jamk.fi

Työasemavirtualisoinnilla toteutettu palvelinvirtualisointi VMware vSphere -ohjelmistolla

Juuso Niemensyrjä

Opinnäytetyö
Helmikuu 2014

Tietoverkkotekniikan koulutusohjelma
Tekniikan ja liikenteen ala

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

KUVAILULEHTI

Tekijä(t) Niemensyrjä, Juuso	Julkaisun laji Opinnäytetyö	Päivämäärä 04.02.2014
	Sivumäärä 103 + 3	Julkaisun kieli Suomi
		Verkkojulkaisulupa myönnetty (X)

Työn nimi
Työasemavirtualisoinnilla toteutettu palvelinvirtualisointi VMware vSphere -ohjelmistolla

Koulutusohjelma
Tietotekniikka

Työn ohjaaja(t)
Rantonen, Mika; Häkkinen, Antti

Toimeksiantaja(t)
Jyväskylän Ammattikorkeakoulu, Jokinen, Juha

Tiivistelmä

Opinnäytetyön tarkoituksena on perehtyä VMware vSphere -nimisen ohjelmistotuoteperheen hyödyntämistä palvelinvirtualisointiin työasemavirtualisoinnilla. Työn perustuksena käytetään VMWare Workstation -ohjelmaa, jolla virtualisoidaan VMWare vShpere -palvelinvirtualisointiohjelmistoa. Ohjelmistoa käytetään suurten palvelinsalien resurssien maksimaaliseen hyödyntämiseen palvelujen tuottamisen nykypäivän standardien mukaisesti, mutta varsinaisen palvelinraudan puutteen vuoksi työ haluttaan suorittaa virtualisoituna työasemaraudan päällä.

Ympäristön pystyttämisen jälkeen on tavoitteena kartoittaa ohjelmiston tuomat mahdollisuudet ja rajoitteet palvelinympäristöjen testaus ja koulutuskäyttöön. Lisäksi tarkoituksena on selvittää ohjelmiston lukuisten ominaisuuksien toiminnallisuutta, kuten virtuaalikytkimet, korkean käytettävyyden ominaisuudet sekä resurssien jako ja -käyttö.

Työn käytännön osuuden suunnittelu tehdään yhteistyössä työn tilaajan ja päävastuussa olevan ohjaavan opettajan kanssa. Käytännön osuuden tarkoituksena on tuottaa valmis konsepti, jonka runkoa ja toiminnallisuutta opiskelijat voivat harjoitella kursseilla. Lisäksi tuotettua teoriaosuutta halutaan käyttää jatkossa kurssien käytännön osuuden tukimateriaalina.

Avainsanat (asiasanat)
VMware Workstation, VMware vSphere, virtualisointi, palvelinympäristö

Muut tiedot

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

Description

Author(s)	Type of publication	Date
Niemensyrjä, Juuso	Bachelor's Thesis	04.02.2014
	Pages 103 +3	Language Finnish
		Permission for web publication (X)

Title
Data center virtualization executed with desktop hardware using VMware vSphere product

Degree Programme
Information Technology

Tutor(s)
Rantonen, Mika; Häkkinen, Antti

Assigned by
JAMK University of Applied Sciences, Jokinen Juha

Abstract

The purpose of this thesis was to study how data center virtualization could be executed with ordinary desktop hardware using VMware vSphere products. The basis of this study was VMware's own virtualization program called VMware Workstation which was then used to virtualize VMware vSphere data center virtualization software. In normal circumstances this software is used at large data centers to use hardware resources in order to produce maximal benefit as producing services. However, there was not enough proper server hardware to use, thus the testing was carried out using desktop virtualization.

After establishing the testing environment the task was to chart in the potential and the limits of the vSphre software in this kind of technical arrangement as well as to focus on the numerous features of this software such as virtual switches, high availability and distributed resource management. This knowledge would be later used as study material for the future courses.

The practical part of this thesis was designed in cooperation with the assigner and main supervisor. The point here was to produce a complete concept to be used and practiced by other students for future courses. The theory part of this thesis will also be used as a study material in these courses.

Keywords
VMware Workstation, VMware vSphere, virtualization, data center

Miscellaneous

SISÄLTÖ

KUVIOT

TAULUKOT

Käsitteitä

ARP/RARP	Address resolution Protocol/ Reverse Address resolution Protocol. Protokolla, jolla verkkolaitteet pyrkivät selvittämään verkkolaitteen MAC-osoitteen IP-osoitteen perusteella tai muuntamaan kyseistä tietoa.
CPU	Central Processing Unit. Tietokoneen prosessori, jonka tehokkuus ilmoitetaan yleensä gigahertseinä eli kuinka monta toimintoa prosessori pystyy suorittamaan sekuntia kohti.
Guest	Virtualisoitavasta järjestelmästä käytetty termi. Voi viitata myös virtuaalikoneeseen.
Host	Virtualisoinnin yhteydessä termillä puhutaan yleisesti järjestelmästä tai koneesta, joka toimii virtualisoinnin alustana.
I/O	Input/Output. Termi kuvaa kommunikaatiota kahden laitteen tai komponentin välillä. Input on laitteen omasta näkökannasta sille tulevan tiedon määritelmä ja output laitteelta lähtevän tiedon määritelmä.
IEEE 802.1Q	Standardi, joka määrittelee VLAN-leimausta ja siihen liittyvää tekniikkaa tietoverkoissa.
IP	Internet Protocol. Verkkolaitteiden väliseen viestintään käytettävä protokolla.
Kytkin	Tietoverkkolaite, joka operoi yleensä OSI-mallin toisella kerroksella toimittaen datapaketteja laitteille MAC-osoitteiden perusteella.
NFS	Network File System. Avoimeen standardiin perustuva protokolla tiedostojärjestelmien jakamiseen verkoissa.
NAT	Network Address Translation. Verkkoprotokolla, joka mahdollistaa usean verkkolaitteen käyttävän samaa IP-osoitetta.
NIC	Network Interface Card. Tietokoneen tai muun laitteen verkkokortti, jonka avulla voidaan yhdistää laite muuhun tietoverkkoon.
MAC	Media Access Control Address. Verkkolaitteiden rajapintoja identifiointiin suuniteltu osoitteistus. Osoite koostuu laitevalmistajan ja rajapinnan uniikista osista ja sitä käytetään OSI-mallin toisen kerroksen viestintään.

OS	Operating System. Lyhennelmä käyttöjärjestelmästä.
OSI	Open System Interconnection. Seitsämästä kerroksesta koostuva malli, jolla pyritään standardisoimaan verkkoliikenteen toimintaa. Kerrokset ovat: 1. Fyysinen kerros, 2. Siirtokerros (MAC), 3. Verkkokerros (IP), 4. Kuljetuskerros (TCP,UDP), 5. Istuntokerros, 6. Esitystapakerros ja 7. Sovelluskerros.
QoS	Quality of Service. Tarkoittaa yleisesti liikenteen luokittelua, jolla pyritään varmistamaan riittävät resurssit korkean prioriteetin liikenteelle ja tarvittaessa antamaan lupa jättää alimman tason liikenne vähemmälle palvelulle ruuhkatilanteiden sattuessa.
RAM	Random Access Memory. Tietokoneen nopea välimuisti, jonka kautta siirretään suoritettavaa dataa tietokoneen eri komponenttien välillä.
Reititin	Tietoverkkolaite, joka operoi IP-verkkokerroksella. Osaa reitittää eri aliverkkojen välistä liikennettä.
SNMP	Simple Network Management Protocol. Tietoverkkojen hallinnassa käytetty protokolla, jolla voidaan kysyä esimerkiksi verkkolaitteen tilaa tai antaa hälyytyksiä verkon toiminnasta.
TCP	Transmission Control Protocol. Tietoliikenneprotokolla, jolla luodaan tiedonsiirtoa varten istunto kahden verkkolaitteen välille.
VM	Virtual machine. Yleinen käsite, jolla tarkoitettaan virtualisoitavaa käyttöjärjestelmää virtualisointiohjelmistossa.
VLAN	Virtual Local Area Nework. IP-verkkoliikenettä erotteleva leimaustekniikka.

1 Työn lähtökohdat

1.1 Tausta

Opinnäytetyön tarkoituksena on perehtyä VMware-ohjelmistotuottajan tarjoamiin tuotteisiin ja selvittää niiden mahdollisuuksia sekä soveltuvuutta oppilaitoksen käyttötarpeisiin. Tarkemmin sanottuna työssä pystytetään palvelinvirtualisointiin tarkoitettu ympäristö, jota virtualisoidaan työasemalla. Kyseinen järjestely ei ole optimaalinen asian tutkimiseen, sillä oikeassa tilanteessa palvelinvirtualisointiympäristön tulisi olla asennettuna suoraan palvelinkäyttöön suunnitellulle raudalle. Työssä käytettävä menetelmä tuottaa ylimääräistä resurssinkäyttöä ympäristöa ylläpitävälle raudalle, kun palvelinvirtualisointiympäristöä joudutaan erikseen vielä virtualisoimaan, luoden omat haasteensa käytössä oleville komponenteille ja ohjelmistolle.

Ajatus tähän työhön syntyi Jyväskylän Ammattikorkeakoulun tarpeesta selvittää aikaisemmin mainitun kaltaisen ympäristön hyödyntäminen opetus- ja kehitystyössä. Aikaisemmin vastaavaa ympäristöä on toteutettu opetustarkoituksissa osittain Microsoft Windows - tuotteita hyväksikäyttäen, mutta tällöinkin VMware-tuotteet ovat olleet kuitenkin läsnä virtualisointiohjelman muodossa. Työ toteutettiinn hyödyntäen oppilaitokselta saatuja tietokoneita ja ohjelmistolisenssejä.

1.2 Tavoitteet ja tehtävät

Työn tavoitteena on luoda toimiva ympäristö tuotteiden ominaisuuksien havainnoimista varten ja niiden toiminnallisuuden määrittelemiseksi. Tavoitteena on lisäksi tuottaa kirjallinen tuotos tämän kuvaamiseksi ja varmistua halutun kaltaisen järjestelyn olevan mahdollinen, jotta sitä voitaisiin hyödyntää oppilaitoksen tarpeiden mukaisesti jatkossa kohtuullisilla investoinneilla. Ohjelmiston kaikkia ominaisuuksia ei ollut tarkoitus käydä työn kuluessa läpi, vaan tilaajan kanssa tarkastettiin lista läpikäytävistä asioista. Muun muassa klusterin tietoturva ei kuulunut tämän työn osalta oleellisten asioiden listalle.

2 Virtualisointi

2.1 Mistä virtualisointi sai alkunsa?

Ajatus virtualisointiin sai alkunsa 1960-luvulla tietokoneiden välimuistin niukkuuden takia. Koska tuolloin muistia oli rajallisesti, alkoi idea virtuaalisesta muistista kehittyä. Tarkoitus oli saada tietokone luulemaan, että siinä onkin enemmän muistia käytettävissä kuin todellisuudessa. Käytännössä tämä tarkoitti erillistä levyä, virtuaalilevyä, jota tietokone pystyi käyttä-

mään välimuistin kaltaisiin toimituksiin. Idealtaan samanlainen virtuaalimuisti on edelleen läsnä nykypäivän tietokoneiden käyttöjärjestelmissä. (Baroudi 2009, 59-60.)

IBM jatkoi uranuurtajana rautavirtualisoinnin parissa, kunnes Unix- ja RISC-järjestelmätoimittajat alkoivat siirtää painotusta rautavirtualisoinnista sovelluspohjaiseen virtualisointiin 1970-luvulla. Kuitenkin tekniikan läpimurtona pidetään VMwaren julkaisemaa PC-arkkitehtuuria virtualisoivan ohjelmiston julkaisua ennen vuosituhannen taitetta. VMware Workstation -nimeä kantava ohjelmisto virtualisoi onnistuneesti nykyisinkin käytössä olevaa x86-suoritinarkkitehtuuria ja mahdollisti useiden käyttöjärjestelmien suorittamisen usealla tietokoneella. Ohjelmisto nousi erityisen suosituksi ohjelmistokehittäjien keskuudessa. Nykyisellään virtualisointi on yksi tietotekniikan kulmakivistä sen tuomien etujen vuoksi. (Baroudi 2009, 60-61; Virtualization Overview 2006.)

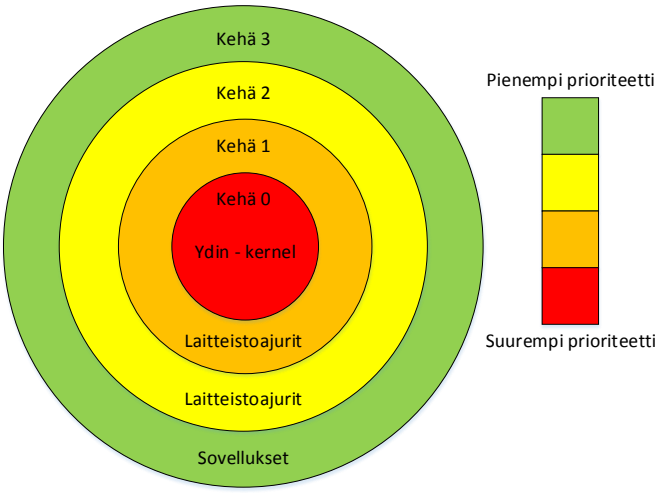
2.2 Virtualisointi käytännössä

2.2.1 Peruskäsitteet virtualisoinnista

Tietokoneiden käyttöjärjestelmä on luotu hyödyntämään sitä varten järjestettyä laitteistoa (muistit, prosessori, tallennusmediat) ja tarjoamaan ympäristö ohjelmistojen suorittamista varten. Kun samaa laitteistoa käyttääkin kaksi tai useampi käyttöjärjestelmä, tulee ymmärtää, ettei tietokoneen laitteistoresursseja voi suoraan käyttää ilman konflikteja. Virtualisoinnissa saman koneen laitteistoresursseja on käyttämässä useampi käyttöjärjestelmä, joten virtualisoinnin tulee tarjota ratkaisu resurssien käyttöön. Esimerkkinä tietokoneen prosessori käyttää omaa sisäistä muistia (memory management unit) eli niin sanottua MMU-yksikköä. Nämä sisäiset muistit pitävät huolta siitä, että prosessori osaa kääntää virtuaalisen muistin osoitteet oikean käytössä olevan muistin osoitteiksi. Ominaisuuden ollessa läsnä ilman virtualisointiakin, täytyy virtualisoinnin yhteydessä estää emuloitavan käyttöjärjestelmän suora pääsy näihin fyysisiin komponentteihin. Virtualisoinnista vastaava hypervisor estää suoran vaikuttamisen fyysiseen rautaan ja ohjaa tässä tapauksessa pyynnöt virtuaaliselle MMU-yksikölle, joka osaa osoittaa muistipyynnöt oikeaan fyysiseen osoitteeseen. Virtualisoinnissa emuloitu järjestelmä uskoo, että se toimii samalla prosessorilla kuin fyysinen käyttöjärjestelmä, kun taas järjestelmän muut fyysiset osat emuloidaan. Tästä syystä huippuunsa viritetyllä tietokoneella emuloidulla käyttöjärjestelmällä voi esimerkiksi olla käytössään huomattavasti tehottomampi näytönohjain kuin fyysisellä tietokoneella. (Novak & Simpson 2010, 405, 407-409.)

Tietokoneen toimintaa ja palveluita varten on kehitetty turvajärjestely kriittisten toimintojen turvaamiseksi. Käyttöjärjestelmissä on sisäänrakennettuna niin kutsutut suojarenkaat eli

kerrokset käyttöoikeuksille, kuten kuviossa 1 on nähtävillä. Ohjelmistot tietokoneella sijoitetaan jollekin turvarenkaalle niiden vaatimien resurssien perusteella. Turvarengas nollalla on täysi pääsy ja korkein palvelutaso laiteresursseihin. Vastaavasti uloimmalla renkaalla olevat ohjelmat joutuvat pyytämään lupaa resursseihin sisemmiltä kerroksilta, ja niitä palvellaan pienimmällä prioriteetilla. Esimerkiksi käyttöjärjestelmän ydin eli kernel pyörii ohjelmistoajurien tavoin kehällä nolla, käyttöjärjestelmän palvelut kehillä yksi ja kaksi ja sovellukset uloimmalla kehällä. Mikäli uloimmalla kerroksella oleva sovellus tarvitsee resursseja käyttöönsä, se joutuu tekemään pyynnön ytimelle eli suorittamaan ”system call” -toiminnon jolloin käyttöjärjestelmän ydin päättää, onko turvallista antaa sovelluksen käyttää haluamiaan resursseja. (Novak & Simpson 2010, 405-406.)



Kuvio 1. Suojarengasmalli

Virtualisoinnin tapauksessa virtualisoitu käyttöjärjestelmä ei välttämättä edes tiedä olevansa virtualisoitu, vaan haluaisi käyttää yhtälailla suoraan laitteiston resursseja. Tästä syystä virtualisoidun käyttöjärjestelmän pyynnöt tulee käsitellä laitteistolle erillisellä tavalla. Klassinen virtualisointi on toinen tapa toteuttaa tämä ja sen toteutus perustuu ”trap-and-emulate”-menettelyyn. Tämä IBM:n vuonna 1974 kehittämä tapa antoi VM-koneen tehdä pyyntöjä suoraan laitteistolle, ja tarkoituksena oli, että pyynnön tullessa virtuaalikoneelta syntyy virhetilanne prosessorilla. Virhe havaitaan ja vangitaan (trap), mikä taas mahdollistaa virtualisointiohjelmiston suorittaa säätöjä (emulate) havaitulle virhetilalle. Tällä mahdollistetaan sekä isäntäkoneen että virtuaalikoneen yhtäaikainen toiminta. Ratkaisu vaatii kuitenkin käytettävältä laitteistolta tuen toimiakseen. x86-arkkitehtuuri ei luo samalla tavalla virheitä, joita voitaisiin vangita ja emuloida. x86-virtualisointi on tästä syystä huomattavasti monimutkaisempi ja vaatii erilaisia tekniikoita, joita selitetään luvussa 2.2.2. x86-arkkitehtuurilla

tarkoitetaan yleisesti käytössä olevaa prosessoriarkkitehtuuria. (Novak & Simpson 2010, 406.)

Virtualisointi ei rajoitu vain käyttöjärjestelmien virtualisoinnille. Tekniikka mahdollistaa myös esimerkiksi sovellusten tai työpöytäympäristöjen virtualisoinnin, mutta koska tässä työssä keskitytään lähinnä käyttöjärjestelmävirtualisointiin, jätetään muut kuin käyttöjärjestelmävirtualisointi vähemmälle huomioille.

2.2.2 Virtualisoinnin toteutustavat

Virtualisointia varten tarvitaan niin kutsuttu hypervisor tai virtual machine monitor (VMM) eli ohjelma, jolla ajetaan virtualisoituja tietokoneita. Hypervisor voi olla toteutettuna hyvin monella tavalla, ja jokaisella toteutustavalla on tietysti omat huonot ja hyvät puolensa. (Novak & Simpson 2010, 406.)

Paravirtualization on yksi tapa toteuttaa hypervisor. Siinä VM muokataan toimimaan yhdessä hypervisorin kanssa. Normaalien järjestelmäpyyntöjen sijaan VM suorittaa hyperkutsuja hypervisorille, joka välittää pyyntöjä eteenpäin. Vieraana olevan käyttöjärjestelmän täytyy tukea ominaisuutta tai olla yhteensopiva ajureiden kanssa, jolla tätä ominaisuutta toteutetaan. (Novak & Simpson 2010, 407.)

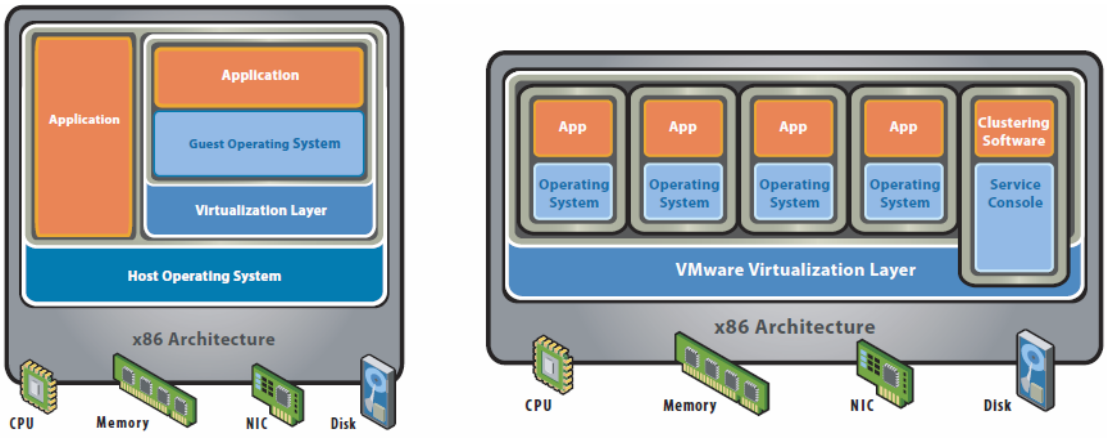
Binary translation tarkoittaa tapaa suorittaa virtualisointi lisäämällä järjestelmäpyyntöihin ylimääräisiä määritelmiä. Tämän menetelmän voisi mieltää reaaliaikaiseksi koodin kääntäjäksi, joka ottaa suorituksen alla olevaa koodia ja muokkaa sitä niin, ettei se sotke isäntänä toimivan järjestelmän toimintaa. Lisämääreiden luoma overhead vaikuttaa myös tietokoneen muistin käyttöön, minkä vuoksi määreitä täytyy vielä erikseen tarkentaa, jotta muistiviittaukset toimisivat. Kyseinen prosessi on vielä jokseenkin yksinkertainen, kun virtuaalista x86-järjestelmää ajetaan x86-järjestelmässä, mutta menettely muuttuu huomattavasti monimutkaisemmaksi prosessoriarkkitehtuurin vaihtuessa emuloitavan järjestelmän osalta. Vaikka binary translation aiheuttaa prosessoinnille lisää työtä, se on huomattavasti tehokkaampaa kuin klassisen trap-and-emulate-tekniikan käyttö x86-arkkitehtuurin kanssa. Siinä missä klassinen virtualisointi aiheuttaisi useiden tuhansien ohjeiden overheadin, päästään binary translation -tekniikalla muutamien satojen ohjeiden overheadiin. (Novak & Simpson 2010, 407.)

Virtualisoinnin suunta näyttää olevan nykyisellään yhä enemmän siirtymässä laitteistovirtualisointiin. Nykytekniikoilla laitteistovirtualisointi hyödyntää edellä mainittuja tekniikoita mahdollisimman optimaalisen suorituskyvyn takaamiseksi. Menetelmästä käytetään myös nimikettä bare metal hypervisor. Pääasiassa tämä tekniikka luottaa prosessorin ominaisuuk-

siin osata hoitaa virtualisointi jo komponenttitasolla, jotta ohjelmallinen overhead saataisiin mahdollisimman pieneksi. Tekniikka muuttaa kuviossa 1 mainittua rengasajattelua lisäten kehää nolla suuremmalla prioriteetilla olevan kehän -1. Tässä kehämallissa hypervisor toimii uudella kehällä, jolloin virtualisoitava järjestelmä saadaan toimimaan kehälle nolla. Prosessorivalmistajat AMD ja Intel ovat kumpikin julkaisseet omat versionsa tästä tekniikasta, ja ne on nimetty hyvin valmistajapohjaisesti AMD Virtualization (AMD-V) ja Intel Virtualization Technology (Intel VT). (Novak & Simpson 2010, 409.)

2.2.3 Tyypin yksi ja kaksi virtualisointi

Virtualisointi voidaan jakaa kahteen eri tyyppiin toteutustapansa perusteella, eli tyypin yksi tai tyypin kaksi hypervisor-arkkitehtuuriin. Tyypin yksi toteutustapa tarkoittaa, että virtualisointia varten asennetaan sovellus suoraan tietokoneraudan päälle. Tämä toteutustapa ei siis vaadi erillistä käyttöjärjestelmää virtualisointia varten, vaan ainoastaan virtualisointialustan asennettuna laitteistolle. Esimerkkinä tällaisesta toteutustavasta on muun muassa Microsoftin Hyper-V ja VMwaren vSphere ESXi. Tyyppiin yksi viitataan usein myös niin sanottuna paljaan raudan ratkaisuna (bare metal hypervisor). Tyypin kaksi arkkitehtuuri eroaa toteutustavaltaan yllä mainitusta niin, että laitteistolle asennetaan erillinen käyttöjärjestelmä, jolla suoritetaan virtualisointia tarjoava ohjelma. Tavallisen käyttäjän näkökulmasta tämä toteutustapa voi olla tullut tutuksi esimerkiksi Virtualbox- tai VMware Workstation-ohjelmilla tehdyillä käyttöjärjestelmäkokeiluina. Kuviossa 2 on esitys näiden toteutustapojen eroista. (Virtualization Overview 2006, 4; Lowe 2011, 4.)



Kuvio 2. Tyypin 1 (oik.) ja 2 (vas.) virtualisointi (Virtualization Overview 2006, 3.)

