Osaamista
ja oivallusta
tulevaisuuden
tekemiseen

Samu Niemipelto

Juniper-virtuaalikoneiden testaaminen VMware-ympäristössä

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikka

Insinöörityö

11.5.2019

Tekijä Otsikko Sivumäärä Aika	Samu Niemipelto Juniper-virtuaalikoneiden testaaminen VMware-ympäristössä 45 11.5.2019
Tutkinto	insinööri (AMK)
Tutkinto-ohjelma	Insinööri (AMK), Tietotekniikka
Ammatillinen pääaine	Tietoverkot
Ohjaajat	Erik Pätynen

Ammattikorkeakoulu Metropolia on ottamassa käyttöönsä Juniper Networksin verkkokursseja, joiden suorittaminen tapahtuu virtuaalisilla versioilla Juniperin laitteista. Tämä tuo hyödyllistä lisävalikoimaa Metropolian opetustarjontaan perinteisten Cisco-kurssien rinnalle.

Tämän opinnäytetyön tarkoituksena alkuperäisesti oli testata virtuaaliympäristöä ja sen sisältämiä virtuaalikoneita etäkäytöllä Metropolian palvelimelta, jolla ympäristö toimii ESXi-hypervisorin kautta. Tässä ympäristössä tulee olemaan opiskelijoille tarkoitettu työpöytä, jolta löytyvät niin tarvittavat virtuaalikoneet, kuin näiden aloituskonfiguraatiot sekä ohjeet laboratoriatöiden suorittamiseen.

Erinäisten syiden seurauksena tässä työssä kuitenkin päädyttiin suorittamaan työ lokaalisti. Työssä siis rakennetaan VMware Workstationissa topologia käyttäen Juniperin virtuaalilaitteita, joilla topologia rakennetaan. Tarkoituksen on Juniper Networksin virtuaalikoneiden testaaminen ja varmentaminen, jotta nämä soveltuvat kurssikäyttöön.

Aluksi työssä käydään läpi virtualisointia yleisesti sekä komponenttejä, joilla Metropolian virtuaaliympäristö verkkokursseja varten on rakennettu. Tämän jälkeen käytännön osuudessa käsitellään lokaalisti rakennetun topologian periaatteita sekä itse konfiguroimista.

Työ oli tekijälle ensikosketus virtualisoinnin maailmaan ja antoi hyvää kokemusta virtualisoinnista yleisesti sekä virtuaaliympäristön rakentamisesta.

Avainsanat	Virtualisointi, Vmware, Juniper

Author	Samu Niemipelto
Title	Testing of Juniper virtual Machines in VMware environment
Number of Pages	45 pages
Date	11 May 2019
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Professional Major	Networks
Instructors	Erik Pätynen

Metropolia University of Applied Sciences is about to start using a series of online courses provided by Juniper Networks. Completing these courses will happen on virtual versions of Juniper Networks devices. The addition of these courses to the course selection provided by Metropolia will add a useful benefit besides the Cisco courses that Metropolia is already providing.

The goal of this thesis was originally to test the virtual environment and the virtual machines within it within the laboratories of Leppävaara campus and with remote use. The environment there will work on an ESXi hypervisor, along with VMware vCenter and vSphere. This environment will include a virtual desktop for students to use and from within that virtual desktop students will find the virtual machines, starting configurations for the devices and instructions for completing the assignments.
However, as a consequence of unfortunate events, this work will be completed locally. This thesis will use VMware Workstation as the hypervisor, in which it will run three virtual machines. A network topology was built on these machines. The main goal of this thesis is to test out those virtual machines and determine whether they are suitable for the completion of these online courses.

In the first chapters the reader will be introduced to the basic concepts of virtualization and the components used for the virtual environments. After this, the actual virtual environment for testing purposes will be built and tested.

This thesis was the first touch into the world of virtualization for the write, and it gave a good experience and challenges along the way

Keywords	Virtualisointi, VMware, Juniper

Sisällys

Lyhenteet

BIOS	Basic Input-Output System. Ohjelma, joka sijaitsee yleensä koneen emolevyllä.
RAID	Redundant Array of Independent Disks. Tapa varmentaa datan säilyvyys.
VLAN	Virtual Local Area Network. Virtuaalinen lähiverkko.
VRRP	Virtual Router Redundancy Protocol. Tapa varmentaa tietoverkon toimivuus.
VPN	Virtual Private Network. Suojattu yhteys kahden tai useamman laitteen välillä.
POSIX	Portable operating System interface. Standardi Unix-käyttöjärjestelmille.
VMM	Virtual Machine Monitor. Ohjelma virtuaalikoneiden luontiin ja hallintaan.
SSO	Single Sign-on. Mahdollistaa käyttäjälle yhden käyttäjätunnus/salasana-kombinaation useaan palveluun.
SSH	Secure Shell. Tietoliikenneprotokolla salattua tietoliikennettä varten.
UUID	Universally Unique Identifier. Universaali ja uniikki tunniste laitteistolle.
vSS	Virtual Standard Switch. Standard-versio virtuaalikytkimestä.
vDS	Virtual Distributed Switch. Distributed-versio virtuaalikytkimestä.
vSRX	Virtual SRX. Virtuaalinen versio Juniperin SRX-laitteesta.
vMX	Virtual MX. Virtuaalinen versio Juniperin MX-laitteesta.
vQFX	Virtual QFX. Virtuaalinen versio Juniperin QFX-laitteesta.

VR	Virtual Router. Virtuaalinen reititin.

1 Johdanto

Tämän opinnäytetyön idea lähti liikkeelle hankkeesta, jossa Metropolia Ammattikorkeakoulu ottaa koulutustarjontaansa mukaan joukon Juniper Networksin tarjoamia verkkokursseja. Näiden verkkokurssien aihepiirit keskittyvät tietoverkkoihin, ja ne sisältävät aiheita tietoverkkojen reitityksestä, Layer 2-tekniikoista sekä ongelmanratkaisusta. Opinnäytetyön alustana käytetään VMwaren kehittämää virtualisointiympäristöä, johon tullaan rakentamaan virtuaalinen työpöytä opiskelijoiden käyttöön. Tältä virtuaaliselta työpöydältä opiskelijat löytävät keskitetysti VMwaren virtuaalilaitteet, joilla itse Juniperin kurssit suoritetaan sekä laboratoriotyöohjeet.

Tämän insinöörityön tarkoitus on tuoda lukijan tietoon yleistä tietoa virtualisoinnista, sen historiasta, sen eri käyttökohteista ja menetelmistä. Näiden lisäksi lukijan tietoon saatetaan menetelmät, joilla tällainen ympäristö, joka Metropolia Ammattikorkeakoululla on käytössään, on rakennettu. Näin ollen lukijalla on tämän insinöörityön luettuaan hyvät perusvalmiudet ja tietämys, mikäli hän haluaa rakentaa vastaavanlaisen ympäristön esimerkiksi kotioloihinsa harjoittelumielessä tai erilaisiin työelämän käytännön ratkaisuihin. Huomioitavaa kuitenkin on, että työn tarkoituksena ei ole käydä yksityiskohtaisesti läpi toteutukseen käytettävien komponenttien asennusprosessia, sillä tämä on tehty hyvin suoraviivaiseksi ja selkeäksi. Lisäksi valmistajien sivuilta löytyvät asennusprosesseihin mainiot ohjeistukset. Komponenttien asennusprosessien sijaan tässä työssä käsitellään virtuaaliympäristön käyttöönottoa ja sen testaamista. Työn loppupuolella testataan myös hieman itse Juniperin verkkokurssien suorittamista erilaisilla Juniperin virtuaalilaitteilla.

Tämä opinnäytetyö sisältää aluksi teoriaosuuden, jonka jälkeen työssä siirrytään käsittelemään varsinaista käytännön osuutta. Teoriaosuudessa käsitellään ensiksi lyhyelti virtualisoinnin historiaa, sekä sitä, miltä sen tilanne näyttää nykypäivänä verrattuna sen ensiaskeliin. Tämän jälkeen virtualisointia käsitellään yleisesti hieman pidemmin. Työssä kerrotaan myös virtualisoinnin hyödyistä, käyttökohteista ja mahdollisista riskitekijöistä, jotka tulee ottaa huomioon.

Työn toisessa osiossa, eli varsinaisessa käytännön osuudessa tuodaan lukijan tietoon step-by-step-tyylisesti selkeät suuntaviivat, miten tämänlainen ympäristö on rakennettu ja käyttöönotettu. Käytännön osuus sisältää myös virtuaalilaitteiden testaamista. Työssä käydään myös läpi sitä, miten opiskelija pääsee suorittamaan näitä Juniper Networksin verkkokursseja. Lopussa käydään läpi hieman kirjoittajan pohdintaa näistä kursseista, virtuaaliympäristöstä sekä virtualisoinnista yleisesti.

2 Virtualisoinnista yleisesti

Mikäli virtualisointi pitäisi sisällyttää yhteen lauseeseen pähkinänkuoressa, olisi se fyysisten laitteiden jakamista tai yhdistämistä loogisiksi resusseiksi. Wolf ja Halter (2005, s.23) määrittelevät virtualisoinnin olevan fyysisten teknologioiden rajojen abstraktointia. Esimerkiksi työasemat ja palvelimet eivät enää tarvitse dedikoitua laitteistoa, kuten keskusyksikköä tai emolevyä voidakseen toimia itsenäisinä entiteetteinä. Sen sijaan ne voivat toimia virtuaalikoneen sisällä.

Virtualisoinnilla voidaan jakaa yksi fyysinen resurssi, kuten vaikkapa palvelin, monen eri loogisen järjestelmän käytettäväksi. Tästä hyvänä, monelle tietotekniikan opiskelijalle tuttuna esimerkkinä voisi toimia hyvin vaikkapa kiintolevyn osiointi, joka on myös eräänlaista virtualisoimista, vaikkei sitä tule ajatelleeksi. Kiintolevyn osioinnissa käyttäjä haluaa jakaa yhden fyysisen kiintolevyn resurssit kahdeksi tai useammaksi loogiseksi asemaksi. Fyysisesti kiintolevy siis pysyy täysin samanlaisena yhtenäisenä laitteena kuin aina ennenkin, eikä sitä tule fyysisesti rikkoa moniksi kappaleiksi. Sen sijaan se esiintyy osioinnin jälkeen loogisella tasolla eri tavalla. Loppukäyttäjä ei siis fyysisesti näe mitään eroa virtualisoidun ja ei-virtualisoidun laitteen välillä, vaan ero on siinä, miten laitteet loogisesti toimivat.

Virtualisoinnilla voidaan siis jakaa yksi fyysinen resurssi moneen eri osaan, kuten edellisestä esimerkistä kävi ilmi. Se toimii kuitenkin myös toisinpäin, eli on mahdollista yhdistää useampi looginen resurssi yhdeksi suureksi entiteetiksi. Tästä hyvinä esimerkkeinä voisivat toimia verkkovirtualisoinnin alueelta virtaaliset lähiverkot VLAN:t sekä linkkiaggregaatiotekniikat, kuten vaikkapa EtherChannel.Virtuaalisia lähiverkkoja hyväksikäyttäen on mahdollista jakaa tietoverkko haluttuun määrään loogisia aliverkkoja,

esimerkiksi erottelemalla jonkin yhtiön eri osastot omiin loogisiin aliverkkoihinsa, VLAN:ihin. Tällä menetelmällä tulee mahdolliseksi hallita näitä virtuaalisia aliverkkoja toisistaan erillään ja niihin voidaan soveltaa eri sääntöjä keskenään. EtherChannel puolestaan on linkkiaggregaatiotekniikka, joka mahdollistaa kahden tai useamman fyysisen Ethernet-linkin niputtamisen yhdeksi isoksi loogiseksi kanavaksi. Tämän käyttötarkoitus on luoda vikatoleranssia sekä nostaa linkin nopeutta.

Mainittava asia ovat myös resource poolit, eli resurssiryhmät. Käytännössä niillä voidaan jakaa fyysisen laitteiston CPU- ja muistiresursseja virtuaalikoneille. Ne ovat tapa jakaa näitä fyysisiä resursseja loogisiin osiin, joita voidaan määritellä tilanteen vaatimalla tavalla. Esimerkkinä tilanteesta, jossa resurssiryhmät osoittautuvat hyödyllisiksi, on tilanne, jossa yrityksen eri osastot tarvitsevat erilaiset määrittelyt. Osastosta riippuen kaikki osastot eivät välttämättä tarvitse yhtä suurta määrää resursseja. Resurssiryhmillä voidaan jakaa yrityksen eri osastot eri ryhmiin sekä määrittää näille tarpeenmukaiset asetukset, joissa suurempi määrä fyysisiä resursseja allokoidaan sille ryhmälle, joka niitä enemmän tarvitsee. [5, s. 92.]

Virtualisointi tuo siis mukanaan monia hyötyjä, mutta se tuo mukanaan myös uusia haasteita alan ammattilaisille. Virtualisoinnin mukanaan tuomia hyötyjä, kuten myös sen haasteitakin käsitellään tarkemmin myöhempänä luvuissa 2.2 ja 2.3.

2.1 Virtualisoinnin historia

Laitemäärät ovat kasvaneet ympäri maailman huimaa vauhtia. Tämä on luonut huutavan resurssitarpeen, mikä pakottaa eri toimijoita etsimään uusia ratkaisuja tilanpuutteen, skaalautuvuuden ja myös liikkuvuuden vuoksi. Voitaisiin siis helposti kuvitella, että virtualisointi on nykypäiväisten innovaatioiden tuotos, mutta asia ei kuitenkaan aivan näin ole. On totta, että virtualisointi on kehittynyt viime vuosina hurjasti, mutta sen juuret juontavat pidemmälle. Idea järjestelmistä, jotka mahdollistaisivat fyysisten ja loogisten resurssien erittelemisen toisistaan juontaa juurensa jo myöhäiselle ja varhaiselle 70-luvulle. Tällöin uuden tietotekniikan alueelle uuden tulokkaan, virtualisoinnin, uranuurtajana toimi tietotekniikan jättiläinen IBM. Noina päivinä virtualisointi oli kutenkin vielä aivan lastenkengissään, ja vaikka idea olikin hyvä, niin ei tekniikka kuitenkaan ollut läheskään sillä tasolla, millä sen nykypäivänä tiedämme. Kuitenkin jo 1980-luvulla

maailma sai nähdä ensimmäiset esimerkit sovellusvirtualisoinnista sekä virtuaaliverkoista.

Harppaus ajassa eteenpäin vuoteen 1998 toi mukanaan yhtiön, joka kenties monelle tulee ensimmäisenä mieleen nykypäivänä, kun virtualisointi nousee puheeksi. Tällöin kuvaan astui mukaan nimittäin Yhdysvaltojen Palo Altosta kotoisin oleva VMware, josta nopeasti tuli yksi virtuaalimaailman kärkitekijöistä. Vuonna 1999 Vmware julkaisi maailman ensimmäisen x86-pohjaisen täysvirtualisointiin kykenevän sovelluksen nimeltään VMware Workstation. Tämä tuote on varmaankin monelle lukijalle tuttu, sillä se on vieläkin käytössä kantaen myös samaa nimeä. Työn kirjoittamisen aikana uusin versio tästä sovelluksesta on versio 15.0.

