolle, että se voidaan auditoida ja saada myönnytys tietoturvasertifikaatille. Suomessakin käytetty kansainvälinen ISO/IEC 27001-standardi antaa asiakkaalle luotettavan kuvan palveluntarjoajasta. /13/

4.2. Tietojen säilyvyys

Arkaluontoisten tietojen säilyttäminen on riski riippumatta niiden sijainnista. Ongelmatilanteiden minimoimiseksi on mahdollista ja järkevää säilyttää varmuuskopiot paikallisilla palvelimilla, jotka synkronoidaan myös pilvipalveluihin. Pilvipalveluissa tietojen säilyvyys on varmennettu sillä, että tiedot ovat jaettuina useille palvelimille. /15/

5. YKSITYISEN PILVIPALVELUN ASENNUS

Työssä toteutetaan normaalilla työpöytätielokoneella virtualisoitu pilvipalvelu, joka perustuu Ubuntun Enterprise Cloud -järjestelmään. Palvelu toteuttaa IaaS-tyypin pilvipalvelujärjestelmän.

5.1. Ohjelmistojen valinta

Ohjelmistojen valintaan vaikutti hinta ja saatavuus. Tästä syystä tuli Microsoftin ja Applen-käyttöjärjestelmät jättää pois. Käyttöjärjestelmistä suurin osa Linux-jakeluista on ilmaisia. Muissa tapauksissa yleensä maksetaan käyttöjärjestelmälle tarkoitettu tuesta ja muista palveluista, jotka auttavat käyttäjää järjestelmän ylläpidossa. Käyttöjärjestelmään liitetystä ja maksullisista palveluista voidaan pitää esimerkkinä Red Hat -jakelua, joka tarjoaa asiakkaille asennusopastusta, virhetilanteissa neuvontaa ja erillisiä kurseja, joissa opetetaan uusia tapoja hyödyntää avoimia käyttöjärjestelmiä. /30/

Koska lähtökohtaisesti tässä opinnäytetyössä oli tarkoitus käyttää ilmaista ohjelmistoa, täytyi valinta toteuttaa muista järjestelmistä. Alun perin isäntäkoneessa tarkoituksena oli käyttää Debian-pohjaista jakelua, koska aiemmat kokemukset useamman palvelimen asennuksista ja ylläpitämisistä kyseistä jakelua käyttäen olisi luonut tutumman lähestymisen. Myöhemmin jakelu vaihdettiin toiseen. Uudeksi jakeluksi valittiin Fedora, joka pohjautuu Red Hat:n jakeluun ja on sen sponsoroima. Etuna Debianiin verrattuna on muun muassa se, että Red Hat on yritysomisteinen ja kehitys tapahtuu vakaammalla pohjalla mitä useissa yhteisökehitteisissä jakeluissa. Red Hat:lle kehitetyt päivitykset julkaistaan ja testataan ensiksi Fedorassa. Tämän vuoksi Fedoran oma pakettitarjonta on yleensä muita jakeluita edellä. Lisäksi Fedorasta löytyy hyvä tuki virtualisoinnille. Muutoin on periaatteessa aivan sama mitä jakelua käyttää, koska samat ohjelmistot on saatavilla jokaiseen. Käytännössä vain asennustavat voivat vaihdella. /30/

5.2. Palvelinkoneen asennus

Fyysinen isäntä

Laite mihin ohjelmistot asennetaan rakentuu seuraavista osista:

- Intel i5 2500K suoritin
- 8GB keskusmuistia
- 120GB SSD-kiintolevy
- 2TB kiintolevy
- 1Gb verkkosovitin.

Opinnäytetyön teko aloitettiin asentamalla isäntälaitteeseen Fedora 15-jakelu 64-bit Xfce-työpöytäympäristöllä. Työpöytäympäristön valintaan vaikuttivat aikaisemmat mieltymykset sen ulkonäköön ja toimivuuteen. Asennusmedia voitiin ladata ilmaiseksi Fedoran kotisivuilta. Oletuksena lataukselle annettiin 32-bittinen levykuva. Muut versiot (64-bit ja muut työpöytäympäristöt) löytyvät kohdasta ”Muut latausvaihtoehdot... / More download options...”. Levykuva toimii fyysisen median kopiona, joka voidaan joko polttaa CD:lle tai DVD:lle. Lisäksi levykuva voidaan asentaa USB-massamuistitikulta. Koska isäntäkoneesta ei löydy optista asemaa, vaihtoehdoksi jäi USB:ltä asentaminen. Fedora tarjoaa asennusmedian luomiseen oman ohjelmiston ja ohjeet sen käyttämiseen. Asennus tapahtui käyttäen kohdemediaa 120GB:n SSD-kiintolevyä ja oletusasetuksia. Käyttöjärjestelmän asennukseen on olemassa huomattava määrä valmiita ohjeita, joten niiden kertaaminen tässä työssä ei ole tarpeen.

Käyttöjärjestelmän asennuksen jälkeen aloitettiin ohjelmistojen asennukset, joilla pilviverkko toteutettiin. Asennuksiin käytettiin Red Hat:n pakettihallintaa RPM:ää.

Fedoralla on käytössä yum-työkalu mitä käytetään RPM:n kanssa. Nykyiset pakettihallintatyökalut ovat yleistyneet Linux-käyttöjärjestelmissä. Esimerkkinä Debianin apt, joka käyttää dpkg-pakettihallintaa ja Arch Linuxin pacman. Etu käyttäessä kyseisiä työkaluja ja hallintaohjelmistoja on niiden kyky tarkistaa pakettiriippuvuudet ja laitteiston asetukset. Haittapuolena voidaan pitää ohjelmistojen saatavuutta. Pakettihallintajärjestelmät noutavat ohjelmistot niille määrättyistä pakettivarastoista, jotka

eivät sisällä kaikkia mahdollisia ohjelmistoja tai niiden tuoreimpia versioita. Jotkut ohjelmistojulkaisijat ylläpitävät omia pakettivarastojaan, joiden osoitteet ja käyttöohjeet löytyvät yleensä heidän kotisivuiltaan. Julkaisijoiden omat pakettivarastot sisältävät viimeisimmät versiot heidän paketeistaan. Pakettien asennus onnistuu myös itse kääntämällä, jos kääntötyökalut ovat asennettuina. /29/

Ensimmäiseksi asennettiin tuki KVM:lle komennolla *yum install kvm*. Fedoran dokumentaation mukaan on suositeltavaa asentaa myös seuraavat paketit: /7/

- *python-virtinstall*
- *libvirt*
- *libvirt-python*
- *virt-manager*.

Pakettien asennus onnistuu komennolla *yum install virt-manager libvirt libvirt-python python-virtinst*.

Seuraavaksi mahdollistettiin tulevien virtuaalikoneiden pääsy ulkoverkkoon konfiguroimalla siltaava verkkosovitin. Ensiksi luodaan verkonhallintaohjelmistolle asetukset verkkosovittimille. Asetukset (merkkikokoriippuvaisia!) tallennetaan kansioon */etc/sysconfig/network-scripts/*. On syytä huomioida laitteiston nimet ja MAC-osoitteet, sillä ne ovat laitteistokohtaisia. MAC-osoite saadaan esimerkiksi komennolla *ifconfig* halutun laitteenimen alta. Laitteiston nimeksi määräytyy yleensä jokin *eth*-alkuinen nimi, mutta tässä tapauksessa *em1*.

Asetukset isäntäkoneen verkkosovittimelle tiedostoon *ifcfg-em1*:

DEVICE=em1

HWADDR=14:DA:E9:43:1D:36

ONBOOT=yes

BRIDGE=br0

NM_CONTROLLED=no

Tiedostoon asetetaan laitteen nimi kohtaan DEVICE, laitteen MAC-osoite kohtaan HWADDR, käynnistyminen isännän yhteydessä kohtaan ONBOOT, silta-adapterin nimi kohtaan BRIDGE ja Fedoran verkonhallintaohjelmiston mahdollisuus muuttaa asetuksia kohtaan NM_CONTROLLED.

Asetukset siltaavalle verkkosovittimelle tiedostoon *ifcfg-br0*:

DEVICE=br0

TYPE=Bridge

BOOTPROTO=dhcp

DNS1=8.8.8.8

DNS2=8.8.4.4

ONBOOT=yes

DELAY=0

NM_CONTROLLED=no

Tiedostoon asetetaan tiedot, kuten edellä mainittuun *ifcfg-em1*, mutta seuraavin poikkeuksin: kohtaan TYPE annetaan sovittimen tyyppi Bridge (huomioi iso-B), dynaaminen IP-osoitteen käyttö ja haku DHCP:llä kohtaan BOOTPROTO, vaihtoehtoisten DNS-palvelimien määrittäminen kohtaan DNS1 ja DNS2 ja käynnistymisen viive kohtaan DELAY.

Fedoran oletuksena käyttämä verkonhallintaohjelmisto NetworkManager ei tue siltaavia verkkosovittimia, joten se tuli vaihtaa komentotason network-ohjelmistoon komennoilla:

chkconfig NetworkManager off

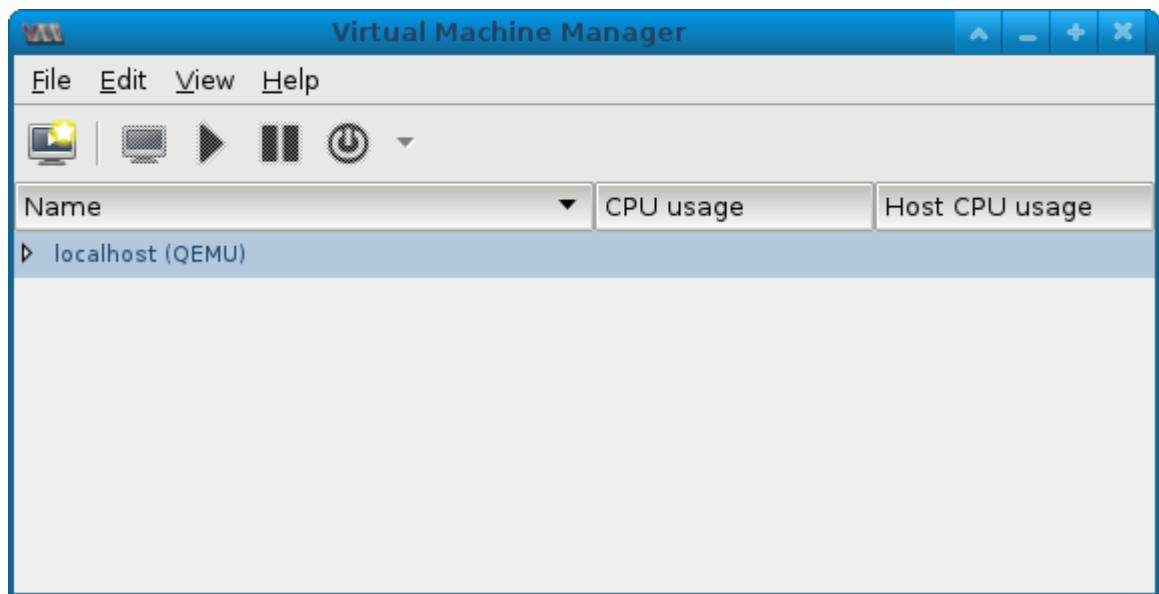
chkconfig network on

service NetworkManager stop

service network start

VMM

Fedorassa on käytössä virtuaalikoneiden hallintaan Virtual Machine Manager -työkalu, lyhennettynä VMM tai pakettinimeltään virt-manager. VMM perustuu GNU GPL -lisenssiin. VMM:ssä on graafinen käyttöliittymä, mutta sitä on mahdollista käyttää myös komentoliittymän kautta esimerkiksi etänä SSH:n avulla.