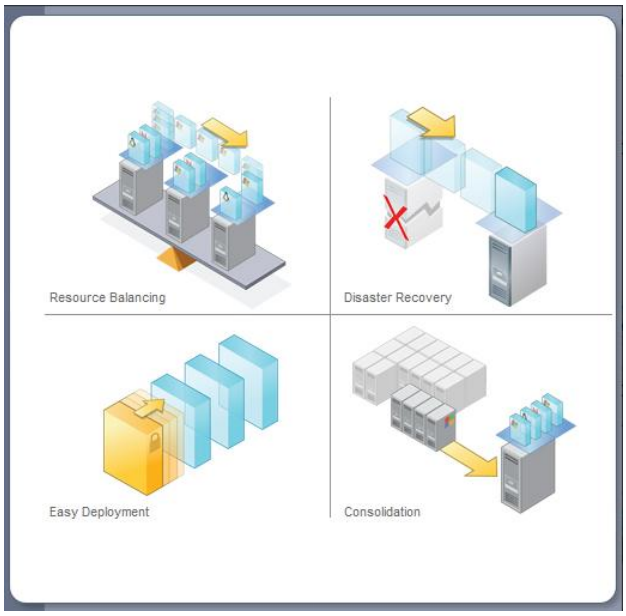
Konkreettisina erona näillä kahdella toteutustavalla on resurssien käyttö. Hosted-ratkaisussa eli tyypin kaksi virtualisoinnissa joudutaan varaamaan resursseja tietokoneen oman käyttöjärjestelmän sekä virtualisointiohjelman suorittamiseen. Tyypin yksi ratkaisussa taas saadaan

varattua enemmän resursseja itse virtuaalikoneille käyttöjärjestelmän puuttuessa. Hosted-ratkaisu tarjoaa kuitenkin laajemman laitteistotuen kuin paljaan raudan ratkaisu. (Virtualization Overview 2006, 4.)

2.2.4 Miksi virtualisoida?

Luvussa 2.2 puhutaan paljon virtualisoinnin teknisestä monimutkaisuudesta, joten miksi siis virtualisoida, jos se kerran on jo teknisesti haastavaa. Vastaukset löytyvät suoraan kustannustehokkuudesta. Erityisesti palvelinpuolella tietyt palvelut vaativat käytettävyytensä vuoksi koko palvelimen resurssit. Tällä ideologialla fyysisten palvelimien määrä kasvaa suoraan verrattuna haluttujen palveluiden määrään. Mitä enemmän käyttäjiä, sitä enemmän palveluja tarjoavia koneita eli fyysisiä laitteita. Tällainen yhtälö aiheuttaa vielä lisää kustannuksia tilan suhteen. Lisäksi kasvava koneiden määrä tarkoittaa suurempaa sähkönkulutusta ja jäähdytyksen tarvetta. Virtualisoimalla usea palvelu/palvelin samalle tehokkaalle palvelintietokoneelle saadaan aikaan selviä säästöjä niin tilan kuin jäähdytyksenkin tarpeisiin. Tämän perusteella voidaankin sanoa virtualisoinnin edistävän virheää informaatioteknologiaa. Lisäksi virtualisointi auttaa jakamaan fyysisen raudan tuomat resurssit optimaalisesti palvelimien kesken ja mukautumaan helpommin vaihtuviin tarpeisiin. Lopullisena tulemana selvitään vähemmällä määrällä palvelimia, jotka toimivat tehokkaammin. (Baroudi 2009, 60-61.)

VMware vSphere -ohjelmiston oma sisäinen manuaali kiteyttää hyvin virtualisoinnin hyödyt yhteen kuvaan, josta kuvankaappaus kuviossa 3. Hyvällä ohjelmistolla ja keskitetyllä hallinnalla saadaan yksittäisistä palvelintietokoneista helposti hallittava kokonaisuus, jossa kaikkien palvelimien resurssit voidaan helposti jakaa virtuaalikoneiden kesken. Virtualisointi myös mahdollistaa vikatilanteissa jatkuvuutta palveluihin erinäisin vikasietoisuus- ja palautustoimenpitein. Tekniikka mahdollistaa lisäksi helpon tavan ottaa käyttöön nopeasti uusia koneita virtuaalikoneista tehtävien pohjien ja kloonaamisen avulla. Tekniikan mahdollisuus usean palvelun pyörittämiseen samalla raudalla, kuitenkin erillisinä koneina, auttaa säästämään kaiken kattavasti resursseja, niin komponenttien, tilan kuin sähkönkin määrässä. (Benefits of server virtualization 2013.)



Kuvio 3. Virtualisoinnin hyödyt (Benefits of server virtualization 2013.)

3 VMware-tuotteita ja ominaisuuksia

3.1 Snapshots

Monien ohjelmistojen tavoin VMware tarjoaa mahdollisuuden ottaa palautuspisteitä. VMwaren tapauksessa Snapshot-toiminnolla tarkoitetaan mahdollisuutta ottaa kopio virtuaalikoneen kovalevystä tietyllä hetkellä ja käyttää tarvittaessa tätä kopiota palauttamaan virtuaalikone esimerkiksi virhetilanteesta. Snapshoteja voidaan tarvittaessa ottaa useista virtuaalikoneen vaiheista. Kun käyttäjä haluaa luoda palautuspisteen Snapshot-toiminnolla, kirjoitetaan koneen tila erilliseen tiedostoon, ja tiedostosta tulee vain luettavassa moodissa oleva tiedosto. Mikäli käyttäjä haluaa palauttaa koneen tilan takaisin Snapshotin ottohetkeen, ohjelmisto poistaa koneen nykyisen suorituksen luomat tiedostot ja ottaa käyttöön Snapshotin luomisen yhteydessä kopioidun tiedoston. Snapshot-toiminnon ei mainosteta olevan pelkästään käytettynä keino varmuuskopioiden ottamiselle. (Rouse 2012.)

3.2 VMware Worksation

Tuotteena VMware Workstation on monesti palkittu työasemavirtualisointisovellus. Tunnustusta se on 20-vuotiaan historiansa aikana saanut muun muassa laajasta käyttöjärjestelmätuesta, kattavista ominaisuuksistaan ja hyvästä suorituskyvystä. Käytännössä Workstation on ohjelmistotuote, joka mahdollistaa erinäisten käyttöjärjestelmien asentamisen virtuaalikoneina testaus- ja tuotantokäyttöä varten. Ohjelmisto tarjoaa suljetun ympäristön, jossa luoduista virtuaalikoneista voi halutessaan ottaa täysin itsenäisiä klooneja ja palautuspisteitä

(snapshot). Nämä ominaisuudet tukevat tuotantokäyttöön tehtyjen koneiden osalta nopeaa palautumista ja helppoa tapaa kokeilla uusia ohjelmistorevisioita ennen tuotantokäyttöön siirtämistä. Ohjelmisto mahdollistaa myös vanhojen tietokonekomponenttien hyödyntämistä alustana useille virtuaalikoneille tuottamaan palveluita ympäristön tarpeisiin. Ohjelmisto tarjoaa myös kohtalaisen laajat virtuaaliset verkko-ominaisuudet virtuaalikoneiden yhteenliittämiseksi Workstationin sisällä ja niiden liittämiseen ulkomaailmaan tietokoneen fyysisen verkkokortin kautta. Virtualisoitujen koneiden hallinnointi ja käyttäminen on mahdollistettu joko ohjelman itsensä kautta tai etäkäytön avulla. (VMware Workstation 2013; Happe, Humphrey, Muller & Wilson 2005, 2.)

3.3 VMware ESXi

VMware ESXi huolehtii varsinaisen työn suorittamisesta VMware vSphere -ohjelmiston palvelinvirtualisoinnin osalla. Ohjelmisto toimii hypervisorina suoraan tietokoneraudan päällä tarjoten alustan virtualisoinnille. Vielä edellisessä versiossa (4.0) hypervisorin hallintaan käytettiin Linux-käyttöjärjestelmästä johdettua palvelukomentopäätettä, joka tarvitsi toimiakseen muun muassa SNMP-protokollan käytön ja web-palvelimen. Nykyisessä 5.0-versiossa nämä toiminnallisuudet on sisällytetty suoraan VMkernelille. Tällä toimenpiteellä hypervisorista on saatu entistä kevyempi, mutta myös monipuolisempi kuin aiemmin. (Lowe 2011, 3-4.)

Hypervisorillakin on rajansa, nimittäin laitteistoon kohdistuvan tuen määrän osalla. Nämä rajoitteet kohdistuvat nimenomaan laitteiston määrään, jota voidaan osoittaa ESXi-palvelimella pyöriville virtuaalikoneille. Versio 5.0 sallii määrittää maksimissaan yhdelle virtuaalikoneelle 2048 virtuaalista CPU-yksikköä, 160 prosessoriydintä, 25 virtuaalista CPU-yksikköä per prosessoriydin ja 2 teratavua RAM-muistia. Versiossa 3.5 pystyi esimerkiksi määrittämään maksimissaan 32 prosessoriydintä yhdelle virtuaalikoneella ja maksimaalinen muistin määrä yhdelle koneelle oli 128 gigatavua. (Lowe 2011, 5.)

3.4 VMware vCenter

Jotta ESXi-palvelinkokonaisuutta on helpompi hallita, tarjoaa VMware omaan tuoteperheeseensä keskitettyä hallintaa tarjoavan palvelimen eli vCenter-ohjelmiston. Tämä ohjelmisto tarjotaan joko Windows-palvelinkäyttöjärjestelmille asennettavana pakettina tai vapaan lähdekoodin Linux-pohjaisena virtuaalikonepakettina, joka on optimoitu pyörittämään vCenter-sovelluksia ja siihen liittyviä palveluja. Näistä kahdesta vaihtoehdosta Windows-pohjainen asennus on ominaisuuksiltaan laajempi (esimerkiksi tuki IPv6-protokollalle), mutta

kyseinen vaihtoehto vaatii Windows-pohjaisen palvelinalustan. (Configuring the VMware vCenter server appliance 2013; Lowe 2011, 5.)

Ohjelman ideologiana on tarjota ESXi-palvelimille keskitetty hallinta yhden yhteyden kautta. ESXi-palvelimien hallinta tapahtuu normaalioloissakin joko selainpohjaisen hallintatyökalun avulla tai siihen erikseen räätälöidyn vSphere Client –sovelluksen avulla. Mikäli ympäristöstä puuttuu vCenter-hallintapalvelin, jouduttaisiin jokaiselle käyttäjälle luomaan omat tunnukset jokaista ESXi-palvelinta kohti. Tämä onnistuu vielä muutaman palvelimen tapauksissa, mutta määrien kasvaessa tarvittavien hallintaikkunoiden määrä nousee radikaalisti. vCenter-palvelin tuo avun tämän kaltaisiin tapauksiin, sillä tämä palvelin asetetaan hallitsemaan haluttuja ESXi-palvelimia ja hallintaa varten tarvitaan vain yksi hallintayhteys vCenter-palvelimelle. (Lowe 2011, 5.)

Keskitetyn hallinnan lisäksi vCenter-palvelin tarjoaa käyttäjälleen mahdollisuuden päästä käsiksi tuoteperheen ominaisuuksiin klusterin hallitsemisessa. vCenter-palvelimen käyttöönotto mahdollistaa klusterin rakentamisen siihen liitetyistä ESXi-palvelimista ja tuo mahdollisuuden hyödyntää koko klusterin resursseja virtuaalikoneiden ajamiseen. Tällainen ratkaisu mahdollistaa esimerkiksi seuraavat ominaisuudet:

- **Enhanced vMotion Compatibility** - mahdollistaa laajemman laitetuen käyttämisen Intelin ja AMD valmisteisten prosessoriarkkitehtuurien välillä käytettäessä resurssien jakamisasetuksia.
- **Storage I/O -hallinta** - mahdollisuus vaikuttaa klusterin varastolevyjärjestelmien käytettävyyteen ja priorisoida kriittisten palvelujen pääsyä levyjärjestelmiin toiminnallisuuksien varmentamiseksi.
- **vSphere Distributed Switches** - virtuaalikytkimet, jotka mahdollistavat koko klusterin kattavien tietoverkkopalveluiden hallitsemisen yhdellä komponentilla.
- **Distributed Resource Scheduler** - Lukuisat ominaisuudet keskitettyyn resurssien hallintaan ja niiden jakamiseen koko klusterin koneiden käyttöön.

(Lowe 2011, 8.)

3.5 VMware vSphere Client

VMware vCenter- tai ESXi-palvelimen ominaisuuksien hallinta ei onnistu suoraan kyseiseltä koneelta, vaan tätä käyttöä varten on oma hallintasovelluksensa. Ohjelmalla on mahdollista muodostaa hallintayhteys palvelimen kanssa ja hoitaa konfiguraatiot ynnä muut määritykset tämän ohjelman kautta. Ohjelma tarjoaa kohtalaisen selkeän graafisen käyttöliittymän palve-

limien hallinnointiin ja onkin palvelimien asentamisen jälkeen pääkäyttäjien ykköstyökalu VMware-palvelinvirtualisointiympäristön hallinnoimiseen. Palvelimia on myös mahdollista hallinnoida ottamalla internetselaimella yhteys halutun palvelimen osoitteeseen, jolloin aukeaa web-käyttöliittymä palvelimen toimintoihin. Tämä web-käyttöliittymä on paljon niukempi ja ominaisuuksiltaan suppeampi, joten yleisesti suositellaan käytettäväksi varsinaista vSphere Client -ohjelmaa. (Lowe 2011,7.)

3.6 VMware vMotion

Ominaisuutena vMotion-tarjoaa ESXi-virtualisointiin mahdollisuuden siirtää käynnissä olevia virtuaalikoneita fyysiseltä alustalta toiselle ilman käyttökatkosta. Tarkoituksena on siis mahdollistaa esimerkiksi huollon sattuessa palvelujen jatkuvuus mahdollisuutena siirtää fyysisen ESXi-palvelimen hallinnoimat virtuaalikoneet toiselle ESXi-palvelimelle ilman, että virtuaalikonetta tarvitsee sulkea. Kyseisen siirron aikana siirrettävän koneen palvelut ovat käytettävissä myös tietoverkon yli, eli katkosta ei tule verkko-ominaisuuksienkaan osalta. Huoltotoimien lisäksi ominaisuutta mainostetaan myös helpoksi ratkaisuksi tasata ESXi-palvelimien kuormaa, jota virtuaalikoneet aiheuttavat. Mikäli yksi palvelin alkaa viedä entistä enemmän resursseja tai vaatii käytettävyytensä vuoksi enemmän resursseja, voidaan ESXi-palvelimen taakkaa helpottaa siirtämällä virtuaalikone tehokkaammalle alustalle. (Lowe 2011, 9-10.)

Siirron aikana siirretään siis virtuaalikoneen suoritus ja allokoidaan prosessorin ja muistin olemus fyysiseltä ESXi-palvelimelta toiselle, mutta varsinaiseen kovalevyllä olevan datan siirtämiseen ei oteta kantaa. Koska vMotion vaatii ominaisuutena jaetun verkkolevyjärjestelmän käyttöönsä, tulee käyttöönoton yhteydessä varmistua riittävin levyresurssein koko klusterin tarpeisiin niin, että jokaisen virtuaalikoneen kovalevyt ja muu datavarastointi saadaan mahtumaan näihin verkossa oleviin levyjärjestelmiin. (Lowe 2011, 9.)

Sen lisäksi, että vMotion siirtää virtuaalikoneiden suoritusta alustalta toiselle, on siitä olemassa myös versio, jolla voidaan siirtää suoritettavan virtuaalikoneen virtuaalilevyt toiselle verkkolevylle virtuaalikoneen yhä ollessa käynnissä. Storage vMotion sallii mainitun kaltaiset virtuaalilevyjen siirtämiset levyjärjestelmältä toiselle. Näin ollen pystytään myös huolehtimaan palvelujen käynnissä olemisesta, vaikka verkkolevyjärjestelmiin jouduttaisiin tekemään muutoksia tai levyt alkaisivat olla kapasiteettinsa osalta täynnä. (Lowe 2011, 9.)

3.7 VMware vSphere DRS & Storage DRS

Lyhyesti Distributed Resource Scheduler tarjoaa mahdollisuuden automatisoida vMotion-ominaisuuksien hyödyntämisen. Virtuaalikoneen käynnistyksen yhteydessä vSphere DRS etsii

klusterista vähimmällä rasituksella olevan ESXi-palvelimen haluttujen sääntöjen perusteella ja määrää kyseisen palvelimen vastaamaan virtuaalikoneen suorittamisesta. Ominaisuus tarkkailee käynnissä olevia virtuaalikoneita ja tilanteissa, joissa resurssit uhkaavat loppua, suojaa kriittisimpiä palveluita siirtämällä ne vMotion-siirtoina toisille ESXi-palvelimille. Automatisoinnin määrästä riippuen ominaisuus voi myös tehdä pelkkiä ehdotelmia siirroista ja jättää pääkäyttäjä hyväksymään siirrot. vSphere DRS valvoo siis pääasiassa muistin ja prosessorien käyttöä ja tekee päätöksensä näiden resurssien perusteella. (Lowe 2011, 10-11.)

vSphere Storage DRS huolehtii taas levyjärjestelmien rasituksesta ja pyrkii huolehtimaan riittävästä tallennustilasta virtuaalikoneiden tarpeisiin. Virtuaalikoneen luomisen yhteydessä luodaan virtuaalikiintolevy, jolle VM-koneen tallennus tapahtuu. Storage DRS pyrkii huolehtimaan, että levyn sijoitus tapahtuisi riittävät resurssit omaavalle verkkolevylle. Käynnissä olevien virtuaalikoneiden osalta ominaisuus voi antaa ehdotelmia tiettyjen levyjen siirtämisestä klusterin verkkolevyjen kesken, jotta rasitusta saataisiin jaettua tasaisesti eri tallennusmedioiden välille tai suorittaa näitä siirtoja automaattisesti. (Lowe 2011, 11-12.)

3.8 VMware vSphere HA ja FT

Ennen virtualisointia yhden palvelimen fyysinen laiterikko vaikutti ainoastaan kyseisen palvelimen tuottamaan palveluun, nyt virtualisoinnin aikakautena yhden koneen fyysinen laiterikko voi lamauttaa hyvin suuren määrän palveluja. Epäkäytettävyyttä pyritään estämään korkean käytettävyyden (High Availability) ja vian sietokyvyn (Fault Tolerance) takaavilla ominaisuuksilla. High Availability ominaisuutena pyrkii havaitsemaan mahdollisimman nopeasti ESXi-palvelimen laiterikon aiheuttaman katkoksen palveluihin ja käynnistämään virtuaalikoneet toisella alustalla. Ominaisuus ei hyödynnä vMotion-siirtoa, sillä äkillinen katkos koneen toiminnassa aiheuttaa suoritusta kuvaavien tietojen menetyksen. Ominaisuutta käytettäessä laiterikko aiheuttaa fyysisen katkoksen virtuaalikoneiden toiminnassa, mutta automaatio pyrkii käynnistämään palvelut mahdollisimman nopeasti toimivalla alustalla. Huonosti suunniteltuna katkos voi venyä pitkäksi, sillä uudelleen käynnistettävät koneet joutuvat kilpailemaan resursseista uusilla alustoilla. (Lowe 2011, 13.)

Fault Tolerance pyrkii estämään äkillisistä laiterikoista koituvat katkokset ja estää epäkäytettävyyden syntymisen. Ominaisuudella suojatuista virtuaalikoneista pidetään koko ajan niin kutsuttua peilikuvaa toisella fyysisellä ESXi-alustalla. Käytännössä suojattava virtuaalikone toimii omalla alustallaan primaarin ominaisuudessa ja alati primaarin muutoksia seuraava sekundaarikone toisella alustalla. Mikäli primaarivirtuaalikoneen alusta kokee fyysisen laiterikon, eikä kykene jatkamaan toimintaansa, siirretään virtuaalikoneen suoritus sekundaarivir-

tuaalikoneen alustalle. Sekundaarista tulee uusi primaari ja sen suoritusta aletaan kopioida uudeksi sekundaariksi toiselle alustalle. Ominaisuus varaa paljon resursseja käyttöönsä ja sen käyttöä ei välttämättä kannata käyttää kuin kriittisimpien koneiden osalla. (Lowe 2011, 14-15.)

4 Virtuaaliverkot

4.1 Virtuaaliverkon ominaisuuksia

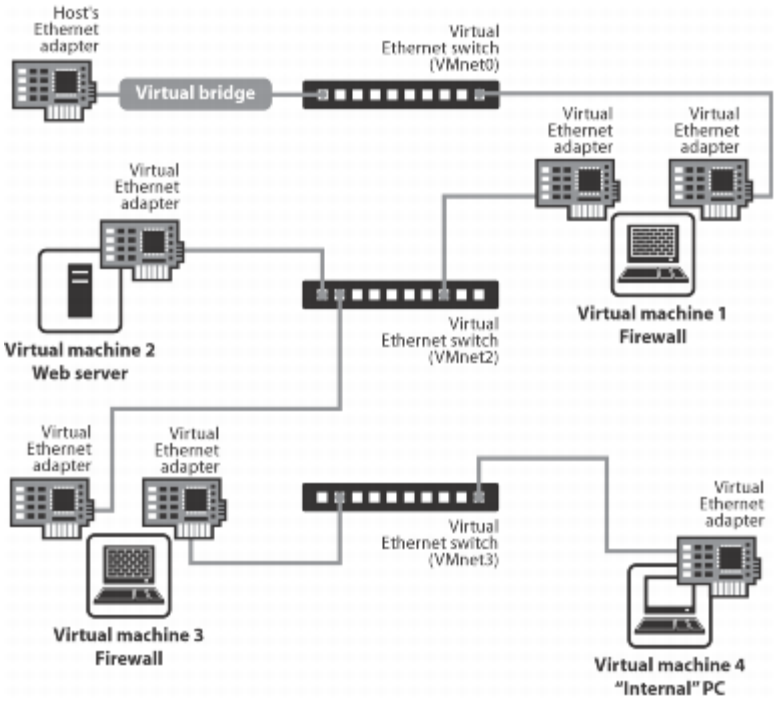
Virtuaaliverkoilla tarkoitetaan tässä työssä tietokoneessa ohjelmiston sisällä tapahtuvaa tietoverkkoja matkivaa liikennöintiä eri virtuaalikoneiden välillä. Fyysisellä tietokoneella on tietenkin oltava fyysinen verkkoliitäntä eli niin sanottu network interface card, jolla tietokone voi ottaa yhteyttä palveluihin ja muihin tietokoneisiin verkkojen yli. Virtualisoitu verkko toimii siis vain tietokoneella olevan ohjelmiston sisällä, mutta mahdollistaa myös rajapinnan luomisen fyysisen verkkokortin ja itsensä välille. Järjestelynä tällainen erillinen sisäinen verkko mahdollistaa helposti niin kutsutun hiekkalaatikko-ratkaisun eli suljetun testiympäristön luomisen, vaikka fyysinen tietokone olisikin kytkeytyneenä verkkoon.

Suunnittelussa onkin hyvä miettiä eri virtuaalikoneiden tarvetta olla yhteydessä fyysisen verkkokortin kanssa, sekä harkita eri mahdollisuudet virtuaalikoneiden sisäisten yhteyksien (host-only, internal) hyödyntämisestä. Näissä sisäisissä yhteyksissä fyysisen kortin ja virtuaalisen verkkoliitännän välille ei siis silloin synny yhteyttä. Sisäisissä verkkoliitännöissä on yleensä myös mahdollista tehdä useita sisäisiä liitäntöjä ja näin erottaa eri verkkoja toisistaan edelleen virtualisointiympäristön sisällä. Verkkoliikennöintiä varten virtuaaliverkkorajapinnat tarvitsevat MAC-osoitteen ja IP-osoitteen aivan kuten normaalikin verkkorajapinta. Erona tässä on kuitenkin, että virtualisointiohjelma generoi satunnaisen MAC-osoitteen virtuaalisille verkkoliitännöille. Osoitteessa käytetään kuitenkin valmistajan omaa etukäteen määriteltyä esiosaa aivan kuten fyysisissä laitteissa. Tarvittaessa niin MAC- kuin IP-osoitteenkin voi asettaa haluamakseen ohjelman kautta.

4.2 VMware Workstation Network Editor

VMware tarjoaa hyvin kattavat verkko-ominaisuudet ohjelmiinsa helpottamaan tuotanto- ja testiverkkojen luomista ja hallitsemista. Workstation tarjoaa pelkistetyt, mutta toimivat ratkaisut verkkojen luomiseen. Yksinkertaisimmillaan VM-koneelle voi valita yhden kolmesta valmisvaihtoehdosta verkkokortin liittämistyypiksi tai vaihtoehtoisesti luoda täysin omilla asetuksilla oleva verkkoliitäntä. Havainnollistus erilaisista verkkoliitännöistä on kuviossa 4. Kuviosta voi nähdä, miten eri verkot, sisäiset ja ulkoiset, ovat yhdistyneenä useisiin virtuaali-

siin kytkimiin (VMnetx). Näin voikin ajatella ja sanoa, että jokaisella sisäisellä ja ulkoisella yhteydellä on olemassa oma kytkimensä, johon kaikki tähän verkkoon kuuluvat liitännät ovat kytkettyinä. Tämä helpottaa jo itsessään virtuaaliverkkojen rakentamista ja ymmärtämistä. (Al-Dabbas 2012; Using the Virtual Network Editor in VMware Workstation (1018697) 2013.)