Tämän jälkeen markkinoilla alkoi esiintyä liuta muitakin nimiä, jotka keskittyivät nimenomaan Vmwaren pioneeraamiin x86-pojaisiin ratkaisuihin. Näistä tuolloin mainittavimpana nimenä XenSource Inc., jonka XEN-virtualisointisovellus oli maailman ensimmäinen avoimeen lähdekoodiin perustuva virtualisointisovellus vuonna 2003. Myöhemmin XenSourcen osti Citrix Systems, ja tämän nimen alla nykyisinkin virtualisointiratkaisu Citrix toimii. Vuosina 2005 ja 2006 Vmware toi markkinoille Vmware Playerin sekä Vmware Serverin, joista nämä molemmat ilmestyivät ilmaisina. Vuonna 2008 kaikille tuttu Microsoft lähti myös peliin mukaan tuomalla markkinoille Windows-ympäristöön tarkoitetun Hyper-V:n, jonka julkaiseminen tapahtui Windows Server 2008:n julkaisemisen rinnalla.

Nykyisellään Vmware on edelleen yksi maailman mainittavimmista nimistä, kun puhutaan virtualisoinnista. Heidän tarjoamiensa virtualisointisovellusten kirjo on hyvin laaja. VMwaren tunnetuimpia tuotteita ovat VMware Server, VMware Workstation, VMware Player sekä VMware vSphere.

Virtualisointiratkaisut ovat saavuttaneet nykyisellään nopeasti suosiota, niin ikään virtuaalisten palvelimien määrä on kasvanut rajusti. Jo vuonna 2009 virtuaalisten palvelinten määrä oli fyysisten palvelinten määrää suurempi. [1, s.12; 2.]

2.2 Virtualisoinnin hyödyt

Nykyajan alati kasvavassa globaalissa yhteiskunnassa ongelmaksi ovat nousseet IT-infrastruktuurien vaatimien laitteistojen ja näin ollen myös niiden tarpeisiin vaadittavien tilojen määrän räjähdysmäinen kasvu. Näiden mukana myös olennaisesti nousee ratkaisevalla tavalla myös kysymys hinnasta. Eritoten suuret ja keskisuuret yritykset pystyvät karsimaan tarvitsemaansa laitemäärää ja tämän myötä myös kustannuksiaan ottamalla käyttöönsä virtualisoitiratkaisuita. Menneinä vuosina datakeskuksissa vallitsi varsinainen villi länsi, ja ne olivat pulllollaan palvelimia, joita ei hyödynnetty tavalla, jolla niin suuri laitemäärä olisi ollut kustannustehokasta. Huomioitavaa kuitenkin on, että tuo valtava laitemäärä oli kenties yrityksen toiminnalle välttämätöntä. Nykypäivänä virtualisoinnin ansiosta voidaan yhdeltä palvelimelta toimittaa useita palveluita, niin laitteiston sekä myös tarpeellisen vaaditun tilan määrä vähenee. Hyvänä esimerkkinä ajasta ennen päteviä virtualisointiratkaisuja, yrityksen halutessa käyttää Windows- ja Unix-palvelimia samanaikaisesti näille molemmille vaadittiin kullekin oma fyysinen palvelimensa. Nykyään vastaavanlainen ratkaisu voidaan virtualisoinnin ansiosta toteuttaa ainoastaan yhdellä palvelimelle, jossa esimerkiksi UNIX toimii virtualisoituna kerroksena Windowsin kanssa samalla palvelimella. Nämä ovat loogisesti eroteltu toisistaan eivätkä näin ollen aiheuta ristiriitaa keskenään. Tämänlaista palvelinten yhdistämistä yhdeksi kutsutaan nimellä konsolidaatio. Konsolidaation mittaa kutsutaan nimellä consolidation ratio, ja se lasketaan siitä, montako virtuaalikonetta palvelimella on. Ylläolevassa esimerkissä, jossa UNIX- ja Windows-palvelimet toimivat yhdellä fyysisellä palvelimella cosolidation ratio olisi siis 2:1. [1, s. 10.]

Itseasiallisen fyysisen laitteiston määrän vähentyessä yrityksille aukenee mahdollisuus myös karsia kustannuksiaan pienemmiksi, ja tästä johtuen myös asentamiseen ja ylläpitoon tarvittavan henkilöstön määrä vähenee. Näin ollen henkilöstöä, jota ennen virtualisointia tarvittiin valtavan laitteistomäärän ylläpitoon, voidaan siirtää vaativampiin asiantuntijatehtäviin. Tämä luonnollisesti myös mahdollistaa henkilöstömäärän leikkaamista, mikäli yrityksellä ei ole mahdollisuutta tai tarvetta siirtää tätä osaa henkilöstöstään uusiin haasteisiin. Virtuaalikoneiden hallinta on myös helpompaa, ja se voi tapahtua myös etäkäytöllä. Tästä johtuen ylläpitäjien aikaa vapautuu muiden tehtävien hoitamiseen. Etätyömahdollisuuksien lisääntyessä saadaan myös kitkettyä ruuhkaliikenteen määrää, mikä on aina positiivista - katsoi sitä miltä kantilta hyvänsä.

Virtuaalikoneiden erinomainen skaalautuvuus on myös suuressa roolissa, kun mietimme virtualisoinnin tuomia hyötyjä. Virtuaaliset järjestelmät skaalautuvat puhtaasti fyysisiin järjestelmiin verrattuna paremmin ja helpommin sekä myös vikatilanteita silmällä pitäen virtualisointi on luotettavampi ratkaisu. Järjestelmän ollessa virtualisoitu, ongelmatilanteen esiintyessä palvelimia tai ohjelmistoja ei tarvitse rakentaa uudelleen, sillä virtuaalikoneiden imaget ovat helposti palautettavissa. Esimerkiksi VMwarella on ongelmatilanteita silmälläpitäen kehitetty kaksi ohjelmaa, jotka ovat osa VMware vSphere -ohjelmistoa: Vmware High Availability ja Vmware Fault Tolerance. Nämä on suunniteltu ja kehitetty palauttaman virtuaalikoneet toimintaan hyvin lyhyessä ajassa. Näitä komponentteja käsitellään tässä työssä tarkemmin luvuissa 5.4 ja 5.5. On myös mahdollista siirtää virtuaalikoneita palvelimelta toiselle ennaltaehkäisevästi. Tämä tulee hyödylliseksi toiminnoksi, jos on esimerkiksi tiedossa, että jonkin datakeskuksen alueelle on tulossa tornado tai jokin muu luonnonkatastrofi. Siirto tapahtuu lähes silmänräpäyksessä eikä aiheuta käyttäjille päänvaivaa. [1, s. 11-14.]

Modernissa ja alati kasvavassa yhteiskunnassa, jossa ilmastonmuutos on noussut kriittiseksi ongelmaksi, virtualisointi tuo mukanaan pelkkää hyvää. Jo edellä mainittu etätyön lisääntyminen on tästä hyvä esimerkki. Tämän lisäksi erityisesti suurten datakeskusten sekä yritysten laitteistotarpeiden vähetessä näiden energiantarve vähenee, jonka myötä näiden hiilijalanjälki on pienempi.

2.3 Virtualisoinnin haitat

Vaikkakin virtualisoinnin mukanaan tuomat hyödyt painavat vaakakupissa mahdollisia haittoja enemmän, on tarpeellista käsitellä myös näitä haittapuolia. Ensimmäisenä mahdollisena haittapuolena tulevat vastaan sen tuomat aloituskustannukset. Virtualisoinnin alkukustannukset voivat nousta korkeiksikin, varsinkin jos jo olemassa oleva fyysinen laitteisto on vanhaa ja tehotonta. Tällöin on virtualisointiin mahdollisesti liittyvien lisenssien lisäksi otettava huomioon myös uuteen laitteistoon kuluvat kustannukset. Tämä on kuitenkin hieman kaksiteräinen miekka, sillä kuten jo aiemmin on mainittu, virtualisointi luo myös mahdollisuuden vähentää fyysisen laitteiston tarvetta, joten initiaaliset kustannukset riippuvat täysin jo olemassa olevasta infrastruktuurista sekä halutuista virtualisointilisensseistä. Monilla yrityksillä infrastruktuuri on varmastikin

pysynyt ajan hermoilla, joten näin ollen jäljelle jäävät ainoastaan lisensointiin kuluvat kustannukset.

Toisena haasteena on uuden infrastruktuurin opetteleminen. Virtuaalisen infrastrukstuurin hallinta vaatii täysin uudenlaista osaamista verrattuna perinteiseen puhtaasti fyysisen laiteiston hallintaan. Olemassa olevan IT-henkilöstön osaamisesta riippuen voi edessä olla uudelleenkouluttamista, mutta se voi vaatia myös täysin uuden henkilöstön rekrytoimista. Virtuaalimaailman osaajien asiantuntemus on kullanarvoista, ja se näkyy myös asiantuntijoiden palkoissa. Työnhakusivusto Indeed.comin mukaan tämän tyyppisten osaajien keskiarvoinen palkka on noin 70 000 dollaria vuositasolla. Huomionarvoista ovat myös resurssien vääränlainen allokointi tai joissain tapauksissa yliallokointi. Tämä voi johtaa suorituskyvyn heikkenemiseen tai huonoimmassa tapauksessa jopa palveluiden toimimattomuuteen. Tässä nimen omaan astuu kuvaan henkilöstön kouluttaminen tai osaavien asiantuntijoiden rekrytoiminen, jotta tämänkaltaiset tilanteet voitaisiin välttää.

Kenties pahimpana riskinä kuitenkin ovat virtualisoinnin mukanaan tuomat tietoturvariskit. Esimerkiksi hypervisorit tuovat mukanaan uuden kerroksen, joka voi joutua hyökkäyksen kohteeksi. Kuten esimerkiksi päivittämättömät Windows-käyttöjärjestelmät ovat alttiita hyökkäyksille, on asia samankaltainen päivittämättömien hypervisorien kanssa niiden ollessa myös eräänlaisia käyttöjärjestelmiä. Yksikin saastunut virtuaalikone voi pahimmassa tapauksessa saastuttaa kaikki virtuaalikoneet, jotka toimivat samalla palvelimella saastuneen koneen kanssa. Tilannetta, jossa administraattori ei voi enää hallita virtuaalikoneitaan tehokkaasti kutsutaan nimellä VM Sprawl. [3; 4.]

3 Virtualisointimenetelmät ja hypervisorit

Virtualisointityyppejä on nykyisellään olemassa useita, ja niiden käyttötarkoitukset vaihtelevat aina käyttöjärjestelmien virtualisoinnista tietoverkkojen virtualisointiin asti. Tässä luvussa käsitellään näitä menetelmiä sekä niiden käyttötarkoituksia tarkemmin.

3.1 Palvelinvirtualisointi

Suurin virtualisoinnin osa-alue on palvelinvirtualisointi. Palvelinvirtualisoinnissa kyse on siitä, että yhden laitteen fyysiset resurssit voidaan jakaa usean itsenäisen virtuaalikoneen käytettäväksi. Itsenäisellä tässä tapauksessa tarkoitetaan sitä, että virtuaalikoneet eivät aiheuta ristiriitaa keskenään, vaikka ne toimivatkin samalla fyysisellä alustalla.

Laitteen fyysinen kerros abstraktoidaan hypervisorin toimestaja esitetään tällä tavalla virtuaalikoneille käytettäväksi. Hypervisorin tulee tässä tapauksessa olla niin kutsuttu ’”bare metal” -hypervisor, eli ensimmäisen tyypin hypervisor, joka on asennettuna suoraan itseasialliselle fyysiselle laitteistolle ilman välissä olevaa käyttöjärjestelmää. Eri virtuaalikoneille on mahdollista jakaa mielimääräisesti fyysisiä resurssejä joko niiden määrittelyvaiheessa tai myöhemmin, ja näiden fyysisten resurssien jakamisesta vastaa niin ikään myös hypervisor. Hypervisoreita käsitellään tässä työssä tarkemmin luvussa 4.

Käyttämällä hyödyksi palvevinvirtualisoinnin suomia mahdollisuuksia laitteen fyysisiä resurssejä voidaan nykyään hyödyntää erinomaisen hyvin. Tämä johtuu suurilta osin siitä, että virtuaalikoneet on eroteltu fyysisestä kerroksesta, ja pystyvät toimimaan samalla palvelimelle aiheuttamatta ristiriitaa keskenään. Esimerkiksi Windows- ja Linux-palvelimet voivat virtualisoituina toimia samalla palvelimella nykyään, kun taas ennen se ei ilman virtualisointia ollut mahdollista. Näin saadaan kitkettyä fyysisen laitteiston hukkaresursseja ja ottamaan ne hyödylliseen käyttöön. On siis tapahtunut suurta edistystä palvelinten saralla verrattuna aikaan, jolloin virtualisointi ei ollut mahdollista. Ei siis liene yllätyksellistä, että jo vuonna 2009 raportoitiin virtuaalisten palvelinten määrän ylittävän fyysisten palvelinten määrän. [1, s. 12; 1, s. 16.]

3.2 Työpöytävirtualisointi

Toisia yleisiä kohteita virtualisoinnille ovat työpöydät. Työpöytävirtualisoinnilla voidaan tarjota loppukäyttäjälle samankaltaiset palvelut, kuin mitä hän saisi normaalisti PC:tä käyttäessäänkin. Erona tässä on se, että työpöytä sekä niin ikään myös sen sisältämät

ohjelmat eivät varsinaisesti toimi suoraan hänen koneellaan, vaan ne tulevat palvelimen kautta. Yleensä virtuaalisten työpöytien käytössä hyödynnetään niin kutsuttuja ”thin clientteja”, eli kevyitä asiakaspäätteitä. nämä ovat suurimmaksi osaksi halvempia kuin perinteiset PC:t, mutta mikä alhaisessa hinnassa näkyy, niin se suoritustehossa puuttuu. Tehokkaita niiden ei tosin tarvitsekaan olla, sillä työpöytä ja ohjelmistot toimivat käyttäen hyödyksi palvelimen huomattavasti tehokkaampaa laitteistoa.

Suuri etu työpöytävirtualisoinnille on myös datan säilyvyys. PC:n hajotessa kaikki data oli tuolla PC:llä, tai hyvässä tapauksessa ulkoisella kovalevyllä, tai kenties pilvipalvelussa. Usein kuitenkin peruskäyttäjällä data on ainoastaan hänen käyttämällään PC:llä, joten tällöin tämän PC:n hajotessa sen sisältämää dataa on vaikeaa, ellei jopa mahdotonta palauttaa. Kun taas käytetään virtuaalista työpöytää, niin kaikki data säilyy palvelimella datakeskuksessa, jossa dataa hallitsee ammattilainen eikä peruskäyttäjä, jota varmuuskopiointi ei voisi vähempää kiinnostaa. [1, s. 18.]

3.3 Tallennusjärjestelmävirtualisointi

Tallennusjärjestelmien virtualisointi tarkoittaa kahden tai useamman tallennusjärjestelmän yhdistämistä siten, että ne ilmenevät käyttöjärjestelmälle yhtenä loogisena järjestelmänä. Myös RAID-järjesteltyä tallennustilaa voidaan pitää eräänlaisena tämän alueen osana, jolloin useat fyysiset levyt voidaan esittää yhtenä levynä joka prosessien taustalla kopioi datan jollekin tai mahdollisesti myös kaikille näistä levyistä siltä varalta, että jokin näistä levyistä lakkaa toimimasta tai tuhoutuu.

3.4 Verkkovirtualisointi

Ensimmäisessä luvussa, jossa kerrottiin virtualisinnista yleisesti nousi esille kaksi esimerkkiä virtualisoinnista. Nämä VLAN:t sekä EtherChannel kuuluvat juurikin verkkovirtualisoinnin alueelle. Verkkovirtualisoinnissa tarkoituksena on luoda loogisia verkkoja tai jakaa jo olemassa olevat verkot tai niiden osa-alueet virtuaalisiin osiin. Edellä olevien esimerkkien lisäksi hyvänä esimerkkinä on myös Virtual Router Redundancy Protocol, VRRP. Tällä tekniikalla kahden tai useamman reitittimen välille konfiguroidaan tämä VRRP, jolloin yksi reititin toimii masterina ja muut toimivat tällöin backup-tilassa.