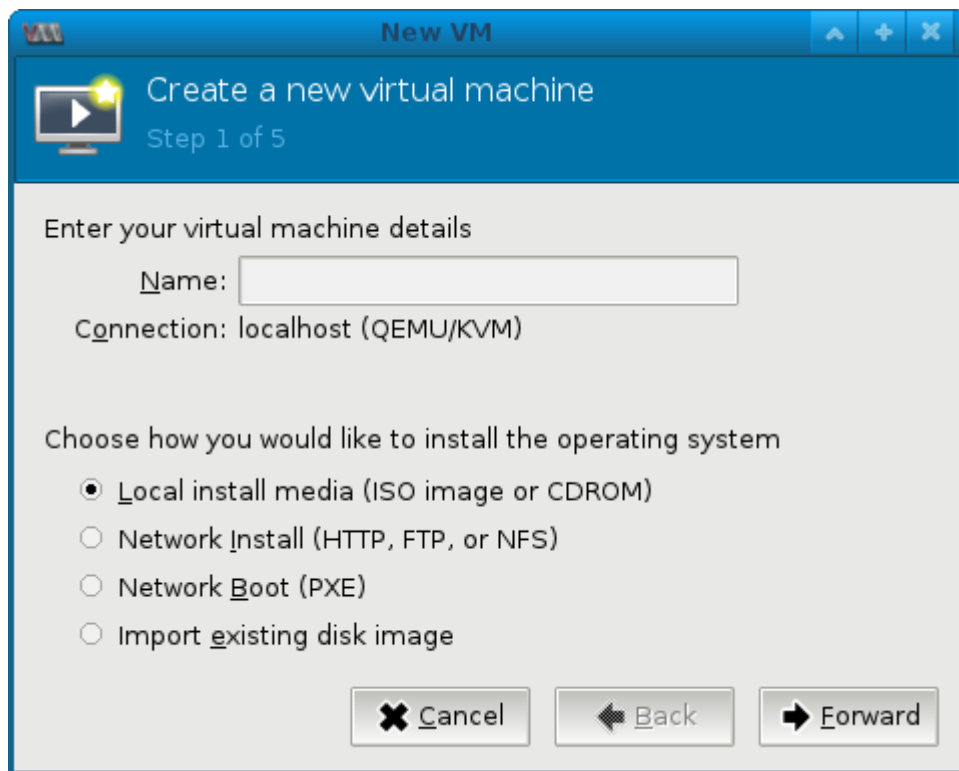


Kuva 4. VMM aloitusnäky

Aloitusnäky mikä näkyy kuvassa 4 on selkeä; ylhäällä näkyvät hallintapaneelit ja työkalupalkki. Palkin alapuolella on yleisnäky käytössä oleviin emulaattoriyhteyksiin ja sen virtuaalikoneisiin. Hallintapaneelin File-välilehdestä voidaan luoda uusi emulaattoriyhteys ja piilottaa tai sammuttaa virtualisointi. Edit-välilehdestä voidaan tarkkailla ja muuttaa olemassa olevien emulaattoriyhteyksien asetuksia, jotka sisältävät virtuaalikoneiden muistinkäytön, verkkoyhteydet ja tallennuskapasiteetin. Lisäksi Edit-välilehdestä voidaan poistaa emulaattori, tarkastella tietyn virtuaalikoneen asetuksia tai muuttaa UI:n asetuksia. View-välilehdestä voidaan muuttaa yleisnäkyssä esitettäviä tietoja (oletuksena CPU usage ja Host CPU usage). Help-välilehdestä aukeaa About-ikkuna mistä näkee VMM:n version, tekijänoikeudet, tekijätiedot ja lisenssin. Työkalupalkista voidaan nopeasti hallita valitun virtuaalikoneen tilaa (käynnistys/sammutus..).

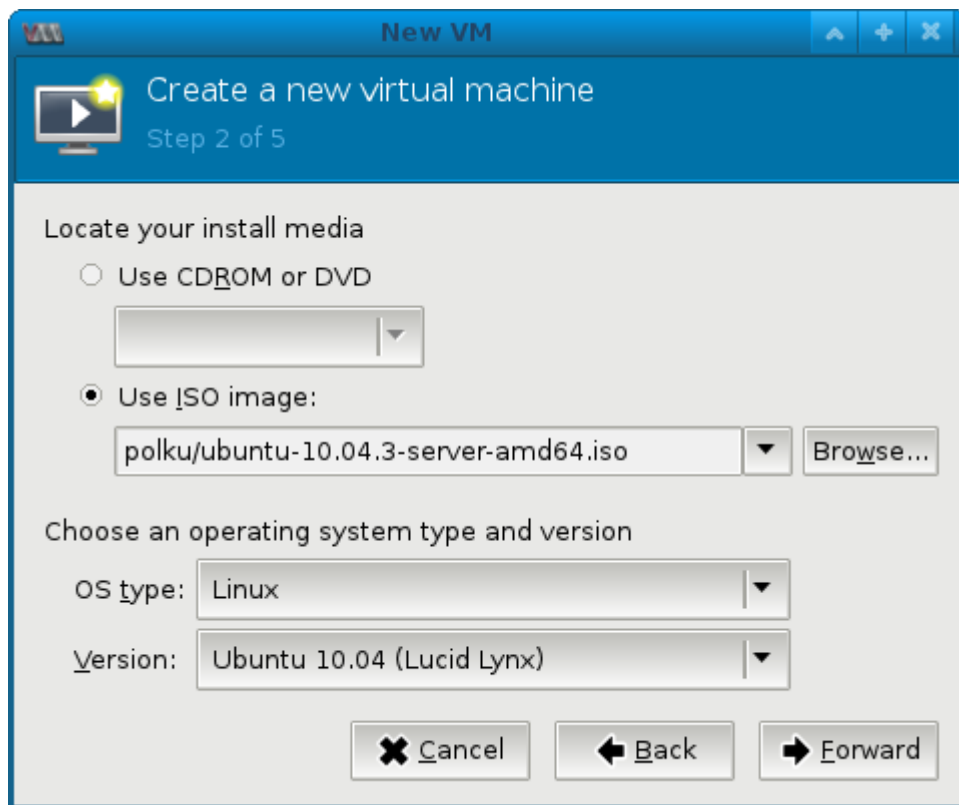
5.2.1. Ensimmäinen testivirtuaalikone

Ensimmäiseksi testinä luotiin virtuaalikone oletusarvoilla, jotta pystyttiin testaamaan siltauksen toimivuutta käytännössä. Virtuaalikone voidaan luoda painamalla emulaattoriyhdyden kohdalla hiiren oikeaa näppäintä ja valitsemalla New.



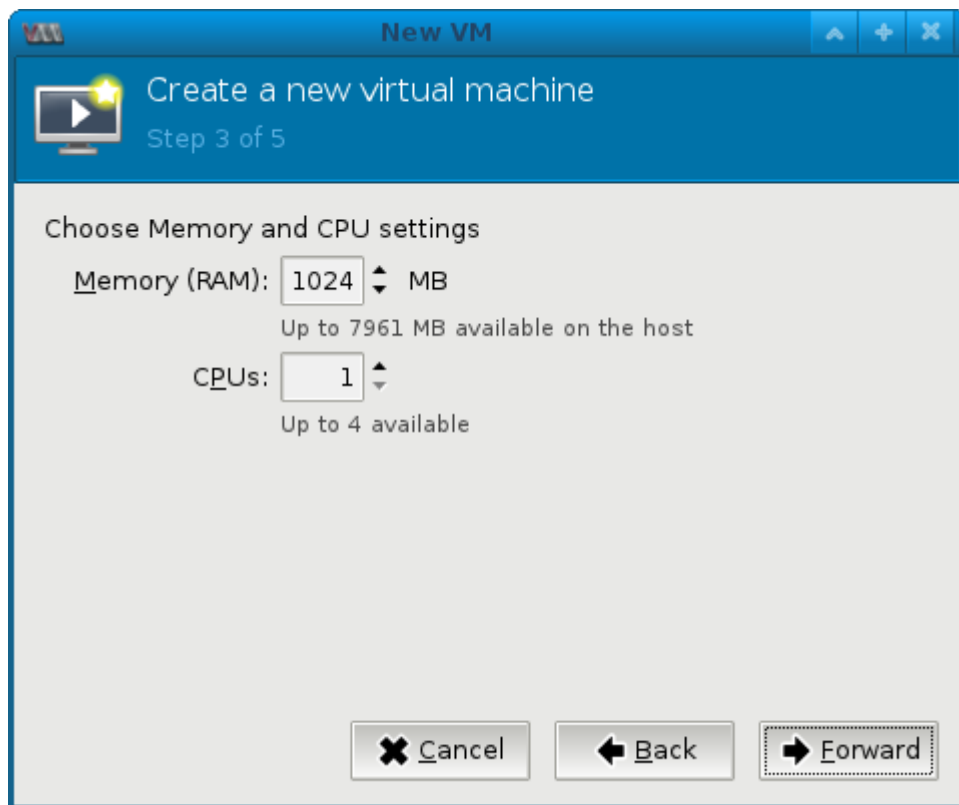
Kuva 5. Asetukset virtuaalikoneelle

Tämän jälkeen aukeaa kuvan 5. mukainen ikkuna virtuaalikoneen alustukselle. Ikkunasta voidaan antaa virtuaalikoneelle nimi ja lähdemedian sijainti. Nimi kannattaa valita siten, että siitä selviää virtuaalikoneen tehtävä, esimerkiksi ”Node Controller”. Lähdemediana on Ubuntu kotisivuilta ladattu *.iso -levykuva, joten valinta kuten kuvassa. Haluttujen asetusten jälkeen painetaan Forward.