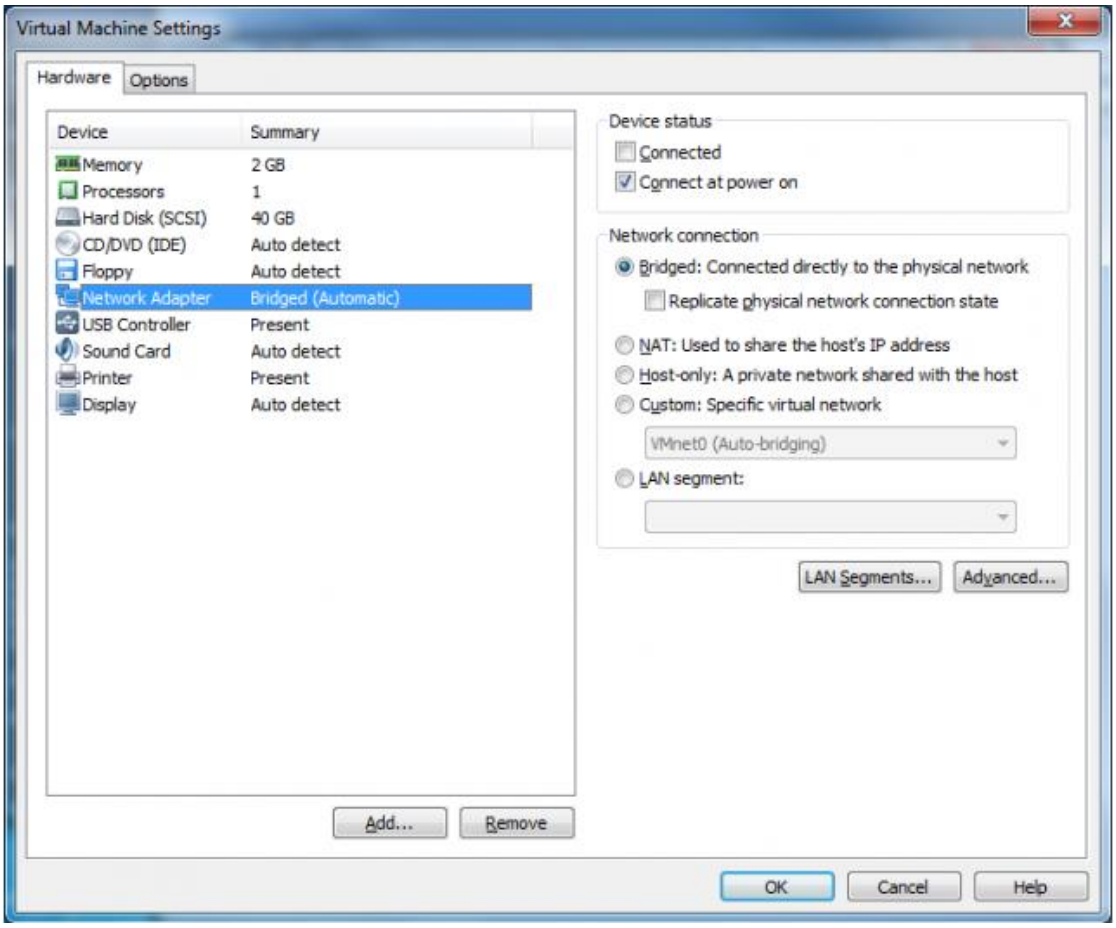
Kuvio 4. Esimerkki virtuaaliverkoista (VMware Workstation 5.5 Custom Networking Configurations 2006.)

Siltaava verkkoliitäntä (bridged) on yksi toteutustapa mahdollistaa VM-koneen kommunikointi ulkomaailman kanssa. Tällöin tietokoneen fyysinen verkkokortti välittää reitittimen tavoin liikenteen virtuaalikoneelle. Tässä tapauksessa virtuaalikoneen rajapinta saa myös itselleen IP-osoitteen ulkoverkosta, tai ilman DHCP-palvelua tarvitsee käsin asetetun osoitteen ulkoverkon osoitealueelta liikennöinnin onnistumiseksi. Näin VM myös näkyy fyysisessä tietoverkossa omana erillisenä koneenaan. Optiona tähän asetukseen voidaan asettaa toiminto, joka matkii fyysisen verkon kytkennän tilaa. Tämä saa aikaan osoitteen uudistumisen virtuaalirajapinnalle myös silloin, kun fyysinenkin verkko vaihtuu tai muuttuu. Kuviossa 4 VMnet0 edustaa siltaavaa verkkorajapintaa. (Al-Dabbas 2012; Using the Virtual Network Editor in VMware Workstation (1018697) 2013.)

NAT-verkkoliitäntä on toinen tapa toteuttaa virtuaalikoneen yhteydellisyys ulkoverkon kanssa. Tämä on myös yleisesti oletuksena oleva asetus uuden virtuaalikoneen luomisen yhteydessä, sillä se ei mahdollista suoraan kontaktin ottamista virtuaalikoneen kanssa fyysisen verkon yli. Tässä toteutustavassa isäntänä toimiva kone fyysisine verkkorajapintoineen toimii

edelleen reitittävänä laitteena ulkoverkon ja virtuaalikoneen välillä, mutta virtuaalikone käyttää fyysisen rajapinnan IP-osoitettta liikennöintiin. Näin ollen yhteydellisyys ulkomaailmaan on varmistettu, mutta virtuaalikone ei suoraan voi tarjota muiden verkossa olevien koneiden käyttöön palveluita sen ollessa piilossa fyysisen koneen takana. Tämä olisi ohitettavissa porttiohjauksella. Vaikka virtuaalikoneen IP-osoite näkyy ulkomaailmaan samana kuin fyysisen koneen osoite, saa virtuaalikone kuitenkin virtuaaliselta DHCP-palvelulta IP-osoitteensa. Kuviossa 4 VMnet0 voisi olla toteutettu NAT-verkkoliitäntänä, mutta tällöin virtuaalikoneella kaksi oleva verkkosivupalvelin olisi ulkomaailman saavuttamattomissa ja sitä olisi mahdollista käyttää vain sisäisen verkon puolelta. (Al-Dabbas 2012; Using the Virtual Network Editor in VMware Workstation (1018697) 2013.)

Host-only eli niin sanottu sisäinen verkkoliitäntä on kolmesta oletusliitäntätavasta viimeinen. Tässä toteutustavassa virtuaalista verkkokomponenttia ei luoda fyysisen verkkokortin ja virtuaalikoneen väliin, vaan virtuaalikoneiden välille. Oletuksena tähän verkkoon liitetyt virtuaalikoneet saavat ohjelman sisäiseltä virtuaaliselta DHCP-palvelimelta IP-osoitteen liikennöintiä varten. Mikään ei tietenkään estä osoitteen vaihtamista VM-koneella kiinteäksi, mutta liikennöinnin varmistamiseksi tulee kiinteän osoitteen olla sisäisen verkon osoitealueelta. Sisäinen verkko ei suoraan voi liikennöidä ulkomaailman kanssa, mutta kuten kuviossa 4 on toteutettu, voi samassa virtuaalikoneessa olla usea verkkokortti. Tällä järjestelyllä mahdollistetaan eri verkkojen kytkeytyminen toisiinsa ohjelman sisällä, mutta useaan verkkoon liitetyn virtuaalikoneen tulee osata reitittää liikennettä täyden toimivuuden varmistamiseksi. Kuviossa 4 sisäisenä verkkona toimii esimerkiksi VMnet2. Kuviossa 5 on kuvankaappaus verkkoliitäntöjen valitsemisen asetuksista VMware Workstation-ohjelmassa. Kuviossa on näkyvillä mainitut kolme oletusliitäntää, sekä valinta oman virtuaaliverkon valitsemiselle. (Al-Dabbas 2012; Using the Virtual Network Editor in VMware Workstation (1018697) 2013.)

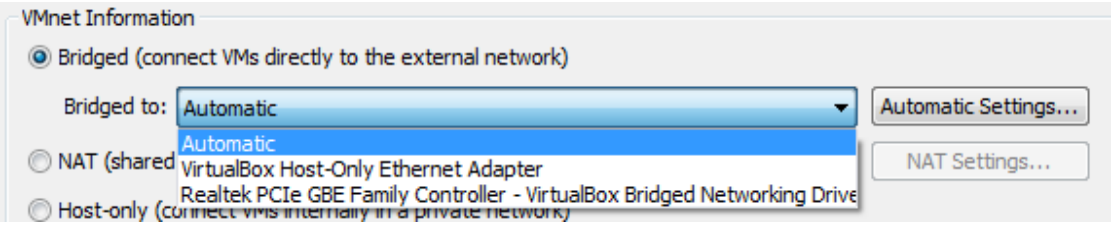


Kuvio 5. Verkkosovittimen asetusvalikko VMware Workstation -ohjelmassa

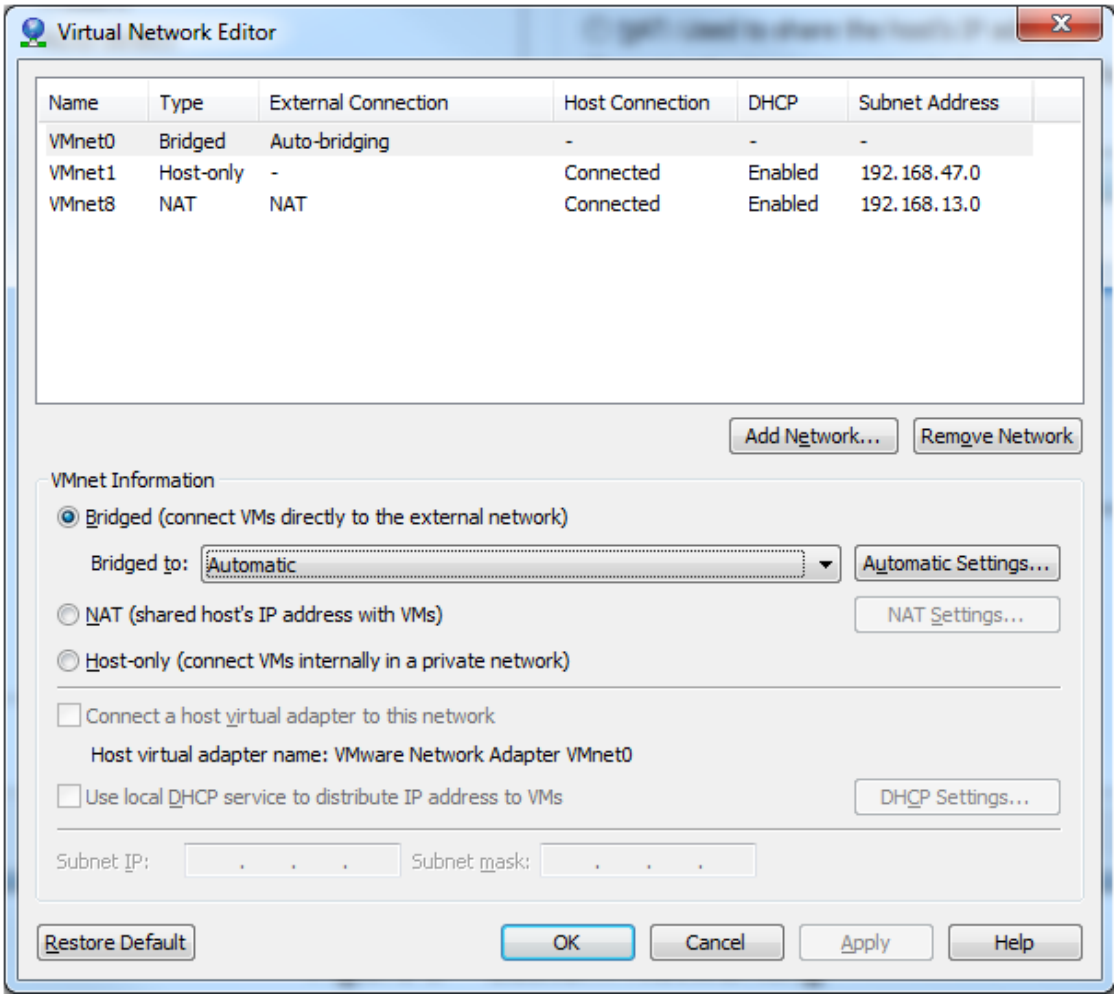
Neljäs vaihtoehto on oma verkkoasetus eli custom. Kuvion 4 tapauksessa tämä voisi tarkoittaa VMnet3 verkkoa, joka on tehty toimimaan samoin kuin oletustoiminnoillaan oleva sisäinen verkko, mutta eri osoitteistuksella. Yleisesti oma asetus antaa mahdollisuuden muokata jo olemassa olevia oletusverkkoliitäntöjä, jotka mainittiin aikaisemmin, mutta myös luomaan uusia. Workstation tarjoaa versiosta riippuen yleensä käyttöön VMnet0-9 -rajapinnat (versio 10 mahdollistaa jopa VMnet19 käytön), jotka voi muokata vastaamaan parhaiten omia tarpeita. Nämä kymmenen pitävät jo siis sisällään oletusrajapinnat. Liitäntätyypin omalle VMnet-rajapinnalle voi valita siltaavan -, NAT- ja sisäisen rajapinnan väliltä. (Al-Dabbas 2012; Using the Virtual Network Editor in VMware Workstation (1018697) 2013.)

Siltaavan verkkotyypin osalta voidaan määrittää erikseen, minkä verkkorajapinnan kanssa siltaaminen suoritetaan. Valinta voi kohdistua mihin tahansa toimivaan fyysiseen verkkokorttiin, ohjelman sisäiseen virtuaalirajapintaan tai jopa toisen ohjelmistovalmistajan virtualisointisovelluksen virtuaalirajapintaan kuten kuviossa 6 on osoitettu. NAT-asetuksen valittuaan on mahdollista määrittää erikseen DHCP-palvelun jakama osoitealue sekä määrittää tarvittavat porttiohjaukset palveluiden toiminnallisuuden mahdollistamiseksi. Sisäisen verkkoliitännän

osalla on mahdollista määrittää DCHP-palvelun olemassaolo ja sen jakama osoitealue. Kuvissa 7 on vielä näytetty asetusvalikko virtuaaliverkoille. Virtuaaliverkkoja varten fyysinen kone näyttää lisätyt virtuaaliverkkojen liitäntäkortit myös omissa asetuksissaan asetusten muokkaamista varten. (Al-Dabbas 2012; Using the Virtual Network Editor in VMware Workstation (1018697) 2013.)



Kuvio 6. Siltauksen kohteena voi olla verkkokortti tai esimerkiksi Virtualbox-ohjelman virtuaaliadapteri



Kuvio 7. Valikko VMnet-virtuaaliverkkojen luomiseen ja muokkaamiseen

4.3 VMware vSphere ESXi vSwitch

4.3.1 Komponentit

ESXi- ja vCenter-palvelimet mahdollistavat entistä laajemmat ominaisuudet virtuaaliverkkojen toteuttamiseen. Käytännön ajattelu suunnittelussa ei eroa juurikaan fyysisten tietoverkkojen osalta, mutta komponentit ja verkon laitteet ovat osaltaan myös palvelimen sisällä. vSwitch tuo mukanaan erinäisiä virtuaalikomponentteja verkkoa varten ja tässä on listattu tärkeimmät:

- **vSphere Standard Switch** - on ohjelmistopohjainen kytkin. Se tarjoaa yhteydellisyyden yhden ESXi-palvelimen sisällä olevien virtuaalikoneiden välille ja toimii virtuaalikoneen ytimen eli kernelin osana.
- **vSphere Distributed Switch** - on myös ohjelmistopohjainen kytkin. Tämä kytkin on kuitenkin jaettu kaikkien toisiinsa liitettyjen ESXi-palvelimien välille. Se tarjoaa yhteydellisyyden useiden ESXi-palvelimien sisällä olevien virtuaalikoneiden välille ja toimii virtuaalikoneen ytimen eli kernelin osana.
- **Portti/Porttiryhmä** - kytkimen osa, joka tarjoaa palveluitaan VMkernelille tai virtuaalikoneille. Virtuaalikytkimessä voi olla VMkernel portteja tai virtuaalikoneille omistettuja porttiryhmiä. Jaetussa kytkimessä myös portit ovat jaettuja.
- **VMkernel-portti** - tällä portilla on oma IP-osoitteensa ja sen kautta hoidetaan ESXi-palvelimen hallintaliikenne. VMkernel-portteja käytetään myös muun muassa vMotion-ominaisuuden sekä verkossa olevia verkkolevyjen (iSCSI, NAS, NFS) käyttöä varten.
- **VM-porttiryhmä** - virtuaalikoneille varattu porttiryhmä, joka mahdollistaa virtuaalikoneiden keskinäisen ja ulkoisen liikennöinnin. Jaetun kytkimen yhteydessä voidaan puhua dvport-ryhmistä (distributed virtual port group)
- **Trunk-portti** - portti, joka osaa kuunnella ja välittää 802.1q-protokollalla leimattua liikennettä. Ominaisuutta käytetään kytkinten välisessä viestinnässä, jotta protokollalla leimattu saadaan välitettyä verkon yli. Tämä ominaisuus on siis sisällytetty virtuaalikytkimiin, jotta 802.1q-protokollan ominaisuudet saadaan käyttöön.
- **Access-portti** - portti, joka on liittyneenä vain yhteen VLAN-verkkoon ja se osaa liittää tai purkaa leiman, jotta tietokone osaa lukea paketin sisällön.
- **Network Interface Card Team** - fyysisten verkkorajapintojen yhteen liittämistä tarkoittava termi, jolla usea NIC sidotaan yhteen yhdeksi loogiseksi tiedonvälityskanavaksi. Tällä saadaan luotua kuormanjakoa tai virheensietoisuutta.

- **vmxnet Adapter** - virtualisoidun verkon virtuaalikoneen verkkorajapinta. Adapterilla on suuri, 1Gbps, välityskyky, mutta toimii vain VMware Tools-lisäosan ollessa asennettuna. Tätä adapteria kutsutaan joskus paravirtualisoiduksi ajuriksi.
- **vlance Adapter** - oletusverkkorajapinta virtuaalikoneella, joka toimii vain 10/100Mbps. On käytössä, kunnes VMware Tools-lisäosa saadaan asennettua.
- **e1000 Adapter** - virtuaalinen verkkorajapinta, joka jäljittelee Intelin valmistaman verkkokortin ominaisuuksia. Toimii 1Gbps nopeudella ja on yleisemmin käytössä 64-bittisten järjestelmien kanssa.

Kuten listasta voidaan huomata, tukee vSwitch-kytkin muun muassa liikenteen erottelua VLAN-leimauksilla. Sen lisäksi virtuaalinen kytkin osaa myös monia asioita, joita varten fyysiset kytkimet vaatisivat erillisen protokollan. (Lowe 2011, 169-171.) Taulukossa 1 on vielä listattu maksimaaliset määrät ESXi-palvelimen verkkokomponenteille. Taulukon tiedot löytyivät Lowen kirjan sivulta 208.

Taulukko 1. ESXi-palvelimen maksimaaliset verkkokomponenttimäärät

Komponentti	Maksimimäärä
Virtuaalikytkimien määrä	248
Portit per virtuaalikytkin	4088
Porttien määrä per virtuaalikone (vSS/vDS)	4096
Porttiryhmien määrä per virtuaalikytkin	256
Uplinkit per virtuaalikytkin	32
VMkernel verkkokorttien määrä	16
Suurin määrä aktiivisia portteja per virtuaalikone (vSS/vDS)	1016

4.3.2 vSphere vSwitch-kytkimet

ESXi-palvelimilla voi siis hyödyntää kahta erilaista virtuaalista kytkintä eli valittavissa on joko Standard Switch tai Distributed Switch. Distributed Switch eli niin sanottu jaettu kytkin on näistä kahdesta monipuolisempi toiminnoiltaan, mutta vaatii myös enemmän työtä. Molemmat virtuaalikytkimet ovat verrattavissa oikeisiin fyysisiin kytkimiin, sillä nekin operoivat

OSI-mallin toisella kerroksella, tukevat 802.1q-protokollaa, pitävät yllä MAC-osoitetaulua ja osaavat ohjata kehykset näiden osoitteiden perusteella oikealle portille. Erojakin on sillä virtuaalikytkimet eivät osaa neuvotella DTP-protokollalla (Dynamic Trunking Protocol) tai hyödyntää porttien yhdistämiseen tehtyä PAgP-protokollaa (Port Aggregation Protocol). Lisäksi virtuaalista kytkintä ei voida kytkeä suoraan toiseen virtuaaliseen kytkimeen. Koska tämä on ohjelmallisesti tehty mahdottomaksi, ei STP-protokollan (Spanning Tree Protocol) kaltaista silmukan estämisjärjestelyä tarvita. Silmukoilla tarkoitetaan tietoverkoissa tapausta, jossa toisella OSI-mallin tasolla operoivat laitteet välittävät kehyksiä vanhojen ja väärien osoitetietojen perusteella. Tällöin kehykset kiertävät verkossa pääsemättä perille ja paketin jäädessä matkalle, alkaa verkko täyttyä uudelleenlähetetyistä kehyksistä. (Lowe 2011, 172-173.)

Virtuaalikytkin voi siis olla joko jaettu ESXi-alustojen kesken tai tavanomainen yhdellä ESXi-alustalla toimiva. Molempien osalta fyysisistä verkkorajapinnoista käytetään nimityksenä Uplink adapter. Yksi virtuaalikytkin voi olla kiinnitettynä yhteen tai useampaan fyysiseen verkkokorttiin tai olla ilman fyysistä verkkokorttia, jolloin voidaan puhua sisäisestä verkosta. Kytkimiä voidaan tarvittaessa luoda useita, mutta uudet luodut kytkimet eivät voi ottaa käyttöönsä toisiin virtuaalikytkimiin kiinnitettyjä uplink-rajapintoja silmukoinnin estämiseksi. Silmukointia on estämässä myös se, että liikenne, jonka virtuaalikytkin saa yhdestä uplink-rajapinnasta, ei koskaan välity toiselle saman kytkimen uplink-rajapinnalle. (Jorgenson 2012; Lowe 2011, 172, 176-178.)

Virtuaalikytkin myös mahdollistaa uplink-rajapintojen sitomisen yhteen eli niin sanotun NIC Teaming-ominaisuuden käytön. Ominaisuus mahdollistaa vikasietoisemman ympäristön luomisen lisäksi myös kuormanjaon usean uplink-rajapinnan välille. Virtuaalikytkin tietää lisäksi aina kaikkien siihen liittyneiden virtuaalikoneiden MAC-osoitteet. Se osaa myös suoriutua multicast-liikenneteestä ilman IGMP-protokollaan, koska virtuaalikytkin tietää oletuksena kaikkien koneidensa haluista olla mukana multicast-liikennöinnissä. Suurimpana erona jaetun ja tavallisen kytkimen välillä on lopulta se, kuinka monella ESXi-alustalla kytkin toimii samanaikaisesti. Jaetun kytkimen toimiessa usealla ESXi-alustalla, täytyy sen hallinnointi järjestää keskitetysti. Tästä syystä jaettu (Distributed vSwitch) kytkin on mahdollista luoda vain vCenter-palvelimen kautta, mistä myös kytkimen hallinnointi järjestyy. (Jorgenson 2012; Lowe 2011, 174)

4.3.3 Hallinnointi- ja VM-verkkot

ESXi-palvelimet hoitavat siis hallintaliikenteensä VMkernel-porttien avulla. VMkernel portit yhdistävät hypervisorin TCP/IP-kerroksella muuhun verkkoon ja vaikka liikenne kulkee samo-

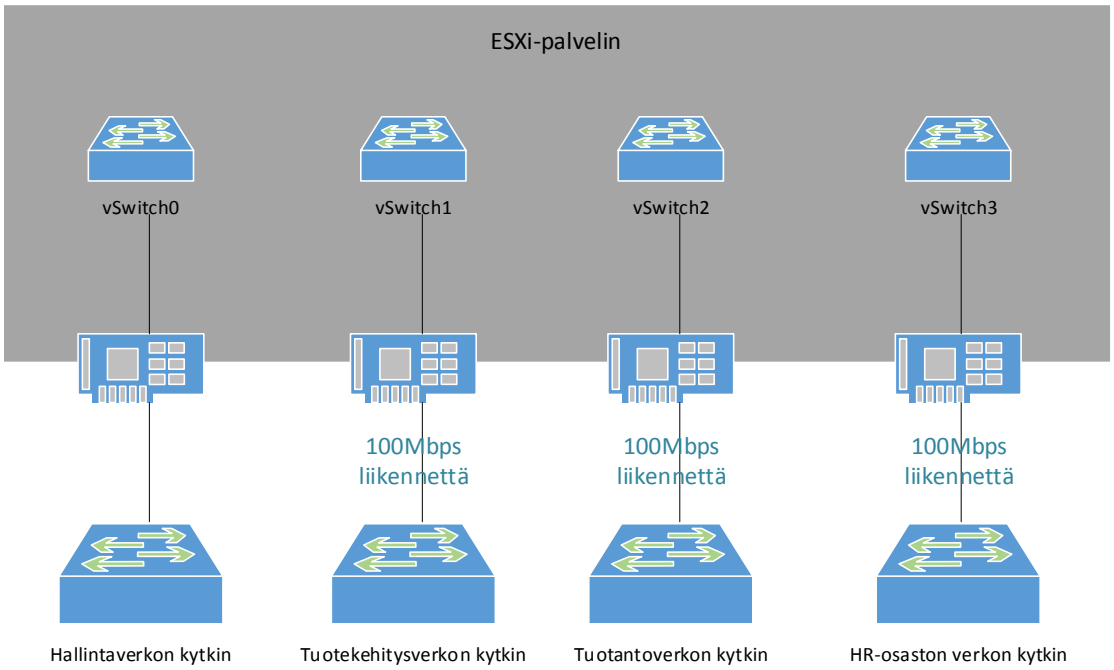
jen vSwitch-kytkimien läpi kuin virtuaalikoneiden liikenne, on hallintaliikenne erotettu tästä liikenteestä ja täysin itsenäistä. Hallintaverkko luodaan oletuksena palvelimen asennuksen yhteydessä ja vaaditaan pakollisena ominaisuutena, jotta palvelinta voidaan ylipäätään hallita. Mikäli toimivaa hallintaverkkoa ei konfiguroida heti asennuksessa, on hallintaverkko mahdollista vielä asettaa toimintaan käyttämällä Direct Console User Interfac-käyttöliittymää, eli ESXi-palvelimen minimaalista omaa käyttöliittymää, suoraan palvelimelta. DCUI on erittäin karsittu käyttöliittymä, eikä se tarjoa juurikaan mahdollisuutta tehdä palvelimen asetuksille muuta kuin määrittää hallintaosoite. Kun ympäristö on jaloillaan, voidaan vSphere Client-ohjelmistolla määrittää laajemmat verkkoasetukset. (Lowe 2011, 179.)