Master-tilassa toimivan reitittimen pettäessä jokin backup-reitittimistä ottaa omakseen masterin roolin ja kykenee ohjaamaan liikennettä. Master– ja backup-reitittimet määritellään painoarvojen mukaan. Tällä tavalla käyttämällä hyödyksi virtualisoinnin tarjoamia mahdollisuuksia eliminoidaan yksittäinen piste, jonka hajotessa koko palvelu lakkaisi toimimasta.

Myös Virtual Private Networkit, VPN:t ovat merkittävä osa verkkovirtualisointia. Nämä toimivat eräänlaisina putkina kahden pisteen välillä internetin yli. Näitä käyttääkseen käyttäjän on ladattava koneelleen ohjelmisto, kuten esimerkiksi Cisco AnyConnect. VPN-tekniikkaa hyväksikäyttäen käyttäjä pääsee vaikka kotoaan tai kirjastosta julkisen verkon yli turvallisesti ikään kuin omaa salattua tunneliaan pitkin työpaikkansa sisäverkkoon. Tämä tekniikka on varmasti ainakin etätyötä tekeville tuttu. [5, s. 27.]

3.5 Sovellusvirtualisointi

Sovellusvirtualisoinnin päällimmäisenä tarkoituksena on saada suoritettua sovelluksia, jotka ovat käyttäjän natiivin käyttöjärjetelmän kanssa ristiriidassa, tai kyseinen ohjelma ei ole saatavilla hänen käyttöjärjestelmälleen. Mikäli haluttu sovellus on ristiriitainen käyttöjärjestelmän kanssa, se voi aiheuttaa käyttöjärjestelmän hidastelua tai kaatumista. Haluttu applikaatio erotetaan sovellusvirtualisoinnilla varsinaisesta käyttöjärjestelmästä tarjoamalla se virtuaalisen kerroksen kautta, joka toimii käyttöjärjestelmän päällä. [5, s. 40.]

3.6 Hypervisorit

Vaikka tietysti jokainen virtualisoinnin komponentti on virtuaaliympäristön kannalta olennainen, niin näistä osista kuitenkin tärkeimmäksi nousee hypervisor. Sitä voisi nimittää koko virtualisointiarkkitehtuurin sydämeksi, eikä ilman sitä koko virtualisointi olisi mahdollista. Hypervisor on tietokoneen fyysisen laitteiston ja sen ohjelmiston väliin sijoitettu ohjelma, joka hallitsee luotuja virtuaalikoneita.

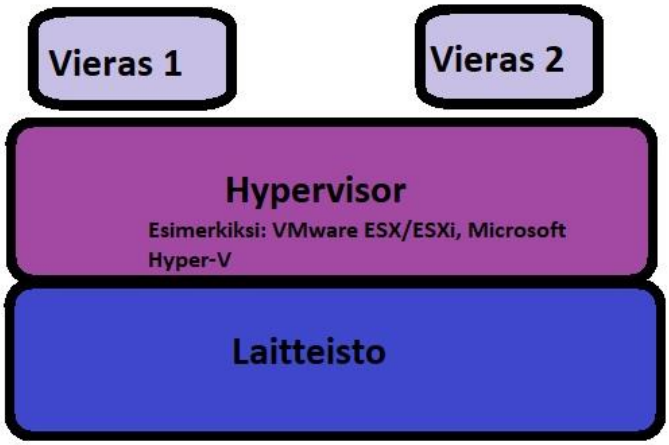
Käytännössä hypervisorit mahdollistavat useiden virtuaalikoneiden hallinnan samalla laitteistolla ja niitä voidaankin pitää eräänlaisena käyttöjärjestelmänä virtuaalikoneille,

joka loogisesti erottelee virtuaalikoneet toisistaan. Virtuaalikoneiden ollessa loogisesti eroteltuina toisistaan, yhden virtuaalikoneen kaatuessa muut virtuaalikoneet pystyvät jatkamaan toimintaansa normaaliin tapaan. Hypervisorit vastaavat myös fyysisten resurssien allokoinnista virtuaalikoneille. [6.]

Hypervisoria valittaessa on otettava huomioon, että hypervisor-tyyppejä on olemassa kahdenlaisia, tyypin yksi sekä tyypin kaksi hypervisorit. Nämä kaksi tyyppiä eroavat toisistaan merkittävällä tavalla, ja näiden eroja selitetään tässä luvussa.

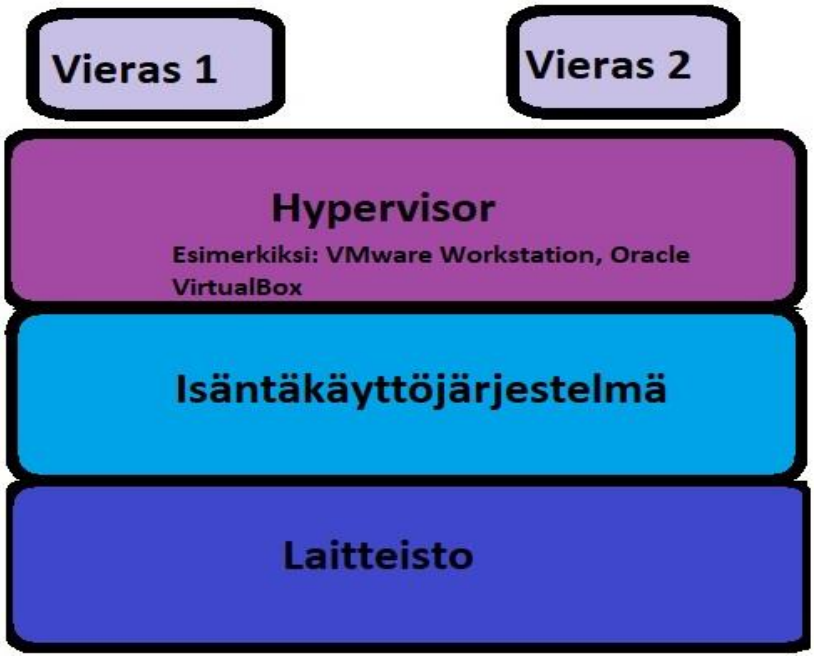
Ensimmäinen tyyppi on natiivi hypervisor, joka asennetaan suoraan isäntäkoneen laitteistolle, eikä se näin ollen vaadi sen alla pyöriväksi erillistä käyttöjärjestelmää, kuten Windowsia tai Linuxia toimiakseen. Nimityksen ’’natiivi hypervisor’’ lisäksi tämä ensimmäinen tyyppi kulkee myös, aivan totuudenmukaisesti, nimellä ’’Bare Metal Hypervisor. Tämä kuvastaa hyvin tämän tyyppisen hypervisorin toiminnallisuutta, sillä ilman välissä olevaa käyttöjärjestelmää tämän tyyppiset hypervisorit pääsevät suoraan kommunikointiyhteyteen fyysisen laitteiston kanssa. [1, s. 24.]

Esimerkkejä ensimmäisen tyypin hypervisoreista ovat Microsoftin Hyper-V, Oracle VM Server for x86 sekä myös tässä insinöörityössä käytetty Vmware ESXi, joka toimii Metropolian palvelimella ja on osa suurempaa VMware vSphere -tuotekokonaisuutta. vSphere-tuotekokonaisuuteen myös kuuluvaa vSphere Clientia käytetään niin ikään tässä työssä tämän ESXi-hypervisorin hallintaan. Luvussa viisi käsitellään vSphereä kokonaisuutena sekä myös sen sisältämää ESXi:äkin hieman tarkemmin.



Kuva 1. Ensimmäisen hypervisor-tyypin malli

Toisen tyypin hypervisor eroaa ensimmäisestä tyypistä jo heti asennusvaiheessa. Toisin kuin ensimmäinen tyyppi, tämän tyyppiset hypervisorit asennetaan isäntäkoneella jo toimivan käyttöjärjestelmän päälle. Näissä tapauksissa hypervisor erottelee loogisella tasolla virtuaalisen käyttöjärjestelmän koneen natiivista käyttöjärjestelmästä. Tämän vuoksi toisen tyypin hypervisoreita kutsutaankin nimellä Hosted Hypervisor. Koska toisen tyypin hypervisorit ovat riippuvaisia isäntäkoneen käyttöjärjestelmästä, ne ovat myös ainoastaan niin vakaita kuin niiden alla sijaitsevan isäntäkoneen käyttöjärjestelmät ovat. Esimerkkejä tyypin kaksi hypervisoerista ovat Vmware Workstation, Vmware Player sekä Oracle VirtualBox. [1, s. 26.]



Kuva 2. Toisen tyypin hypervisorin malli

Periaatteessa molemmat näistä hypervisor-tyypeistä ajavat saman asian, mutta niiden suorituskyvyissä on huomattavia eroja. Ensimmäisen tyypin ollessa asennettuna suoraan palvelimen laitteistolle, ja näin ollen sen ollessa riippumaton isäntäkoneen omasta käyttöjärjestelmästä, on se resurssien kannalta tehokkaampi. Toinen tyyppi jää tässä jälkeen sen ollessa riippuvainen isäntäkoneen käyttöjärjestelmästä. Käytännössä siis ensimmäisen tyypin hypervisorit toimivat suoraan palvelimelta, kun taas toisen tyypin edustajat toimivat paikallisesti käyttäjän koneelta käsin. [1, s. 26.]

4 VMware vSphere

Tässä opinnäytetyössä käytetään virtuaalikoneiden hallinnassa VMwaren kehittämää vSphere-tuotekokonaisuutta, ja eritoten sen sisältämää vSphere Clientia. vSphere on administraattorin tai käyttäjän tietokoneelle asennettava ohjelmisto, joka sisältää Vmwaren valmistamia useita komponentteja, kuten vCenter Serverin, hypervisor ESXi:n sekä vSphere Clientin. Tässä luvussa käsitellään kutakin näistä komponenteista yksityiskohtaisemmin. VMware vSphere ei siis ole yksittäinen ohjelma, vaan sitä voi verrata esimerkiksi Microsoft Officeen, joka sisältää useita Microsoftin kehittämiä ohjelmia. Vmware vSphere ja Microsoft Office ovat molemmat tuoteperheitä, jotka

sisältävät useita eri ohjelmia, joista esimerkkeinä Microsoftin tapauksessa olisivat Word, Excel sekä Powerpoint.

Tällä hetkellä vSphere-tuotekokonaisuudesta on saatavilla neljä versiota: vSphere Standard, vSphere Enterprise plus, vSphere with Operations Management Enterprise Plus sekä vSphere Platinum. Jokaisella näistä on hieman eri käyttökohteensa sekä hintaluokkansa, mutta jokainen näistä sisältää joitakin samoja komponentteja, kuten esimerkiksi vCenter Serverin standard-version. Jotkin versiot tietysti sisältävät asioita, joita muissa versioissa ei ole. Esimerkiksi vSphere Platinum on ainoa versio, jossa on Vmware AppDefense, joka on tarkoitettu datakeskuksessa toimivien virtualisoitujen applikaatioiden toiminnan turvaamiseen. Muilta osin on vSphere Enterprise Plus näistä ominaisuuksiltaan laajin, joka toki näkyy myös hinnassa. [7.]

4.1 ESX ja ESXi

vSpheren komponenteista ätrkein on itse virtualisoinnin sydän, hypervisor ESX tai ESXi, jotka molemmat ovat ensimmäisen tyypin hypervisoreita. Ne siis toimivat suoraan fyysiseltä laitteistola, eivätkä ne tarvitse erillistä käyttöjärjestelmää toimiakseen. ESXi on tässä työssä käytetty hypervisor, josta työn kirjoittamishetkellä on käytössä versio 6.0. Kaikki virtuaalikoneet, kuten myös opiskelijan virtuaalinen työpöytä, on asennettu ESXi-palvelimelle.

Itse hypervisor on kuitenkin hyödytön, ellei sitä pääse hallinnoimaan. Jotta käyttäjä voisi hallita ESXi-palvelimella toimivia virtuaalikoneita, hän tarvitsee siihen sopivan ohjelman. Käytettäessä VMwaren tuotteita tähän tarkoitukseen soveltuu vSphere Client tai vSphere Web Client. Näitä käsitellään tässä työssä myöhemmin luvussa 5.3.

Kun pohditaan ensimmäisen tyypin hypervisoreita, on Vmwaren tuotteista valittavissa kaksi vaihtoehtoa: ESX tai ESXi, joiden väliset erot ovat selkeät. Näistä vaihtoehdoista ESX on vanhempi alusta, ja se sisältää sisäänrakennetun Linux-pohjaisen palvelukonsolin. Tämä palvelukonsoli voi vaikuttaa varsinkin Linux-ympäristöihin perehtyneille asiantuntijoille houkuttelevalta vaihtoehdolta, mutta on kuitenkin otettava huomioon, että vanhempi ESX on uudempaan ESXi:n verrattuna ominaisuuksiltaan köyhempi. Uudempaan ESXi-hypervisoriin tämänlaista palvelukonsolia ei sisälly, vaan

sen sijaan ESXi:n hallinta tapahtuu graafisen käyttöliittymän kautta. On hieman ristiriitaisen tuntuista, että ESXi-hypervisorista on saatavilla ilmainen kokeiluversio, joka on voimassa 60 päivän ajan, kun taas vanhemmasta ESX-hypervisorista tätä ei ole saatavilla.

> “Se fakta, että vanhempi ESX ei ole myös saatavilla ilmaiseksi on johtanut ihmisiä uskomaan ESXi:n olevan huonompi tai vähintääkin ominaisuuksiltaan köyhempi kuin ESX. Tämä ei kuitenkaan pidä paikkaansa, vaan itse asiassa päinvastainen on totta.” [8.]

Vaikka näiden kahden toiminnallisuus ja performanssi ovatkin samankaltaiset, Vmware kuitenkin kannustaa uudemman ESXi:n käyttämistä kaikissa uusissa virtuaalitoteutuksissa sen paremman arkkitehtuurin vuoksi. Tämän lisäksi ESXi:n ollessa uudempaa teknologiaa, VMware aikoo nykyhetkestä eteenpäin panostaa yksinomaan tämän kehittämiseen ja tukemiseen. Vanhemman ESX:n jäädessä enenevissä määrin historian hämärään tuki sille loppuikin jo vuonna 2009.

ESXi:stä on olemassa kahta eri versiota: VMware ESXi Embedded ja VMware ESXi installable. ESXi Embedded on laiteohjelmisto, joka tulee suoraan rakennettuna palvelimen fyysiseen laitteistoon. ESXi Installable puolestaan on asennettava ohjelma, joka on saatavilla CD-Rom Boot Imagena. Lisäksi ESXi:stä on myös saatavilla edellä mainittu ilmaisversio, mutta tämä ei luonnollisesti sisällä lisensoidun version kaikkia ominaisuuksia, eikä tämä ilmaisversion ole hallittavissa vCenter Serverin kautta, ja se on voimassa vain 60 päivää. ESXi:n perustana toimii Vmwaren kehittämä VMkernel, joka on POSIX-tyyppinen käyttöjärjestelmä. Se toimii suoraan ESXi:n päällä ja hallitsee suurinta osaa fyysisen laitteiston resursseista, kuten muistia, suorittimia sekä tallennustilaa. Käytännössä se siis vastaa resurssien jakamisesta virtuaalikoneille niiden tarpeen ja määrityksien mukaan. Se toimii yhteydenpitäjänä virtuaalikoneiden ja fyysisen laitteiston välillä Tiedostojärjestelmänä Vmkernel käyttää VMware Virtual Machine File Systemia (VMFS). Tämä on suunniteltu tukemaan isojakin tiedostoja, kuten virtuaalilevyjä. Toinen tärkeä ESXi:n osanen on Virtual Machine Monitor (VMM), joka vastaa itse virtualisoinnista. [9, s. 25.]