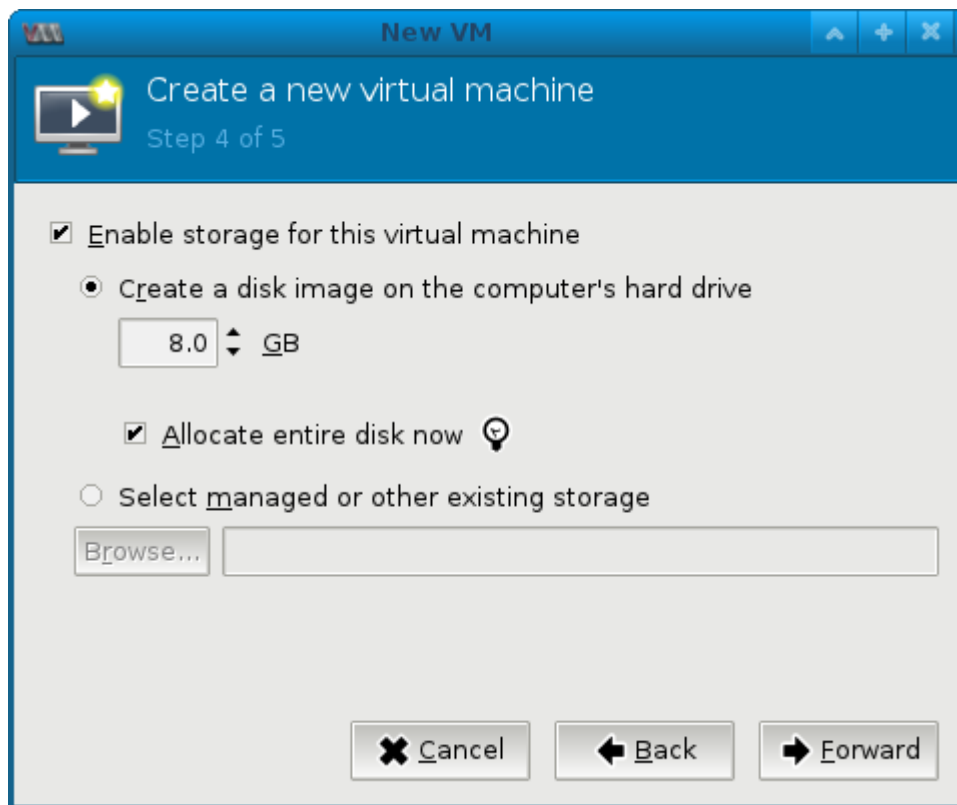
Kuva 6. Virtuaalikoneen lähdemedia

Seuraavaksi määritetään polku lähdemediaan kuvassa 6 näkyviin kenttiin. Tässä tapauksessa, koska käytettiin levykuvan lataukseen nettiselainta, tallentui se selaimessa määritettyyn kohdekansioon, eli kotihakemiston Downloads-kansioon. Käyttöjärjestelmän tyyppi voidaan määrittää lähdetiedoston alle. Tämän jälkeen voidaan siirtyä seuraavaan kohtaan painamalla Forward.



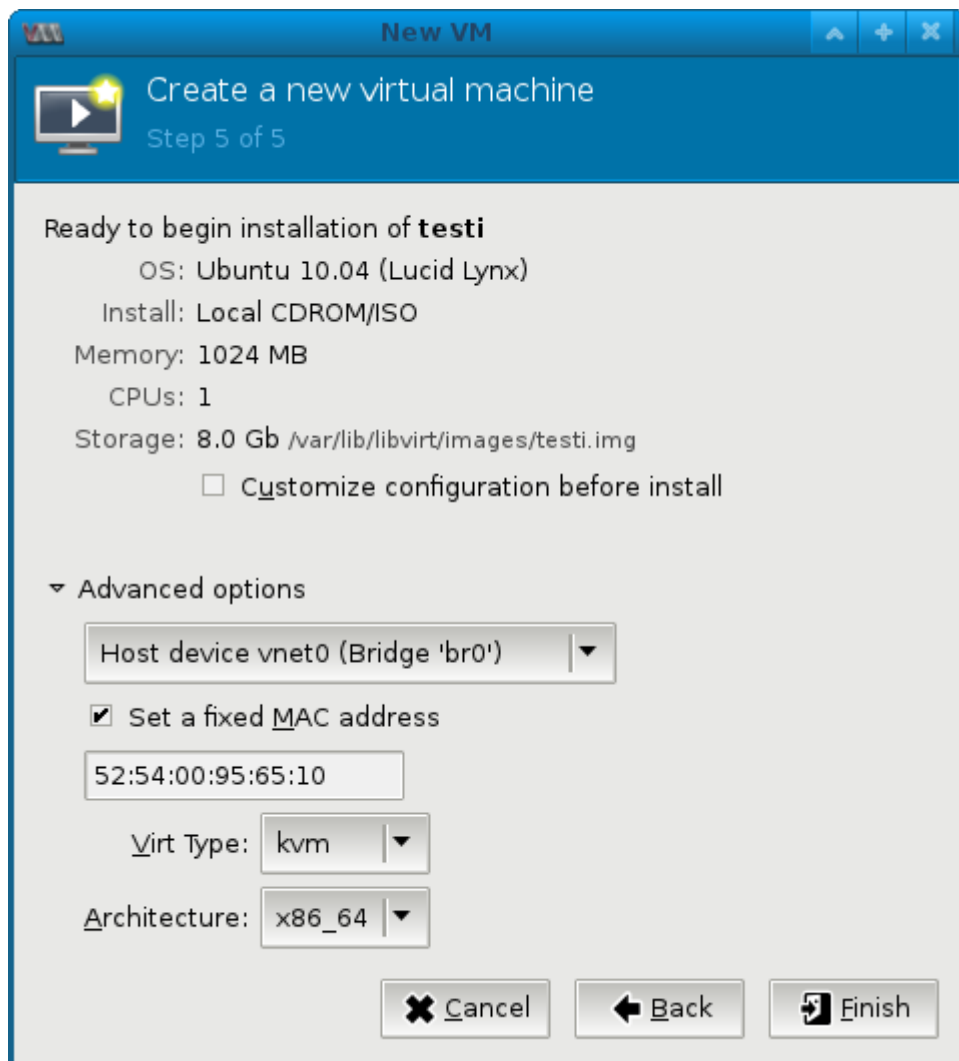
Kuva 7. Virtuaalikoneen muisti- ja prosessoriasetukset

Tämän jälkeen asetetaan virtuaalikoneelle varattavan muistin ja suorittimien määrä kuvan 7 esittämiin kenttiin. Arvoiksi annettiin kuvassa näkyvät ja oletuksenakin annetut arvot, sillä ensimmäisen asennuksen oli määrä toimia testinä. Haluttujen arvojen syötön jälkeen painetaan Forward.



Kuva 8. Virtuaalikoneen tallennuskapasiteetti ja kohde

Seuraavassa ikkunassa kuvan 8 mukaisesti virtuaalikoneelle asetetaan tallennuskapasiteetti ja sen kohdemedia. Oletuksena VMM antaa virtuaalikoneelle tilan samalta kohdelevyltä jonne isäntäkäyttöjärjestelmä on asennettuna, eli tässä tapauksessa 120GB:n SSD-kiintolevyltä. Testiasennukselle annetaan käyttöön oletussijainti ja -kapasiteetti, mutta samalla kannattaa huomioida riittääkö se jatkoa ajatellen. Koska kyseessä oli vain testiasennus, eikä tarkoituksena ollut luoda mitään lopullista, voidaan kohdat jättää myöhempään tarkasteluun. Kohta, jossa annetaan virtuaalikoneelle suoraan asetettu tila käyttöön, säilytetään aktivoituna. Arvojen asetuksien jälkeen painetaan Forward.



Kuva 9. Virtuaalikoneen tietojen tarkistus

Seuraavassa ikkunassa avautuu kuvan 9 mukainen näkymä. Tässä ikkunassa voidaan tarkistaa virtuaalikoneelle määritetyt asetukset ja vaihtaa sen käyttämä verkkosovitin. Advanced-valikosta varmistetaan, että virtuaalikone käyttää aikaisemmin luotua siltaavaa verkkosovitinta. Kun asetukset on varmistettu, voidaan aloittaa virtuaalikoneelle käyttöjärjestelmän asennus painamalla Finish.

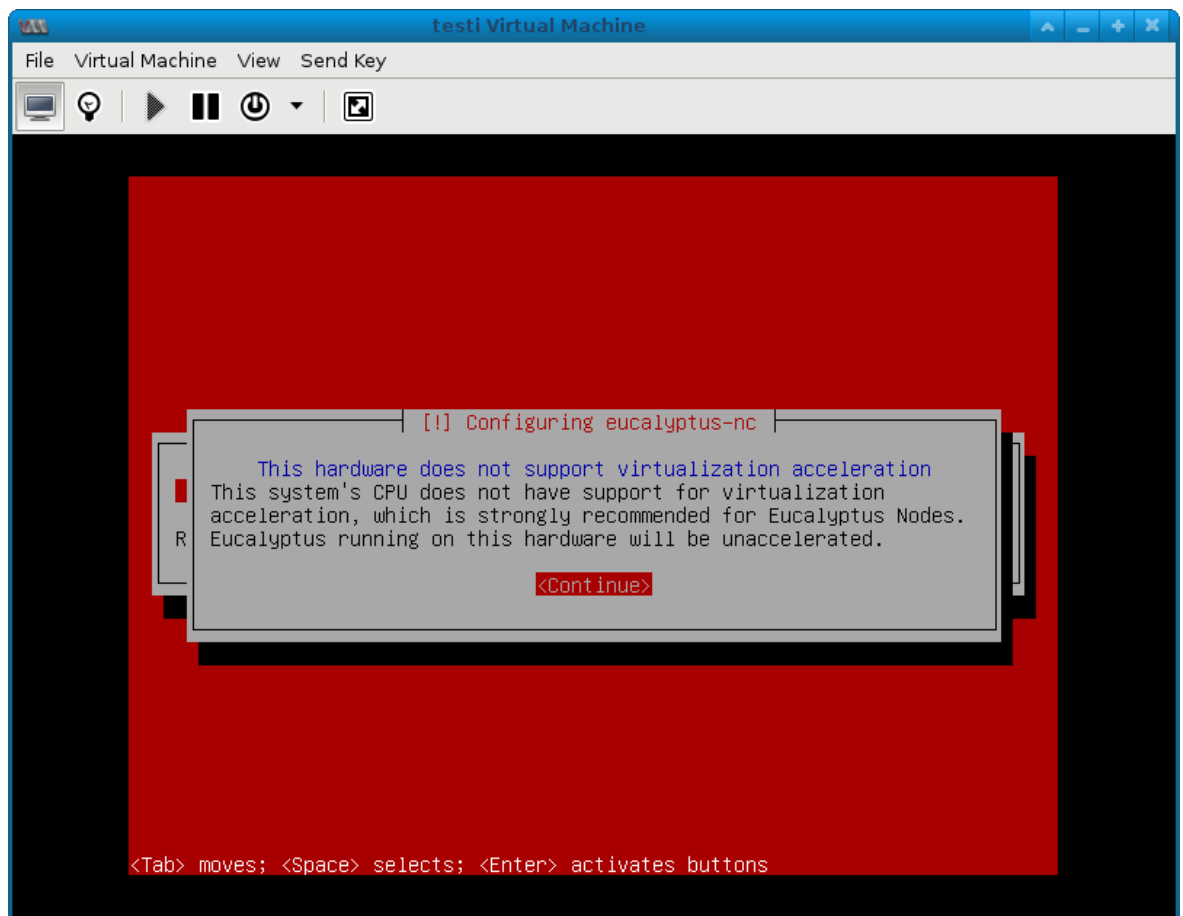
Käyttöjärjestelmän asennuksesta löytyy kuvalliset ohjeet internetistä, joten tässä käydään lävitse tarvittavat valinnat vain sanallisesti. Ensimmäiseksi annetaan asennuksessa käytettävä kieli esimerkiksi oletuksena oleva englanti. Toisessa kohdassa valitaan normaalista asennuksesta poiketen kohta ”Install Ubuntu Enterprise Cloud”, minkä jälkeen valitaan asennuskieli uudelleen. Tämä kielivalinta vaikuttaa myös asennettavan