Siinä missä luodut VMkernel-portit vaativat IP-osoitteen toimiakseen, voidaan virtuaalikoneille luoda omia portteja ilman osoitteita. VM-porttiryhmät mahdollistavat virtuaalikoneiden liikennöimisen verkkoon ja ilman niitä virtuaalikone istuisi palvelimella täysin eristyksissä muusta maailmasta. VM-porttiryhmiä voidaan luoda useita samalle kytkimelle ja jokaisen porttiryhmän osalle voidaan määrittää erikseen siihen kuuluvat virtuaalikoneet. Eri ryhmien liikenteen erottamiseen voidaan käyttää IEEE 802.1Q standardisoitua VLAN-leimausta. Porttiryhmälle voidaan määrittää virtuaalikytkimen asetuksissa leiman numero, jota ryhmä käyttää kaikessa ryhmän virtuaalikoneiden luomassa liikenteessä. (Lowe 2011, 186-187.)

Mikäli leimausta halutaan käyttää palvelimelta ulospäin suuntautuvassa liikenteessä, täytyy tämä ottaa huomioon myös fyysisen verkon rakenteessa. Palvelinta seuraavan fyysisen kytkimen tulee osata käsitellä palvelimelta tulevaa porttia trunked-porttina, eli VLAN-leimoja välittävänä porttina, ja verkkotopologiasta riippuen välittää leimattu liikenne tai poistaa leima, jotta liikenteen sisältöä voitaisiin lukea. Vaikka VLAN-leimaus vaatiikin teknisesti enemmän työtä verkon osalta, voidaan sillä laskea fyysisten rajapintojen määrää. Mikäli leimausta ei oteta käyttöön, jouduttaisiin jokaista porttiryhmää varten sitomaan yksi fyysinen rajapinta, jotta liikenne saataisiin eroteltua. (Lowe 2011, 187-188.)

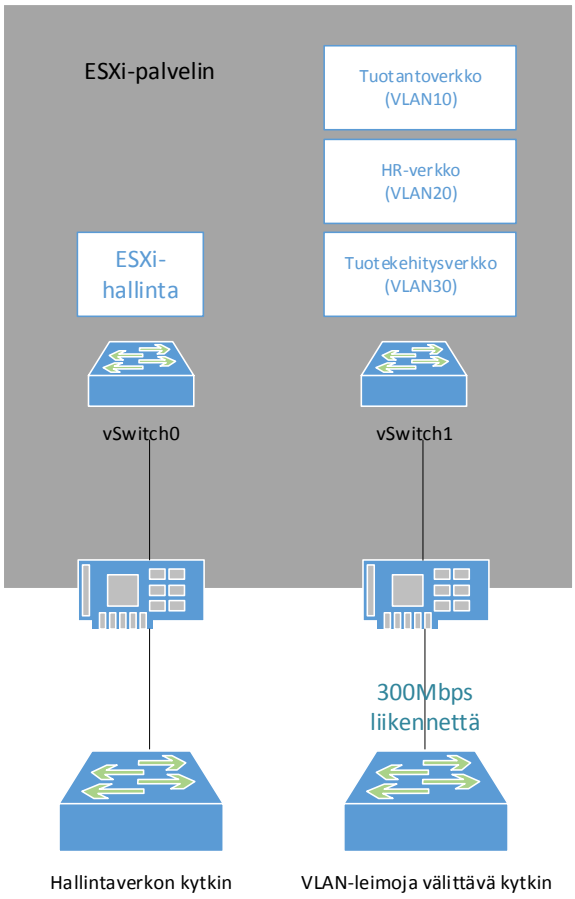
VLAN-leimoille voidaan normaalioloissa käyttää numeroita 1-4094, mutta ESXi-ympäristössä on mahdollista käyttää myös VLAN-leimaa numero 4095. Tämä ylimääräinen leimanumerointi mahdollistaa leimatietojen suoran välityksen virtuaalikytkimen takana oleville virtuaalikoneille. Ominaisuus on hyödyllinen vain tapauksissa, joissa virtuaalikone ymmärtää ja tukee VLAN-leimoja ja se on nimeltään Virtual Guest Tagging (VGT). Vaikka VLAN-leimaus mahdollistaakin leimoilla erotellun liikenteen siirtämisen yhtä fyysistä väylää pitkin, tulee suunnittelussa huomioida fyysisen kapasiteetin tuomat rajoitukset. (Lowe 2011, 187-188.)

Kuvioissa 8 ja 9 on pyritty selventämään VLAN-leimauksen etuja erotella liikenne tietoverkossa. Kuviossa 8 jokaiselle liikennetyypille on määritelty oma virtuaalikytkin. Tällä järjestelyllä hallintaverkosta ei päästä esimerkiksi tuotantoverkkoon, mutta erottelu vaatii kaiken kaikkiaan neljän fyysisen verkkokortin olemassaolon palvelimella.



Kuvio 8. Palvelimen verkkoratkaisu ilman VLAN-leimausta

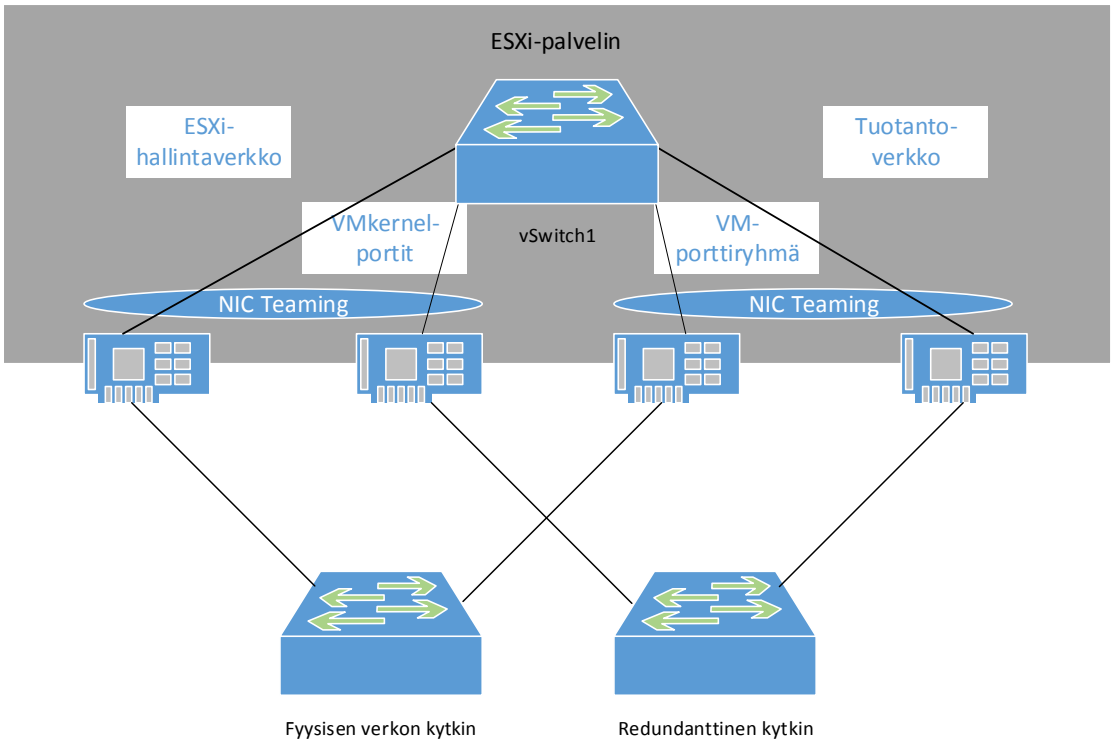
Kuviossa 9 on esitetty vastaava verkkojärjestely niin, että virtuaalikoneverkot on eroteltu VLAN-leimoilla, mutta käyttävät jokainen samaa fyysistä siirtoväylää. Kuvioista selviää myös se, että pienempi määrä fyysisiä rajapintoja ei ole kaikessa paras tapa hoitaa asioita. Liikenteen aiheuttama kuorma on eräs asia, joka täytyy ottaa huomioon suunnittelussa. Verkon suunnittelussa tulisi myös miettiä vaihtoehtoja kuormanjakoon useiden palvelimen rajapinnan välillä, mutta tästä lisää luvussa 4.3.4.



Kuvio 9. Palvelimen verkkoratkaisu VLAN-leimauksella

4.3.4 NIC Teaming ja kuormanjako

Fyysinen vika laitteistossa tai verkon siirtoväylissä voi pahimmassa tapauksessa lamauttaa kokonaisia palveluita. ESXi-palvelin tarjoaa vikasietoisuutta omiin verkko-ominaisuuksiinsa NIC Teaming-ominaisuudella. NIC Teaming -ominaisuudella yhdistetyt verkkorajapinnat hoitavat yhteistyössä liikenteen välittämisen. Ominaisuudella voidaan myös tarjota kuormanjakoa rajapintojen välille. Huomioitavaa on kuitenkin virtuaalikytkimen rajoitukset, eli ESXi-palvelin pystyy tukemaan maksimissaan 32 verkkorajapintaa ja että samaa fyysistä rajapintaa ei voida osoittaa usealla vSwitch-kytkimelle. Toimivan kokonaisuuden rakentaminen vaatii myös, että samaan NIC Teaming -ryhmään sidotut rajapinnat on yhdistetty samaan broadcast-alueeseen, eli OSI-mallin toisen kerroksen yhteydellisyys pitää olla alueen laitteiden kesken. Samaan broadcast-alueeseen kuuluminen on erityisen tärkeä tarkistaa, kun VLAN-leimaus on käytössä. Kuviossa 10 on esitetty tilanne, jossa palvelimen hallintaverkko sekä virtuaalikoneiden liikennöintiin varattu verkko on kahdennettu kahdella fyysisellä rajapinnalla ja kytkimellä. Yhden fyysisen linkin, verkkokortin tai kytkimen rikkoontuminen ei kuvion tapauksessa vaikuttaisi palvelujen toimintaan. (Lowe 2011, 192-193.)



Kuvio 10. Redundanttinen verkkoratkaisu

Jotta NIC Teaming -yhdistetyt rajapinnat saadaan todella vikasietoisiksi ja havaitsemaan viko-ja, täytyy ryhmä konfiguroida joko seuraamaan linkkien tilaa tai käyttämään beacon-probing -metodia. Linkin tilaan perustuva tunnistus toimii perustuen uplink-rajapinnan fyysiseen toimintaan. Käytännössä mikä tahansa vika, jolla fyysinen portti menettää yhteydellisyytensä, huomataan portin tilan muutoksena ja tällöin portti/linkki todetaan vialliseksi. Vian havaitseminen on hyvin yksiselitteistä, eli joko kaikki on kunnossa tai sitten jokin aiheuttaa yhteyden katkeamisen, mutta mikään ei anna viitteitä vian aiheuttajaan. Lisäksi vika tulee olla portin ja fyysisen kytkimen välillä, jotta se huomataan. Beacon-probing -tekniikalla verkkoon lähetetään Ethernet Broadcast-lähetyksenä kehyksiä, joilla pyritään havaitsemaan vika verkossa. Mikäli lähetetty beacon-viesti ei palaa takaisin sen lähettäneeseen rajapintaan, suljetaan rajapinta liikenteeltä. Tällä tekniikalla pystytään havaitsemaan yhteyden katkeamista pidemmältä verkosta, kuin pelkästään portin ja fyysisen kytkimen välillä. (Lowe 2011, 200.)

Vian havaitsemisen jälkeen, kun portti suljetaan liikenteeltä, tulee aika päättää minne liikenne ohjataan. vSwitch antaa pääkäyttäjän määrittää NIC teaming- ryhmän uplink-rajapinnoille tilaksi joko aktiivisen, valmiustilan tai käyttämättömän. Aktiiviset rajapinnat ovat käytettävissä missä tahansa tilanteessa ja riippuen käytetäänkö täsmällistä vikasietoisuusjärjestystä, valitaan seuraava listassa oleva rajapinta. Valmiustilassa olevat rajapinnat otetaan käyttöön mikäli vikatilanne ilmenee, ja täsmällisen vikasietoisuusjärjestyksen ollessa päällä otetaan

aktiivisten rajapintojen loppuessa ensimmäinen valmiustilassa oleva rajapinta liikenteelle. Asetukset tarjoavat vielä määrityksen, mitä tehdään vikaantuneelle rajapinnalle, joka korjaantuu. Oletuksena asetus on kyllä. Oletusasetuksellaan vikatilanteesta toipunut rajapinta palaa takaisin aktiiviseen palvelukseen ja palauttaa itsensä korvanneen, normaalisti valmiustilassa olevan rajapinnan tilalle. Asetuksen ollessa ei, siirtyy viasta palautunut rajapinta ikään kuin valmiustilarajapinnaksi ja korvaa toisen rajapinnan vain uuden vian sattuessa. Tätä asetusta suositellaan esimerkiksi VMkernel-porteille, jotka on osoitettu datavarastojen käyttöön. Mikäli vika ilmestyy ja poistuu jatkuvasti (flapping), eli lepattaa kuin lippu, voi jatkuva uplink-rajapintojen aktivointi/passivointi vaikuttaa negatiivisesti verkon suorituskykyyn. (Lowe 2011, 200-202.)

Asetuksissa voidaan myös määrittää halutaanko fyysistä kytkintä informoida muutoksista. Mikäli asetus aktivoidaan, tiedotetaan fyysistä kytkintä aina kun virtuaalikone rekisteröi itsensä virtuaalikytkimelle, vMotionia käytetään, mikäli jokin MAC-osoite muuttuu tai kun NIC Teaming -vikatilanne syntyy tai korjaantuu. Mikäli ilmoitussanoma lähetetään, hoidetaan se käyttäen RARP-protokollaa (Reverse Address Resolution Protocol). RARP-viesteillä saadaan fyysisen kytkimen osoitetaulu päivitettyä mahdollisimman nopeasti. (Lowe 2011, 203-204.)

Fyysisen verkon redundanttisuuden ja vikasietoisuuden lisäämisen lisäksi NIC Teaming mahdollistaa myös palvelimelta lähtevän liikenteen kuormanjaon. Palvelimelle saapuvan liikenteen tasaamiseen täytyy hyödyntää fyysisten verkkolaitteiden ominaisuuksia. ESXi-palvelimen suorittama kuormantasaus ei yritä tunnistaa liikennettä ja jakaa sen kokonaismäärää tasan ryhmitettyjen verkkokorttien lähetettäväksi. Kuormaa jaetaan kolmen eri metodin mukaan. (Lowe 2011, 195.)

Ensimmäinen näistä on virtuaalikytkimen portteihin pohjautuva tasaus (Virtual Switch Port-Based Balancing), joka myös on oletuksena käytössä. Tämä algoritmi jakaa virtuaalikoneiden portit tasan fyysisten uplink-rajapintojen kesken. Käytännössä neljän virtuaalikoneen käyttäessä kahta NIC Teaming -sidottua rajapintaa, kulkee kahden virtuaalikoneen liikenne ensimmäisen rajapinnan läpi ja kahden muun VM-koneen liikenne toisen rajapinnan läpi. Tämä jako suoritetaan riippumatta tuotetun liikenteen määrästä, joten yksi uplink-rajapinta voi rasittua huomattavasti muita enemmän , vaikka jako menisikin tasan. Porttien jako menee käytännössä uusiksi vain vikatilanteen yhteydessä, kun fyysinen uplink menettää yhteydellisyytensä. Tässä tapauksessa liikenne jaetaan uudelleen ehjien rajapintojen välille. Paluuliikenne löytää tiensä takaisin saman fyysisen kytkimen ja saman uplink-rajapinnan kautta fyysisen kytkimen osoitetaulujen perusteella. Algoritmia suositellaan käytettäväksi tilanteissa, joissa fyysisten käytettävissä olevien uplink-rajapintojen määrä on sama tai suurempi kuin

virtuaalikoneiden määrä, jolloin jako on maksimissaan kone per rajapinta. Tällöin jokainen ryhmän virtuaalikone saisi liikenteelleen oman verkkorajapinnan. (Lowe 2011, 196.)

Toinen valittava algoritmi on lähettäjän MAC-osoitteeseen perustuva tasaus (Source MAC-Based Load Balancing). Tekniikka toimii käytännössä samalla tavalla kuin portteihin perustuva tasaus, mutta erona on, että koneet jaetaan virtuaalikoneiden MAC-osoitteiden perusteella. Algoritmilla on myös samat heikkoudet kuin aiemmin mainitussa, mutta algoritmin toiminta myös estää, ettei sama virtuaalikone lähetä liikennettään monen eri fyysisen rajapinnan kautta ulos palvelimelta. (Lowe 2011, 197.)

Kolmas algoritmi on nimeltään IP-osoitteen sekoitteeseen perustuva kuormanjako (IP Hash-Based Load Balancing). Algoritmi nojaa siihen, että yhdestä koneesta voi muodostua eri reitti ulos palvelimelta riippuen liikenteen kohteesta. Algoritmi laskee yhteydelle hash-funktion käyttäen lähettäjän ja vastaanottajan IP-osoitetta. Laskettu hash-funktio määrää käytettävän uplink-rajapinnan, joten saman virtuaalikoneen vaihtaessa dataa usean ulkopuolella olevan koneen kanssa, voi tietokone lähettää ja vastaanottaa dataa useamman uplink-rajapinnan kautta riippuen keskustelukumppanistaan. Tekniikka tasoittaa muita helpommin yhden koneen aiheuttaman liikenteen usealle rajapinnalle ja ongelmia tulee lähinnä kun kahden koneen välillä siirretään paljon suurta dataa. Koska osoitetiedot eivät muutu siirron aikana, kohdistuu rasitus yhteen rajapintaan koko siirron ajan. Algoritmin luonteesta johtuen, tulee kaikkien NIC Teaming-ryhmitystä käyttävien rajapintojen olla suoraan yhteydessä samaan fyysiseen kytkimeen ja fyysisen kytkimen on kyettävä suorittamaan linkkien yhdistämistä osaavaa protokollaa. ESXi-alusta tukee kyllä normaalia manuaalista 802.3ad-protokollan mukaista linkkien yhdistämistä, mutta tukea ei ole LACP- (Link Aggregation Control Protocol) tai PAgP-protokollille (Port Aggregation Protocol). Näin monimutkainen rakenne varmistaa, että virtuaalikone voi lähettää ja vastaanottaa dataa usean fyysisen portin kautta samanaikaisesti. (Lowe 2011, 198-199.)

4.3.5 Distributed vSwitch ja sen käyttöönotto

VMware tarjoaa mahdollisuuden luoda tavallisten virtuaalikytkimien lisäksi usean palvelimen kattavan jaetun virtuaalikytkimen (vSphere Distributed Switch). Jaettu kytkin vähentää konfiguroinnin määrää ja helpottaa uusien jäsenten lisäämisen virtualisointiklusteriin. Jaettu kytkin omaa samat perustoiminnot kuin tavallinen virtuaalikytkin, eli se tarjoaa yhteydellisyyden VMkernelille ja virtuaalikoneille, se käyttää fyysisiä rajapintoja uplink-rajapintoina tarjoten yhteydellisyyden ulos palvelimelta ja siinä on mahdollistettu verkon segmentointi VLAN-leimauksella. Erojakin toki on. Esimerkiksi jaettua kytkintä ei voi luoda, ellei klusterin hallintaan ole asennettu vCenter-palvelinta. (Lowe 2011, 209, 210, 212.)

Jaetun kytkimen asennuksessa voidaan suoraan lisätä dvUplink-portteja, jotka ovat jatkossa virtuaalisia kytkimen portteja ulkomaailmaan. Tämän lisäksi asennus kysyy ESXi-palvelimet, jotka halutaan lisätä osaksi jaettua kytkintä ja mitkä fyysiset verkkokortit otetaan käyttöön jaetun kytkimen liikenteelle. Nämä kaikki asetukset voi muuttaa täysin jaetun kytkimen luomisen jälkeen. Mikäli kytkimen haluaa jossain vaiheessa poistaa klusterin komponenteista, täytyy ensin kaikki ESXi-palvelimet irrottaa kytkimestä. Lisäksi täytyy muistaa, ettei palvelinta voi irrottaa, mikäli sillä olevia virtuaalikoneita on liitettynä jaetun kytkimen porttiryhmiin. (Lowe 2011, 211-216.)

Jotta jaetun kytkimen saa todella käyttöön, täytyy kytkimelle luoda dvPort Group, eli jaettu virtuaalinen porttiryhmä. Porttiryhmälle voidaan yksinkertaisesti määrittää nimi, mahdollisten porttien määrä sekä laittaa VLAN-leimojen käsittelykyky päälle. Mikäli leimausta ei oteta käyttöön, ei kyseinen porttiryhmä kykene käsittelemään leimattua liikennettä, jos muu verkko sitä sille tarjoaa. VLAN-tyypin valinnasta voidaan valita siis jonkin seuraavista:

- **None** - porttiryhmä kykenee käsittelemään ainoastaan leimaamatonta liikennettä.
- **VLAN** - ryhmä suostuu vastaanottamaan uplink-rajapinnasta ilmoitetulla VLAN-leimanumerolla varustettua liikennettä. Fyysisen rajapinnan ja seuraavan verkkolaitteen tulee olla trunk-tilassa linkin osalta.
- **Trunking** - ryhmä välittää leimatietoja virtuaalikoneille asti. Asetuksiin täytyy määrittää sallitut VLAN-leimanumerot. Toiminta vaatii virtuaalikoneilta kykyä käsitellä leimattua liikennettä.
- **Private VLAN** - tällä asetuksella voidaan edelleen eristää portteja VLAN-leimauksen sisällä. Liikenne jaotellaan sisään ja ulos liikkuvaksi kukin omilla VLAN-tiedoillaan.

Luodun porttiryhmän tietoja voidaan tarkastella inventaarion kautta. Lista näyttää jokaisen virtuaaliportin omalla rivillään ja kertoo portissa kiinni olevasta virtuaalikoneesta, MAC-osoitteesta ja VLAN-tiedoista. Lisäksi tietoja voi selata käytössä olevista osoiteavaruuksista ja hälytyksistä. (Lowe 2011, 217-219, 231.)

Lyhyesti sanottuna jaettu virtuaalikytkin vähentää konfiguroinnin tarvetta järjestelmää pystyttäessä, vaikka onkin monimutkaisempi ymmärtää. Yllä mainittujen erikoisuuksien lisäksi jaettuun kytkimeen voidaan soveltaa myös tavallisen virtuaalikytkimen mukaisia NIC teaming -ominaisuuksia kuormantasaamiseen tai vikasietoisuuden nimissä. Ominaisuudet sallivat myös liikenteen määrän rajoittamisen rajapinnoissa, sekä liikenteen monitoroinnin NetFlow-ominaisuuden avulla. Jaettujen kytkinten toimintaa voi osaltaan laajentaa myös Cisco Sys-

tems -yrityksen kanssa yhteistyössä tehdyn Cisco Nexys 1000V -ohjelmistokytkimen avulla. (Lowe 2011, 228, 234.)

5 Levyjärjestelmät

Pitkin tätä opinnäytetyötä löytyy viittauksia jaetun levyjärjestelmän tärkeyteen klusterin moninaisten ominaisuuksien toiminnan kannalta. Jaettu levyjärjestelmä ei rajoitu vain virtuaalikoneiden virtuaalikiintolevyjen säilytykseen, vaan myös ESXi-palvelimet voidaan asentaa jaetulle levyjärjestelmälle ja jättää paikalliset kovalevyt näiden osalta kokonaan pois. Levyjärjestelmän tuomat mahdollisuudet avaavat joka tapauksessa muun muassa korkean käytettävyyden tuomat edut ja mahdollisuudet. Korkeasta käytettävyydestä on kirjoitettu lisää luvussa kuusi. (Lowe 2011, 252, 254, 257.)

Tässä opinnäytetyössä haluttiin keskittyä nimenomaan VMware vSphere -tuotteisiin ja koska levyjärjestelmälle ei ole omaa VMware-tuotetta, päätettiin ottaa kantaa ainoastaan käytännön osuuteen tulevaan tekniikkaan. Scott Lowe esittelee kyllä kirjassaan levyille kirjoittamisen varmennustekniikoista (RAID, Redundant Array of Independent Disks) kilpailevaan levyjärjestelmätekniikkaan nimeltä Fibre Channel. Fibre Channel vaatii osaltaan erityistä laitetekniikkaa ja työn pienuuden takia tietojen varmentamisesta levyille RAID-tekniikoilla ei koettu tarpeellisena. Näistä syistä priorisointi keskittyy teoriankin osalta vain iSCSI-levyjärjestelmään. (Lowe 2011, 260-274.)