4.2 vCenter Server

Metropolian palvelimella pyörii myös vCenter Server, jota usein kutsutaan pelkästään nimellä vCenter. Ennen nykyistä nimeään vCenter Server tunnettiin aiemmin nimellä VMware VirtualCenter. VMware vCenter Server on laajentuva ja hyvin skaalautuva ympäristö, jonka käyttötarkoitus on toimia keskitettynä hallintajärjestelmänä kaikille ESXi-hosteille ja näin ollen myös tämän hostin sisältämille virtuaalikoneille. Hyvällä skaalautuvuudella tässä tapauksessa tarkoittaa sitä, että useiden virtuaalikoneiden useiden virtuaalikoneiden hallinnointi on tehty suoraviivaisemmaksi ja helpommaksi. Kuvitellaan esimerkiksi tilanne, jossa käyttäjän salasana muuttuu. Ilman keskitettyä hallintajärjestelmää olisi tämä salasana käytävä muuttamassa jokaiselle ESXi-hostille erikseen. Kiitos hyvin skaalautuvan vCenterin ja sen sisältämän Single Sign-On-ominaisuuden (SSO) tämänkaltainen tilanne saadaan vältettyä. Single sign-on toimii jokaisella käyttäjällä, joka antaa käyttäjälle yhden käyttäjätunnuksen ja salasanan, jolla hän pääsee tarvitsemiinsa palveluihin. Käytännössä siis tilanteessa, jossa esimerkiksi käyttäjän salasana muuttuu, on ainoastaan tämän SSO:n salasana muutettava, jonka jälkeen käyttäjä pääsee taas kaikkiin tarvitsemiinsa palveluihin kuten ennenkin. Huomionarvoista on, että kaikki Spheren tunnetuimmat ominaisuudet, kuten VMware High Availability, Fault Tolerance, Storage Vmotion sekä Dsitributed Resource Scheduler vaaitvat vCenteriä toimiakseen. vCenteriin yhdistmäinen tapahtuu vSphere Clientin tai vSphere Web Clientin kautta. [9, s. 60.]

4.3 vSphere Client ja vSphere Web Client

Aluksi voi tuntua hieman sekavalta erottaa vSphere ja vSphere Client toisistaan nimien ollessa niin samankaltaiset. Pähkinänkuoressa määriteltynä vSphere on siis tuotekokonaisuus, joka sisältää liudan VMwaren tuotteita, mukaanlukien käyttöliittymä vSphere clientin. vSphere Client on graafinen käyttöliittymä, jolla käyttäjä pääsee tarkastelemaan ja hallinnoimaan vCenter Serverin tarjoamia työkaluja, sekä myös hallinnoimaan ESXi-hosteja sekä niiden sisältämiä virtuaalikoneita. vSphere Client toimii siis administratiivisena graafisena rajapintana. Pääkäyttäjät voivat vSphere Clientin avulla tarkkailla virtuaalikoneiden performanssia, allokoida resursseja ja hallita käyttäjien oikeuksia. Nykyisellään viimeisin version vSphere Clientista on versio 6.0e ja VMware

on siirtynyt perinteisestä vSphere Clientistä kehittämään HMTL5-pohjaista vSphere Web Clientiä, joka toimii selaimen kautta.

Ennen vanhaan tämä vsphere Web Client sisälsi vain joitakin vSphere Clientin sisältämiä ominaisuuksia, mutta versiosta 5.5 lähtien Web Clientin tarjonta on päässyt samalle tasolle normaalin clientin kanssa. Nykyisellään VMware suositteleekin Web clientin käyttämistä, sillä version 5.5 jälkeen ominaisuuksia ei tulla enää lisäämään perinteiseen vSphere Clientiin, vaan tuki siirtyy yksinomaan uudemmalle Web Clientillä. [9, s. 62.]

vSphere Web Client on siis käytettävissä suoraan selaimella, mutta se vaatii tuen Adobe Flashille, josta tulee olla asennettuna vähintäänkin version 11.1. Yhdistäminen vCenter Serveriin käyttämällä vSphere Web Clientia tapahtuu seuraavasti:

- Mennään selaimella osoitteeseen https://client-hostnimi:portti/vsphere-client. Portti on oletuksena 9443, mutta se on muutettavissa Web Clientin asennuksen yhteydessä.
- Server-alasvetovalikossa, valitaan vCenter Server, johon halutaan yhdistää
- Syötetäänkäyttäjätunnus ja salasana, jonka jälkeen kirjaudutaan sisään. [10.]

vSphere Web Client on siis näistä kahdesta tuoreempi, mutta on huomionarvoista, ettei se ole käytettävissä ympäristöissä, joissa ei ole asennettuna vCenter Serveriä. Tällöin käytettäväksi jää vsphere Client. [9, s. 8.]

4.4 VMware High Availability

Nykypäivän kiireisessä yritystoiminnassa on hyvin tärkeää, että toiminta pystyy jatkumaan häiriöttömänä, tai vähintäänkin että vikatilanteen sattuessa saadaan toiminta nopeasti palautettua normaaliksi. Tämän vuoksi järjestelmien tulee olla hyvin vikasietoisia, eli redundanttisia. Käytettäessä VMwaren tuotteita tämänlaisiin tilanteisiin soveltuu VMware High Availability. VMware HA:n käyttötarkoitus on tuoda virtuaalikoneille suurta saatavuutta sekä se antaa mahdollisuuden klusteroida ESXi-hostit yhdeksi pooliksi. Yhden hostin alla voi siis toimia suurikin määrä virtuaalikoneita, eli nämäkin päätyvät hostiensa mukana saman klusterin alaisuuteen. Jonkin näistä

monitoroiduista klustereista vikaantuessa High Availability siirtää vikaantuneen hostin sisältämät virtuaalikoneet uudelle, samassa klusterissa sijaitsevalle hostille.

VMware HA:ssa host-tyyppejä on kahdenlaisia, nimittäin hosteja sekä secondary hosteja. Ensimmäiset viisi klusteriin lisättyä hostia toimivat primaryinä ja tämän jälkeen lisätyt toimivat secondary hostin roolissa. Mikäli jokin primary hosteista poistetaan klusterista, niin High Availability nostaa jonkin secondaryistä sen tilalle. Jokin primaryista toimii myös erikoisroolissa. Se nimittäin toimii niin sanottuna Active Primaryna, jolloin sen tehtäväksi lankeaa virtuaalikoneiden uudelleenkäynnistämisen ajastaminen, epäonnistuneiden uudelleenkäynnistysyritysten seuraaminen sekä päätös siitä, onko uudelleenäynnistäminen ylipäätään tarpeellista tai suotavaa. [11.]

5 Virtuaaliympäristön käyttöönotto

Käytännöllisesti katsoen VMwaren infrastruktuurin käyttöönottaminen on pitkälti suoraviivaista ja sisältää vain muutamia vaiheita kun poissuljetaan yksittäisten komponenttien asennusvaiheet. Ympäristön rakentaminen alkaa hypervisorin valinnasta ja asentamisesta palvelimelle, jolta löytyvät tarpeelliset resurssit virtuaalikoneiden provisiointia varten. Tässä työssä käytetään VMwaren kehittämää ESXi-hypervisoria, joka on ensimmäisen tyypin hypervisor. Tämä valikoitui käytettäväksi, sillä Metropolialla on jo se käytössään, ja virtuaalinen infrastruktuuri on rakennettu VMwaren tuotteilla. Tällä hetkellä käytössä on ESXi:n versio 6.0. Metropolialla on tästä tietenkin käytössään maksettu lisensoitu versio, mutta siitä on saatavilla myös ilmaisversio. Tämän ilmaisversion toiminnallisuus on kuitenkin rajoitettua, ja se on voimassa vain 60 päivää. Ilmaisversiolla tämänkaltaisen kampusympäristön rakentaminen, eikä ylläpito ei olisi mahdollista, sillä ilmaisversiossa esimerkiksi ESXi:n hallinta vCenter Serverin kautta on riisuttu pois eikä valmistajan tukea ole saatavilla sitä mahdollisesti tarvittaessa. Lisäksi ilmaisversiossa fyysisten suorittimien määrä hostia kohden on rajoitettu kahteen, ja virtuaalikoneiden määrä on maksimissaan kahdeksan. Fyysisen muistin eikä suorittimien ydinten määrää ei ole kuitenkaan rajoitettu. Alla löytyy listattuna osa hypervisor ESXi:n vaatimuksista, joista loput löytyvät tämän työn lähteistä:

- tuettu palvelinalusta

- isäntäkoneen, jolla on vähintään kaksi suoritinydintä
- 64-bittisen x64-prosessorin
- NX/XD-bitin tulee olla laitettuna päälle BIOS-asetuksista
- vähintään 4BG fyysistä RAM-muistia. [12.]

Ilmaisversio ei siis olisi soveltuva tällaiseen ympäristöön ympäristön ollessa niin laaja. Mikäli ilmaisversiota kuitenkin haluaa kokeilla, on siitä saatavilla 60 päivän ajan samat ominaisuudet kuin kokoversiossakin. Huomionarvoista on myös, että mikäli käyttäjällä on suunnitelmissaan rakentaa pienempi virtuaaliympäristö ilmaisversion rajoitteiden puitteissa, voi tämän ilmaisversion käyttöä jatkaa myös tuon 60 päivän jälkeen. Tällöin tosin ilmaisversiosta katoaa suuri osa tärkeistä ominaisuuksista, mitkä kokonaisversiossa olisivat. Pienemmän ympäristön hallinnoimiseen riittää ESXi-hypervisor sekä tämän hallinnointiin vSphere Client tai Web Client, eikä näin ollen vCenter Serveriä tarvita, mikä on ainoastaan kokoversion komponentti.

Seuraava vaihe tämänlaisen ympäristön rakentamisessa on vCenter Serverin asentaminen palvelimelle, jolta virtuaalikoneiden provisioiminen tapahtuu. Asentaminen voidaan toteuttaa Windows- tai Linux-palvelimelle. Kuten aikaisemmassa luvussa 5.2 käsiteltiin, vCenter Server on VMwaren tuotteille kehitelty keskitetty hallintakeskus, jolla käyttäjä voi helposti hallita suurempiakin virtuaalitoteutuksia. On totta, että pienemmissä ympäristöissä hallinta voidaan toteuttaa puhtaasti pelkällä ESXi-hypervisorilla ja vSphere Clientilla tai Workstationilla, mutta suuremmissa ympäristöissä vCenterin käyttö osoittautuu nopeasti lähestulkoon välttämättömäksi. Tämä johtuu esimerkiksi siitä, että olemassaolevien virtuaalikoneiden kloonaaminen onnistuu vain vCenter Serverin kautta. Kloonaaminen säästää huomattavia määriä aikaa suurien struktuurien rakentamisessa, sillä jokaista virtuaalikonetta ei kloonaamisen ansiosta tarvitse määritellä erikseen, vaan ne voidaan kopioida yhdestä toimivasta mallista.

vCenter Serverin asennuksessa on valittavissa kaksi vaihtoehtoa. Se voidaan asentaa virtuaalikoneena ESXi-palvelimen päälle tai se voidaan asentaa myös suoraan fyysiselle palvelimelle. vCenterin hallinta tapahtuu vSphere Clientin tai Web Clientin kautta, joista

nykyisellään VMware suosittelee käytettäväksi Web Clientia. Näitä käytetään vCenteriin yhdistämiseksi, ja vCenter puolestaan hallinnoi ESXi-palvelinta.

5.1 Virtuaalikoneiden luonti

Kun palvelimelle on saatu ESXi sekä vCenter toimimaan, on aika käydä itse asiaan eli virtuaalikoneiden luomiseen. Käytännössä virtuaalikoneet ovat vain kasa tiedostoja, joista tärkeimmät ovat konfiguraatiotiedosto sekä virtuaaliset levytiedostot. Käytännöllisesti katsoen virtuaalikoneiden luonti tapahtuu vCenter Serverillä, mutta itseasiallinen työ tapahtuu ESXi-palvelimelle, jota vCenterillä hallinnoidaan. Täällä luominen tapahtuu vSphereen rakennetun ’’Create New Virtual Machine”-wizardin avulla. Mikäli vCenter Serveriä ei ole, kuten esimerkiksi ilmaisversiota käytettäessä, myös suoraan yhdistäminen ESXi-palvelimeen on mahdollista.

Virtualikoneiden luominen on tehty melko suoraviivaiseksi ja helpoksi, sillä se on suurilta osin automatisoitu, käyttäjäystävällinen prosessi, jossa wizard-ohjelma vaihe vaiheelta pyytää käyttäjältä oleelliset asiat ja hoitaa itse loput. Virtuaalikoneiden luomiseen on olemassa eri tapoja, mutta yleisimmät ovat luoda joko täysin uusi virtuaalikone tai kloonata jo olemassa olevasta virtuaalikoneesta itsenäinen kopio. Kloonaaminen osoittautuu varsinkin suuremmissa ympäristöissä tärkeäksi elinvoimaksi, sillä se eliminoi tarpeen rakentaa pahimmassa tapauksessa jopa satoja virtuaalikoneita, kutakin alusta alkaen erikseen. Lisäksi eräänä metodina on myös fyysisen koneen muuntaminen virtuaaliseksi, joka on mahdollista käyttäen ilmaista VMware Converter -sovellusta. Virtuaalikonetta luodessa se assosioidaan johonkin tiettyyn datakeskukseen, hostiin tai muuhun resurssiin. [9, s. 488.]

5.2 Virtuaalikoneiden kloonaaminen

Edellisessä kappaleessa sivuttiin hieman sitä, mitä virtuaalikoneiden kloonaaminen on, mutta tässä luvussa käsitellään aihetta hieman tarkemmin. Suuria virtuaaliympäristöjä rakennettaessa, joissa tarvitaan useita identtisiä virtuaalikoneita, on kloonaaminen pätevä vaihtoehto saada suoritettua rakentaminen nopeasti. Virtuaalikoneiden kloonaaminen, kuten luominenkin, on varsin suoraviivaista, ja se on kaikissa tapauksissa

nopeampaa kuin suora kopioiminen. Alkuperäistä virtuaalikonetta kutsutaan kloonaamisen yhteydessä parentiksi. Varsin kätevää kloonaamisessa on myös se, kun kloonaus on suoritettu loppuun, tulee kloonatusta virtuaalikoneesta parentista täysin erillinen ja itsenäinen kokonaisuus, jolla on oma MAC-osoite sekä UUID. Hyötynä tässä on se, että parentiin tehdyt muutokset eivät vaikuta klooniin, eivätkä niin ollen kloniin tehdyt muutokset vaikuta parent-virtuaalikoneeseen Kloonaamisessa on käytettävissä kaksi erilaista tapaa:

- Linked-kloonit ovat kopioita virtuaalikoneista, jotka jakavat virtuaalisen levyn parent-koneen kanssa.

- Full-kloonit ovat täysin parentista erillisiä ja itsenäisiä, jotka eivät siis jaa parentin kanssa mitään.

Kloonaaminen osoittautuu tärkeäksi myös testaamisessa ja vianselvityksessä. Mikäli esimerkiksi olemassa olevaan virtuaalikoneeseen halutaan tehdä muutoksia, joista ei olla aivan täysin varmoja, voidaan tästä virtuaalikoneesta tehdä klooni, jolla testaaminen voidaan suorittaa turvallisesti. [13.]