järjestelmän oletuskieleen. Seuraavaksi valitaan järjestelmän sijainti. Tässä tapauksessa käytettiin valintaa ”other > Europe > Finland”. Tämän jälkeen annetaan järjestelmässä käytettävän näppäimistön merkkiasettelu. Valinnassa voidaan käyttää joko asettelun tunnistavaa vaihtoehtoa (Yes) tai listalta valitsemalla (No). Tunnistavaa valintaa on hyvä käyttää, jos ei ole varma käytössä olevasta näppäinasettelusta. Tässä tapauksessa valinta oli ”No > Finland > Finland”. Seuraavaksi annetaan järjestelmälle nimi. Tämä voi olla sama mikä on annettu virtuaalikoneelle tai jokin vastaava, mutta mielellään lyhyt ja havainnollistava.

Seuraavaksi valitaan järjestelmän rooli pilvipalveluympäristössä. Myöhemmin tässä opinnäytetyössä kerrotaan eri roolien käyttötarkoituksista, joten tässä ensiasennuksessa voidaan hyväksyä oletuksena annetut. Tämän jälkeen valitaan tapa kohdemedian osioinnille. Seuraavassa kohdassa on mahdollista määrittää salaus taltionhallinnalle, mutta testiasennuksen toiminnan nopeuttamiseksi jätetään salaus pois ja valitaan ”Guided – use entire disk and set up LVM”. Seuraavaksi valitaan kohdemedia, eli virtuaalikoneen tapauksessa ”Virtual disk 1 (vda)”. Tämän jälkeen asennus kysyy varmistusta tiedostojärjestelmän kirjoittamiselle kohdemediaan, mihin vastataan ”Yes”. Seuraavaksi annetaan järjestelmän koko kohdemediassa, joka on joko oletus 8.3GB, max tai 100%. Tämän jälkeen asennusohjelma kysyy vielä kerran varmistusta tiedostojärjestelmän kirjoittamiselle kohdemediaan, mihin vastataan ”Yes”. Tämän jälkeen asennuksen esiasettelut ovat valmiit ja käyttöjärjestelmä asentuu.

Virhe asennuksessa

Asennus jatkui hetken ennen seuraavaa kuvassa esiintyvää virheilmoitusta:



Kuva 10. Virhe asennuksessa

Kuvassa 10 esiintyvässä virheilmoituksessa todetaan, että järjestelmässä oleva suoritin ei tue laitteistopohjaista virtualisointia, eikä tästä syystä järjestelmässä käytettävällä Eucalyptuksella ole mahdollisuuksia kiihdytykseen. Asennus jatkuu kuitenkin painamalla ”Continue”.

Laitteistoon asennettu suoritin tukee Intel VT-x-tekniikkaa, joten edellä esiintynyt virhe johtui jostain ohjelmistopohjaisesta ongelmasta. Asia varmistui käyttämällä komentoa `cat /proc/cpuinfo | grep vmx`, joka antaa tulosteen, jos se kuuluu prosessorin ominaisuuksiin. Isäntäkoneen tulosteessa näkyi `vmx` listattuna, joten seuraavaksi kokeillaan vastaavaa komentoa virtuaalikoneessa. Virtuaalikoneen prosessorin ominaisuuksiin se ei kuulunut, joten komento ei antanut mitään tulostetta.

Viitteitä vastaavanlaisiin ongelmiin löytyi internetin keskustelupalstoilta ja muualtakin. Koska pilvipalvelun oli tarkoitus käyttää virtualisointia ja järjestelmä oli asennettu virtuaalikoneeseen oli siinä käytettävä pinoutuva virtualisointia. Ongelmaan ei aluksi löytynyt ratkaisua. Myöhemmistä hauista paljastui, että Fedora 15 -jakelun mukana tulevassa kernelissä ei ole tukea Intelin pinoutuvalle virtualisoinnille ja, että kyseisen ongelman parissa työskennellään. Tämä johtui siitä, että AMD:n suorittimien käskykanta on hiukan yksinkertaisempi, joilla pinoutuva virtualisointi on ollut mahdollista jo reilusti aikaisemmin. Myöhemmässä Fedora 16 -jakelussa oli käytetty uudempaa 3.1.x-version kerneliä, minkä dokumentaatiosta paljastui, että tuki pinoutuvalle virtualisoinnille oli lisätty. Tämä tarkoitti sitä, että isäntäkoneelle jouduttiin asentamaan käyttöjärjestelmä uudelleen käyttäen uudempaa Fedora 16 64-bit -jakelua. Työpöytäympäristöksi valittiin Xfce. /8/ , /16/

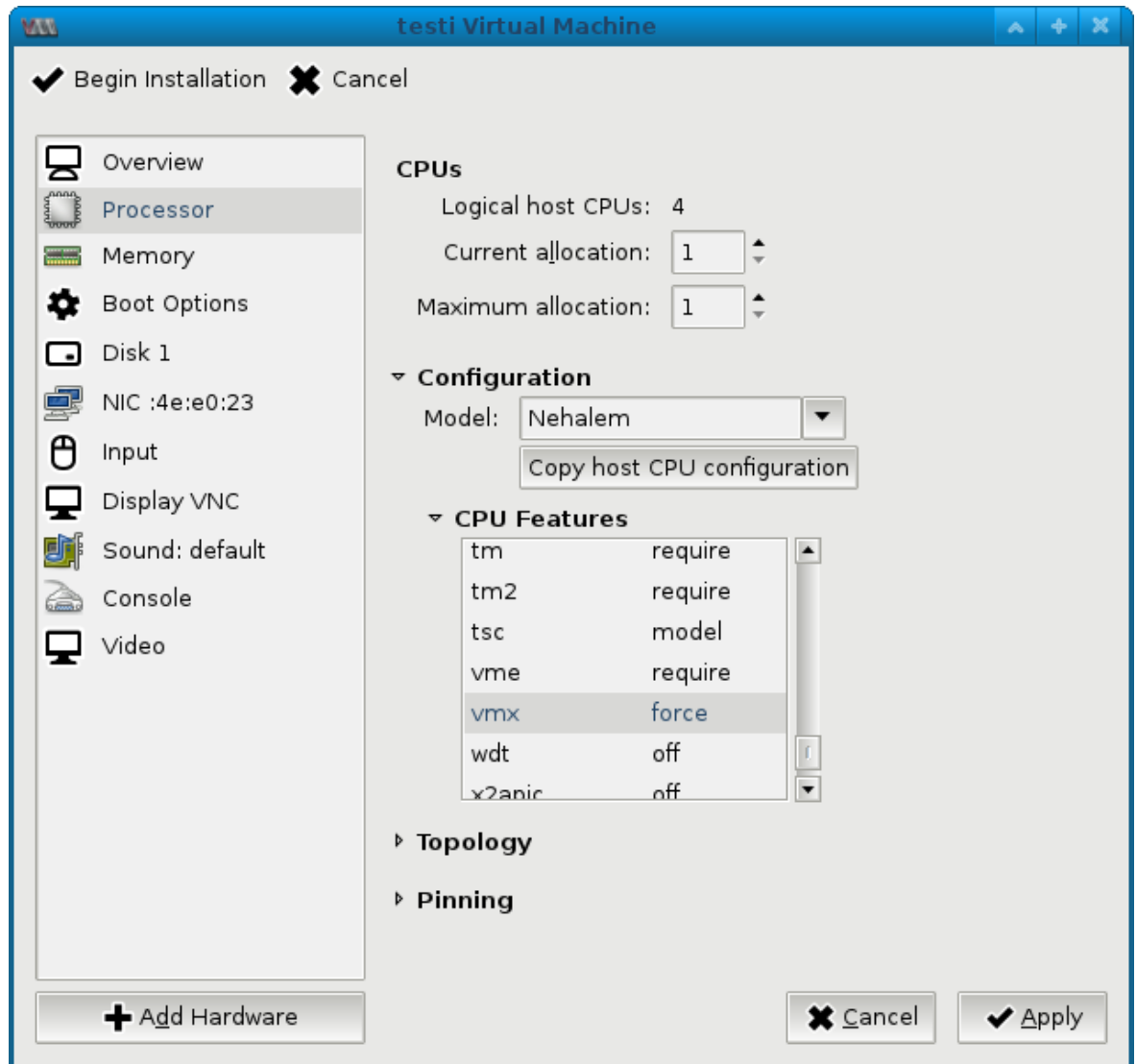
Uusi yritys

Asennuksen jälkeen aloitettiin järjestelmän asetusten määrittämisellä kuten aiemmin, eli asentamalla tuki KVM:lle ja luomalla siltaavan verkkosovittimen. Tämän jälkeen asennettiin testikäyttöön virtuaalikone oletusasetuksilla kuten aiemmin. Uudessakin asennuksessa sama virhe toistui. Kernelin ja käyttöjärjestelmän päivityksen jälkeen ei periytyvä virtualisointi toiminut oletetusti.