5.1 iSCSI

iSCSI (Internet Small Computer System Interface) on IP-verkkoprotokollaan pohjautuva standardi datan siirtämisen varaston ja asiakkaan välillä verkon yli. Koska standardin kehitys on suunnattu toimivaksi juuri IP-protokollan kanssa, onkin iSCSI levinnyt kohtalaisen yleiseksi ratkaisuksi datan siirtoon niin lähiverkoissa kuin Internetin yli. Standardin mukaisesti loppukäyttäjän tai sovelluksen vaatiessa dataa, hoitaa käyttöjärjestelmä sopivanlaisen SCSI-pyynnön, joka tarvittaessa salataan. Pakettiin lisätään tämän jälkeen normaalin käytänteen mukainen IP-otsikko ja paketti lähetetään normaalisti Ethernet-verkkoon omalla kehyksellään. Paketti puretaan sen saavuttua perille ja paketissa ollut SCSI-pyyntö välitetään SCSI-ohjaimelle. Ohjain hakee tarvittaessa halutulta levyltä tarvittavan datan ja valmistelee sen takaisinlähetystä varten. Standardi sallii pyyntöjen lähettämisen myös toiseen suuntaan. (Rouse, M. 2011.) Kuviossa 11 on kuvattuna iSCSI-kehysrakenne.

Kuvio 11. iSCSI-tiedonsiirrossa käytetty kehysrakenne

Standardiin liittyy paljon terminologiaa ja tässä kappaleessa käydäänkin nopeasti läpi tärkeimmät. Asiakkaan nimityksenä käytetään iSCSI Initiator, jolla SCSI-toimintoja voi olla suorittamassa joko ohjelmistopohjainen- tai fyysinen-iSCSI Initiator. Ohjelmistopohjaisella tarkoitetaan esimerkiksi tietokoneen käyttöjärjestelmään asennettavan ohjelman kykyä hoitaa pyyntöjen välittäminen palvelimelle ja fyysisellä taas puhutaan erillisistä väyläkorteista, jotka voidaan lisätä koneeseen hoitamaan datan välitystä. Palvelimesta käytetään taas nimitystä iSCSI Target. Target-palvelimelle määritellään halutut fyysiset levyt jaettavaksi datan varastointiin ja näitä medioita kutsutaan loogisiksi yksiköiksi eli iSCSI LUN. Loogisia yksiköitä voidaan asettaa yksi tai useita per Target-palvelin. Network Portal on nimitys, jota käytetään iSCSI-laitteen kyvystä käyttää yhtä tai useaa IP-osoitetta liikennöintiin. Jotta jokainen Initiator, Target ja levyjako tunnistettaisiin toisistaan, asetetaan näille kullekin oma nimi, iSCSI Qualified Name. Lisäksi tietoturvaa standardille on tuomassa CHAP ja IPsec. CHAP (Challenge Authentication Protocol) on haaste-vastine -autentikointiprotokolla, jolla Initiator ja Target tunnistautuvat toisilleen. IPsec on tarvittaessa luomassa turvaa IP-verkoissa liikkuville paketeille ja salaamassa niiden sisältöä. (Lowe 2011, 275-276.)

iSCSI-standardi käyttää yksiköiden eli Target-palvelimien ja initiator-asiakkaiden nimeämiseen tietyn kaavan mukaista nimeämiskäytäntöä. Koska nimet ovat mahdollisesti globaalissa käytössä, on niihin siksi asetettu muuttujia muun muassa organisaatiokohtaiseen erotteluun. Yleisempi näistä kahdesta tavasta on niin kutsuttu IQN-formaatti (iSCSI Qualified Name). Formaatin nimen osat erotetaan toisistaan aina pisteillä, paitsi loppuosan uniikki osuus, joka erotetaan rungosta kaksoispisteellä. Formaatin mukainen nimi alkaa aina iqn-tekstiosalla. Seuraava osuus pitää sisällään nimeäjäauktoriteetin perustamisvuoden ja kuukauden. Aikatietojen jälkeen annetaan tieto nimeäjäauktoriteetista, joka on yleensä auktoriteetin verkko-osoite, kuitenkin käänteisessä järjestyksessä. Auktoriteetti päättää runko-osan, jonka jälkeen voidaan antaa yksittäistä objektia koskeva nimi. Auktoriteetin täytyy varmistua, että tämä kyseinen nimi on aina uniikki. VMware antaa verkkodokumentoinnissaan esimerkkejä IQN-formaatin nimeämisestä. Yksi näistä on iqn.1998-01.com.vmware.iscsi:name1, jossa isc-

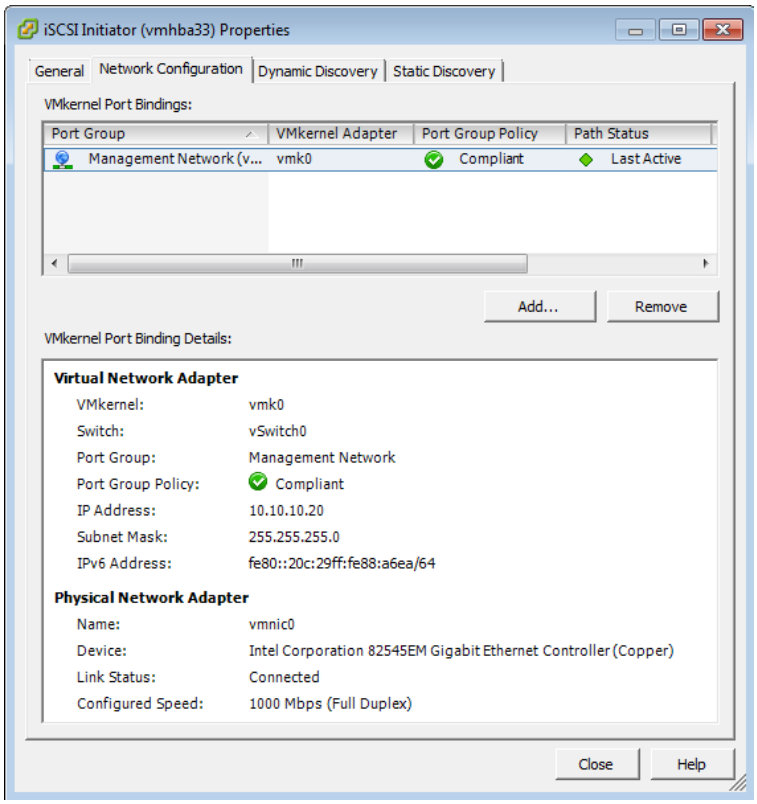
si.vmware.com on siis nimeäjäauktoriteetin osoite tässä esimerkissä. (iSCSI Naming Conventions, 2013.)

Normaaleissa iSCSI-käytänteissä voi yhdessä istunnossa olla useampia TCP-yhteyksiä. Tämä tarkoittaa, että samaa dataa voidaan lähettää ja vastaanottaa myös usean verkkokortin kautta kahden laitteen välillä. VMware ei tue suoranaisesti tätä ominaisuutta, vaan ESXi-palvelimet hyödyntävät omanlaistaan ominaisuutta nimeltä Multipathing. Ominaisuudella annetaan tuki luoda ohjelmistotasolla useita yhteyksiä istunnon läpi ja hyödyntää suurempaa tiedonsiirtoväylää datansiirtoa varten. (Lowe 2011, 277,286-287.)

5.2 ESXi-alustan liittäminen iSCSI-palvelimeen

ESXi-palvelimen valmistaminen iSCSI-levyjärjestelmää varten alkaa verkkoasetusten tekemisestä. iSCSI-liikenne on yksi liikennetyypeistä, joita kuljetetaan VMkernel-porttien kautta, ja tästä syystä onkin hyvä aloittaa konfigurointi verkkoasetuksista. Hallintayhteyden avaamisen jälkeen siirrytään networking-välilehden kautta tarkastelemaan virtuaalikytkimiä. Haluttuun virtuaalikytkimeen täytyy luoda VMkernel-portti, jolle laitetaan määritys iSCSI-liikenteelle sekä valitaan yksi aktiivinen verkkorajapinta käyttöön. Mikäli NIC teaming -ominaisuutta halutaan käyttää, tulee portteja luoda useampi kuin yksi. (Lowe 2011, 304-305.)

Toinen tehtävä toimenpide on luoda adapteri iSCSI Initiator -ohjainta varten. Tämä tapahtuu Configuration-välilehden kautta Storage Adapter -kohdasta. Välilehdeltä valitaan Add-toiminnon avulla uusi Software iSCSI Adapter. Luodun ohjaimen asetusvalikoita selaamalla löytyy neljä välilehteä asetuksia varten. General-välilehden kautta voidaan määrittää nimi, jolla kone näkyy Target-palvelimella, sekä aktivoida tai passivoida ohjaimen. Valikon kautta voidaan myös asettaa käytössä olevat CHAP-kättelyyn käytettävät tunnukset. Network Configuration -välilehden avulla määritellään iSCSI-portit, jota tämä ohjain käyttää. Kuviossa 12 on nähtävillä yksi valittu verkkorajapinta ohjaimen käyttöön.



Kuvio 12. iSCSI initiator -ohjaimen verkkoasetukset

Haluttujen rajapintojen valinnan jälkeen seuraakin Target-palvelimen etsiminen verkosta joko dynaamisella tai staattisella etsinnällä. Dynaaminen etsintä kysyy käyttäjältä Target-palvelimen osoitetta ja porttia, sekä palvelinpään autentikointia. Mikäli dynaaminen haku onnistuu, ilmestyvät osoitetut LUN-verkkolevyt ESXi-hallintavalikoiden Storage-näkymään. Dynaaminen haku onnistuessaan täyttää myös staattisen etsintä -välilehden tiedot automaattisesti. Mikäli Target-palvelimen haluaa syöttää manuaalisesti, tarvitaan autentikointitietojen lisäksi tieto palvelimen sijainnista, eli osoitteesta, sekä palvelimen nimi. (Lowe 2011, 306-309.)

6 Korkea käytettävyys

6.1 Korkean käytettävyyden määritelmä

Korkealla käytettävyydellä tarkoitetaan IT-infrastruktuurin kykyä tuottaa palveluita ilman katkoksia. Termi siis haluaa sanoa, että tuotetaan palveluita, jotka ovat kellon ympäri käytettävissä huolimatta laitteiden tai verkon epäkäytettävyydestä. Yleisesti korkeaan käytettävyyteen (High Availability) pyritään pääsemään kahdentamalla palveluita ja komponentteja, varautumalla ulkoisiin häiriöihin kuten sähkökatkoksiin hoitamalla varavirtaa laitteille tai käyttämällä komponentteja, jotka on helppo vaihtaa laitteen ollessa käynnissä. Käytettävyys

ilmoitetaan yleisesti prosenttilukuna, joka ilmoittaa, kuinka hyvin palvelu on ollut käytettävissä tietyllä ajanjaksolla. Mitä lähemmäksi lukua sata päästään, sitä kalliimmaksi ja haastavammaksi se yleensä tulee palvelun tarjoajan osalla. Kalliiksi korkeampi käytettävyys muodostuu myös palvelua käyttävälle asiakkaalle. (High availability in campus network deployments 2004.)

Keskeisiä termejä käytettävyyden osalta ovat MTBF (mean time between failure) ja MTTR (mean time to repair), jotka käsittävät virhetilanteiden välissä kuluneen ajan ja korjaukseen kuluneen ajan. Näillä arvoilla voidaan laskea prosentuaalisesti palvelun käytettävyys esimerkiksi vuotuisella tasolla. Termeinä MTBF ja MTTR voivat olla haastavia ymmärtää, joten palvelun käytettävyyden voi laskea myös yksinkertaisemmin jakamalla käytettävyysajan itsellään ja vikojen kestolla. Korkeaa käytettävyyttä määrittävät prosenttiluvut ilmoitetaan yleensä yhdeksikköjen määränä. Esimerkiksi kolmen yhdeksikön käytettävyys, eli 99,9%. Keskimääräisesti 99,9% käytettävyys antaisi palvelulle vaateen olla olematta enempää kuin neljä tuntia ja kaksikymmentäkolme minuuttia poissa käytöstä vuoden aikana. (High availability in campus network deployments 2004.)

6.2 Korkean käytettävyyden perusta vSphere-ohjelmistossa

VMwaren tuoma korkea käytettävyys (high availability) on pääasiassa virtuaalikoneiden uudelleenkäynnistämistä ja niiden toiminnan tarkkailua. vSphere HA tarkkailee ESXi-palvelimen toimintaa, mutta sillä voidaan puuttua myös virtuaalikoneiden ja niillä pyörivien sovelluksien vikaantumiseen. Vikatilanteen sattuessa järjestelmä pyrkii uudelleenkäynnistämään vikaantuneen VM-koneen toisella ESXi-alustalla vSphere klusterissa tai käynnistää vikaantuneen ESXi-alustan VM-koneet toisella alustalla. Tämä aiheuttaa kuitenkin hetkellisen katkoksen, jonka kestosta ei voi sanoa mitään varmuutta. Tämä johtuu suoraan siitä, että on mahdotonta arvioida aika, joka kuluu yhden tai useamman virtuaalikoneen uudelleenkäynnistymiseen muuttuvissa resurssioloissa. (Lowe 2011, 371-372.)

Virheen sattuessa on tietenkin mahdollisuus datan häviämiselle, sillä vSphere HA sulkee koneet ja aloittaa uudelleenkäynnistyksen välittömästi. Levylle kirjoittamisen ollessa tällä kyseisellä hetkellä kesken, voi osa datasta korruptoitua. Onneksi mahdollisuudet tähän hävikkiin ovat kohtalaisen pienet Windows- ja joidenkin Linux-jakeluiden tiedostojärjestelmien ansioista. Kriittisissä palveluissa minuuttien pituiset katkokset eivät ole toivottuja, joten tätä varten vSphere pitää sisällään muita ominaisuuksia, mutta niistä tuonnempana. (Lowe 2011, 372-373.)

Toiminnallisuutena vSphere HA käyttää versiosta viisi lähtien uutta kehitystyökalua nimeltään FDM (Fault Domain Manager). FDM korvaa aikaisemmissa versioissa olleen AAM (Automated Availability Manager). Tällä uudistuksella ollaan päästy eroon nimien selvitystarpeesta ja skaalautuvuusongelmista. FDM käyttää yksinkertaistettua orja/isäntä-ajattelua, tukee IPv6-verkkoja, käyttää hallintaverkkoja sekä varastolaitteita kommunikointiin ja ottaa kantaa verkon jaotteluun ja verkosta eristäytymiseen. (Lowe 2011, 373-374.)

Verkon jaottelulla (network partition) tarkoitetaan tilannetta, jolloin orjana toimiva kone ei voi kommunikoida isännän kanssa, vaikka näiden välillä oleva tietoverkko toimisi. Tässä tilanteessa vSphere HA tarkistaa varastolaitteina toimivat levyjärjestelmät erityisten heartbeat-sanomien varalta ja päättää niiden perusteella jatkotoimenpiteistä tavoittamattomissa olevan orjan osalta. (Lowe 2011, 374.)

Eristäytymisellä (network isolation) tarkoitetaan orjan osalta tilannetta, jossa orja on menettänyt kaikki hallintayhteytensä verkko-ongelman vuoksi. Tällä tavoin eristäytynyt orja ei näin ollen voi enää ilmoittaa olevansa elossa heartbeat-sanomilla toisille orjille, ESXi-alustoille, eikä kommunikointi isännänkään kanssa onnistu. Eristyksiin jäänyt orja luo tässä tilanteessa jaetulle varastolaitteelle erityisen binääritiedoston, jolla se yrittää ilmoittaa eristäytymisestään isännälle. (Lowe 2011, 374-375.)

Kun vSphere HA otetaan käyttöön, aloittaa FDM vaalit isännän valitsemisesta ESXi-alustojen kesken ja orjien nimittämisen. Valitun isännän vastuulle jää orjien tarkkailu, klusterissa olevien virtuaalikoneiden luettelointi, klusterissa tapahtuvien konfiguraatiomuutosten välittäminen orjille, heartbeat-sanomien lähettäminen orjille, raportointi vCenter-palvelimelle ja tietysti vikatilanteen yhteydessä virtuaalikoneiden uudelleenkäynnistys. Klusterissa olevat orjat taas vastaavasti tarkkailevat lokaalisti pyörivien virtuaalikoneiden ja verkossa olevan isännän tilaa. Mikäli orjat huomaavat isäntänsä kaatuneen, aloittavat ne uudet vaalit isännän nimittämiseksi. (Lowe 2011, 373-374.)

6.3 vSphere HA -ominaisuuden käyttöönotto ja vaatimukset

Korkean käytettävyyden käyttöönottaminen tarkoittaa koko klusteria koskevien ehtojen täyttymistä. Klusterissa täytyy siis olla levyjärjestelmä, johon kaikki ESXi-palvelimet pääsevät käsiksi. Levyjärjestelmän lisäksi tulee huolehtia, että kaikilla alustoilla olevat virtuaalikytkinten asetukset ovat identtiset tai vaihtoehtoisesti käytössä on kaikille alustoille yhteinen jaettu virtuaalikytkin (vDS). Varsinaisessa käyttöönotossa ilmeni muitakin asioita, joita tulee huomioida, mutta näistä lisää tuonnempana. Käyttöönoton jälkeen tiettyihin toimenpiteisiin täytyy kiinnittää entistä enemmän huomioita. Esimerkiksi huoltotilan asettaminen ESXi-

alustalle voi laukaista FDM-työkalun toiminnan, ellei HA-asetuksista käydä väliaikaisesti ottamassa heartbeat-viestittelyä pois käytöstä. (Lowe 2011, 375-276.)

6.3.1 Admission Control -politiikka

vSphere HA -määritysten myötä tulee klusterin kapasiteetti ja resurssien jakautuminen erittäin konkreettiseksi asiaksi. Admission Control Policy vastaa klusterin resursseista koskien korkeaa käytettävyyttä. Asetuksella on kaksi toiminnallisuutta. Päälle asetettuna ADP estää virtuaalikoneiden käynnistämisen, mikäli resurssit eivät riitä HA-ominaisuuksille tai poistettuna antaa käyttäjän rikkoa resurssirajoja, jotka muuten varattaisiin HA-ominaisuudelle. Tarkemmista säädöistä riippuen valvoo päälle asetettu ADP, että klusterissa on aina vapaana riittävä määrä resursseja, mikäli virtuaalikoneiden uudelleenkäynnistämistä tarvitaan. (Lowe 2011, 378-379.)

Esimerkkinä neljän ESXi-koneen muodostaman klusterin virtuaalikoneet vievät koko klusterin resursseista 75%, joka on samalla asetettu rajaksi ADP:n toiminnalle. HA-suunnittelussa tämä jäljellä oleva 25% resurssisiivu on tarkoitettu fyysisistä vioista toipumiseen. Tässä tilanteessa uuden virtuaalikoneen käynnistäminen pysäytettäisiin, koska tällöin resurssien käyttö nousisi yli asetetun määrän ja uhkaisi koko klusterin toimintaa, mikäli yksi neljästä palvelimesta kaatuisi. Klusteri, jossa ADP on poistettu käytöstä, antaa käyttäjän käynnistää käytännössä rajattomasti virtuaalikoneita, jolloin voidaan päätyä lähelle 100% klusterin resurssinkäytössä. Tällaisessa tilanteessa yhden palvelimen rikkoutuminen vaarantaisi koko muun klusterin toiminnan, kun kaatuneen palvelimen virtuaalikoneet yritetään käynnistää klusterin muilla, jo ylibuukatuilla, palvelimilla. (Lowe 2011, 378-379.)

ADP vaatii päälle laittamisen lisäksi myös määritykset, kuinka ominaisuuden halutaan toimivan. Valittavissa on kolme eri vaihtoehtoa toiminnalle, joista ensimmäinen on ESXi-palvelimien määrä, jonka voidaan sallia vikaantua. Asetus haluaa siis käyttäjältä yksikkömäärän vikaantuvista fyysisistä palvelimista, jonka avulla lasketaan koko klusteria koskeva määritys resursseista, jotka tulee olla vapaana HA-ominaisuuksia varten. Toisena vaihtoehtona voidaan määrittää prosenttiosuus, joka varataan prosessorien ja muistin osalta pois normaalista käytöstä. Kolmas vaihtoehto antaa määrittää tietyt ESXi-palvelimet olemaan varattuina vain vararesurssina olemista varten. Varatut palvelimet eivät siis pyöritä normaalioloissa yhtäkään virtuaalikonetta, vaan osallistuvat klusterin toimintaan ainoastaan vikatilanteissa. (Lowe 2011, 379-380.)

Edellä mainitut määritykset on helpohko ymmärtää, paitsi ensimmäisenä olleen vaihtoehdon osalta. Kyseisessä vaihtoehdossa laskennallisuus menee kutakuinkin seuraavalla tavalla: Oh-

jelma määrittää resurssien varausten (selitetään tarkemmin luvussa 9) perusteella resurssipalalle koon ja käyttää tätä yksikköä määrittämään klusterin resurssien kokonaismäärän. Varauksista käytetään suurinta annettua varauksen määrää, eli jos yhdelle virtuaalikoneelle on määritetty muistin ja prosessorin varausta 2GB ja 2GHz ja muille koneille ei ole määritelty varausta, on resurssipalojen koko 2GB ja 2GHz. Mikäli varauksia ei ole määritelty, määritetään prosessorin osalta palan kooksi 32MHz. Muistille palan koko määräytyy suurimman overheadin perusteella, mikä saadaan aikaan palojen laskennan seurauksena. (Lowe 2011, 380-381.)

Saatujen palojen nimittäjien perusteella lasketaan, kuinka monta palaa klusteri pystyy maksimissaan tukemaan. Tämän jälkeen lasketaan kuinka monta palaa klusteri menettäisi, jos suurimman määrän paloja omaava ESXi-palvelin kaatuisi. Tästä saadaan resurssimäärä, joka täytyy olla vapaana klusterissa. Ongelmia muodostuu, mikäli ESXi-palvelimet klusterissa eroavat paljon toistensa fyysisten ominaisuuksien mukaan, tai jos klusterissa on muutama suurilla varauksilla oleva virtuaalikone ja paljon pienillä varauksilla olevia koneita. On siis suositeltavaa asettaa samankokoiset virtuaalikoneet tai samoilla resursseilla olevat fyysiset palvelimet omiin klustereihinsa tai käyttää prosentuaalista varausta. (Lowe 2011, 381.)

6.3.2 Korkean käytettävyyden määritykset virtuaalikoneille

Resurssit ovat aina rajalliset ja suuren konemäärän keskellä tietyt koneet ovat aina tärkeämpiä kuin toiset. vSphere HA-asetuksissa on mahdollista puuttua virtuaalikoneiden keskinäiseen arvoasemaan, jolla pyritään päättämään järjestys ja prioriteetti uudelleenkäynnistyksiin. VM restart priority -asetuksella voidaan määrittää erikseen jokaiselle virtuaalikoneelle sen saama arvoasema uudelleenkäynnistysjärjestyksessä. Vaihtoehtoina asetukseen on Low, Medium, High ja Disabled. Kriittisimmille koneille tulisi määrittää arvoksi High ja koneille, joiden toimintaa ei välttämättä tarvita, tulisi asettaa arvoksi Disabled. Koneet, jotka halutaan käyttöön, mikäli resursseja on vapaana, tulisi asettaa joko Low tai Medium prioriteetille. (Lowe 2011, 382.)

Asetuksen määritykset astuvat kuvaan vain ja ainoastaan odottamattoman vian sattuessa ja kun klusterista äkkiseltään häviää virtuaalikoneita kannatteleva ESXi-palvelin. Kuitenkin pelkkä prioriteettiarvo High ei suojele kriittisiä palveluita, vaan tilaa on myös löydyttävä virtuaalikoneen käynnistämiseen. Tästä syystä Admission Control ja sen käytön suunnittelu tulee tehdä osaltaan yhteistyössä virtuaalikoneiden prioriteettien määrityksessä. (Lowe 2011, 383.)

Uudelleenkäynnistysprioriteetin lisäksi virtuaalikoneille voidaan määrittää toimenpide, joka suoritetaan palvelimen jouduttua eristyksiin verkossa (Isolation Response). Ominaisuudella pyritään turvaamaan virtuaalikoneiden suoritus mikäli pelkkä hallintaverkko vikaantuu. Näin pyritään estäämään toimivan alustan virtuaalikoneiden uudelleenkäynnistys. Asetus astuu siis voimaan tilanteissa, kun vSphere HA heartbeat -viesteihin ei saada vastausta tai kun ESXi-palvelimien välinen viestittely ei toimi. (Lowe 2011, 384.)