5.3 Virtuaalikoneiden hallinta

Vmwarea käytettäessä virtuaalikoneiden hallinta tapahtuu vSphere Clientin tai vSphere Web Clientin kautta. Kuten aikaisemmin on mainittu, vSphere-version 5.5 jälkeen hallinta tapahtuu Web Clientinlla, sillä se on näistä kahdesta ainut tuettu versio. Metropolian ympäristössä luodaan ensin VPN-yhteys Metropolian verkkoon käyttäen Cisco AnyConnectia. Tämän jälkeen avataan omalle koneelle asennettu vsphere Client, tai mikäli käytössä on Web-Client, niin käytetään selainta. Tällä ollaan yhteydessä vCenter Serveriin, joka puolestaan on yheydessä ESXi-hypervisoriin, joka luo ja hallitsee virtuaalikoneita. On mahdollista yhdistää useampi vCenter Server yhdeksi Connected Groupiksi, jolloin näitä kaikkia Connected Groupin jäseniä voidaan hallita yhdellä vSphere Client -yhteydellä.

Virtuaalikoneiden hallintaan luodut työkalut ovat monet, kuten esimerkiksi:

- Virtuaalikoneiden startup- ja shutdown -asetukset. On mahdollista konfiguroida ESXi:lla luodut virtuaalikoneet käynnistymään sekä sammumaan hostin yhteydessä tai myös ajastetusti.

- Olemassaolevien virtuaalikoneiden lisääminen vCenter Serveriin. Kun lisätään host vCenter Serveriin, se löytää tälle asennetut virtuaalikoneet ja lisää ne vCenterin luetteloon.

- Virtuaalikoneiden poistaminen vCenteristä. Virtuaalikoneen poisto vCenteristä ei varsinaisest poista tätävirtuaalikonetta varastosta. Se vain poistaa tämän kirjaukse vCenterin luettelosta. Tämä kirjaus voidan toki myöhemmin lisätä uudelleen myöhemmin. Mikäli virtuaalikone halutaan oistaa kokonaan, on valittavissa komento Delete From Disk. Tämä poistaa myös virtuaalikoneen tiedostot sekä konfiguraation.

- Virtuaalikoneiden laitteiston muokkaus. [9, s. 516.]

5.4 Snapshotit

Spanshotit astuvat mukaan, kun virtuaalikoneiden tila halutaan tallentaa tai palauttaa johonkin tiettyyn tilaan tiettynä ajankohtana. Snapshotit sisältävät seuraavat asiat:

- virtuaalikoneen muistin sisältö

- virtuaalikoneen asetukset

- virtuaalikoneen virtuaalilevyjen tila.

Snapshoteilla on mahdollista tallentaa virtuaalikoneen tila kyseisen snapshotin ottohetkellä. Menneistä tapahtumista ei siis ole mahdollista jälkikäteen ottaa snapshotia. On oltava siis tarkkana, millon näitä snapshotteja on syytä ottaa. Voi osoittautua hyvinkin harmiliseksi, mikäli huomataan, että olisi palattava menneeseen tilaan, mutta se ei ole mahdollista, sillä snapshot on jäänyt ottamatta siltä hetkeltä. Hyvänä esimerkkinä

tilanteesta, jossa snapshottiin halutaan palata, ovat vikatilanteet. Käyttäjä voi esimerkiksi tehdä muutoksia virtuaalikoneeseen, mikä johtaa tämän vikaantumiseen. Vian kesto saadaan kuitenkin minimoitua palaamalla johonkin snapshottiin, jolloin voidaan miettiä, mistä syystä vika saattoi johtua samalla, kun palvelu toimii entiseen tapaansa viatta. Ensialkuun saattaa tuntua siltä, että snapshotit ovat oiva työkalu virtuaalikoneiden varmentamiseen. VMware ei tosin ainakaan tämänlaista käytäntöä suosittele, sillä suuren spapshottien määrän hallinta saattaa osoittautua hankalaksi, ne vievät huomattavan määrän levytilaa, eikä niitä itse laitteiston hajotessa ole suojattu. Backupien ottamiseksi snapshotien sijaan VMware tarjoaa VMware Data Recovery -ohjelmaa.

Huomionarvoista on, että snapshotit toimivat ainoastaan yksittäisillä virtuaalikoneilla. Mikäli siis käytössä on esimerkiksi joukko virtuaalikoneita, on näille kullekin otettava oma snapshotinsa. Snapshotin ottaminen onnistuu virtuaalikoneen ollessa käynnissä, pois päältä ja niin ikään myös virtuaalikoneen ollessa suspended-tilassa. Lower & Marshall kertovat kirjassaan parhaasta ajasta ottaa snapshot seuraavasti:

”Paras aika snapshotin ottamiselle on, kun mikään applikaatio virtuaalikoneessa ei kommunikoi toisten koneiden kanssa. Potentiaalisuus ongelmille on suurimmillaan, jos virtuaalikone kommunikoi toisen tietokoneen kanssa, erityisesti tuotantoympäristöissä”.

Mikäli snapshotteja halutaan poistaa, on se myös mahdollista. Kuten edellä mainittiin, nämä vievät paljon levytilaa, joten ajoittainen poistaminen on suotavaa, varsinkin sitä mukaa kun uudempia snapshotteja otetaan. Tällöin snapshottien ja edellisen levyn tilan väliset muutokset yhdistetään ja kaikki data poistetsta snapshotista kirjoitetaan isäntälevylle vain käyttäjän niin valitessa. Tämä syö paljon tehoa ja heikentää virtualikoneen toimintaa, kunnes toimenpide on suoritettu loppuun. [9, s. 524.]

5.5 Sisäkkäinen virtualisointi

Sisäkkäinen virtualisointi, eli nested virtualization on tekniikka, jolla voidaan suorittaa hypervisoria virtuaalikoneena jonkin toisen virtuaalikoneen sisällä. Tällä tekniikalla on esimerkiksi mahdollista ajaa ESXi-hypervisoria (tyypin 1 hypervisor) VMware Workstation alla (tyypin 2 hypervisor). Sisäkkäisessä virtualisoinnissa käytettävien

hypervisorien ei siis tarvitse olla homogeenisiä keskenään. Huomioitavaa kuitenkin on, että eri valmistajien hypervisorit eivät välttämättä toimi sisäkkäin keskenään ja tämä on syytä tarkistaa valmistajien tuotetiedoista. Esimerkiksi VMwaren ESXi toimii Microsoft Hyper-V:n, Citrix XenServerin sekä Linux KVM:n kanssa. Sisäkkäisessä virtualisoinnissa hypervisoria, joka toimii suoraan fyysisellä laitteistolla, kutsutaan nimellä level 0 ja vieraana toimivaa hypervisoria kutsutaan nimellä level 1.

Sisäkkäistä virtualisointia käyttäen on mahdollista luoda virtuaaliympäristöön joustavuutta sekä myös säästää kustannuksissa, sillä se mahdollistaa eri työkalujen käyttämistä vaatimatta uuden laitteiston ostamista. Käyttötarkoituksia sisäkkäiselle virtualisoinnille ovat esimerkiksi testiympäristön rakentaminen tai loppukäyttäjien virtualisointi vieraskäyttöön. Tällä hetkellä huomionarvoista kuitenkin on, että VMware ei pysty takaamaan sisäkkäisen virtualisoinnin vakautta tuotantoympäristöissä. Tämän vuoksi, mikäli haluaa kokeilla sisäkkäistä virtualisointia, on hyvä keskittyä ainoastaan tuotteiden testaamiseen tai kotilaboratoriakäyttöön harjoittelumielessä. Mikäli siis sisäkkäistä virtualisointia halutaan tällä hetkellä käyttää varsinaisessa tuotannossa, on käytettävä muita ratkaisuja. Esimerkiksi Microsoftin Hyper-V on hyvä vaihtoehto. [14.]

5.6 Virtuaalikytkimet

Olennainen osa virtuaaliympäristöjä ovat virtuaalikytkimet. Virtuaalikytkimet ovat loogisia kytkimiä, jotka on mallinnettu fyyfisten ethernet-kytkimien mukaan. Ne eivät kuitenkaan vastaa aivan täysin fyysisiä kytkimiä, eikä niihin pääse esimerkiksi telnetillä kiinni, eikä niitä voi kytkeä toisiin virtuaalikytkimiin. Näin ollen virtuaalikytkimissä ei ole esimerkiksi Spanning Tree -protokollaa.

Virtuaalikytkimet astuvat kuvaan, jotta virtuaalikoneet voisivat kommunikoida toistensa sekä koneiden kanssa, jotka ovat itseasiallisen virtuaaliympäristön ulkopuolella. Virtuaalikytkin toimii loogisena osana fyysisen verkkokortin ja virtuaalikoneiden välillä ja luo yhteyden näiden välille.

Käytettäessä VMwarea on valittavana kaksi kaksi vaihtoehtoa virtuaalikytkimien toteutukseen: Standard vSS sekä Distributed-tyyppi vDS. Sen lisäksi että toteuttamistapoja ovat nämä kaksi, on näille vieä kaksi erilaista yhdistämistapaa: Virtual

Machina Port Groupit sekä Vmkernel-portit. Virtual machine port groupeja käytetään virtuaaliympäristön sisäisten sekä ulkoisten yhteyksien luomiseen. Vmkernel-portteja puolestaan käytetään IP-osoitteiden varastointiin sekä ESXi:n hallintayhteydelle.

VMwarea käytettäessä on siis olemassa kahta tyyppiä virtuaalikytkimien toteutukseen. Standard-tyyppiä käytettäessä on hyvä ottaa huomioon sen rajoitukset. Sitä pystyy nimittäin käyttämään ainoastaan yhden ESXi-hostin kanssa. Se on toki ilmainen, distributed-tyypin ollessa maksullinen. Se soveltuu kyllä hyvin käytettäväksi toteutuksissa, joissa on tosiaan vain tuo yksi ja ainoa ESXi-host. Kun halutaan toteuttaa kompleksisempaa ympäristöä, jossa hosteja on monia, tulee käytettäväksi distributed-virtuaalikytkin. Sen avulla on mahdollista saada monia ESXi-hosteja toimimaan samalla virtuaalikytkimellä. Edellytyksenä tälle on, että nämä hostit ovat samassa klusterissa. Klusterointia käsiteltiin tässä työssä luvussa 5.4. Yläraja hostien määrälle on 500 hostia yhtä distribute-virtuaalikytkintä kohden.

Ongelmaksi distributed-tyyppiä käytettäessä nousee monien hostien hallinta. Tähä on kuitenkin jo ratkaistu ongelma ja keskitetty hallinta on mahdollista. Kuten aikaisemmin mainittiin, on mahdollista saada yhdelle virtuaalikytkimelle kokonainen klusterillinen hosteja. vDS kykenee monitoroimaan kunkin tämän klusterin sisältämää ESXi-hostin konfugaariota ja toimintaa.

On siis selkeää, missä tilanteissa tulisi käyttää vDS:aa yksinkertaisemman vSS:n sijaan. Sen lisäksi että distributed-tyyppi voi sisältää klusterillisen hosteja yhden hostin sijaan, se sisältää myös muita ominaisuuksia, joita standar-tyypissä ei ole. Näistä mainittavimpina tuki vMotionille, yksityiset VLAN:t sekä port state monitoring. [9, s. 189.]

5.7 Opiskelijan työpöytä

Metropoliassa on opiskelijoille luotuna oma virtuaalinen työpöytänsä, jota käytetään verkkokurssien suorittamiseen. Tämä työpöytä löytyy jokaiselta työasemalta tietotekniikan laboratorioluokissa. Se on virtuaalinen ympäristö, johon opiskelijat pääsevät käsiksi vSphere Clientilla. Tämä löytyy myös jokaiselta koneelta valmiksi asennettuna, joten yhdistämiseen tarvitsee käyttäjätunnuksen ja salasanan, jonka ohjaaja kertoo opiskelijalle. Myös etäkäyttö on mahdollista. Tämä vaatii opiskelijan

koneelle asennettavan VPN-ohjelmiston, Cisco AnyConnectin, joka on ilmaiseksi ladattavissa Ciscon sivuilta. VPN-ohjelman avulla pääsee yhdistämään etänä koulun verkkoon vaikka kotoaan tai kesämökiltä. VPN:n käyttö mahdollistaa siis joustavan etätyöskentelyn, kun kampukselle pääseminen ei jostain syystä ole mahdollista. Etäkäyttö vaatii myös vSphere Clientin käyttämistä aian kuten kampuksellakin, joten opiskelijan on ladattava vSphere Client tai käytettävä Web Clientia.

Virtualisoidulta työpöydältä löytyy tarpeelliset välineet Juniperin verkkokurssien suorittamiseen. Huomionarvoista on, että joillekin näistä verkkokursseista ei tällä hetkellä, eikä mahdollisesti tulevaisuudessakaan ole VMwaren ympäristöön soveltuvaa virtuaalikonetta. Näiden kurssien suorittaminen on kuitenkin mahdollista VirtualBoxilla, joka niin ikään löytyy koulusta jokaiselta koneelta. Opiskelijan virtuaalipöydältä löytyvät myös Juniperin virtual routerit, vMX-, vSRX-, vQM-laitteet sekä myös laboratoriotöiden tehtävät ja ohjeet näiden suorittamiseksi.

6 Juniperin virtuaalilaitteet

Juniperin tuotevalikoimaan kuuluu perinteisten fyysisten laitteiden lisäksi myös liuta virtuaalilaitteita, kuten virtuaalisia palomuureja, virtuaalireitittimiä sekä virtuaalikytkimiä. Toiminnallisuuksiltaan kuten myös nimiltään virtuaalilaitteet ovat hyvin samankaltaisia kuin fyysiset versionsakin. Nimeämiset ovat selkeitä ja jokaisen tuotteen eteen on vain lisätty etuliite v kuvaamaan tuotteen virtuaalisuutta. Vaikkakin nämä virtuaalilaitteet siis vastaavat fyysisiä laitteita, käydään tässä luvussa niitä hieman läpi, sillä ne eivät ole välttämättä lukijalle tuttuja. Asennusprosessi näille virtuaalikoneille on suoraviivainen ja selkeä, esimerkkinä vSRX:n asennus:

- Ladataan vSRX paketti Juniperin sivuilta.
- Importoidaan virtuaalikone haluttuun ympäristöön.
- Konfiguroidaan interfacet.
- Käynnistetään virtuaalikone ja konfiguroidaan JunOS:ssa. [15.]

Pääpiirteissään esimerkiksi vSRX-laitteen asentaminen onnistuu ylläolevin keinoin, ja sama asennusprosessi koskee myös muita Juniperin virtuaalilaitteita. Tämän työn tarkoituksena ei kuitenkaan ole käydä näiden asennusprosessia yksityiskohtaisemmin läpi.

6.1 vSRX

Juniper vSRX on fyysistä SRX-sarjan palomuurilaitetta vastaava virtuaaliversio. Se tarjoaa skaalautuvaa ja turvallista suojaa julkisille, privaateille ja hybridipilville. Se sisältää paljolti samoja ominaisuuksia kuin perinteinen fysinen SRX-laite, mutta siitä kyllä puuttuu joitakin ominaisuuksia. Lista näistä puuttuvista ominaisuuksista fyysiseen versioon verrattuna on varsin pitkä, joten ne löytyvät liitteestä. [16.]