Jatkotutkimusten jälkeen saatiin selville, että kvm-moduulin parametri ”Nested” ei ole oletuksena käytössä. Moduulin parametrit voidaan tarkistaa komennolla `sysctl -m kvm_intel -v | grep nested` (sysctl-työkalun käyttö vaatii sysfsutils-paketin asentamisen, ellei sitä löydy järjestelmästä). Tässä vaiheessa näytölle tulostui ”nested = ”N””. Moduulin parametreihin pystyi vaikuttamaan luomalla kansioon `/etc/modprobe.d/` tiedosto nimeltä `kvm_intel.conf` ja lisäämällä sinne rivi ”options kvm_intel nested=1”. Tämän jälkeen muutokset aktivoituivat palveluiden uudelleenkäynnistyksellä, mikä varmistettiin käynnistämällä koko isäntäkone uudelleen.

Uudelleenkäynnistymisen jälkeen varmistettiin asetustiedoston toiminta komennolla `sysctl -m kvm_intel -v | grep nested`. Tällä kertaa saatiin tulosteeksi ”nested = ”Y””, mikä

tarkoitti, että pinoutuva vmx pitäisi olla toiminnassa. Seuraavaksi poistettiin VMM:llä testiasennuksena toiminut virtuaalikone ja luotiin se uudelleen. Tällä kertaa asetettiin myös virtuaalikonetta luodessa täppä viimeisen vaiheen kohtaan ”Customize configuration before install”, jonka jälkeen seuraavassa vaiheessa pystyttiin määrittämään asetuksia tarkemmin.



Kuva 11. Suorittimen asetukset virtuaalikoneelle

Asetuksiin luotiin kuvassa 11 esiintyvät muutokset varmistukseksi pinoutumisen toimivuudelle. Mallin kohdalta ensiksi ”Copy host CPU configuration”, jonka seurauksena alempaan listaan kopioitui isäntäkoneen suorittimen ominaisuudet. Tämä valinta antoi kuitenkin malliksi vanhemman sukupolven Westmere-arkkitehtuurin. Kyseisellä hetkellä

VMM:ssä ei ollut nykyistä Sandy Bridge -arkkitehtuuria valittavana, joten Westmeren tilalle valittiin tuoreempi Nehalem-arkkitehtuuri. Tämän jälkeen valittiin ”CPU Features”-listasta vielä käsin ”vmx – force”. Muutokset hyväksyttiin valinnat painamalla ”Apply” ja ”Begin Installation”. Tällä kertaa käyttöjärjestelmä asentui ilman virheilmoitusta ja virtuaalikoneen virtualisointiominaisuudet varmistettiin komennolla `cat /proc/cpuinfo | grep vmx`, joka palautti tulosteen, missä vmx oli listattuna.

5.2.2. Pilvipalvelun asentaminen

Ongelmien selvittyä aloitettiin ensimmäiset virallisemmat asennukset. Tarkoituksena oli saada UEC toimintakuntoon ja muutama virtuaalipalvelin sen päälle pyörimään. Palvelimien konfigurointi suoritetaan Ubuntun ja CSS Corp:n dokumentoinnin mukaan, mutta pieniä muutoksia soveltaen. /2/

Asennukset tulevat sisältämään kaksi kappaletta virtualisoituja palvelimia ja yhden virtualisoidun työpöytäkäyttöjärjestelmän. Ensimmäinen palvelin toimii niin sanottuna ”front end”:nä, missä toimivat:

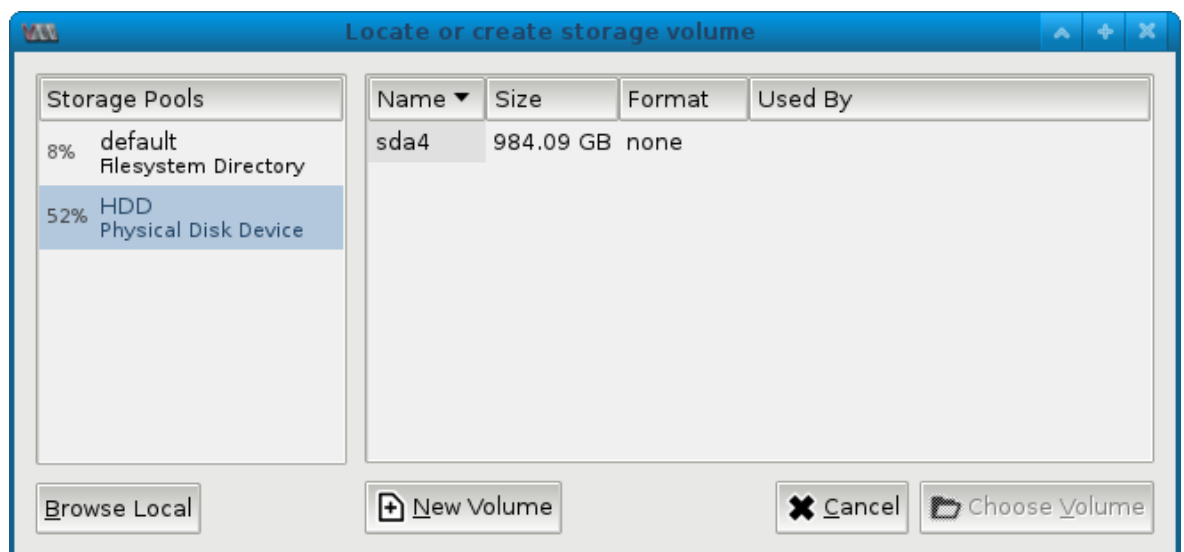
- eucalyptus-cloud
- eucalyptus-cc
- eucalyptus-walrus
- eucalyptus-sc.

Eucalyptus-cloud, eli cloud controller, toimii järjestelmän käyttöliittymänä. Toimintana on luoda web-käyttöliittymä (Amazon EC2/S3-yhteensopiva) asiakkaalle ja ohjata käskyt oikeaan paikkaan. **Eucalyptus-cc**, eli cluster controller. Cluster controller toimii klusterissa skedulerina ja verkkoyhteyksien hallitsijana. Lisäksi se ohjaa vähintään yhtä tai tarvittaessa useampaa node controlleria. **Eucalyptus-walrus**, eli S3-type storage service. Walrus toimii levykuvien ylläpito-ohjelmistona SOAP-protokollan ja REST-arkkitehtuurin avulla, sekä tiedostonhallintaohjelmistona S3:n kanssa. **Eucalyptus-sc**, tai puhekielellä storage controller. Storage controller toimii klusterissa luomassa instansseille virtuaalisia

tallennusasemia tarpeen mukaan. Toinen palvelin toimii ”node controllerina”, ja siinä toiminnassa oleva palvelu on **eucalyptus-nc**. Node controller ohjaa instanssien elämänsykliä. /33/

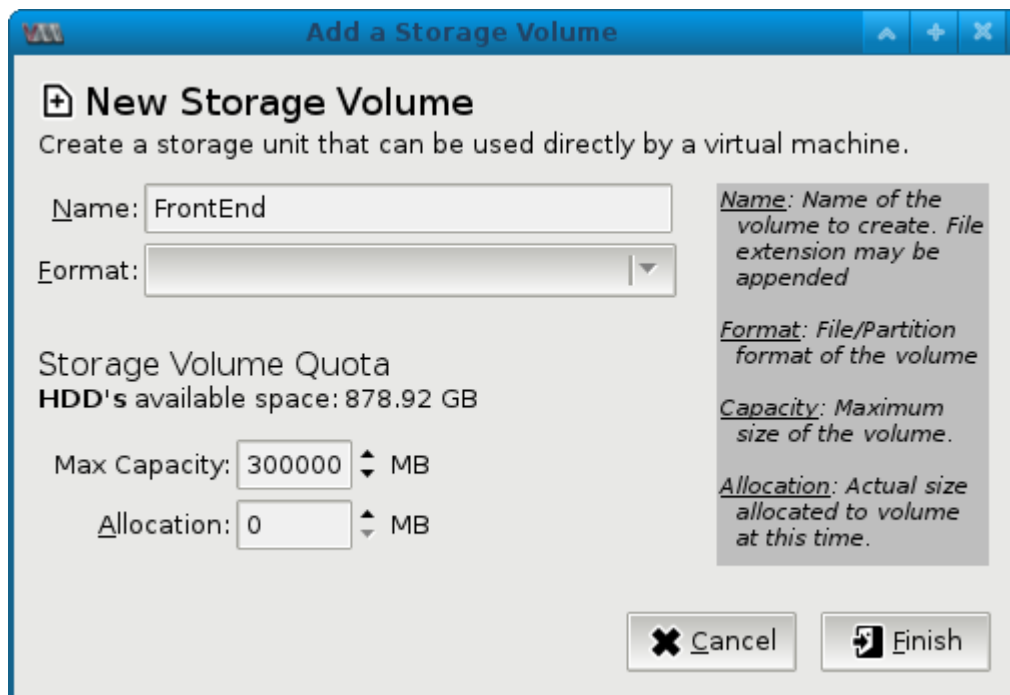
Front end

Ensimmäinen virallinen asennus aloitetaan luomalla uusi virtuaalikone VMM:n avulla. Asetuksien vaiheet voidaan tarkistaa aiemmasta osiosta missä luodaan ensimmäinen testivirtuaalikone. Virtuaalikoneen nimeksi annettiin asetusten ensimmäisessä vaiheessa ”FrontEnd”. Kolmannessa vaiheessa koneelle määritettiin käyttöön 2048MB muistia ja kaksi ydintä suorittimelta. Neljännessä vaiheessa valitaan testiasennuksesta poiketen ”muu” kohdeasema, joka haetaan painamalla ”Browse”. Syy tähän on isäntäjärjestelmän tallennuskapasiteetin vähyys, koska asennusmedia toimii 120GB SSD-kovalevy. Virtuaalikoneen tallennustilaksi määritetään kohdeasemaksi 2TB Sata III-kovalevy.



Kuva 12. Virtuaalikoneen tallennustilan määrittäminen

Seuraavassa vaiheessa, kun ”Browse”-nappia on painettu aukeaa kuvan 12 mukainen ikkuna, josta nähdään isäntäjärjestelmään luodut asemat. Tässä tapauksessa valittiin alempi HDD, minkä jälkeen luotiin uusi osio painamalla ”New Volume”-painiketta.



Kuva 13. Uuden osion luominen virtuaalikoneelle

Tämän jälkeen uuteen ikkunaan aukeaa kuvan 13 mukaiset valinnat osionin määrittämiselle. Nimeksi osiolle VMM antaa saman mikä on määritettyä virtuaalikoneelle, joka on tässä tapauksessa hyvä. Oletuksena VMM antaa kohdeosiolle 1000MB, eli 1GB:n kapasiteetin. Tämä ei riitä, joten sitä kasvatettiin 300GB:n kokoon. Allokointia ei käytetä, joten asetusten määrittämisen jälkeen hyväksytään valinnat painamalla ”Finish”. Tämän jälkeen luotu osio valitaan ja jatketaan asetusten määrittämisestä. Loput asetuksista määritettiin kuten aiemmin, mukaan lukien virtualisointituen varmistaminen suorittimen arkkitehtuurin käsinvalinnalla. Tämän jälkeen asennus on valmis alkamaan.