Kuvatussa tilanteessa kone pyrkii ottamaan yhteyttä isolation address -osoitteeseen. Mikäli vastaus palautuu tästä osoitteesta, tietää kone kärsivänsä verkon jakaantumisesta ja reagoi asetusten mukaisella tavalla. Mikäli vastausta ei kuulu isolation address -osoitteestakaan, yrittää ESXi-palvelin ottaa yhteyden jaettuun datavarastoon tai levyjärjestelmään ja muokata siellä olevaa host-X-poweron-tiedostoa. Master-koneena oleva palvelin tarkkailee tätä kyseistä tiedostoa. Bittimuunnoksen havaittuaan Master lukitsee erään toisen tiedoston datavarastossa, jonka perusteella eristyksissä oleva kone tietää viestin menneen perille ja että Master ottaa vastuun eristyneen koneen virtuaalikoneiden uudelleenkäynnistämisen organisoinnista. Asetuksina tätä tapahtumaa muokkaamaan voidaan valita toimenpiteet, joita eristynyt palvelin suorittaa omille virtuaalikoneille. Käytännössä tämä siis tarkoittaa, jätetäänkö virrat päälle vai sammutetaanko eristyksissä oleva järjestelmä. (Lowe 2011, 385.)

Eristäytymisen havainnointiin liittyy siis keskeisenä erillinen yhteisessä käytössä oleva levyjärjestelmä ja isolation address. Isolation address on siis verkossa käytössä oleva IP-osoite, joka vastaa tarvittaessa sille lähetettyihin vastauspyyntöihin. Osoite on oletuksena verkon gateway-osoite, mutta tarvittaessa sen voi käsin muokata vSphere HA -ominaisuuden parametreihin. Määritys tehdään advanced-asetusten kautta antamalla parametri das.isolationaddress ja perään arvoksi haluttu osoite. Levyjärjestelmän käytöstä taas käytetään HA-liitoksissa nimitystä Datastrose Heartbeating. Ominaisuutta varten valitaan joko manuaalisesti tai automaattisesti vähintään kaksi verkossa olevaa levyä, joita käytetään jatkossa normaalin toiminnan ohella HA-viestintään. Koska tämä ominaisuus on turvaamassa klusteria hallintaverkon osittaisenkin vikaantumisen aikana, on suositeltavaa eriyttää levyjärjestelmiin liitoksissa oleva verkko muusta hallintaverkosta. (Lowe 2011, 386,390.)

vSphere HA antaa vielä määrittää virtuaalikoneiden toiminnallisuutta tarkkailevan monitoroinnin. Tämä ominaisuus vaatii VMware Tools -ohjelmiston asentamisen virtuaalikoneelle, sillä paketti vastaa ominaisuuden vaatimasta viestinnästä virtuaalikoneen ja ESXi-palvelimen välillä. Käyttöönoton jälkeen ESXi-kone tarkkailee Tools-paketin lähettämien heartbeat-sanomien lisäksi levyn käytön I/O-toimintoja sekä virtuaalikoneen verkon I/O-toiminteita. Mikäli mikään näistä ei hetkeen näytä palauttavan mitään dataa, käynnistää ESXi-palvelin

automaattisesti virtuaalikoneen olettamuksenaan, että virtuaalikoneen käyttöjärjestelmä vikaantui. Viantutkinnan helpottamiseksi ottaa HA-toiminto myös tallenteen virtuaalikoneen konsolista ennen käynnistämistä ja tallettaa sen myöhempää tarkastelua varten. (Lowe 2011, 387-388.)

Toiminnallisuuden tarkkailua voi säätää kolmella asetuksella. Vikojen aikaväli (failure interval) muuttaa aikaa, jonka HA-toiminnallisuus odottaa ennen uudelleenkäynnistystä. Esimerkiksi asetuksen ollessa minuutissa, odottaa HA viimeisen I/O-toiminnon tai saadun heartbeat-viestin jälkeen kokonaisen minuutin ennen uudelleenkäynnistystä. Vikojen maksimilukumäärä (maximium failures) kertoo, kuinka monta kertaa kone voidaan yrittää korjata pelkällä uudelleenkäynnistyksellä. Maksimin saavuttamisen jälkeen HA-toiminnallisuus ei enää uudelleenkäynnistä konetta. Toiminnallisuutta voidaan myös rajata ajan suhteen (failure window) eli määrittää aika, jonka sisällä lasketaan uudelleenkäynnistyksiä. Eli jos vikojen maksimimäärä on kolme ja aika asetus on asetettu vuorokauteen, jättää HA-toiminto uudelleenkäynnistämättä virtuaalikoneen, jos se vikaantuu neljännen kerran saman vuorokauden aikana. Virtuaalikoneen sovellusten toimintaa voidaan myös tarkkailla, mutta se vaatii kolmannen osapuolen sovelluksen. (Lowe 2011, 388-389.)

6.4 vSphere Fault Tolerance -ominaisuus ja käyttöönotto

Fault Tolerance, eli lyhyesti FT (vikasietoisuus), käyttää VMwaren vuonna 2006 esittelemää record/replay-tekniikkaa, jota nykyisellään nimitetään VMware vLockstep -tekniikaksi. Käytännössä tekniikka tarjoaa jatkuvaa käytettävyyttä kopioimalla primäärikoneella tapahtuvan suorituksen sekundaarikoneelle. Tämä tarkoittaa prosessorin tapauksessa, että sama data ajetaan molempien VM-koneiden suorittimissa, jotta koneet ovat koko ajan samassa tilassa. Toiminnallisuudet esimerkiksi verkossa, levyillä, näppäimistöllä tai laitteiston keskeytykset kopioidaan koneelta toiselle ja toistetaan sekundaarilla. Yksinkertaisimmillaan toimintaa voi todentaa avaamalla molempien koneiden työpöydät eteensä ja katsoa hiiren osoittimen liikkumista lähes yhtäaikaisesti molemmilla koneilla. (Lowe 2011, 393.)

Ominaisuutena FT on erittäin tarkka vaatimustensa kanssa. Klusterin tasolla jokaisen ESXi-palvelimen täytyy käyttää samaa FT-versiota ja HA-toiminnallisuus täytyy olla käytössä. Mikäli vSphere DRS -ominaisuuksia halutaan käyttää, täytyy VMware EVC (Enchanced vMotion Compatibility) olla päällä. Muussa tapauksessa DRS-toiminteet otetaan FT-koneelta pois käytöstä. ESXi-palvelimien tasolla jokaisella palvelimella täytyy olla pääsy samoihin datavarastoihin ja tietoverkkoihin ja laitteistovirtualisointi täytyy olla käytössä ESXi-palvelimen BIOS-valikosta. Prosessorien täytyy myös olla yhteensopiva FT-ominaisuuden kanssa ja lista yh-

teensopivista prosessoreista löytyykin VMwaren verkkosivuilta. Tämän lisäksi FT-lokitoimintaa varten täytyy olla verkon kautta yhteydellisyys ESXi-palvelimien välillä vähintään gigabitin verkkokortin kautta. VMwaren suosituksissa on, että verkkoa varten tulisi järjestää omat rajapinnat, mutta mikään ei estä käyttämästä FT-ominaisuutta varten osoitettua VMkernel-porttia muuhunkin toimintaan. (Lowe 2011, 394.)

Kun klusterin ja palvelimien yhteensopivuus on tarkastettu, täytyy vielä tarkistaa seuraavat asiat virtuaalikoneesta, joka halutaan varmentaa FT-ominaisuudella:

- Virtuaalikoneessa saa olla vain yksi virtuaaliprosessori tai kone ei ole yhteensopiva.
- Virtuaalikoneen käyttöjärjestelmän tulee olla tuettu ominaisuudelle.
- Virtuaalikoneen tiedostojen tulee olla jaetulla levyjärjestelmällä, johon kaikki ESXi-palvelimet pääsevät käsiksi, ja virtuaalikovalevy tulee olla thick provisioned -formaatissa tai virtuaalisessa RDM-moodissa.
- Virtuaalikone ei saa olla linkitetty klooni toisesta koneesta.
- Virtuaalikoneen asetuksissa ei saa olla USB-laitteita, äänilaitteita, sarjaportteja tai rinnakkaisportteja.
- Virtuaalikone ei saa käyttää N_Port ID -virtualisointia.
- Virtuaalikoneessa ei saa olla vanhanmallista vlance-verkkokorttia tai sen verkkorajapinnoissa ei saa olla käytössä NIC passtrough -ominaisuutta.
- Virtuaalikoneen CD-ROM -asema ei saa osoittaa fyysiseen levyasemaan.
- Virtuaalikone ei saa käyttää paravirtualisoitua kerneliä, vaan se täytyy kytkeä pois päältä.
- Virtuaalikoneen laitteistoon ei saa tehdä muutoksia FT-ominaisuuden päälle kytkemisen jälkeen, eikä näin ollen verkkoasetuksiinkaan.

(Lowe 2011, 394-395.)

Kaiken kaikkiaan FT on ominaisuutena kohtalaisen vaativa ja yleisiä rajoituksiakin löytyy. Esimerkiksi ESXi-palvelimien prosessorien yhdenmukaisuus tulisi edelleen edistää ottamalla power capping -asetus pois käytöstä BIOS-asetusten kautta. FT myös estää Storage vMotion -ominaisuuden käytön, vaikka normaali vMotion onkin käytettävissä, eikä Snapshot-tallennus ole tuettu vSphere FT -ominaisuuden kanssa. (Lowe 2011, 395.)

Varsinainen käyttöönotto alkaa valitsemalla vCenter-palvelimeen muodostetun hallintayhteyden kautta valikosta jo luotu VM, joka halutaan varmentaa. Koneen valikoista löytyy HA-ominaisuuden käyttöön oton jälkeen Turn On Fault Tolerance -vaihtoehto. Tämän valitsemal-

la seuraa muutamia varoituksia ja ilmoituksia, mutta näiden hyväksymisen jälkeen alkaa klusterissa tapahtua. vCenter-palvelin huolehtii tässä vaiheessa, että halutusta virtuaalikoneesta luodaan kopio toiselle alustalle. Kopiointiin käytetään vMotion-toimintoa muistuttavaa siirtotapaa. Joka tapauksessa virtuaalinen kovalevy jää siis yhteiseksi molemmille virtuaalikoneille, mutta suorituksen tapahtumien kopioinnista vastaa VMware vLockstep, joka pitää molemmat koneet synkronoituna. Tapahtumien tallennus hoidetaan suoraan ESXi-palvelimien välillä aiemmin puhutun lokitusyhteyden avulla. Kopioinnin jälkeen virtuualikoneen tiedoista näkee, että millä ESXi-aluistoilla primääri ja sekundaari fyysisesti sijaitsevat ja koneen voi tämän jälkeen käynnistää. (Lowe 2011, 396-398.)

Koneen käynnistettyä kopioidaan kaikki ensisijaisen virtuaalikoneen suorittamat toiminnot myös varakoneella. Vikatilanteen sattuessa pääasiallisen virtuaalikoneen alustalla, ottaa toissijainen kone välittömästi virtuaalikoneen suorittamisen itselleen ja verkkoon lähetetään RARP-viesti. Välittömästi suorituksen siirryttyä toissijaiselle koneelle, aloitetaan uudestaan kopiointiprosessi ja synkronointi uuden kopion kanssa kolmannelle alustalle. (Lowe 2011, 398.)

Erikoistapauksiakin on, eli esimerkiksi tilanne, jossa molempien varmennukseen osallistuvien koneiden alustat vikaantuvat samanaikaisesti. Tässä vaiheessa automaatiosta vastaa vSphere HA, joka aloittaa välittömästi uudelleenkäynnistystoimenpiteet, mutta katkokselta ei tässä tilanteessa vältytä. Toinen erikoistapaus johon vikasietoisuus ei auta, on virtuaalikoneen käyttöjärjestelmän kaatuminen. Tässä tilanteessa kaatuminen toistuu myös toissijaisella koneella ja koneiden uudelleen käynnisty jää HA -toiminteen suoritettavaksi, mikäli koneiden monitorointi on käytössä. Muissa tapauksissa aina vikojen ilmaantuessa tai synkronoinnin pettäessä siirretään suoritus toiselle koneelle ja kopiointi toistetaan. (Lowe 2011, 398-399.)

7 Virtuaalikoneiden luominen

VMware on katsonut parhaan laitteistotuen muodostuvan käyttämällä pääosin laitteistovalmistaja Intelin virtualisoituja komponentteja. Näillä valinnoilla on pyritty saavuttamaan laajin yhteensopivuus erinäisten käyttöjärjestelmien ja muiden virtualisoitavien järjestelmien osalle. Virtuaalikoneita pyörittävät seuraavat laitteistokomponentit:

- Phoenix BIOS
- Intelin emolevy
- Intelin PCI IDE ohjain
- IDE CD-ROM ajuri

- BusLogic rinnakkais SCSCI, LSI Logic rinnakkais SCSI tai LSI Logic SAS ohjain
- AMD:n tai Intelin prosessori, riippuen fyysisestä raudasta
- Intelin e1000 tai AMD PCnet verkkokortti
- Yleinen VGA näytönohjain

Osalle näistä komponenteista löytyy fyysinen vastinkappale fyysisestä raudasta, kuten verkkokortti tai SCSI-ohjain, mutta osa komponenteista paravirtualisoidaan. Paravirtualisoiduilla komponenteilla ei ole fyysisiä laitteita vastaamaan toiminnasta, joten virtuaalikoneelle asennetaan tarvittavat käyttöjärjestelmäkohtaiset laitteistoajurit VMware Tools -ajuripaketin mukana. VMware Tools -ajuripaketti mahdollistaa optimoidut virtualisointiajurit VM-koneen käyttöön. Vaikka virtualisointi tarjoaa rajoja rikkovia mahdollisuuksia toteuttaa asioita, on virtuaalikoneillakin tietynlaisia fyysisiä rajoitteita:

- **Prosessori** - Yhdestä 32 prosessoriin.
- **Muisti** - Maksimissaan 1TB RAM-muistia.
- **SCSI adapteri** - Maksimissaan neljä SCSI adapteria, joissa jokaisessa voi olla 15 SCSI-laitetta.
- **Verkkorajapinta** - Maksimissaan 10 verkkorajapintaa.
- **Sarjaportti** - Maksimissaan neljä sarjaporttia.
- **CD/DVD** - Maksimissaan neljä CD/DVD-asemaa, kuitenkin maksimissaan niin, että IDE-laitteita ja CD/DVD-asemia ei ole yli neljää samaan aikaa käytössä.
- **Levykeasema** - Maksimissaan kaksi asemaa, jotka jakavat yhteisen ohjaimen.
- **USB** - Yksi ohjain ja maksimissaan 20 yhdistettyä USB-laitetta.
- Näppäimistö, näytönohjain ja hiiri.

Kovalevyjä koskevat rajoitteet ovat siis sisällytettynä CD/DVD-asemien lukumäärään, koska vSphere ESXi-ympäristössä pyritään käyttämään SCSI-laitteistoja tallennusmedioina. (Lowe 2011, 457-459.)

Kun virtuaalikone luodaan, syntyy siitä VMX-tiedosto. Tiedosto määrittää virtuaalikoneen fyysisen rakenteen, eli siihen liitetyt ohjaimet, ovatko ohjaimet kiinnitetty suoraan käynnistyksessä ja tarkennukset ohjaimiin, kuten verkkorajapintojen MAC-osoitteet. Virtualisoinnista vastaava ohjelma tekee muutokset tähän tiedostoon mikäli koneen fyysisiä komponentteja muokataan ohjelman kautta, mutta tiedostoa on myös mahdollista muokata suoraan tekstieditorilla. Varsinainen virtuaalikoneen data ei kuitenkaan ole tässä tiedostossa, vaan virtuaalista kovalevyä varten luodaan omat VMDK-tiedostot. Jokainen virtuaalinen kovalevy esitetään fyysisellä muistilla omina VMDK-tiedostoinaan. Varsinaisesti yhtä virtuaalilevyä varten

luodaan kaksi VMDK-tiedostoa, toinen sisältää varsinaisen levylle kirjoitetun datan binäärikirjoituksena ja toinen on selväkielinen otsikkotiedosto. Otsikkotiedosto pitää sisällään osoittimet varsinaiseen datatiedostoon. (Lowe 2011, 461-463.)

Uuden virtuaalikoneen luominen on hyvin suoraviivainen prosessi. Koneen voi luoda joko käyttäen kokonaan omia asetuksia tai luoda VMwaren mielestä tyypillisen virtuaalikoneen, jonka asetuksia ei niin paljon pääse muokkaamaan. Suositeltavaa onkin tehdä täysin itse kustomoitava VM. Asennus pyytää koneelle nimen, sijainnin virtuaalikoneen suoritukselle ja paikan virtuaalikoneen kovalevyn sijainnille. Näiden asetusten jälkeen päästään valitsemaan haluttu määrä virtuaaliprosessoreita ja RAM-muistia. Muistia voidaan allokoida tietenkin enemmän kuin ESXi-palvelimella on tarjota, mutta tämä saattaa vaikuttaa koneen suoritukseen. Tästä aiheesta puhutaan lisää seuraavassa luvussa 8. Prosessorien osalta prosessorisoketteja sekä ytimiä voi kumpiakin valita 1-16, mutta niin että maksimaalinen ytimien määrä on enintään 32. Viimeisinä asetuksina luodaan haluttu määrä verkkokortteja, sekä luodaan halutun kokoinen kovalevy. Levytila voidaan varata kokonaan kerralla tai käyttää laajentuvaa kovalevyä asetettuun rajaan asti. Lopulta asennus esittelee tehdyt valinnat yhteenvetonäkymänä ja koneen luominen on valmis. Virtuaalikoneen asetuksia voidaan myös jälkikäteen muokata virtuaalikoneen Edit Setting -valikon kautta. (Lowe 2011, 464-475.)

Luotuun virtuaalikoneeseen täytyy vielä asentaa käyttöjärjestelmä, jotta konetta voitaisiin käyttää. ESXi tukee tiettyjä käyttöjärjestelmiä, joten kannattaa varmistaa tuen löytyminen ennen asennusta. Lista on kuitenkin hyvin kattava ja täydellisen listan voi hakea VMware Compatibility Guide -verkkosivun avulla valitsemalla Guest OS ja haluamansa ESXi-version. Tässä kuitenkin lista yleisimmistä käyttöjärjestelmistä, jotka ovat tuettuina ESXi-versiossa 5.5:

- Apple Mac OS X 10.6.x ja 10.7.x 32-bittinen tai 10.7.x ja uudemmat 64-bittisenä.
- Ubuntu Linux versiot 10.04-13.10 32- ja 64-bittisinä.
- CentOS Linux versiot 4.9-6.5 32- ja 64-bittisinä.
- Debian Linux versiot 6-7 32- ja 64-bittisinä.
- FreeBSD versiot 7-9.2 32- ja 64-bittisinä.
- Red Hat Enterprise Linux versiot 4.9-6.5 32- ja 64-bittisinä.
- Windows XP SP 3 32-bittisenä.
- Windows Vista SP 2 32- ja 64-bittisinä.
- Windows 7 ja SP1 32- ja 64-bittisinä.
- WIndows 8 ja 8.1 32- ja 64-bittisinä.

- Windows Server 2012 ja 2012 R2 64-bittisinä.
- Windows Server 2003 ja 2008 useat SP-paketit 32- ja 64-bittisinä.

Tuetun käyttöjärjestelmän asennus voidaan hoitaa, joko ESXi-palvelimen fyysiseen CD/DVD-asemaan asetettavalla asennuslevykkeellä, tai osoittaa asennuksen käyttöön tarkoitettu tiedosto esimerkiksi levyjärjestelmäpalvelimelta. Asennukseen voidaan tarjota myös levyasemaa, joka sijaitsee fyysisesti koneella, jolta vSphere Client -ohjelmaa käytetään klusterin hallintaan. (Lowe 2011, 478-479; VMware Compatibility Guide 2014.)

Käyttöjärjestelmän asentamisen jälkeen on suositeltavaa asentaa käytettävyyttä parantava VMware Tools -paketti. Paketin luvataan ainoastaan parantavan virtuaalikoneen suorituskykyä sekä lisäävän siihen tuet erinäisiin VMware vSphere -toimintoihin. Tools-paketin mukana asennetaan paravirtualisoidut laitteistoajurit, jotka voivat olla käyttöjärjestelmäkohtaisia, parantamaan konsolin käyttöä video- ja hiiriajureilla. Lisäksi paketin mukana asennetaan optimoitu SCSI-ajuri. Taustalle asioita parantamaan asennetaan parannettu muistinhallinta, VM heartbeat -ominaisuus sekä kyky hetkellisesti pysäyttää virtuaalikone Snapshot-toimintoa tai varmuuskopiointia varten. (Lowe 2011, 484.)

8 Resurssit ja resurssien jaon hallinnointi

vSphere ESXi tarjoaa erinäisiä tapoja hallita klusterissa olevia resursseja VM-koneiden käyttöön tai tarvittaessa tarjota lisäresursseja kovassa rasituksessa olevalle virtuaalikoneelle. Kuten aiemmin virtualisoinnin hyödyissä mainittiin, että virtualisoimalla meidän ei tarvitse ostaa palvelinrautaa yksittäisen palvelimen tarpeisiin, vaan voimme suunnitella muistin ja prosessorin ominaisuudet jokaisen virtuaalikoneen tarpeiden. Muistin ja kiintolevyn osalta virtuaalikoneissa on läsnä vaikeus hahmottaa tarpeellinen resurssimäärä ja vaikka virtuaalikoneille osattaisiin varata riittävät resurssit, alkavat ESXi-alustojen resurssit loppua aina jossain vaiheessa. Tilanteessa, jossa resurssit uhkaavat loppua tai kun virtuaalikone pyytää enemmän resursseja kuin sille on varattu, on hyvä mieltää mahdollisuudet resurssien hallinnoimiseen vSphere-ohjelmiston osalla. Resurssien hallinnoinnin suhteen voidaan asetuksilla määrittää resurssien varaukset, rajat ja jakamiset. (Lowe 2011, 537-538.)

Mikäli halutaan, että virtuaalikone saa tilanteesta huolimatta tietyn määrän resursseja käyttöönsä, voidaan asia huolehtia määrittämällä varaukset (reservation) resursseihin. Varatut resurssit ovat vain ja ainoastaan määritetyn virtuaalikoneen käytettävissä, eikä ESXi-alusta anna niitä minkään toisen virtuaalikoneen käyttöön. Toinen tapa hallinnointiin on määrittää raja-arvo (limits) resurssille. Tällä tavalla voidaan määrittää maksimiarvo jokaiselle resurssille

erikseen, minkä virtuaalikone voi saada käyttöönsä, mikäli resursseja on ylipäänsä vapaana. Raja-arvot toimivat hiukan eri tavoin riippuen hallittavasta resurssista. Jaot-ominaisuudella (shares) voidaan määrittää prioriteetti virtuaalikoneen resurssinkäytölle. Prioriteetti määrittää järjestyksen, jossa virtuaalikoneiden resurssintarpeita palvellaan kyseisellä ESXi-alustalla. Tässäkin isomman prioriteetin omaava virtuaalikone on ensimmäisenä saamassa haluamansa resurssit toimittaakseen tehtävänsä. (Lowe 2011, 538.)

8.1 Virtuaalinen muisti

Virtuaalikoneita luodessa tarjoaa luontityökalu keskimääräisen suositusarvon muistin määrälle asennettavan käyttöjärjestelmän perusteella. Asetettava muistin määrä toimii virtuaalikoneella aivan samalla tavalla kuin fyysiselle tietokoneelle asetettavat muistikammat. Mikäli asetamme fyysiseen koneeseen neljän gigatavun edestä muistikampoja tai asetamme virtuaalikoneelle muistin määräksi samat neljä gigatavua, on tämä neljä gigatavua maksimaalinen käytössä oleva muistin määrä. Tilanteessa, jossa fyysiselle ESXi-alustalle on asennettu 16 GB edestä muistia, jää meillä muiden virtuaalikoneiden käyttöön 12 GB, kun annamme ensimmäiselle 4 GB. Esimerkki antaa kuvan, että resurssien laskenta on hyvin yksinkertaista, mutta todellisuudessa asennetusta muistista menee pieni osa ESXi-alustan omaan toimintaan. Lisäksi ensimmäinen virtuaalikone käyttää virtuaalimuistia kuin se olisi fyysistä muistia, mutta käytöstä muodostuu hiukan ylimääräistä otsikointia eli overheadia. Näin laskenta ei olekaan täysin yksioikoista. Virtuaalikone, jolle on asetettu muistin määräksi neljä gigatavua ja jonka muistin käyttö on hetkellisesti 100%, käyttääkin fyysisen koneen muistista enemmän kuin neljä gigatavua overheadin vuoksi. (Lowe 2011, 539-540.)

Overheadin määrää juontaa juurensa VMkernelin toimintaan ja riippuu virtualisoitujen prosessorien ja muistin määrästä, koska prosessorit tarvitsevat toimintaansa prosessorin omaa muistia ja virtuaalinen muisti tarvitsee ylimääräiset osoittimet oikeaan muistiin. Jatketaan kuitenkin skenaariota niin, että luodaan vielä kolme muuta samankokoista virtuaalikonetta. Nyt allokoitu muistin määrä ylittää jo fyysisen muistin määrän. Tämä ei johda kuitenkaan alustan kaatumiseen, vaan tilanteeseen, jossa koneet joutuvat rasittuessaan kilpailemaan resursseista. Mikään ei myöskään estä käynnistämästä viidettä virtuaalikonetta samalla määrällä muistia, mutta tällä toimenpiteellä aiheutamme varmasti käytettävyysongelmia kaikille virtuaalikoneille resurssien loppuessa kesken. (Lowe 2011, 539-540.)