Käytännön toteutuksissa SRX-laitteita käytetää verkon reunalla eli edgellä niiden ollessa palomuurilaitteita. Uuden sukupolven palomuurina Juniper SRX sisältää paljon hyödyllisiä tietoturvaominaisuuksia, kuten palomuurin, VPN:n, NAT-mahdollisuuden, Application Security-, Intrusion Detection- sekä Intrusion Prevention -ominaisuudet. Näiden lisäksi vSRX tarjoaa myös pilvipohjaista anti-malware-palvelua, joka perustuu dynaamiseen analyysiin.

vSRX nousee esille, kun puhutaan virtuaalilaitteiden turvaamisesta, sillä se on yksi kolmesta tavasta suojata niitä. Nämä kolme tapaa ovat liikenteen ohjaaminen fyysisen tietoturvalaitteen läpi, Gues-käyttöjärjestelmien tietoturvaohjelmistot tai virtuaalinen tietoturvalaite vSRX. Liikenteen ohjaamisessa fyysisen tietoturvalaitteen lävitse hyödyksi nousee tarve konfiguroida ainoastaan yhtä laitetta, sekä mahdollisuus käyttää jo olemassa olevaa IT-asiantuntemusta. Ongelmakohdaksi kuitenkin tässä nousee fyysisen laitteen resurssipoolin rajoittuneisuus. Toisessa vaihtoehdossa jokaiselle virtuaalikoneelle tulee asentaa sama tietoturvaohjelma kuin fyysisellä palvelimellakin on. Tässä ongelmakohdiksi nousevat hinta ja suorituskyky. Virtuaalilaitteesta halutaan saada kaikki teho irti ja jokaisella virtuaalikoneella toimiva tietoturvaohjelmisto veisi vain turhaan resursseja, sillä voimme käyttää vSRX-laitetta. Virtuaalinen vSRX toimittaa palomuurin tehtävää verkon reunalla. Tässä ainoaksi haittapuoleksi ilmenee fyysisen palvelimen nouseva resurssitarve.

vSRX tukee VMware ESXi – sekä Linux KVM-hypervisoreita. tätä laitetta käytetään useissa Metropolian tarjoamissa Juniperin verkkokursseissa. [17.]

6.2 vMX

Juniper vMX on virtuaalinen versio fyysisestä MX-reitittimestä. Se asennetaan x86-pohjaiselle palvelimelle, ja pääpiirteittäin sen toiminnallisuus vastaa fyysistä versiota. Aivan kuten fyysisillä MX-reitittimillä, myös vMX:n käyttöjärjestelmänä toimi JunOS. Käyttäminen on täten helppoa ja tuttua niille, joilla on jo entuudestaan kokemusta kyseisestä käyttöjärjestelmästä. vMX on mahdollista konfiguroida toimimaan jokoa lite-tilassa tai performance-tilassa. Lite-tilassa laitteen resurssivaatimukset ovat pienemmät. Lisäksi se käyttää pienempää kaistanleveyttä. Performance-tilassa laite käyttää suurempaa kaistanleveyttä sekä resurssivaatimukset kasvavat. Oletuksena laite toimii performance-tilassa, ja lite-tilaan vaihtaminen onnistuu komennon set chassis fpc 0 lite-mode avulla. [18.]

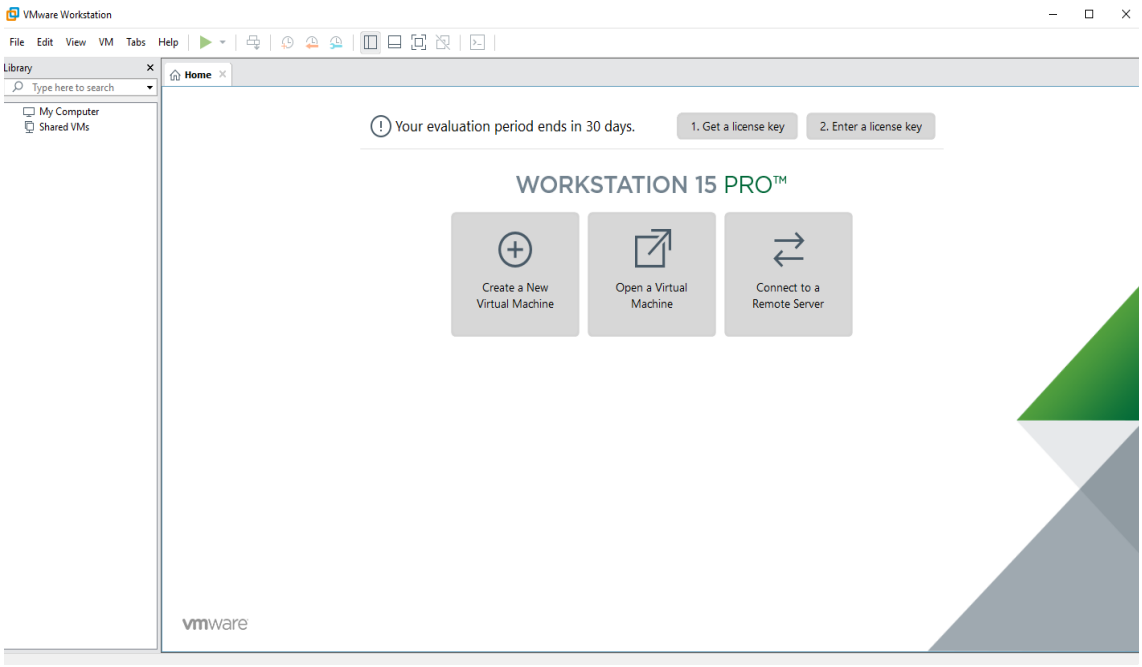
6.3 vQFX

vQFX-laitteet ovat virtuaalisia versioita Juniper QFX-sarjan datacenter-kytkimistä, joita opetetaan Juniperin verkkokursseissa.

7 Virtuaalikoneiden testaaminen

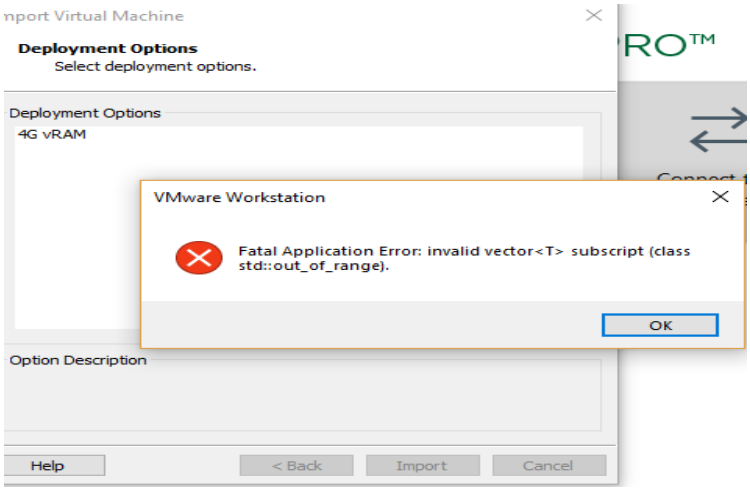
Tässä työssä testaaminen jouduttiin suorittamaan paikallisesti. Käytössä ei siis ole VMware vSphere Clientia eikä vCenter Serveriä, vaan testaaminen tapahtui käyttäen VMware Workstationia, joka on tyypin 2 hypervisor. Testaamiseen tarvitaan siis VMware Workstation, jota käsiteltiin tässä työssä luvussa 5.4 sekä tämän lisäksi Juniperin virtuaalikoneiden imageja, joita ajetaan kyseisellä Workstationilla. VMware Workstation on ladattavissa ilmaiseksi VMwaren sivuilta ja tästä on ilmaisena 30 päivän ajan ilmainen trial-versio. Kokoversio maksaa reilusti yli 100 euron verran. Varsinaisiin verkkokursseihin opiskelija saa ohjaajalta ohjeet sekä pohjakonfiguraatiot Juniperin

virtuaalilaitteille, jotta tehtävien suorittaminen onnistuu ilman tarvetta konfiguroida koko laitetta.



Kuva 3. VMware Workstationin etusivu

Kuten kuvasta käy ilmi, VMware Workstationin käyttäjäliittymä on hyvin käyttäjäystävällinen ja selkeä. Huomionarvoista on, että VMware Workstation ei ole virallisesti tuettu alusta Juniperin vSRX:lle, joten aivan ongelmitta imagen lataaminen ei onnistu. Kun valitaan ”Open Virtual Machine, ruudulle ilmestyy virheilmoitus:



Kuva 4. Virheilmoitus avattaessa vSRX-imagea Workstation 15:lla

Ongelma tässä tapauksessa piili Workstationin versiossa 15 ja vSRX:n imagen yhteensopivuudessa. Sama ongelma toistuu myös käytettäessä Workstationin versiota 14. Vaihdettaessa vanhempaan versioon VMware Workstationista image lataantui vailla ongelmia

Kuva 5. Virtuaalikone odottaa käynnistämistä

7.1 Virtuaalikoneiden asetukset ja kloonaaminen

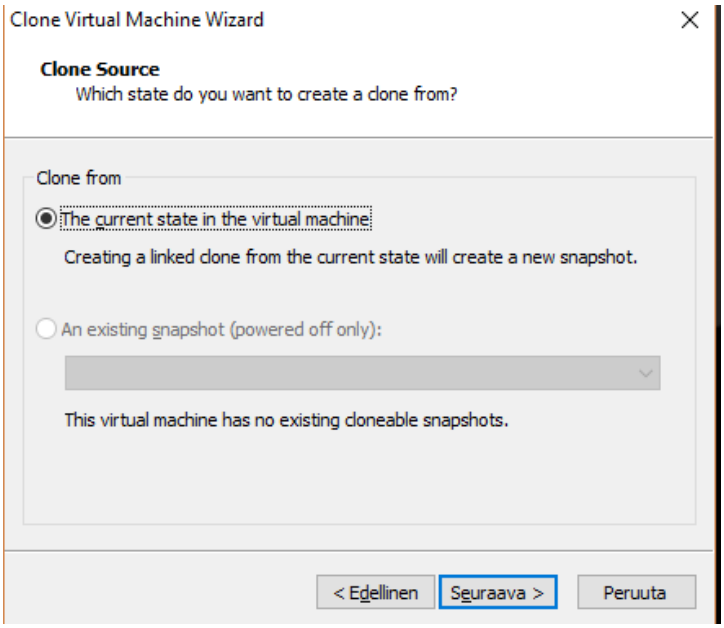
Tässä tilassa käyttäjällä on mahdollisuus muokata virtuaalikoneen asetuksia, kuten niille allokoitua muistia, prosessoreita sekä verkkoadaptereita. Tässä työssä muokattiin ainoastaan verkkoadaptereiden asetuksia. Oletuksena näitä on kolme kappaletta, jotka riittävät tämän työn tarpeisiin. Mikäli näitä tarvittaisiin enemmän, voi niitä helposti luoda lisää. Verkkoadaptereihin on valittavissa viisi eri tilaa:

- Sillattu (bridged). Tämä vaihtoehto siltaa valitun virtuaalisen verkkoadapterin isäntäkoneen tietoverkkoon. Tämä tarkoittaa sitä, että se saa IP-osoitteen samasta verkosta kuin isäntäkonekin.
- NAT. IP-osoitteeksi tulee privaattiosoite, joka on samassa aliverkossa kuin isäntäkone
- Host-only. Virtuaalinen verkkoadapteri saa IP-osoitteen VMwaren määrittelemästä aliverkosta. Tällä tyypillä yhteyksiä voidaan luoda vain VMwaren sisällä.

- Custom. Käyttäjän muokattavissa oleva valinta. Esimerkiksi DHCP-poolit ova muokattavissa.
- LAN-segmentti. Käyttäjän muokattavissa olevat LAN-segmentit

Tässä työssä valittiin ensimmäisen verkkoadapterin tyypiksi sillattu, sillä sitä haluttiin käyttää SSH-yhteyttä varten. Toisia verkkoadaptereita käytettiin LAN-segmentteihin. Näitä on tässä työssä käsitelty myöhempänä lisää, kun itse verkkotopologiaa alettiin rakentamaan.

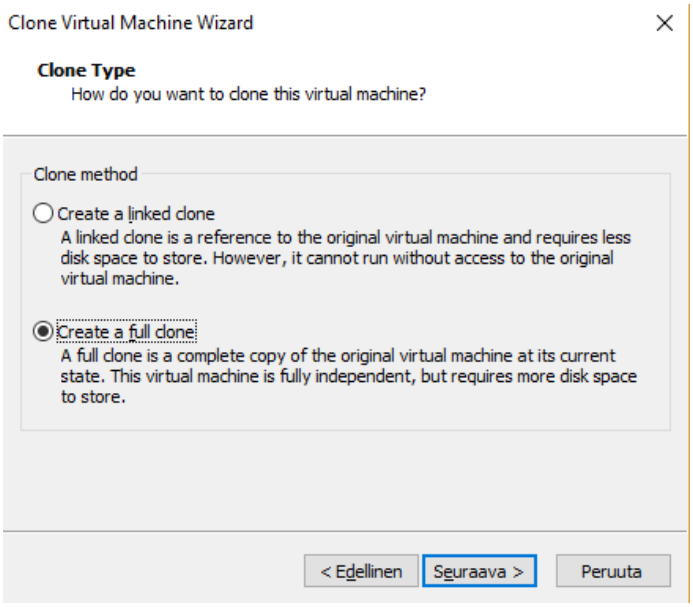
Yhdellä virtuaalikoneella ei vielä kovin pitkälle pääse testaustarkoituksissa, joten tässä työssä luotiin tuon ensimmäisen vSRX:n rinnalle lisäksi toinen vSRX-laite sekä yksi Virtual Router (VR), joille testaustopologia rakennetaan. Tässä tilanteessa hyödylliseksi osoittautui virtuaalikoneiden kloonaaminen, jota käsiteltiin tässä työssä luvussa 6.2. On siis mahdollista ottaa jo olemassaolevasta virtuaalikoneesta kopio kloonaamalla se. Valitaan VMware Workstationissa kohta VM, Manage, Clone. Tällöin aukeaa Clone Virtual Machine Wizard, jossa voidaan tehdä määrityksiä siihen, miten virtuaalikone halutaan kloonata.



Kuva 6. Clone Virtual Machine Wizard

Valittavina siis on luoda kloonaamalla uusi virtuaalikone käyttämällä joko emokoneen nykyistä tilaa tai snapshoteja. Snapshoteja käyttäen on mahdollista ottaa klooni jostakin emokoneen menneestä hetkestä, mikäli snapshotteja on siis otettu. Kuten kappaleessa

6.4 käsiteltiin, snapshotit eivät tule automaattisesti, vaan käyttäjän tulee ne ottaa. VMware Workstation esimerkiksi kuitenkin antaa käyttäjälle mahdollisuuden ottaa snapshot nykytilasta tai palata edellisen snapshotin tilaan, kun virtuaalikone suljetaan. Tässä tapauksessa valittiin klooni emokoneen nykytilasta, sillä snapshotteja ei vielä ollut. Seuraavassa vaiheessa asennustyökalu kysyy, halutaanko luoda linked-klooni vai täysklooni. Linked-klooni siis on osittain riippuvainen alkuperäisestä virtuaalikoneesta, kun taas täysklooni on täysin itsenäinen. Täysklooni toki vie enemmän levytilaa, mutta tässä työssä valittiin se käytettäväksi, sillä tällöin sen suorituskyky on hieman parempi. Tämä johtuu siitä, että linked-kloonissa levytilaa vaaditaan vähemmän suorituskyvyn kustannuksella.



Kuva 7. Kloonityypin valinta

Viimeisessä asennustyökalun vaiheessa klooni tulee nimetä ja valita asennuslokaatio, jonka jälkeen VMware Workstation luo kloonin. Kloonin luomisessa ei kestä pientä hetkeä pidempään.