Asennuksen alkuvaiheessa valitaan ”Install Ubuntu Enterprise Cloud”, syötetään järjestelmän kieli ja näppäinasettelu. Tämän jälkeen asennus tarkistaa jo olemassa olevia cloud controller -asennuksia, joita ei pitäisi tässä vaiheessa löytyä. Tämä kohta voidaan ohittaa painamalla ”Continue”, jonka jälkeen annetaan palvelimelle sen tehtävät. Tehtäviksi valitaan jo aikaisemmin läpikäyty, eli oletuksenakin esitetyt valinnat: cloud, cc, walrus ja sc.

Järjestelmälle voidaan asettaa automaattiset päivitykset, vain automaattiset turvallisuuspäivitykset tai käsin päivitettävä. Tässä tapauksessa valitsin automaattiset turvallisuuspäivitykset. Seuraavassa vaiheessa annetaan klusterille nimi, mutta koska järjestelmä tulee sisältämään vain yhden klusterin, voidaan nimi valita vapaammin. Nimeksi tässä tapauksessa tuli FrontEndCluster, joka viittaa jo virtuaalikoneellekin annettuun nimeen. Seuraavaksi annetaan pilvipalvelun käyttämät IP:t. Kannattaa valita selvästi erotettavissa oleva IP-ryhmä, jotta on mahdollista erottaa palomuurin puolelta isäntäkone, sen alla pyörivät virtualisoidut palvelimet sekä virtualisoidussa pilvipalvelussa pyörivät palvelimet hyvin toisistaan. Tässä asennuksessa käytettiin seuraavaa allasta: 192.168.10.10-192.168.10.100. Asennus vielä varmistaa GRUB:n asennuksesta käynnistyssektorille, mihin vastataan kyllä, ja asennus on valmis.

Uudelleenkäynnistymisen jälkeen voidaan aloittaa järjestelmän esiasetusten suorittaminen. Ensimmäisenä on suositeltavaa ajaa järjestelmän päivitykset läpi komennoilla: *sudo apt-get update*, *sudo apt-get upgrade* ja *sudo apt-get dist-upgrade*. Viimeisin komento tarvitsee järjestelmältä uudelleenkäynnistämisen, koska päivitys kohdistuu Linuxin ytimeen.

Päivityksien jälkeen voidaan varmistaa eucalyptuksen komponenttien toimivuus seuraavilla komennoilla:

```
sudo netstat -tnlp | grep 8443
```

```
sudo euca_conf --list-walruses
```

```
sudo euca_conf --list-clusters
```

```
sudo euca_conf --list-scs.
```

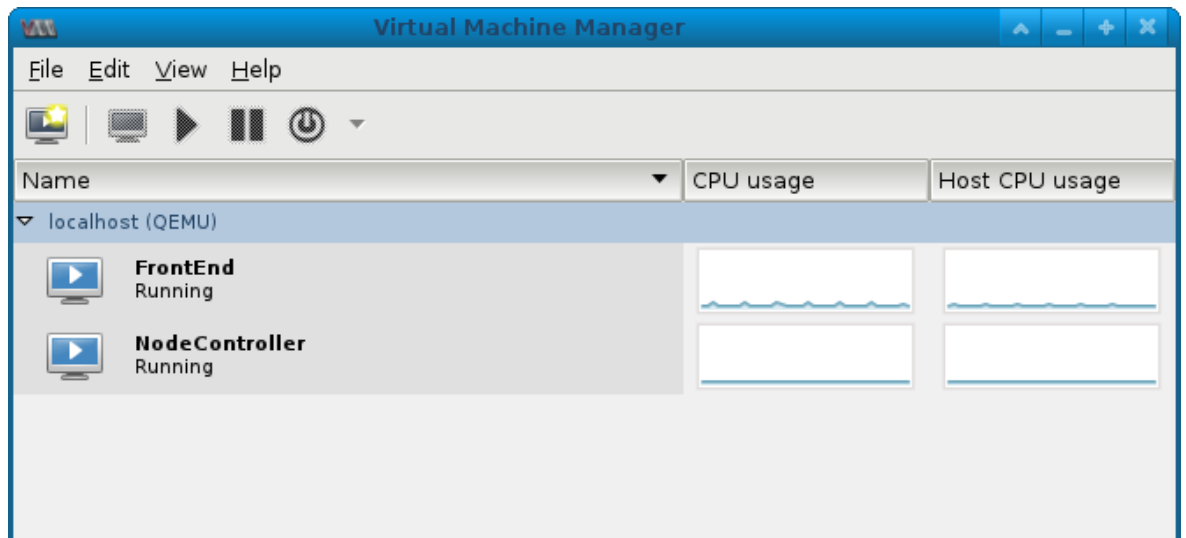
Ensimmäinen komento palauttaa prosessin ID:n ja nimen ”eucalyptus-clo”, jos palvelu on käynnistetty kyseiseen porttiin. Kolme viimeistä komentoa palauttavat IP:n ja komponentin tai palvelun nimen mihin ne ovat sidoksissa, jos asennus on onnistunut.

Node controller

Front end -palvelimen päivittämisen ja esiasetteluiden suorittamisen jälkeen aloitetaan seuraavan palvelinkoneen asentaminen. Asentaminen aloitetaan tuttuun tapaan luomalla VMM:llä uusi virtuaalikone. Virtuaalikoneen nimeksi annetaan tällä kertaa NodeController, koska se kuvastaa sen tehtävää. Virtuaalikoneen asetukset määritellään, kuten front end:n, eli 300GB tallennustila 2TB kiintolevyllä, 2048MB keskusmuistia ja kaksi ydintä suorittimelta.

Käyttöjärjestelmänkin asennus suoritetaan kuten edellisen palvelimen kanssa, mutta järjestelmän nimeksi annetaan sama kuten virtuaalikoneella, eli NodeController. Nimeämisen jälkeen asennus kysyy järjestelmän tehtäviä, missä oletuksena on valittuna ”Node controller”, ja lisäksi valittavina on Cluster controller ja Storage controller. Koska järjestelmään tarvitaan vain yksi klusteri ja siitä puuttuu node controller, pitäydytään oletuksena annetuissa valinnoissa ja jatketaan asennusta painamalla ”Continue”. Asennus ei tällä kertaa kysy käyttäjältä tunnuksia, koska ne saadaan olemassa olevalta front end -palvelimelta.

Asennuksen jälkeen palvelin päivitetään, kuten edellisenkin palvelimen kohdalla, käyttäen komentoja: *sudo apt-get update*, *sudo apt-get upgrade* ja *sudo apt-get dist-upgrade*. Päivityksen jälkeen huomioitava, että viimeisin komento vaatii järjestelmän uudelleenkäynnistämisen. Uudelleenkäynnistymisen jälkeen on hyvä testata node controllerin toiminta komennoilla: *euca-describe-availability-zones verbose*, joka antaa tulosteen cluster controllerin hallitsemista virtuaaliprosessoreista. Jos tulosteessa näkyy free/max kohdassa 0, voidaan olettaa, ettei yhteys toimi kunnolla, tai cluster controller ei toimi oikein. Jos yhteys toimii, ja tuloste palauttaa virtuaalikoneelle annettuja suorittimien määrän, voidaan seuraavaksi antaa front end -palvelimen hakea node controlleri komennolla *sudo euca_conf --discover-nodes*.



Kuva 14. Asennetut virtuaalikoneet

Kahden onnistuneen virtuaalikoneen asennuksen jälkeen VMM:n yleisnäkymässä on nähtävissä QEMU-yhteyden alla kuvassa 14 näkyvät kaksi palvelinta ja niiden suorittimien käyttö.

Client

Kahden virtualisoidun palvelimen asennuksen jälkeen aloitetaan hallintaan käytettävän työpöytäkäyttöjärjestelmän asennus. Tämä vaihe on periaatteessa vapaaehtoinen, koska hallinnointi voidaan suorittaa myös isäntäkoneella.

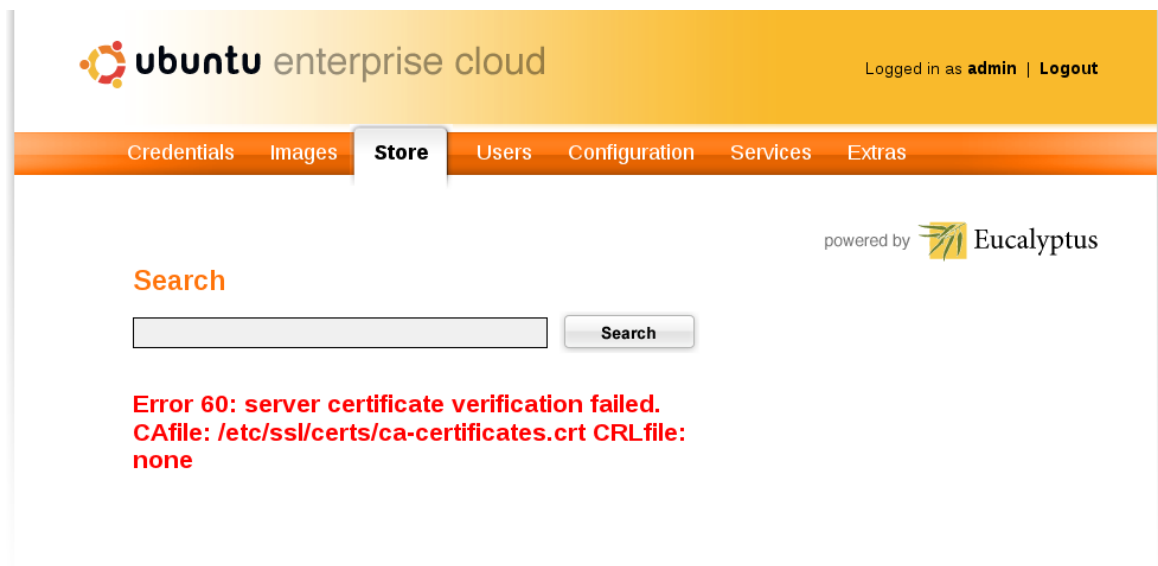
Asennus aloitetaan tuttuun tapaan luomalla VMM:llä uusi virtuaalikone. Virtuaalikoneen nimeksi annetaan Client, tallennustilaksi 200GB partitio, 2048MB keskusmuistia ja kaksi ydintä suorittimelta sekä lisäksi käsin määritetty virtualisoinnin valinta prosessorin arkkitehtuurista. Työpöytäkäyttöjärjestelmäksi valitaan Xubuntu 10.04 LTS 64bit. Asennus tapahtuu normaalisti käyttäen asennusmedian graafista käyttöliittymää. Järjestelmän nimen valinnassa on kuitenkin suotavaa käyttää sellaista nimeä, jolla virtuaalikone voidaan erottaa muista lähiverkon koneista.