8.1.1 VMware ESXi:n käyttämät muistitekniikat

VMware ESXi käyttää neljää erilaista tekniikkaa hyödyntääkseen käytettävissä olevan fyysisen muistin mahdollisimman tehokkaasti. Lähteenä käytetyn kirjan kirjoittajan sanojen mu-

kaan vSphere ESXi oli vuonna 2011 markkinoiden ainoa ohjelmistoratkaisu, joka pystyi suorittamaan muistin varaamista yli fyysisen muistin määrän käyttöjärjestelmästä riippumatta. Vaikka näillä tekniikoilla voidaankin antaa virtuaalikoneille enemmän virtuaalista muistia käyttöön kuin mitä varsinaista fyysistä muistia on käytettävissä, eivät ne täysin korvaa suunnitelmallista priorisointia muistin varaamisella, rajaamisella ja jakamisella - kolmella aikaisemmin mainitulla tavalla. (Lowe 2011, 540-541, 543.)

Transparent Page Sharing on näistä tekniikoista yksi ja sen ideana on hyödyntää useiden virtuaalikoneiden samanlaisia muistipaloja. Tarkemmin sanottuna käytössä on yleensä 4 MB kokoisia muistisiivuja (memory page), joista yritetään löytää sellaisia siivuja, jotka sisältävät saman sisällön. Samaa sisältöä omaavista siivuista muodostetaan tiiviste tietyn kaavan mukaan niin, että useiden virtuaalikoneiden muistisiivu voidaan esittää yhdellä siivulla ja tunnistus tapahtuu tiivisteen (hash) perusteella. Näin esimerkiksi neljä samanlaista konetta eivät käytä saman toiminnon suorittamiseen nelinkertaista määrää muistia, vaan tieto on yhtenä siivuna ja kunkin koneen käyttöoikeus tunnistetaan jokaisen oman tiivisteen avulla. Tiivistys eli hashing luo muistisiivuille overheadia, mutta säästää toiminnallaan käytettävän muistin määrää. Transparent Page Sharing toimii ominaisuutena riippumatta virtualisoitavasta käyttöjärjestelmästä. (Lowe 2011, 541.)

Ballooning on riippuvainen toiminnasta virtualisoitavan käyttöjärjestelmän kanssa ja tarvitsee toimiakseen VMware Tools -lisäpaketin mukana asennettavan käyttöjärjestelmäkohtaisen ajurin. Asennettu ajuri toimii hypervisorin ja virtualisoitavan käyttöjärjestelmän välillä ja vastaa hypervisorin käskyihin. Käskyt balloon-ajurille ovat yleensä vaatimuksia ottaa virtuaalikoneelle varattua muistia ja määrittää se käytettäväksi toiselle virtuaalikoneelle hypervisorin toimesta. Hypervisor voi siis muistia tarvitessaan käskeä balloon-ajurin paisua (inflate) eli varata virtuaalikoneesta muistia itselleen. Kun ajuri on laajentunut ja varannut halutun määrän muistisiivuja, antaa ajuri ne hypervisorin käyttöön. Hypervisor hyödyntää saamansa siivut toisen virtuaalikoneen resursseiksi. Virtuaalikone voi antaa, käskyn niin vaatiessa, muistisiivuja, joita se ei kyseisellä hetkellä tarvitse. Näin toimiessaan muistin uudelleen allokointi ei vaikuta virtuaalikoneen toimintaan, mutta mikäli virtuaalikoneen muisti on jo käytössä, hoitaa balloon-ajuri lisää muistia esimerkiksi Swapping-tekniikalla, jottei virtuaalikoneen suorituskyky kärsisi. Tekniikan etuna on, että ajuri näkyy virtuaalikoneelle ohjelmana, joka välillä vaatii muistia käyttöönsä ja näin ollen virtuaalikone saa itse päättää antamistaan muistisiivuista, eli normaalilla toiminnallaan se pyrkii antamaan käyttämättömiä siivuja. (Lowe 2011, 541-542.)

Swapping on kolmas vSphere ESXi -palvelimen käyttämistä muistitekniikoista ja sen voi edelleen jakaa kahteen alakategoriaan riippuen käyttääkö hypervisor (hypervisor swapping) vai VM (guest OS swapping) tätä tekniikkaa. Virtuaalikoneella tapahtuva swapping tarkoittaa, että virtuaalikone siirtää virtuaalimuistissa olevia muistisiivuja (page) omalle virtuaalikiintolevylleen muistinhallinta-algoritmien avulla. Käytännössä tämä mahdollistaa esimerkiksi neljä gigatavua muistia vaativan koneen ajamisen vain gigatavulla RAM-muistia lopun muistin ollessa tiedosto virtuaalikovalevyllä. Virtuaalikoneen toiminta voi näin kuitenkin hidastua kiintolevyn ollessa hitaampi kuin varsinainen välimuisti. Tämä tekniikka on täysin riippuvainen virtuaalikoneen omista päätöksistä. (Lowe 2011, 542.)

Hypervisorilla tapahtuva swapping voidaan kuvata viimeiseksi vaihtoehdoksi, mikäli mikään aikaisemmin mainituista ei auta muistin osalla. Tekniikka mahdollistaa ESXi-palvelimen vaihtaa kiintolevyllä olevia muistisiivuja ottaakseen ne muistina käyttöön. ESXi-alustan suorittama swapping ei ota ollenkaan kantaa siihen, onko vaihdettava muistisiivu vapaana vai jonkun virtuaalikoneen käytössä. Tästä syystä hypervisor swapping on viimeinen mahdollisuus vastata muistinvarauksen tarpeisiin. (Lowe 2011, 542.)

Kun virtuaalikone käyttää swapping-muistia, tallentuu vswp-päätteinen tiedosto samaan tiedostokansioon, jossa virtuaalikoneen kovalevytiedosto on. Tiedoston koko on maksimissaan asetuksissa varatun virtuaalikoneen RAM-muistin suuruinen, eli kun koneelle varataan 4 GB muistia, voi vswp-tiedosto olla maksimissaan 4GB. Swapping-muisti ei ominaisuuksiltaan pärjää varsinaiselle RAM-muistille. Lowe esittääkin kirjassaan vertailevan laskun, jossa RAM-muistin lukuajaksi ilmoitetaan 10 nanosekuntia ja kovalevylle 8 millisekuntia. Nopealla laskulla RAM-muisti on siis 800,000 kertaa nopeampi lukea kuin kovalevy. (Lowe 2011, 542.)

Viimeisenä tekniikkana on memory compression, joka esiintyi ensimmäisen kerran vSphere versiossa 4.1 ja on myös nykyisissä versioissa mukana. ESXi-palvelimen joutuessa tilanteeseen, jossa hypervisor swapping tulee kysymykseen, yrittää ESXi-alusta saada muistisiivuilla olevaa dataa pakattua tiiviimmin. Lohkot, jotka saadaan pakattua ainakin 50 % alkuperäisestä, siirretään pakattuun muistiin, eikä niitä kirjoiteta levylle. Pakkaamisella pyritään ehkäisemään tilannetta, jolloin joudutaan käyttämään swapping-tekniikkaa ja mikäli pakkaaminen onnistuu, ei palvelun suorituskyky alene kriittisesti. (Lowe 2011, 542-543.)

8.1.2 Muistin varaus, rajoitus ja jakaminen

Muistin varaus on valinnainen asetus ja oletuksena asetettuna nollaan megatavuun eli, että muistinvarausta ei ole käytössä. Mikäli varausta ei näin ollen ole asetettuna, saa ESXi-alustan muistinhallinta päättää täysin, mistä virtuaalikone saa muistinsa. Annettu numeerinen arvo

määrittää tässä tapauksessa, kuinka paljon RAM-muistia ESXi-palvelimen täytyy aina kyetä tarjoamaan virtuaalikoneen käyttöön. Mikäli arvo on nollassa, voi virtuaalikoneen muisti olla järjestetty vaikka kokonaan swapping-tekniikalla, eikä varsinaisella fyysisellä RAM-muistilla. Vaikka skenaario on mahdollinen, niin tosiasiassa ESXi-pyrkii järjestämään RAM-muistin virtuaalikoneille fyysisestä muistista parhaansa mukaan ja käyttää muita tekniikoita vain tarvittaessa. Varauksen tarkoituksena on siis antaa virtuaalikoneelle käytettäväksi vähintään määritetty määrä fyysistä ja nopeaa RAM-muistia. Virtuaalikoneelle varattu muisti varataan vain kyseisen koneen käytettäväksi, eikä mikään toinen virtuaalikone voi käyttää varattua muistilohkoa, paitsi osana transparent page sharing -tekniikkaa. (Lowe 2011, 544-547.)

Muistin rajoituksella voidaan asettaa maksimaalinen muistinkäytön raja. Esimerkiksi VM, jolle on asetettu RAM-muistin määräksi 4GB luulee siis, että sillä on käytössään tuo määrä muistia. Mikäli asetamme rajoituksen tässä tapauksessa 2GB, tulevat aiemmin mainitut muistitekniikat käyttöön muistinkäytön ylittäessä 2GB. Virtuaalikoneella on siis edelleen käytössään 4GB RAM-muistia, mutta kone voi maksimissaan käyttää 2GB fyysistä muistia aiemmin mainitulla asetuksella. Asetus kuulostaa jokseenkin turhalta, mutta esimerkiksi huoltotoimien yhteydessä virtuaalikoneiden vMotion-siirtojen ajaksi, saadaan ei-niin-tärkeiden virtuaalikoneiden fyysisen muistin käyttö laskettua minimiin ilman suuria vaikutuksia palveluihin. (Lowe 2011, 547-548.)

Jakamisella pyritään ratkaisemaan tilanteet, jossa ESXi-alustan täytyy päättää, millä prioriteetilla palvellaan muistinvarauksensa ylittäneitä virtuaalikoneita. Esimerkkinä tilanne, jossa kaksi virtuaalikonetta ylittää varauksensa ja molemmat vaativat lisää fyysistä muistia. Virtuaalikoneille on määritetty jaot niin, että virtuaalikone A:n arvo on 2000 ja B:n arvo 1000. Tässä tilanteessa VM A saa prosentuaalisesti enemmän muistia verrattuna VM B:hen. Käytännössä VM A saa kaksi muistisiivua jokaista virtuaalikone B:n yhtä muistisiivua kohti. Jaon numeerinen arvo on oletuksena virtuaalikoneelle määritetyn muistin suuruinen eli 4GB RAM-muistia sisältävällä koneella 40960. Tämä oletusmääritys takaa sen, että koneelle annetaan prioriteetti siihen määrään muistia, joka sille on alunperin asetettu. (Lowe 2011, 549-550.)

8.2 Virtuaalikoneiden prosessorikäyttö

Virtuaalikoneen luomisen yhteydessä määritetään virtuaalisten prosessorien määrä ja ytimien määrä prosessoreissa. Suorittimien määrä on näillä kahdella asetuksella mahdollista määrittää 1 ja 32 suorittimen välille riippuen tietenkin virtualisoitavan käyttöjärjestelmän fyysisistä rajoitteista prosessorien hyödyntämiseen. Vaikka ESXi-palvelin emuloi Intelin emolevyä kaikkine PCI- ja I/O-väylineen, on prosessorin kohdalla periaatteessa tyhjä aukko, josta näkee

suoraan fyysiseen prosessoriin. Näin VMwaren teknikot saivat vältettyä hukkaamasta arvokkaita resursseja prosessorien emuloimiseen ja myös vältytään turhalta overheadilta. Tämä toimenpiteenä vaatii tietenkin prosessorin, joka tukee virtualisointia laitetasolla ja saa aikaan sen, että virtuaalikoneissa on ominaisuuksiltaan ja arkkitehtuuriltaan vastaava prosessori kuin fyysisessä koneessa. (Lowe 2011, 552-553.)

8.2.1 Prosessorivaraus, -rajoitus ja -jako

Edellisestä poiketen ESXi-asetukset tarjoavat neljä vaihtoehtoa säätää prosessorien resurssin käyttöä. Tämä neljäs vaihtoehto on nimeltään CPU affinity. Sen avulla on mahdollista määrittää staattisesti tietty fyysinen prosessorin ydin virtuaalikoneen käyttöön. Monessakaan mielessä tämä ei ole suositeltavaa, sillä toiminto muun muassa estää vMotion-toiminnon käyttämisen ja hankaloittaa hypervisorin mahdollisuuksia jakaa prosessorikuormaa tämän yhden virtuaalikoneen takia. Ominaisuus on kuitenkin olemassa ja käytettävissä, mikäli sitä haluaa hyödyntää. (Lowe 2011, 553-554.)

Varausten hyödyntäminen takaa koneelle palveluaikaa prosessorin toimintasykleissä. Normaalioloissa, kun virtuaalikoneella on työtä prosessorille, se asettaa työn prosessorin käsittelyjonoon. Työ jää odottamaan sykliä, jolloin prosessori ehtii sen käsittelemään. Jos varaustoiminnolla määritetään prosessorille käyttöön tietty megahertsimäärä, on kyseinen määrä prosessorin resursseja aina virtuaalikoneen käytettävissä. Tässä suhteessa varaus toimii prosessorin osalta samoin kuin muistin, eli alustan on pystyttävä tarjoamaan kyseinen resurssi kaikille koneille, joille se on määritetty. Tämä tarkoittaa sitä, ettei ESXi suostu käynnistämään virtuaalikoneita yli sen fyysisten resurssien. Jos jokaiselle virtuaalikoneelle varataan 1024MHz prosessorista ja ESXi-palvelimella on yhteensä 12000MHz resurssina, voidaan samanaikaisesti pitää päällä 11 virtuaalikonetta. Luotuja koneita voi tietenkin olla useampia ja rajoitus nimenomaan koskee kyseisellä hetkellä virroissa olevia virtuaalikoneita. Eroja muistin varaamiseen myös on, sillä mikäli virtuaalikone A on jouten, eikä käytä sille varattuja resursseja, voi toinen virtuaalikone käyttää kyseistä varattua resurssia. Mikäli kone A haluaakin käyttää sille varattua resurssia, ei toinen kone pysty hyödyntämään varattua prosessoriresurssia sillä hetkellä. (Lowe 2011, 554-555.)

Prosessoritehon rajoittaminen toimii hyvinkin eri tavoin kuin vastaava toiminto muistin osalta. Virtuaalikone luulee normaalitilanteessa omaavansa yhtä monella prosessointisyklillä olevan suorittimen kuin fyysinen kone, mutta rajoituksella voidaan alentaa virtuaalikoneen käytössä olevaa hertsimäärää. Näin ollen esimerkiksi kevyempää palvelua varten meidän ei tarvitse hukata prosessorista yhden suorittimen toimintaa antamalla esimerkiksi kokonaista 3GHz suoritinta koneen käyttöön. Asetuksista saadaan annettua yksi suoritin koneelle ja

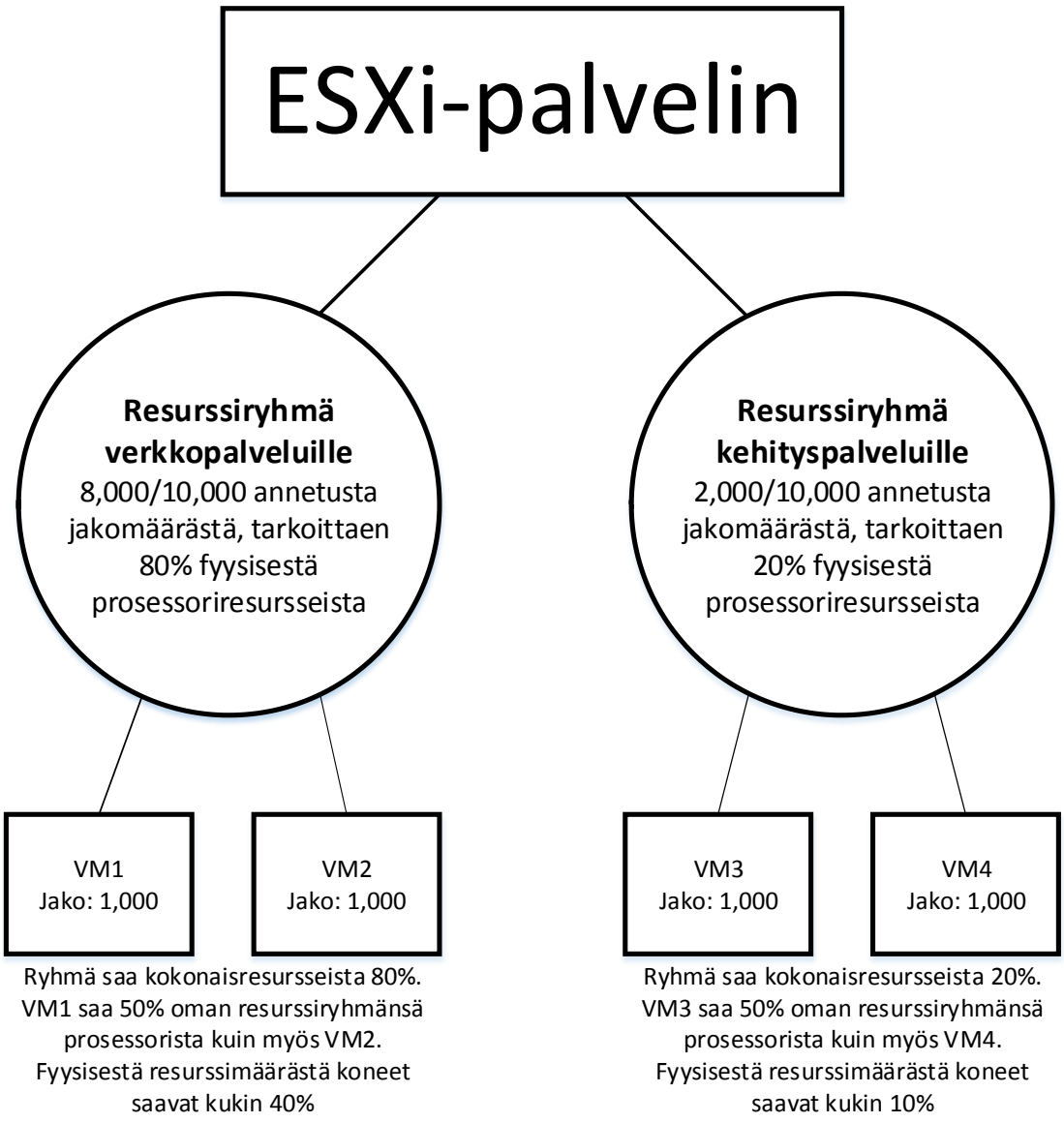
edelleen rajoituksilla laskea suorittimen käyttö esimerkiksi 1GHz:iin. Tämä estää tietenkin virtuaalikonetta käyttämästä enempää prosessorisyklejä, mutta vapauttaa resursseja muille virtuaalikoneille. (Lowe 2011, 555.)

Jakaminen toimii prosessorin osalla samalla tavoin kuin muistinjaon yhteydessä. Kyseinen ominaisuus tulee siis käyttöön tilanteissa, joissa useampi virtuaalikone kilpailee samasta resurssista ja ominaisuuden avulla voidaankin määrittää prioriteettijärjestys, jossa virtuaalikoneita palvellaan kilpailutilanteissa. Jaon prioriteettia tarkastellaan, kun ESXi-palvelin saa enemmän pyyntöjä prosessorin suoritussykleihin kuin se pystyy tarjoamaan ja syntyisi jonotilanne. Mikäli kilpailua resursseista ei synny, ei ominaisuus aiheuta vaikutuksia prosessorinkäyttöön. (Lowe 2011, 556.)

8.3 Resource Pool

Aiemmissa kappaleissa käsiteltiin resurssien hallinnointia yksittäisten koneiden osalla. Yksittäisiin VM-koneisiin kohdistuvien asetusten lisäksi voidaan ESXi-klusteriin määrittää niin sanottu resource pool. Ominaisuudella saadaan varaukset, rajoitukset ja jaot resurssihallinnointiin, mutta kohteena on ryhmä virtuaalikoneita. Ryhmälle määritellään luomisen yhteydessä nimi ja määritetään halutut asetukset prosessori- ja muistiresurssien osalla. Molemmissa resursseissa on käytössä samat kolme tapaa hallinnointiin eli jako, varaus ja rajoitus. Hallinnoitavana resurssina käytetään klusterin resursseja ja ryhmän käyttöön asetetut resurssit periytyvät myös seuraavalle tasolle. Klusteri on oletuksena itsessään yksi suuri resurssiryhmä ja se voidaan jakaa pienempiin ryhmiin, jotka taas voidaan jakaa pienempiin ryhmiin. Alemmat tasot perivät ylemmiltä tasoilta muun muassa rajoitukset kokonaisresurssien määrästä. (Lowe 2011, 559-560.)

Resurssiryhmien luomisella pyritään helpottamaan klusterin resurssien määrittämisestä tietyn virtuaalikoneryhmän käyttöön. Mikäli klusterissa toimii kriittisiä verkkopalveluja, voidaan ryhmillä tehdä määritys koskien näitä koneita ja varmistaa riittävät resurssit esimerkiksi varauksilla. Varatut resurssit ovat tietysti poissa muilta koneilta, joten kokonaisvaltaisella suunnittelulla on suuri rooli tässäkin tapauksessa. Kuviossa 13 on pyritty selventämään resurssien hallinnoinnin kokonaisvaltaista vaikutusta virtuaalikoneisiin prosessorijaon avulla. Kaikilla neljällä virtuaalikoneella on asetettu yhtä suuri prioriteetti jaon osalta, mutta lopullinen määrä fyysisestä resurssista vaihtelee ryhmien avulla huomattavasti. Esimerkiksi kyseisenlaisilla jaoilla VM1 saisi 8GHz ja VM3 2GHz mikäli fyysinen prosessointiresurssi olisi 20GHz. (Lowe 2011, 563.)



Kuvio 13. Resurssijako ryhmien ja yksittäisten koneiden asetusten avulla

8.4 Network I/O Control

Resource pool-ryhmillä voitiin määrittää haluttuja asetuksia prosessorin- ja muistin käytön osalta, mutta vSphere tarjoaa vielä ominaisuuden hallinnoida tietoverkon käyttöä ESXi-palvelimien osalta. Ominaisuutta nimitetään vSphere Network I/O Control, NetIOC. Ominaisuuden käyttöönotto vaatii version 4.1.0 tai uudemman ja se on otettavissa käyttöön vain vSphere Distributed Switch, jaetun virtuaalikytkimen, avulla. Hallinnoinnilla voidaan vaikuttaa vain kytkimestä lähtevään liikenteeseen ja NetIOC-ominaisuuden käyttöönotto aktivoi myös seuraavat kuusi resurssivarantoa verkon osalle: Fault Tolerance -, iSCSI-, hallinnointi-, NFS-, virtuaalikone- ja vMotion-liikennöinnin. Versiossa 5.0.0 tuli myös seitsemäs ominaisuus nimeltään Host Based Replication -liikennöinti. (Lowe 2011, 568.)

vSphere versio 5.0.0 ja uudemmat pitävät siis sisällään erilaisille liikenteille valmiit ryhmät, mutta mikään ei estä tekemästä omia ryhmiä vielä näiden päälle. Omat ryhmät voidaan linkittää haluttuihin porttiryhmiin, joten niillä voidaan helpommin erotella virtuaalikoneita ryhmittäin. Pääpiirteissään yhteen ryhmään on kuitenkin mahdollista määrittää kolme mahdollista asetusta vaikuttaen kyseisen ryhmän lähtevään liikenteeseen. Ensimmäinen näistä on fyysisten rajapintojen jako, joka toimii pääpiirteittäin samoin tavoin kuin muistin tai prosessorin jako. Asetuksella siis ilmoitetaan prioriteetti kyseiselle ryhmälle verkon käyttöön, eli kun verkko on kovassa rasituksessa ja resurssista on pulaa, palvellaan korkeimman ryhmän prioriteettia ensin. Arvot tämän asetuksen osalta menevät prioriteetin mukaisesti 25 - matala, 50 - normaali ja 100 - korkea. Arvon voi myös asettaa käsin yhden ja sadan väliltä. Toinen asetus (Host Limit) antaa mahdollisuuden määrittää tietty kapasiteetti, jonka ryhmä saa käyttöönsä. Tämä tarkoittaa, ettei ryhmä voi käyttää ulospäin suuntautuvaa kaistaa enempää kuin asetukseen on laitettu. Kolmas asetus on käyttää ryhmän ulospäin suuntautuvalla liikenteellä QoS prioriteettileimausta. Asetuksen yhteydessä tulee määrittää leimauksen arvo, joka liitetään jokaiseen tämän ryhmän lähettämään tietoliikennepakettiin. Verkkolaitteet, joille liikenne lähtee ESXi-palvelimelta, voivat soveltaa verkossa käytössä olevaa QoS-politiikkaa leimatulle liikenteelle ja näin voidaan varmentaa tiettyjen elementtien pääsy verkkoon ruuhkatilanteissa tavalla, jonka verkon fyysisetkin laitteet ymmärtävät. (Lowe 2011, 569-570, 572.)