7.2 Virtuaalikoneiden yhdistäminen

Seuraava vaihe oli virtuaalilaitteiden yhdistäminen toisiinsa. Tässä kohtaa virtuaalikoneiden verkkoadaptereiden asetukset tulivat oleellisiksi. Näiden asetuksilla on

mahdollista ikään kuin kaapeloida vSRX-laitteiden interfaceja toisiinsa. Tähän käyttötarkoitukseen tarvitaan LAN-segmenttejä, joten loput verkkoadapterit siis asetettiin LAN segment-tilaan. Jokainen virtuaaliadapteri vSRX-laitteella vastaa tiettyä interfacea laitteella. Ensimmäinen verkkoadapteri on hallintainterface fxp0, toinen verkkoadapteri vastaa interfacea ge-0/0/0, kolmas interfacea ge-0/0/1 ja niin edelleen. Työtä varten tämä määrä interfaceja oli riittävä, joten uusia adaptereita ei tarvinnut lisätä. Mikäli interfacejen lisääminen olisi jossain muussa tapauksessa tarpeellista, tulee lisätä niin monta uutta verkkoadapteria, kuin mikä on vaadittujen interfacejen määrä. Huomionarvoista on myös se, että mikäli interfaceja lisätään, tulee niitä vastaavien verkkoadaptereiden olla oikean tyyppisiä, sillä muutoin virtuaalikone ei toimi. Oletuksena lisätyt adapterit ovat vääräntyyppisiä, ja nämä tulee manuaalisesti muokata tyyppiin vmxnet3.

Verkkoadapterit siis vastaavat vSRX-laitteella olevia interfaceja, toisen verkkoadapterin vastatessa interfacea ge-0/0/0. Kuten aikaisemmin on mainittu, jotta voitaisiin yhdistää vSRX-laitteiden interfaceja toisiinsa, tulee näitä vastaavat verkkoadapterit asettaa samaan LAN-segmenttiin verkkoadapterin asetuksissa. Esimerkiksi tässä työssä haluttiin yhdistää vSRX1 sekä vSRX2 ge-0/0/0 interfacet toisiinsa. Tämän saavuttamiseksi tulee siis molempien laitteiden toinen verkkoadapteri asettaa samaan LAN-segmenttiin. Työssä käytetyt LAN-segmentit:

- vSRX1 ge-0/0/0 -> vSRX ge-0/0/0
- vSRX1 ge-0/0/1 -> VR1 ge-0/0/1
- vSRX2 ge-0/0/1 -> VR2 ge-0/0/1.

7.3 Virtuaalikoneiden konfiguroiminen

Kun virtuaalikoneita oli luotu haluttu määrä, oli aika katsoa laitteiden konfiguraatiota. Ensimmäisenä vaiheena tässä työssä haluttiin käyttää etäyhteyttä virtuaalikoneisiin käyttäen hyväksi SSH:ta. Etäyhteys haluttiin sen vuoksi, että virtuaalikone käyttää amerikkalaista näppäimistöä, jonka sijaan haluttiin käyttää tutumpaa versiota. Tähän käyttötarkoitukseen tarvitaan erillinen SSH-ohjelma, johon tässä tapauksessa valikoitui

ilmainen PuTTY. SSH-yhteyden luomiseksi ensin virtuaalikoneella sallittiin ssh-yhtyedet sekä luotiin superuser-käyttäjä vSRX-virtuaalikoneelle seuraavilla komennoilla:

- set system services ssh. Tällä komennolla sallitaan laitteelle SSH-yhteydet.
- set system login user käyttäjänimi class super-user. Käyttäjän luonti, jossa valitaan haluttu käyttäjänimi.
- set system login user käyttäjänimi authentication plain-text-password. Asetetaan käyttäjänimelle salasana.
- commit. Tallennetaan konfiguraatio.

Tämän jälkeen virtuaalikoneen hallinta-interfacelle tulee asettaa ip-osoite. Tämä hallinta-interface vSRX-laitteilla on fxp0, joten tämä interface konfiguroidaan saamaan suoraan DHPC:n kautta IP-osoite seuraavalla komennolla: set interfaces fxp0 unit 0 family inet dhcp.

```
root@R2# run show interfaces fxp0 terse
Interface               Admin Link Proto    Local                 Remote
fxp0                    up    up
fxp0.0                  up    up   inet     192.168.1.6/24
```

Kuva 8. Hallinta-interface sai osoitteen DHCP:llä

```
C:\Users\Samu>ping 192.168.1.6

Pinging 192.168.1.6 with 32 bytes of data:
Reply from 192.168.1.6: bytes=32 time=2ms TTL=64
Reply from 192.168.1.6: bytes=32 time<1ms TTL=64
Reply from 192.168.1.6: bytes=32 time=1ms TTL=64
Reply from 192.168.1.6: bytes=32 time<1ms TTL=64
```

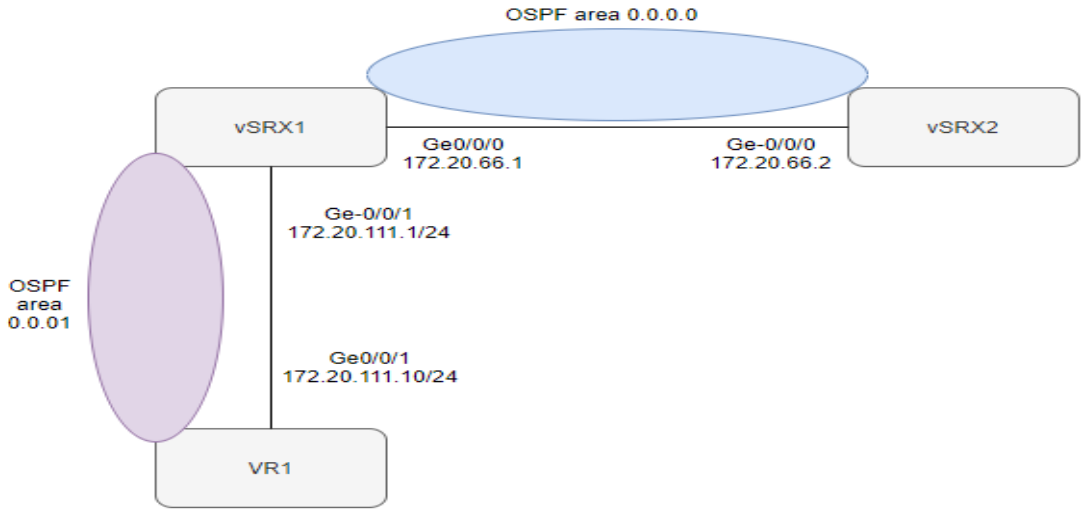
Kuva 9. Virtuaalikoneen pingaaminen työasemalta

Interface siis sai osoitteen ja ping-testi toimii, joten voimme yhdistää siihen valitulla SSH-ohjelmalla käyttäen luotua superuseria.

Kun virtuaalikone käynnistyy, pyytää se käyttäjää kirjautumaan. Juniperin verkkokursseja suorittavat saavat tunnukset ohjaajaltaan. Mikäli kyseessä olisi uusi vSRX, kirjautuminen tapahtuisi käyttämällä käyttäjänimeä *root* ilman salasanaa. Ennen konfiguraation aloittamista tulee koneelle luoda salasana käyttämällä komentoa **set system root-authentication plain-text-password**. Ilman salasanan asettamista laite ei anna tallentaa eli kommitoida konfiguraatioita. Aluksi vSRX on luonnollisesti peruskonfiguraatiota lukuunottammatta tyhjä. Opiskelijan virtuaaliselta työpöydältä löytyvät jokaiselle Juniperin verkkokurssille laitteille pohjakonfiguraatiot. Näiden lataaminen esimerkiksi vSRX:lle tapahtuisi konfiguraatiotilassa seuraavalla komennolla: **load override *hakemisto/tiedostonimi*.config.** Toisin kun esimerkiksi Ciscon laitteita käytettäessä, jossa muutokset tulevat voimaan heti, on Juniperin laitteita käytettäessä muistettava tallentaa konfiguraatio käyttämällä komentoa commit, jotta muutokset tulevat voimaan.

Tämän jälkeen interfaceille konfiguroitiin IP-osoitteet, mutta pingaaminen ei vielä toiminut laitteiden välillä. Tämä johtui siitä, että SRX-laitteet ovat pohjimmiltaan palomuurilaitteita, joissa toimivat security-zonet, joissa ping ei ole sallittu automaattisesti. Tämä voitiin sallia seuraavilla komennoilla: **set security zones security-zone trust host-inbound-traffic system-services all** ja **set security zones security-zone trust interfaces *interface* host-inbound-traffic system-services ping**. Mikäli jostakin syystä näitä policyjä ei haluta käyttää, vaan SRX-laitteita haluttaisiin käyttää ’’normaaleina’’ reitittiminä palomuurin sijaan, saataisiin se aikaan seuraavilla komennoilla: **delete security** ja **set security forwarding-options family mpls mode packet-based**. Kun moodia vaihdetaan, tulee laite käynnistää uudelleen.

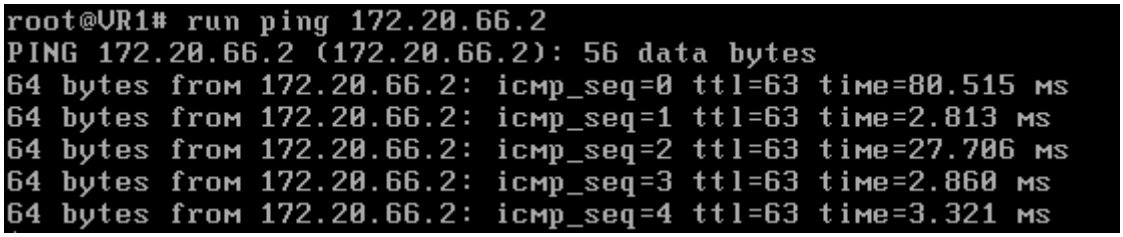
Työn lopussa konfiguroitiin kahden alueen OSPF-protokolla kolmen vSRX-laitteen välille. Topologia on siis suhteellisen yksinkertainen, sillä päätarkoitus työssä on itse virtuaaliympäristön luonti ja sen testaaminen.



Kuva 10. Verkkotopologia

OSPF:ssa käytössä ovat alueet 0.0.0.0 sekä 0.0.0.1, joista ensimmäinen toimii vSRX1:n ja vSRX2:n välillä ja jälkimmäinen on laitteiden vSRX1 ja VR1 välillä. Protokolla konfiguroitiin näiden laitteiden välillä toimiviin interfaceihin ja ne liitettiin kyseisiin alueisiin. Kun käytössä ovat security policyt, tulee tähän policyyn sallia OSPF-protokolla ja sallia globaalilla tasolla liikenne. Tämä tapahtuu samalla tavoin kuin tässä työssä aikaisemmin käytetty komento ping-liikenteelle. Ensiksi suoritettiin komento **set security zones security-zone trust host-inbound-traffic protocols all** ja tämän jälkeen **set groups *nimi* security policies default-policy permit-all**. Nämä komennot suoritetaan kaikilla laitteilla ja ne liitetään samaan ryhmään. Näiden

komentojen jälkeen liikenne toimii laitteiden VR1 ja vSRX2 välillä OSPF-protokollan ansiosta.



Kuva 11. Ping-testi laiteiden VR1 ja vSRX2 välillä. Osoite 172.20.66.2 on laitteen vSRX interfacen ge-0/0/0 osoite.

7.4 Opiskelijan työpöytä ja kurssien tekemisen aloitustilan konfigurointi

Viimeisenä vaiheena tässä työssä on toinen testi, jossa asennettiin opiskelijan virtuaalinen työpöytä sekä konfiguroitiin vSRX-laite Juniperin määrittämille peruskonfiguraatioille kurssien suorittamista varten. Opiskelijan työpöydältä tulee kurssien suorittamista varten saada vSRX-laitteille SSH-yhteys. Tätä varten ympäristöön luotiin yksi vSRX-laite lisää. Opiskelijan työpöytänä toimii CentOS 6.6. Tällä testillä on tarkoituksena luoda vastaavanlainen ympäristö kuin mitä opiskelijat tulevat käyttämään Juniper-verkkokurssien suorittamiseen

Opiskelijan asennustiedostot koostuvat viidestä tiedostosta, jotka tulee asettaa samaan kansioon ja purkaa 7zip-ohjelmalla. Siten näistä muodostuu yksi .OVA-tiedosto, jonka voi exportata VMware Workstationiin virtuaalikoneeksi. Sen asentaminen onnistuu samalla tavoin kuin vSRX-laitteenkin asentaminen. Tällä virtuaalikoneella on kaksi virtuaalista verkkoadapteria, joiden rooli on tärkeä tämän opinnäytetyön kannalta. Kuten aikaisemmassa luvussa kävi ilmi, vSRX-virtuaalikoneella on oletuksena kolme virtuaaliadapteria, jotka vastaavat laitteelta löytyviä interfaceja. Myös työpöydän virtuaalikoneella olevat verkkoadapterit vastaavat siltä löytyviä ethernet-interfaceja eth0 ja eth1. Ensimmäinen adapteri asetettiin siltaavaan tilaan, jolloin eth0-interface saa suoraan verkko-osoitteen reitittimeltä internetyhteyden luomiseksi. Toinen adapteri asetettiin samaan virtuaaliverkkoon kuin vSRX-laitteen fxp0-interface. Virtuaaliverkkoja varten VMwarella on valmiiksi määriteltyjä verkkoja, joilla voidaan yhdistää virtuaalikoneita samaan aliverkkoon internaalisesti. Tässä työssä valittiin virtuaaliverkko VMnet1, jossa on käytössä DHCP-pool. Kun molemmat tarvittavat adapterit oli tähän

verkkoon yhdistetty, ne saivat tästä poolista osoitteet. VMwaren virtuaalisia verkkoja on mahdollisuus myös lisätä sekä muokata niiden asetuksia, kuten esimerkiksi DHCP-poolia, mutta se ei ollut tämän työn suorittamisen kannalta tarpeellista.

Juniperin verkkokursseja varten vSRX-laitteille tuli ladata pohjakonfiguraatio. Pohjimmiltaan Juniperin reitittimet ovat UNIX-palvelimia, joten haluttu tiedosto siirrettiin käyttämällä scp:tä. vSRX-laitteelle sallittiin ssh-yhteys, jotta tiedoston siirtäminen onnistuu.Lisäksi luotiin Juniperille haluttu kansio, johon konfiguraatiotiedosto siirrettiin.

```
C:\Users\Nakki>pscp.exe C:\Users\Nakki\reset.config lab@192.168.1.12:/var/home/lab/JIR
Keyboard-interactive authentication prompts from server:
| Password:
End of keyboard-interactive prompts from server
reset.config              | 1 kB |   1.5 kB/s | ETA: 00:00:00 | 100%
```

Kuva 12. SCP. Tiedoston siirto tiedoston sijainnista haluttuun sijaintiin.

Kun haluttu konfiguraatiotiedosto oli siirretty, sekä tämän sisältämä konfiguraatio tallennettu laitteelle, oli enää pari vaihetta laitteen valmiuteen kurssien suorittamista varten. Laitteelle tuli luoda käyttäjätunus, jotta opiskelijat voivat kirjautua laitteelle tätä tunnusta käyttäen. Laitteelle luotiin käyttäjätunnus lab, jolle asetettiin salasana, jonka opiskelijat saavat ohjaajaltaan. Tässä vaiheessa vSRX-laite oli valmis kuin myös opiskelijan työpöytäkin. Viimeisenä vaiheena testattiin SSH-yhteyden toimivuus.

```
lab@localhost:~
File  Edit  View  Search  Terminal  Help
[lab@localhost ~]$ ping 172.25.11.1
PING 172.25.11.1 (172.25.11.1) 56(84) bytes of data.
64 bytes from 172.25.11.1: icmp_seq=1 ttl=64 time=0.656 ms
64 bytes from 172.25.11.1: icmp_seq=2 ttl=64 time=1.56 ms
64 bytes from 172.25.11.1: icmp_seq=3 ttl=64 time=1.15 ms
64 bytes from 172.25.11.1: icmp_seq=4 ttl=64 time=1.09 ms
^C
--- 172.25.11.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3765ms
rtt min/avg/max/mdev = 0.656/1.118/1.562/0.321 ms
[lab@localhost ~]$ ssh 172.25.11.1
Warning: Permanently added '172.25.11.1' (RSA) to the list of known hosts.
Password:
--- JUNOS 17.3R2.10 built 2018-02-08 02:19:07 UTC
lab@vSRX-1>
```

Kuva 13. SSH-yhteyden testaus.