Clientin asennuttua voidaan se päivittää, joko käyttöliittymän päivitystyökalun tai komentorivin kautta käyttämällä jo aikaisemmin esitettyjä komentoja. Päivityksen ja

uudelleenkäynnistämisen jälkeen tarkistetaan front end -palvelimen IP komennolla *ifconfig*. Client-koneen web-selaimella siirrytään seuraavaksi osoitteeseen <https://<front end IP>:8443>, joka oli tässä tapauksessa <https://192.168.1.9:8443>. Osoite avaa web-käyttöliittymän palvelunhallintaan. Ensimmäisellä kerralla syötetään käyttäjänimi *admin* ja salasana *admin*. Seuraavalla sivulla palvelu pyytää vaihtamaan käyttäjän salasanan. Käyttöliittymästä voidaan tarkistaa eri komponenttien tietoja ja niiden tiloja. Lisäksi ”Store”-näkyvästä voidaan ladata valmiita EMI-levy kuvia, mutta niiden sisältöön ei voida vaikuttaa. Levykuvalla tarkoitetaan tässä tapauksessa käyttöjärjestelmän kopiota, jossa on vain tietty ohjelmistopaketti asennettuna, ja sitä käytetään luomaan pilvipalveluun instanssi. Järkevintä jatkokäytön kannalta on opetella luomaan omat räätälöidyt levykuvat.

Levykuvan asentaminen

Levykuva voidaan asentaa helpoiten käyttämällä front end -palvelimella pyörivää web-käyttöliittymää. Käyttöliittymässä on välilehti nimeltään ”Store”, josta levykuvia instansseja varten voidaan hakea ja ladata. Tämän työn aikana kohdattiin jälleen uusi ongelma. Hakua suoritettaessa ilmestyi seuraava virhe.



Kuva 15. Virhe web-käyttöliittymässä

Virheen syyksi paljastui Canonicalin tarjoama vanhentunut sertifikaatti. Ongelmaan löytyi ratkaisu, mutta se olisi vaatinut käyttöjärjestelmän turvallisuusehtojen muokkaamista ja vähentämistä, joten se ei ollut järkevä vaihtoehto. Muuna keinona on hakea levykuvan pohja Eucalyptuksen sivuilta tai ladata jokin ”Extras”-välilehden vaihtoehtoista. Käyttöhetkellä molemmat vaihtoehtoista tarjosivat, lukuun ottamatta yhtä levykuvaa, samat valinnat. Lisäksi huomattiin, että sijainnit levykuville ovat samat. On täten aivan sama kumpaa vaihtoehtoista käyttää.

Testauksen vuoksi levykuvaksi valittiin CentOS 5.3 64bit. Paketti sisältää vaihtoehdot KVM:lle ja XEN:lle. Instanssin rekisteröimiseen tarvitaan kolmea tiedostoa: kernel-kuvaa, jonka tunnistaa yleensä vmlinuz-alkuisesta nimestä, ramdisk-kuvaa, jonka tunnistaa initrd-alkuisesta nimestä ja levykuvan, jonka tunnistaa yleensä *.img tai *.qcow2 -tiedostopäätteestä. Poikkeuksia tiedostojen nimeämislle voi olla, ja vastuu niiden tiedostamisesta jää ylläpitäjälle. CentOS 5.3:n tapauksessa ja KVM:ää käyttäessä valinnoiksi tulivat seuraavat tiedostot: vmlinuz-2.6.28-11-generic, initrd.img-2.6.28-11-generic ja centos.5-3.x86-64.img. Lisäksi tarvitaan euc2ools-työkalupaketti ja avainpari, jolla palvelin tunnistaa käyttäjätunnuksen. Euc2ools voidaan asentaa paketinhallinnasta. Avainpari voidaan ladata web-käyttöliittymää käyttäen ”Credential”-välilehden kohdasta ”Download Credentials”. Eucalyptuksen ohjeidenkin mukaan on suositeltavaa purkaa avainpari johonkin varmaan sijaintiin. Oletuksena esitetään piilotetun ”.euca/” kansion luomista käyttäjän kotihakemistoon, mutta käytännössä sijainti voidaan ja kannattaa määrittää oletuksesta poikkeavaksi, jotta mahdolliset haitalliset skriptipalvelut eivät sitä osaa hakea.

Avainparin nouto ja aktivoiminen tapahtuu komentoriviltä komennolla `. /polku/eucarc` (huomaa, että komennon alussa piste!). Avainparin noutoon käytetty skripti ei anna onnistuttuaan tulostetta. Avainpari joudutaan noutamaan aina uudelleen kirjautumisen jälkeen, koska sen tallennus on tilapäinen. Jos avainpari puuttuu, saadaan siitä huomautus levykuvaa rekisteröitäessä.

Levykuvan rekisteröimiseen käytetään euc2ools-työkaluja Eucalyptuksen sivuilta löytyvien ohjeiden avulla. On suositeltavaa ajaa komennot root-käyttöoikeuksilla, joka

aktivoidaan komennolla *sudo -i* (käyttöoikeuksien vaihdon jälkeen avainpari on ladattava uudelleen): /6/

Kernel-kuvan rekisteröimiseen:

```
euca-bundle-image -i vmlinuz-2.6.28-11-generic --kernel true
```

```
euca-upload-bundle -b centosbucket -m /tmp/vmlinuz-2.6.28-11-generic.manifest.xml
```

```
euca-register centosbucket/vmlinuz-2.6.28-11-generic.manifest.xml.
```

On suositeltavaa ottaa talteen viimeisimmän komennon palauttama ”eki-xxxxxxx” -arvo.

Ramdisk-kuvan rekisteröimiseen:

```
euca-bundle-image -i initrd.img-2.6.28-11-generic --ramdisk true
```

```
euca-upload-bundle -b centosbucket -m /tmp/initrd.img-2.6.28-11-generic.manifest.xml
```

```
euca-register centosbucket/initrd.img-2.6.28-11-generic.manifest.xml.
```

On suositeltavaa ottaa talteen viimeisimmän komennon palauttama ”eri-xxxxxxx” -arvo.

Levykuvan rekisteröimiseen (seuraavassa kohdassa arvot eki-* ja eri-* korvataan yltä saaduilla arvoilla. Jos arvoja ei jostain syystä ole saatavilla voidaan ne tarkistaa web-käyttöliittymästä ”Images”-välilehdestä):

```
euca-bundle-image -i centos.5-3.x86-64.img --kernel eki-E19B14FB --ramdisk eri-220115DF
```

```
euca-upload-bundle -b centosbucket -m /tmp/centos.5-3.x86-64.img.manifest.xml
```

```
euca-register centosbucket/centos.5-3.x86-64.img.manifest.xml.
```

On suositeltavaa ottaa talteen viimeisimmän komennon palauttama ”emi-xxxxxxx” -arvo..

Instanssi voidaan käynnistää komennolla: *euca-run-instances emi-81BE134B*. Tämän jälkeen työkalu palauttaa instanssin tiedot ja tilan. Tilaksi tulostuu aluksi pending, mutta se muuttuu hetken kuluttua tilaan running. Tila ja tiedot voidaan tarkistaa komennolla *euca-describe-instances*. Jos tietoja halutaan seurata jatkuvasti, voidaan käyttää lisäksi watch-työkalua. Komento on tämän jälkeen *watch -n1 euca-describe-instances*, missä -n1:n tilalle annetaan aika sekunneissa. Nyt käynnissä oleva instanssi toimii periaatteessa kuten normaali virtuaalipalvelin. Loppukäyttäjän tai ylläpitäjän on mahdollista luoda instanssiin

yhteys ssh-pääteohjelmalla ja tehdä tarvittavia tehtäviä ja/tai käynnistää palveluita ajoin. Tarvittaessa instanssi voidaan sulkea komennolla (i-*-arvo saadaan kopioimalla se edellisen työkalun tulosteesta) *euca-terminate-instance i-2E8605B8*.

6. YHTEENVETO

Työssä selvitettiin virtualisoinnin ja pilvipalveluiden mahdollisuuksista yksityisille asiakkaille ja yrityksille. Tuotteiden hinnat asettivat selvän rajauksen esiteltyihin ohjelmiin.

Virtualisointi avaa mahdollisuuksia esimerkiksi ohjelmistojen testaamiselle tai jo olemassa olevien palvelimien laajentamiselle. Virtualisoinnissa tarvittaviin hypervisorihin valittiin esittelyyn KVM ja Xen, jotka ovat GNU GPL –lisenssin alla olevia ohjelmistoja ja siksi ilmaisia. Molemmat toteuttavat tehtävänsä hiukan erillä lailla ja täten valinta kannattaa tehdä käytön mukaan. KVM on helppo vaihtoehto esimerkiksi kotikoneelle, jossa ei ole tarkoitus suorittaa virtuaalikoneilla tehtäviä jatkuvasti. KVM mahdollistaa hypervisorin ja virtuaalikoneiden helpon käynnistämisen ja sammuttamisen tarvittaessa. Xen on puolestaan hyvä valinta palvelinten ylläpitäjille, jotka haluavat laajentaa fyysisen palvelimen toimintaa virtuaalisten palvelinten ylläpitoalustaksi.

Pilvipalveluiden osalta ei voida hinnan perusteella suorittaa näin helppoa rajausta, koska muiden ylläpitämiä palveluita voidaan harvoin tarjota ilmaiseksi. Pilvipalvelut tarjoavat reilusti vaihtoehtoja tarpeen vaatiessa. Nykyään voidaan havaita, että lähes jokainen online-palvelu voidaan sijoittaa johonkin palvelutyyppiin. Työssä esiteltyjen päätyyppien lisäksi on olemassa useita muita tyyppejä, joiden toiminta ja käyttötarkoitus sivuavat päätyyppejä, eikä ole siksi valittuina tähän työhön. Pilvipalveluiden asiakkaina ovat yksityiset henkilöt sekä yritykset ja ryhmät. Kuitenkin pilvipalvelun tilaavat asiakkaat voidaan jakaa tyypeittäin: IaaS-tyypin palvelut keskittyvät suurille ja keskisuurille yrityksille, jotka haluavat siirtää palvelinlaitteistonsa muiden hoidettavaksi, PaaS-tyypin palvelut keskittyvät yrityksille tai ryhmille, jotka haluavat keskitetyn ohjelmiston kaikkien käyttöön, ja SaaS-tyypin pilvipalvelun tilaaja voi olla yksittäinen henkilö tai yritys palvelusta riippuen. PaaS- ja IaaS-tyypin pilvipalveluissa hinnoittelu tapahtuu käytön mukaan. SaaS-tyypin pilvipalvelut ovat näistä kolmesta poikkeus, sillä niissä on useita palveluita, jotka ovat ilmaisia käyttää. Ilmaiset ohjelmistot voivat tarjota lisää suorituskykyä tai ominaisuuksia maksua vastaan, mutta eivät vaadi sitä peruskäyttöön.

Tietoturvaa pidetään riskinä pilvipalveluissa. Sitä voidaan pitää järkevänä ajatteluna oli palvelu mikä hyvänsä. Tietoturva aiheuttaa eri toimia riippuen onko henkilö asiakas tai palvelun ylläpitäjä. Tietoturvaan voidaan pilvipalveluissa lisäksi luokitella tiedon säilyvyys ja sen saatavuus. On mahdollista että palvelukatkoksen, verkkoyhteyden katkeamisen tai palvelimien alasajon ajaksi yhteys palveluun katkeaa. Tämä estää palvelun käyttämisen, mitä voidaan luonnollisesti pitää ongelmana verkossa sijaitseville palveluille.

Pilvipalvelua voi ylläpitää myös itse. Tässäkin opinnäytetyössä toteutettu Ubuntun ja Eucalyptuksen yhteistyönä toteuttama UEC on helppo asentaa ja ylläpitää, jos siihen tarvittavat resurssit ovat saatavilla. Nykyään Ubuntu on ottanut Eucalyptuksen tilalle vastaavan OpenStack-ohjelmistokokonaisuuden. Toteutus on periaatteessa molemmissa vastaava asiakkaan kannalta.

Tämän työn toteutusosa aukaisi itselleni aivan uuden käsityksen palvelinhallinnasta ja sen mahdollisuuksista. Työ oli mielenkiintoinen ja riittävän haastava. Työssä luotu pilvipalvelu asennettiin yhden fyysisen laitteiston päälle virtuaalipalvelimille, mikä aiheutti erinäisiä ongelmia. Käytännössä tämä kyseinen tekniikka ei ole missään mielessä järkevä, koska modulaarinen palvelukokonaisuus on suunniteltu toteutettavaksi vähintään kahdella palvelimella. Alun ongelma, joka koski virtualisoinnin puuttumista virtuaalikoneissa, oli lähellä kaataa koko projektin. Onneksi vain pari viikkoa ongelman ilmaantumisesta julkaistiin päivitys, joka mahdollisti projektin jatkumisen. Työssä saadut tiedot tulevat olemaan itselleni tärkeitä ja aion niitä soveltaa tulevissa palvelinasennuksissani.

7. LÄHDELUETTELO

- /1/ Brodtkin Jon, FAQ: Desktop virtualization, [WWW-dokumentti], [<http://www.networkworld.com/news/2009/021909-desktop-virtualization-faq.html>], 05.01.2012
- /2/ CSS Corp Open Source Services, Eucalyptus Beginner's Guide, [WWW-dokumentti], [http://cssoss.files.wordpress.com/2010/06/book_eucalyptus_beginners_guide_uec_edition_1.pdf], 19.11.2011
- /3/ Desai Anil, Type 2 hypervisor (hosted hypervisor) [WWW-dokumentti], [<http://searchservervirtualization.techtarget.com/definition/hosted-hypervisor-Type-2-hypervisor>], 12.01.2012
- /4/ Dignan Larry, Virtualization: What are the security risks?, [WWW-dokumentti], [<http://www.zdnet.com/blog/security/virtualization-what-are-the-security-risks/821>], 12.01.2012
- /5/ Eucalyptus, Installing Eucalyptus 2.0, [WWW-dokumentti], [http://open.eucalyptus.com/wiki/EucalyptusInstallation_v2.0], 19.11.2011
- /6/ Eucalyptus, Managing Eucalyptus Images (2.0), [WWW-dokumentti], [http://open.eucalyptus.com/wiki/EucalyptusImageManagement_v2.0], 20.01.2012
- /7/ Fedora, Installing KVM packages on an existing Fedora system, [WWW-dokumentti], [http://docs.fedoraproject.org/en-US/Fedora/13/html/Virtualization_Guide/sect-Virtualization-Installing_the_virtualization_packages-Installing_KVM_packages_on_an_existing_Red_Hat_Enterprise_Linux_system.html], 19.11.2011
- /8/ Gianluca Cecchi, nested kvm tests questions, [WWW-dokumentti], [<http://lists.fedoraproject.org/pipermail/virt/2011-June/002702.html>], 20.11.2011
- /9/ Gil Paul, What Is 'SaaS' (Software as a Service)?, [WWW-dokumentti], [http://netforbeginners.about.com/od/s/f/what_is_SaaS_software_as_a_service.htm], 18.01.2012
- /10/ Gite Vivek, 20 Linux Server Hardening Security Tips, [WWW-dokumentti], [<http://www.cyberciti.biz/tips/linux-security.html>], 10.03.2012
- /11/ Gleb Reys, What Hardware Virtualization Really Means, [WWW-dokumentti], [<http://www.desktop-virtualization.com/2008/05/14/what-hardware-virtualization-really-means/>], 10.01.2012

- /12/ IBM, Virtual systems overview, [WWW-dokumentti], [<http://publib.boulder.ibm.com/infocenter/eserver/v1r2/index.jsp?topic=/eicay/eicayvserver.s.htm>], 04.01.2012
- /13/ Inspecta, Tietoturvajärjestelmän sertifiointi, [WWW-dokumentti], [<http://www.inspecta.com/fi/Palvelut/Sertifiointi/Jarjestelmasertifiointi/Tietoturvajarjestelman-sertifiointi/>], 02.02.2012
- /14/ Kangas Erik, What is Cloud Computing? [WWW-dokumentti], [<http://luxsci.com/blog/what-is-cloud-computing-or-how-to-speak-intelligently-about-cloud-and-virtual-private-servers.html>], 16.01.2012
- /15/ Keir Thomas, Choosing Cloud Backup For PCs, [WWW-dokumentti], [http://www.pcworld.com/businesscenter/article/223354/choosing_cloud_backup_for_pcs.html], 03.02.2012
- /16/ Kivity Avi, KVM: nVMX: Documentation, [WWW-dokumentti], [<https://github.com/torvalds/linux/blob/master/Documentation/virtual/kvm/nested-vmx.txt>], 25.11.2011
- /17/ Kolehmainen Aleks, Avoimen koodin OpenStack nousemassa pilven standardiksi, [WWW-dokumentti], [http://www.tietoviikko.fi/kaikki_uutiset/avoimen+koodin+openstack+nousemassa+pilven+standardiksi/a660259], 27.01.2012
- /18/ KVM, KVM, [WWW-dokumentti], [http://www.linux-kvm.org/page/Main_Page], 13.01.2012
- /19/ Larabel Michael, Ubuntu 11.10: Xen vs. KVM vs. VirtualBox, [WWW-dokumentti], [http://www.phoronix.com/scan.php?page=article&item=ubuntu_1110_xenkvm], 04.01.2012
- /20/ Mason Ross, What is PaaS (Platform as a Service), [WWW-dokumentti], [<http://blogs.mulesoft.org/what-is-paas-platform-as-a-service/>], 18.01.2012
- /21/ ”MrPointy”, Is KVM a type 1 or a type 2 Hypervisor?, [WWW-dokumentti], [<http://mrpointy.wordpress.com/2009/05/3/is-kvm-a-type-1-or-a-type-2/>], 04.01.2012
- /22/ Nixu, Tietojärjestelmiä pilvipalveluina – tietoturvallisesti?, [WWW-dokumentti], [<http://www.nixu.fi/artikkelit/2010/2/pilvipalveluista/>], 10.03.2012
- /23/ OpenStack, OpenStack: The Open Source Cloud Operating System, [WWW-dokumentti], [<http://openstack.org/projects/>], 02.02.2012
- /24/ OpenStack, Participating Companies, [WWW-dokumentti], [<http://openstack.org/community/companies/>], 27.01.2012

- /25/ Panettieri Joe, Ubuntu Cloud: OpenStack Wins, Eucalyptus Loses, [WWW-dokumentti], [<http://www.talkincloud.com/ubuntu-cloud-openstack-wins-eucalyptus-loses/>], 13.01.2012
- /26/ Petersen J. S., What is a Thin Client?, [WWW-dokumentti], [<http://www.wisageek.com/what-is-a-thin-client.htm>], 25.03.2012
- /27/ Pirinen Antti, Miten havaita tietomurrot?, [WWW-dokumentti], [<http://h7c.blogspot.com/2011/11/miten-havaita-tietomurrot.html>], 10.03.2012
- /28/ QEMU, QEMU, [WWW-dokumentti], [http://wiki.qemu.org/Main_Page], 13.01.2012
- /29/ Rares Aioanei, Comparison of major Linux package management systems, [WWW-dokumentti], [<http://how-to.linuxcareer.com/comparison-of-major-linux-package-management-systems>], 15.03.2012
- /30/ Red Hat, Red Hat, [WWW-dokumentti], [<http://www.redhat.com/>] 15.03.2012
- /31/ Samson Ted, Year-old OpenStack's cloud future looks rosy, [WWW-dokumentti], [<http://www.infoworld.com/d/cloud-computing/year-old-openstacks-cloud-future-looks-rosy-168165>], 30.01.2012
- /32/ Saper Anthony, Why Is Cloud Computing The Most Popular Technology Of Modern Times, [WWW-dokumentti], [<http://cloudpath.pathcom.com/blog/why-is-cloud-computing-the-most-popular-technology-of-modern-times/>], 16.01.2012
- /33/ “Shaon”, Eucalyptus and it’s components, [WWW-dokumentti], [<http://mdshaonimran.wordpress.com/2011/11/26/eucalyptus-and-its-components/>], 28.11.2011
- /34/ “Solari”, AMD and Intel I/O Virtualization, [WWW-dokumentti], [<http://blog.solari.net/2009/04/26/amd-and-intel-io-virtualization/>], 10.01.2012
- /35/ Timothy Chou, Introduction to CloudComputing, [WWW-dokumentti], [<http://www.scribd.com/doc/64699897/Introduction-to-Cloud-Computing-Business-and-Technology>], 21.01.2012
- /36/ VMware, History of Virtualization, [WWW-dokumentti], [<http://www.vmware.com/virtualization/history.html>], 04.01.2012
- /37/ VMware, VMware ESXi and ESX Info Center, [WWW-dokumentti], [<http://www.vmware.com/products/vsphere/esxi-and-esx/overview.html>], 14.01.2012
- /38/ Xen.org, Xen Hypervisor Project, [WWW-dokumentti], [<http://www.xen.org/products/xenhyp.html>], 13.01.2012