7.5 Työn aikana esiintyneet ongelmat

Vaikka loppujen lopuksi työ saatiin kuntoon lokaalilla suoritustavalla, oli alun perin suunnitelma työn toteuttamiseksi kuitenkin varsin erilainen. Alkuperäisenä suunnitelmana tässä työssä oli suorittaa työ Metropolian kampuksella ja etätyöllä, jolloin yhteys Metropolian palvelimeen oltaisiin otettu VPN:n avulla. Metropolian palvelimella toimi niin ESXi-hypervisor kuin vCenter Serverkin, joita käyttäen virtuaaliympäristö Juniperin verkkokursseja varten toteutetaan tulevaisuudessa. Kuitenkin epäonnisten tapahtumien seurauksena palvelimet jouduttiin sulkemaan, ja sen mukana tämä ympäristö kävi tätä työtä varten mahdottomaksi käyttää. Sen sijaan tässä työssä päädyttiin toteuttamaan virtuaaliympäristön luonti sekä virtuaalikoneiden testaaminen lokaalisti käyttäen VMware Workstationia.

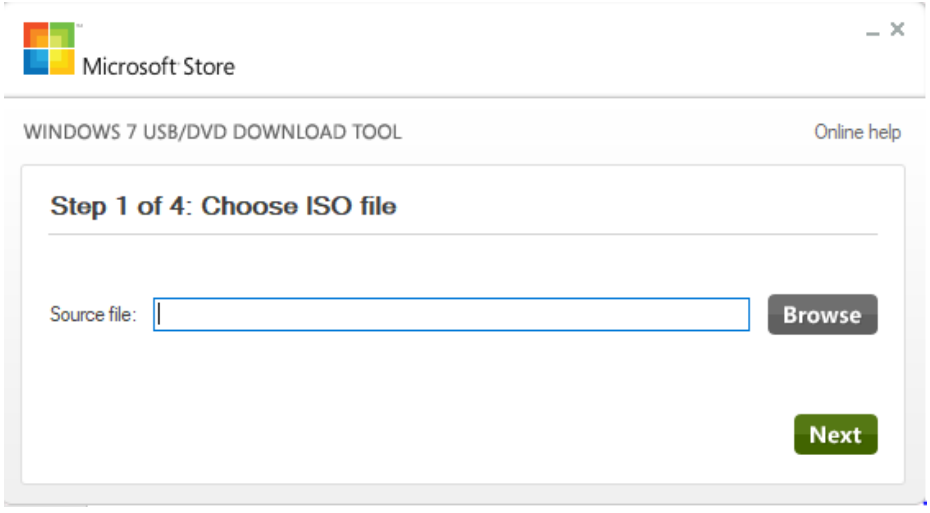
Ensimmäisenä ongelmana ilmeni työssä käytettävän tietokoneen laitteiston riittämättömyys työn suorittamiseen. Jokainen työssä käytetty vSRX-virtuaalikone vaatii 4gb RAM-muistia toimiakseen ja koneen sisältäessä vain 8gb RAM-muistia. Olisi ollut mahdotonta ajaa kaikkia työssä käytettävää neljää virtuaalikonetta samanaikaisesti. Työssä yritettiin säätää virtuaalikoneen asetuksia, ja erityisesti vähentää niiden käyttämää muistin määrää. Tämä osoittautui kuitenkin toimimattomaksi ratkaisuyritykseksi, sillä kävi ilmi, että vSRX-virtuaalikoneet todellakin vaativat tuon 4gb muistia toimiakseen. Kun asetuksia yritettiin säätää alemmas, virtuaalikoneet eivät

suostuneet käynnistymään ollenkaan, vaan ne menivät suoraan JunOS:n alla toimivaan Wind River Linux -kerneliin, josta toiminta ei edennyt mihinkään.

Kuva 14. Wind River

Ongelma ratkaistiin lainaamalla Metropolian tietohallinnolta tietokone, jonka ominaisuudet sekä suorituskyky riittivät työssä käytetyn ympäristön toimintaan.

Lainakoneelle asennettiin Windows 10 -käyttöjärjestelmä luomalla ensin USB-muistitikulle järjestelmän asennustiedosto käyttäen hyödyksi Microsoft USB Download Toolia. Tämä työkalu on ilmaiseksi ladattavissa Microsoftin sivuilta.



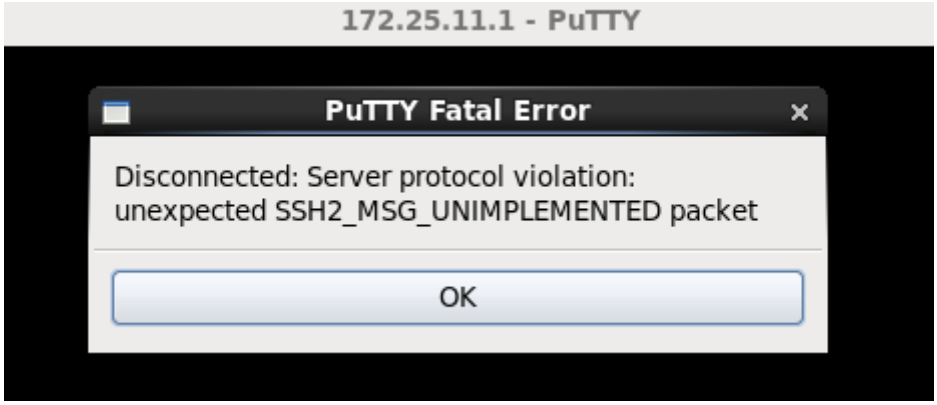
Kuva 15. Windows USB Download Tool

Tämän työkalun avulla on mahdollista tuoda muistitikulle haluttu .ISO-tiedosto muodossa, jossa käynnistäminen ja asentaminen tyhjälle tietokoneelle on mahdollista. Työkalun käyttö on nelivaiheinen ja yksinkertainen. Ensiksi valitaan haluttu .ISO-tiedosto, joka tässä tapauksessa oli ladattu Windows 10 -asennustiedosto. Seuraavaksi valitaan median tyyppi, joka oli tässä tapauksessa USB-laite Työkalulla on mahdollista luoda käyttötarkoitukseen myös DVD. Kahdessa viimeisessä vaiheessa tulee tietokoneeseen laittaa USB-laite kiinni ja suorittaa siirtäminen loppuun. Näiden vaiheiden jälkeen USB-laite on valmis siirrettäväksi tyhjään tietokoneeseen kiinni, josta käynnistämisen yhteydessä käyttöjärjestelmän asentaminen onnistuu.

Sen lisäksi, että luotiin käynnistävä USB-tikku, tuli myös BIOS-asetuksia hieman mukata. Normaalisti BIOS-asetuksissa käynnistys on määriteltynä UEFI:ksi. Jotta se kuitenkin saatiin käynnistymään tikulta, oli käynnistysmoodi asetattava Legacyksi. Tämän lisäksi käynnistämisjärjestystä muokattiin hieman. Ensimmäiseksi käynnistysvaihtoehdoksi asetettiin tietokoneen kiintolevy ja toiseksi USB. Lopulta käyttöjärjestelmä saatiin asennetuksi ja päästiin itse virtuaaliympäristön rakentamiseen.

Opiskelijan työpöydän osalta törmättiin myös ongelmaan. Tämän virtuaalikoneen interfacet eth0 sekä eth1 eivät saaneet IP-osoitteita, vaikka ensimmäinen adapteri oli asetettu suoraan siltaavaksi ja toinen saamaan DHCP:llä osoite VMwaren sisäisestä poolista. Ensimmäiseksi kokeiltiin tarkastaa näiden interfacejen asetukset. Komennolla vi /etc/sysconfig/network-scripts/ifcfg-eth0 päästiin tarkastelemaan interfacen eth0-konfiguraatiota. Tämä tiedosto oli tyhjä, joten ei ollut ihmekään, ettei kyseinen interface saanut osoitetta. Tyhjän tiedoston tilalle kirjoitettiin seuraavaa allekkain: DEVICE=eth0, TYPE=ethernet, ONBOOT=yes, BOOTPROTO=dhcp. Tiedosto tallennettiin sekä linuxin verkkopalvelu käynnistettiin uudelleen. Tämä ei kuitenkaan syystä tai toisesta toiminut, joten jouduttiin kokeilemaan toista komentoa **dhclient -v**, jolla interfacet saivat lopulta osoitteet. Tämän jälkeen varmistettiin, että opiskelijan työpöydältä saadaan SSH-yhteys vSRX-laitteelle. Opiskelijan työpöydältä löytyy SSH-yhteyttä varten PuTTY valmiiksi määriteltynä sekä kolme erillistä sessiota, vSRX-1, vSRX-2 sekä VR1-laitteille kullekin omansa työpöydältä. Kun tässä työssä yritettiin yhdistää esimerkiksi vSRX1-laitteelle

käyttäen valmista PuTTY-yhteyttä, tuli vastaan seuraavanlainen virheilmoitus:



Kuva 16. PuTTY-virheilmoitus

Tämä johtui siitä PuTTY:n vanhasta versiosta, jossa käytössä oli vääränlainen algoritmin valinta. Oikea algoritmi olisi ollut Diffie-Hellman group 14, mutta tätä ei kuitenkaan voinut tässä valmiiksi määritellyssä PuTTYssä vaihtaa. Opiskelijan työpöydän konsolin kautta SSH-yhteyden luominen kuitenkin onnistui vailla ongelmia.

8 Loppupäätelmät

Virtuaalikoneet ovat uusi ja kätevä tapa toteuttaa verkkotopologioita. Tässä työssä harmillinen takaisku oli se, että työtä ei voitu suorittaa varsinaisella ESXi-palvelimella, vaan se loppujen lopuksi jouduttiin suorittamaan lokaalisti käyttäen VMware Workstationia. Tämä kuitenkin osoittautui mielenkiintoiseksi sekä myös opettavaiseksi projektiksi, sillä tekijällä ei ollut minkäänlaista edeltävää tietoa virtuaaliympäristöjen luonnista, vaan se oli tekijälle täysin uutta. Juniperin virtuaalikoneet soveltuvat mainiosti Metropolian tarjoamien verkkokurssien suorittamiseen ja niiden toiminnallisuus vastaa fyysisiä SRX-laitteita. Virtuaalilaitteiden mukanaan tuoma hyöty on myös se, ettei fyysisiä laitteita tarvitse hankkia, jotka veisivät turhaan tilaa, kun on tarjolla virtuaalisiakin koneita. Mielestäni kuitenkaan virtuaalilaitteilla ei voida täysin korvata opetusta fyysisillä laitteilla, sillä mielestäni laitteet oppivat tuntemaan paremmin, kun ne ovat fyysisinä vieressä. Tämän lisäksi laitteiden kaapelointia on tärkeää opetella, joka tuleekin nykyisten Cisco-kurssien yhteydessä varsin tutuksi. Virtuaalikoneilla toteutettava verkko-opetus on kuitenkin varsin hyödyllinen lisä opetustarjontaan, sillä virtualisointi yleistyy

jatkuvasti ja on näin ollen opiskelijoille hyödyllinen taito osata käyttää myös näitä laitteita ja niiden ympäristöä.

Huomionarvoista on, että tässä työssä vSRX-laitteelle ajettiin vain pohjakonfiguraatio scp:tä hyödyksi käyttäen. Todellisuudessa Metropolian tulee siirtää kaikki laboratorioiden konfiguraatiot Juniperin laitteille, jotta opiskelijat voivat ne sieltä helposti ottaa käyttöön. Lisäksi vSRX-laitteita tulee ajaa ympäristöön enemmän kurssien tarpeita vastaavaan määrään. Tällöin oleellista on ottaa huomioon Vmwaressa varsinkin adaptereiden asetukset.

Lähteet

1 Virtualization Essentials, Portnoy 2016.

2 Brief history of Virtualization, Oracle. < https://docs.oracle.com/cd/E26996_01/E18549/html/VMUSG1010.html> . Luettu 11.05.2019.

3 Virtualization Engineer Salaries in the United States, Indeed < https://www.indeed.com/salaries/Virtualization-Engineer-Salaries>. Luettu 11.05.2019.

4 Controlling Virtual Machine Sprawl, VMware < https://www.vmware.com/techpapers/2012/controlling-virtual-machine-sprawl-10339.html>. Luettu 11.05.2019.

5 Virtualization, a Beginner's Guide, Ruest & Ruest 2009.

6 What Is a Hypervisor?, VMware < https://www.vmware.com/topics/glossary/content/hypervisor>. Luettu 11.05.2019.

7 vSphere, VMware. < https://www.vmware.com/products/vsphere.html>. Luettu 11.05.2019.

8 ESXi vs. ESX: A Comparison of Features, VMware .<https://blogs.vmware.com/vsphere/2009/06/esxi-vs-esx-a-comparison-of-features.html>. Luettu 11.05.2019.

9 Mastering VMware vSphere 5.5, Lowe & Marshall 2014.

10 ESXi and vCenter Server 5.1 Documentation, VMware.<https://pubs.vmware.com/vsphere-51/index.jsp?topic=%2Fcom.vmware.vsphere.vcenterhost.doc%2FGUID-CE128B59-E236-45FF-9976-D134DADC8178.html>. Luettu 11.05.2019.

11 vSphere 4.1 – ESX and vCenter, VMware. <https://pubs.vmware.com/vsphere-4-esx-vcenter/index.jsp?topic=/com.vmware.vsphere.availability.doc_41/c_useha_works.html>. Luettu 11.05.2019.

12 ESXi Hardware Requirements, VMware. < docs.vmware.com/en/VMware-vSphere/6.0/com.vmware.vsphere.install.doc/GUID-DEB8086A-306B-4239-BF76-E354679202FC.html>. Luettu 11.05.2019.

13 Cloning Virtual Machines, VMware <https://pubs.vmware.com/workstation-9/index.jsp?topic=%2Fcom.vmware.ws.using.doc%2FGUID-5DE53D02-9A58-4F9F-84BE-FE21AE82EA4E.html>. Luettu 11.05.2019.

14 How Nested Virtualization Works, Microsoft. < https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/user-guide/nested-virtualization#how-nested-virtualization-works>. Luettu 11.05.2019.

15 Installing vSRX with VMware vSphere Web Client. <https://www.juniper.net/documentation/en_US/vsrx/topics/task/installation/security-vsrx-vsphere-client-installing.html>. Luettu 11.05.2019.

16 Junos OS Features Supported on vSRX, Juniper. <https://www.juniper.net/documentation/en_US/vsrx/topics/concept/security-vsrx-feature-support.html>. Luettu 11.05.2019.

17 Understanding vSRX with VMware, Juniper. <https://juniper.net/documentation/en_US/vsrx/concept/topics/security-vsrx-vmware-overview.html>. Luettu 11.05.2019.

18 Getting Started Guide for VMware, Juniper. <https://www.juniper.net/documentation/en_US/vmx/information-products/pathway-pages/getting-started/vmx-gsg-vmware.html>. Luettu 11.05.2019.