8.5 Storage I/O Control

Storage I/O Control (SIOC), eli ohjain datavaraston I/O-toimintaan, tuli niin ikään vSphere version 4.1.0 mukana ja tuki alunperin vain Fibre Channel- ja iSCI-tekniikoita, mutta versio 5.0.0 toi lisäksi tuen NFS-tekniikalle. Monet toiminnot ESXi-palvelimien osalta vaativat kaikkien klusterissa olevien palvelimien pääsyn samaan jaettuun datavarastoon eli verkkokiintolevyjärjestelmään. Siinä missä esimerkiksi muisti tai prosessori ovat selkeästi ESXi-palvelimen hallittavissa, aiheutuu datavaraston hallitsemisessa haasteita, koska kyseinen varasto ei sijaitse fyysisesti minkään ESXi-palvelimen yhteydessä. SIOC-ohjaimen tehtävänä on kertoa kaikille klusterin alustoille eri virtuaalikoneiden jakoarvosta eli prioriteetista käyttää levyjärjestelmää. vCenter-palvelin pitää hallussaan tietokantaa levyjärjestelmien käytössä ja onkin näin ollen pakollinen komponentti SIOC-ohjaimen toiminnan kannalta. Toimivaa kokoonpanoa varten tarvitaan siis yksi vCenter-palvelin, joka hallitsee halutun klusterin osia ja tuettu VMFS-levyjärjestelmä, eli Fibre Cahnnel-, iSCSI- tai NFS-datavaraston. (Lowe 2011, 574.)

Kun SIOC on otettu käyttöön halutulle datavarastolle, voidaan siirtyä yksittäisten virtuaalikoneiden levynkäytön asetuksiin. SIOC antaa mahdollisuuden vaikuttaa kyseisen virtuaaliko-

neen jaon arvoon tai asettaa rajaksi haluttu I/O-toimintojen määrä sekunnissa (IOPS). Jaon arvon määrittely toimii tässäkin tapauksessa antamaan prosentuaalisen pääsyn levyjärjestelmään jaon arvon suhteessa kokonaisjakoon. Esimerkiksi kymmenen virtuaalikonetta, joilla kaikilla on sama arvo, saavat 10% käytön levyjärjestelmään ruuhkatilanteissa. IOPS-määrityksellä voidaan määrittää raja-arvo sille, kuinka monta input- sekä output-toimintoa kyseinen virtuaalikone voi suorittaa levyjärjestelmään sekunnissa. IOPS-määrityksen kanssa tulee olla tarkkana ja tietää mitä tehdä sitä säädettäessä, sillä väärin asetettuna arvo voi selvästi haitata virtuaalikoneen toimintaa. (Lowe 2011, 579-580.)

9 Resurssien käytön tasapainottaminen

VMware vSphere tarjoaa useita ominaisuuksia jakamaan työkuormaa useiden klusterin jäseninä toimivien ESXi-alustojen välillä. Näillä ominaisuuksilla pyritään tarjoamaan hyviä käytännönratkaisuja tilanteisiin, joissa tietty ESXi-alusta on selvästi suuremmassa rasituksessa tai fyysisten palvelimien huoltotilanteissa, joissa alusta tarvitsee sammuttaa ja palvelut siirtää toiselle alustalle. Tähän käyttöön suunnitellut ominaisuudet ovat: vMotion, vSphere DRS, Storage vMotion ja Storage DRS. (Lowe 2011, 585.)

Tässä vaiheessa on hyvä korostaa resurssien käyttö (utilization) ja niiden osoittaminen (allocation) määritetyille komponentille. Resurssin osoittaminen tietylle komponentille tarkoittaa konkreettisesti kakun palojen jakamista syöjien välille eli millaisia siivuja fyysisistä resursseista (CPU, muisti, I/O) annetaan tietylle tai usean virtuaalikoneen ryhmälle. Käyttö taas tarkoittaa syöjien tapaa kuluttaa heille annettu kakun pala eli kuinka kone hyödyntää sille osoitettuja resursseja. Resurssien osoittamiseen on käytössä luvussa 8 mainitut kolme tapaa eli varaus, rajoitus ja jakaminen, mutta näilläkin keinoilla on omat rajoitteensa. Tilanteessa, jossa toinen ESXi käyttää paljon resursseja ja toinen vähän resursseja, emme voi tasata tilannetta osoittamalla resursseja paremmin, sillä nämä kolme keinoa vaikuttivat vain resurssien osoittamiseen. Varsinainen resurssien käytön tasaaminen onkin mahdollista suorittaa seuraavilla VMware vSphere:n ominaisuuksilla:

- **vMotion** – Tunnetaan yleisemmin termillä live migraatio, eli virtuaalikoneen siirtäminen alustalta toiselle sen ollessa käynnissä ja käytettävissä siirron aikana. Tämä metodi auttaa manuaalisesti tasaamaan resurssien käyttöä.
- **vSphere Distributed Resource Scheduler** – vSphere DRS tarjoaa ominaisuutena automaattista resurssien käytön tasaamista usean ESXi-palvelimen välillä samassa klusterissa.

- **Storage vMotion** – Ominaisuutena toimii kuten vMotion, mutta toiminta kohdistuu manuaaliseen datavarastojen käytön tasaamiseen usean datavaraston välillä.
- **Storage DRS** – Automaattinen käytön tasaaja datavarastojen käyttöön.

(Lowe 2011, 585-586.)

9.1 vMotion

vMotion vaatii käyttöönottoa varten pakollisia ja huomioitavia ominaisuuksia. ESXi-alustat, joiden välillä halutaan ajaa vMotion live migraatiota, täytyvät olla yhdistettynä samaan jaettuun datavarastoon ja molemmissa live migraatioon osallistuvissa palvelimissa täytyy olla vähintään 1GBps nopeuteen pystyvä verkkokortti. Verkon osalta on lisäksi oltava VMkernel-portit, joissa on mahdollistettu vMotionin käyttö. On suositeltavaa omistaa täysin oma verkkokortti vMotionin ajamiselle, sillä liikenteen määrä on hetkellisesti hyvin suuri siirron aikana, mutta mikään ei estä jakamasta fyysistä siirtokapasiteettia muun liikenteen kanssa. Lisäksi vSwitch-konfiguraatioiden tuleet olla samanlaiset molemmilla alustoilla, sekä alustojen prosessorien tulisi olla saman valmistajan samaa tuoteryhmää. Siirtoa suunniteltaessa täytyy myös huomioida seuraava lista asioista:

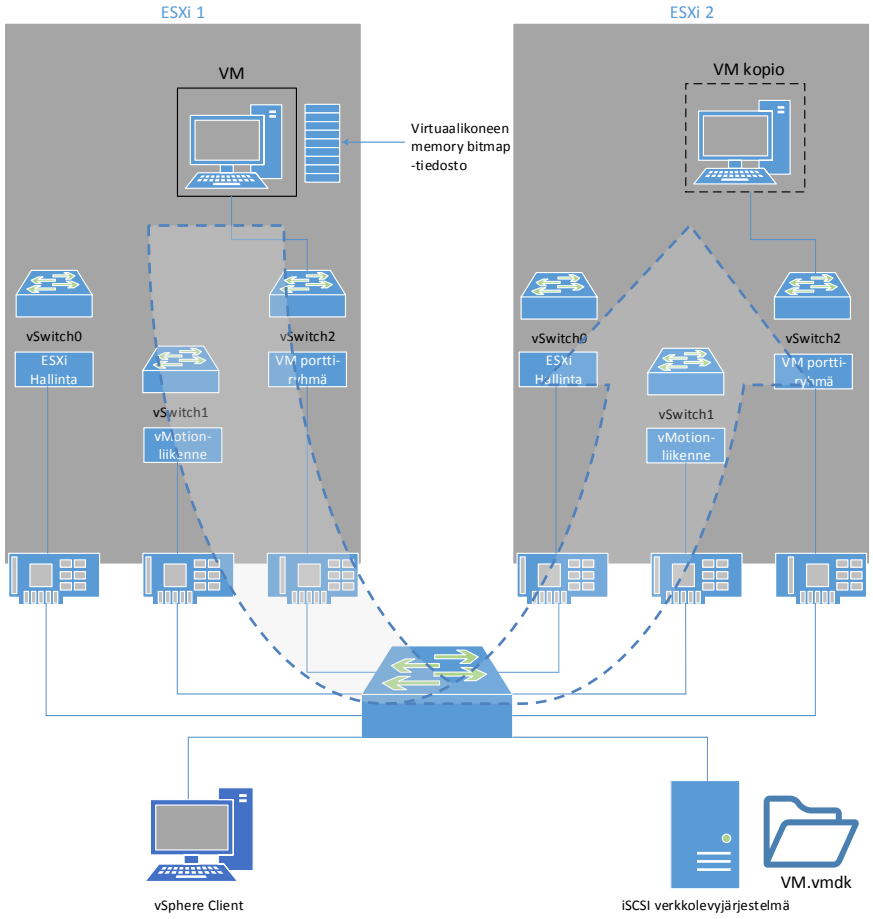
- Virtuaalikoneeseen ei saa olla yhdistettynä fyysisiä laitteita, jotka ovat olemassa vain tietyllä ESXi-palvelimella. Tällaisia fyysisiä laitteita ovat esimerkiksi suoraan virtuaalikoneeseen kytketyt kovalevy ja CD/DVD-asemat. Jos näitä laitteita on, täytyy ne irrottaa virtuaalikoneesta siirron ajaksi.
- Virtuaalikone ei saa olla kytkettynä vain ESXi-palvelimen sisällä liikennöivään kytkimeen eli niin sanottuun internal-only kytkimeen.
- Virtuaalikoneelle ei saa olla tehtynä CPU affinity määritystä.
- Virtuaalikoneen kaikki tiedot, konfiguraatiot, lokit ja NVRAM tiedostot täytyvät olla samalla jaetulla datavarastolla.

(Lowe 2011, 590-592.)

vMotion listattiin aikaisemmassa kappaleessa manuaaliseksi toimenpiteeksi vaikuttaa resurssien käytön tasaamiseen. Ominaisuudesta käytetään myös nimikettä live migraatio ja termiä tämä tarkoittaa ilman keskeytyksiä palvelun siirtämistä alustalta toiselle. Käytännössä virtuaalikone ei sammu siirron aikana, sille osoitettu verkkoliikenne ei katkea, sovellukset pysyvät käynnissä ja loppukäyttäjän näkökulmasta ei näy varsinaista katkosta palvelussa. Live migraatio siirtää varsinaisesti virtuaalikoneen suorituksessa olevat toiminnot sellaisenaan ja ottaa siirron kohteena olevalle alustalle samat resurssiosoitukset, jotka olivat alkuperäisellä

alustalla. Kuitenkin varsinainen virtuaalikoneen kiintolevy pysyy koskemattomana sen ollessa jaetulla verkkolevyjärjestelmällä tallessa. (Lowe 2011, 586.)

Varsinainen siirto voidaan kuvata kuusivaiheisena toimenpiteenä kahden ESXi-palvelimen välillä. Vaiheessa yksi pääkäyttäjä määrittää siirron tapahtuvaksi ESXi 1 -palvelimelta ESXi 2 -palvelimelle. Vaiheessa kaksi ESXi 1 -palvelin aloittaa kopioimaan aktiivisia muistisiivuja, jotka virtuaalikoneella on käytössään ESXi 2-palvelimelle. Toimintoa kutsutaan PreCopy-nimellä. Toiminnon aikana virtuaalikone palvelee edelleen asiakkaitaan ESXi 1-palvelimelta käsin. Muistin kopioimisen aikana muistisiivuihin tulevat muutokset kirjataan aktiiviseen ESXi-palvelimen ylläpitämään lokiin ja tästä lokista käytetään nimitystä memory bitmap. Lokiin kirjoittamista jatketaan, kunnes virtuaalikone on kokonaan siirretty toiselle palvelimelle. Kuviossa 14 on esimerkkiympäristön avulla toteutettu kuvio, jossa katkoviivalla rajattu virtuaalikone on kopioinnin määränpää. Liikenne, jolla VM-kone palvelee asiakkaitaan, kulkee edelleen ESXi 1-palvelimen vSwitch2 kautta, mutta vMotion-liikenne koneen kopioimiseksi kulkee vSwitch1 kautta.



Kuvio 14. vMotion-siirto ja siihen liittyviä komponentteja

Vaihe kolme alkaa kun koko RAM-muistin kaikki siivut on saatu siirrettyä toiselle alustalle. Tässä vaiheessa kone ei enää palvele asiakkaitaan näiden pyytäessä dataa. Vaiheen kolme päätteeksi VM memory bitmap -tiedosto, eli muuttuneet muistiosoitteet, siirretään toiselle alustalle. Neljännessä vaiheessa siirron kohteena oleva ESXi-palvelin lukee muuttuneet muistiosoitteet ja ottaa ne käyttöönsä. Viidennessä vaiheessa siirron kohteena oleva alusta käynnistää virtuaalikoneen. Kone ei käynnisty kokonaan alusta, vaan koneen suoritusta jatketaan kopioidusta tilasta. Lisäksi verkkoon lähetetään RARP-viesti (Reverse Address Resolution Protocol), jolla ilmoitetaan fyysiselle kytkimelle virtuaalikoneen uusi sijainti. Näin asiakasliikenne saadaan siirtymään fyysiseltä alustalta toiselle ja siirron kohteena oleva alusta on valmis virtuaalikoneen palveluiden osalta. Siirto on valmis ja kuudennessa vaiheessa alkuperäinen virtuaalikoneen suoritus poistetaan alkuperäiseltä alustalta. Paperilla siirron sanotaan olevan niin nopea, että mikäli virtuaalikonetta pommittaa PING-viesteillä, hukkaantuu siirron kiireisimmässä vaiheessa korkeintaan yksi paketti. Tämä yhden paketin hävikki on niin lyhyt, että suurin osa sovelluksista ei kärsi näin lyhyestä katkoksesta. Virtuaalikoneen kiintolevy on koko siirron ajan omalla iSCSI-palvelimellaan eli molempien ESXi-palvelimien jaetussa datavarastossa. (Lowe 2011, 586-589.)

9.2 vSphere Distributed Resource Scheduler

vSpheren automaattista kuormantasausta hoitaa siis ominaisuus nimeltään vSphere DRS eli Distributed Resource Scheduler. Ominaisuus hoitaa klusterin kuormantasausta pääasiassa kahden toiminnallisuuden avulla. DRS päättää, mille alustalle käynnistettävä virtuaalikone asetetaan toiminaan (intelligent placement) ja aktiivisesti arvioi klusterin kuormaa. Aktiivisen tarkkailun myötä toiminto ehdottaa pääkäyttäjälle tiettyjen virtuaalikoneiden siirtämistä toiselle alustalle tai automaattisesti ohjaa vMotion-toimintaa tasoittaakseen klusterin kuormaa. Oletuksena tämä aktiivinen tarkastelu tapahtuu viiden minuutin välein. Riippuen konfiguraatioista, voi DRS hoitaa myös uusien virtuaalikoneiden jakojen, varausten ja rajojen hallintaa. vShpere DRS vaatii vCenter-palvelimen toimiakseen. DRS voidaan asettaa toimimaan karkeasti sanottuna manuaalisesti, osittain automaattisesti tai täysin automaattisesti. Ominaisuuden toiminnallisuus on mahdollista määrittää manuaalisesti jokaisen virtuaalikoneen osalta erikseen. Näin voidaan ottaa esimerkiksi vSphere HA käyttöön koko klusterissa kaikkien koneiden osalta, mutta tietyiltä virtuaalikoneilta voidaan estää DRS toiminnallisuus. (Lowe 2011, 601-602.)

Manuaalisella asetuksella toimiva DRS kysyy käyttäjältään jokaisen virtuaalikoneen käynnistämisen yhteydessä fyysistä toiminta-alustaa VM-koneelle. Toiminto suosii vähemmällä käytöllä olevia ESXi-palvelimia, mutta käyttäjällä on viimekäden päätäntävalta. Lisäksi tilanteis-

sa, joissa klusterin kuorma on epätasainen, ilmoittaa DRS käyttäjälle sen ehdottamista vMotion live migraatioista. Siirtoja ei suoriteta ennen käyttäjän hyväksyntää. Osittain automatisoituna DRS sijoittaa käynnistetyt virtuaalikoneet itsenäisesti, mutta kysyy edelleen live migraatioista. Täysin automatisoituna DRS päättää itse käynnistettävien virtuaalikoneiden sijoittamisista ja live migraation käyttämisestä. Asetuksen toiminnallisuudesta voidaan vielä päättää erikseen eli asetuksen sisältä löytyy viisiportainen säätö konservatiivisesta aggressiiviseen. Konservatiivisin asetus automatisoi prioriteetin 1 toiminnallisuudet, mutta kysyy muuten päätökset käyttäjältä ja aggressiivinen ääripää automatisoi prioriteetit 1-5, eikä kysy käyttäjältä päätöksiä. Aggressiivinen asetus voi vaikuttaa myös huonolla tavalla klusterin toimintaan aiheuttamalla käyttöpiikkien perusteella jatkuvia muutoksia. DRS tulee ominaisuutena hyvin käytännölliseksi esimerkiksi huoltotöiden yhteydessä. ESXi-palvelin, joka asetetaan huoltotilaan, tekee automaattisesti 1 prioriteetin ehdotukset virtuaalikoneiden siirtämiseksi toiselle alustalle DRS-ominaisuuden ansiosta. (Lowe 2011, 602-604.)

Klusterissa tapahtuvaa kuormantasausta voidaan siis hienosäätää automaation perusteella, mutta myös erillisten DRS-sääntöjen avulla. Sääntöjä löytyy kaiken kaikkiaan kolme erilaista ja niillä voidaan määrittää tietyt koneet kuulumaan samaan ryhmään keskenään (VM affinity), tiettyjen virtuaalikoneiden erottaminen (VM anti-affinity) tai niiden suhteet fyysiseen ESXi-alustaan (Host affinity). Näiden sääntöjen rikkominen on toinen tavoista, joilla syntyy prioriteetin 1 suositus ja toinen on aikaisemmin mainittu huoltotilan asettaminen. (Lowe 2011, 605.)

Sääntöjen avulla voidaan määrittää riippuvuuksia virtuaalikoneiden välille, joille halutaan taata esimerkiksi nopea tiedonsiirto ESXi-palvelimen oman nopean sisäisen väylän avulla. Tällainen tilanne voi olla kyseessä esimerkiksi verkkosivuja ylläpitämän palvelimen ja tietokantapalvelimen tarpeesta kommunikoida mahdollisimman pienellä vasteella toistensa kanssa. Toisin sanoen nämä virtuaalikoneet halutaan pitää aina yhdessä VM affinity-säännöllä. VM anti-affinity-sääntö on käytännöllinen esimerkiksi tilanteessa, jossa sähköpostipalvelut on kahdennettu usealle palvelimelle. Nämä yksittäiset virtuaalikoneet halutaan kaikissa tilanteissa pitää erillisillä alustoilla, ettei fyysinen laiterikko estä koko palvelun käyttöä. Host affinity-säännöllä voidaan määrittää, mitkä fyysiset alustat voivat ylläpitää tiettyjä virtuaalikoneita. Eli kun kriittisintä palvelua tuottavaa virtuaalikonetta ei missään tilanteessa haluta pyörimään klusterin heikoimmalle koneelle, voidaan tilanne turvata tällä säännöllä. Sääntö saattaa aiheuttaa ristiriitoja esimerkiksi vSphere HA-ominaisuuksien kanssa, mikäli ominaisuuden suorittama siirto ei olisikaan mahdollista Host affinity-säännön perusteella. (Lowe 2011, 605-609.)

9.3 Storage vMotion

vMotion-ominaisuuden avulla voidaan siis siirtää virtuaalikoneen suorituksessa oleva muisti ja prosessointi käynnissä olevasta virtuaalikoneesta fyysiseltä alustalta toiselle aiheuttamatta varsinaista käyttökatkoa virtuaalikoneen toiminnassa. Storage vMotion toimii samalla ideologialla, mutta tällä kertaa siirron kohteena toimii virtuaalikoneen virtuaalinen kovalevy koneen ollessa käynnissä. Ominaisuudella voidaan auttaa datavarastoina toimivien verkkolevyjärjestelmien rasitusta ja tasata fyysisten kiintolevyjen käyttöä datavarastojen välillä. Myös tämä vMotion toiminnallisuus suoriutuu kuudessa vaiheessa. (Lowe 2011, 612.)

Vaiheessa yksi kopioidaan pysyvät tiedostot, joista virtuaalikone muodostuu. Näitä tiedostoja ovat esimerkiksi virtuaalikoneen konfiguraatiotiedosto (VMX), VMkernelin swap-tiedosto, lokit sekä snapshot-kaappaukset. Vaiheessa kaksi vSphere aloittaa aaveeksi tai varjoksi kutsutun virtuaalilevynsiirron kohteena olevalla datavarastolla. Tämä ei siis ole vielä varsinainen virtuaalilevy, joten luomisen jälkeen varjolevy jää odottamaan seuraavia toimenpiteitä. Vaiheessa kolme luodaan varsinainen määränpäälevy. Tämän jälkeen virtuaalikoneen ja taustalla olevan varaston välille asetetaan oma I/O-laite, joka peilaa muutokset uudelle virtuaalilevylle. Vaiheessa neljä aloitetaan levyjen kopiointi eli ne peilataan edellisessä vaiheessa asetetun I/O-laitteen avulla siirron määränpäänä toimivalle datavarastojärjestelmälle. Vaiheessa viisi kopiointi on saatu valmiiksi ja vSphere hetkellisesti pysäyttää virtuaalikoneen ja heti tämän jälkeen jatkaa virtuaalikoneen suorittamista. Tämän nopean pysäytyksen aikana virtuaalikoneen levyn hallinta asetetaan varjolevylle, jolloin siitä tulee virtuaalikoneen pääasiallinen virtuaalilevy. Katkos on niin nopea, ettei se varsinaisesti näy konetta käyttäville. Vaiheessa kuusi vanha virtuaalilevy poistetaan alkuperäiseltä datavarastolta. Mikäli siirrossa tapahtuu virhe, ei vSphere poista vanhaa virtuaalilevyä ennen kuin virhe on ratkaistu ja siirto suoritettu onnistuneesti loppuun. Tällä toiminnallisuudella estetään tietojen häviäminen siirron seurauksena. (Lowe 2011, 612-613.)

9.4 Storage DRS

SDRS (Storage Distributed Resource Scheduler) toimii myös kuten aiemmin mainittu kuorman tasapainottaminen klusterissa, mutta nyt kohteena on levynkäytön tasapainottaminen verkkolevyjärjestelmien välillä automatisoituna. Toiminto puuttuu levyille tallentamiseen levyjen käytön osalta, mutta osaa myös toimia I/O-toimintojen tasapainottamisessa. Toiminnallisuuden automatisoinnin määrää voidaan määrittää asetuksilla ja tarkentaa affinity ja anti-affinity säännöksillä, mutta pääpiirteissään ominaisuudella tuotetaan varastointiklusteri. Kaikki verkkotallennuslaitteet määritetään kuuluvaksi samaan klusteriin ja niiden toiminnallisuus muuttuu niin kuin käytössä olisi vain yksi tallennusmedia. Klusterin käytössä pitää huo-

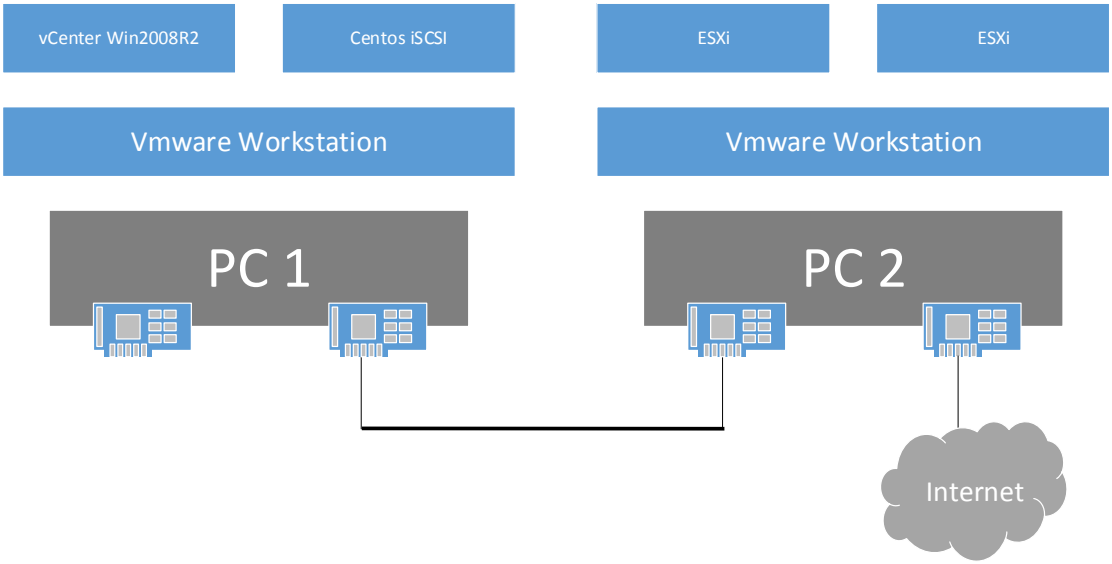
mioida, ettei kahdennettuja ja ei-kahdennettuja varastoja voi yhdistellä keskenään. Yhtälailla NFS- ja VMFS-datavarastoja ei voi käyttää samassa klusterissa, eikä sama dataklusteri voi olla usealla datakeskuksella käytössä. Luomiseen ei vaikuta esimerkiksi mikäli varastot eroavat toisistaan I/O-toiminnallisuuden, kapasiteetin tai valmistajan välillä. (Lowe 2011, 614-615.)

Dataklusterin asetuksista voidaan puuttua SDRS-toimminnallisuuteen. Automaation tasoissa SDRS on hyvin kaksijakoinen, sillä klusteri voidaan asettaa soveltamaan kuormanjakoa joko automaattisesti tai ilman automaatioita, sekä määrittää esimerkiksi ajastus jommalle kummalle toiminnallisuudelle. Automaattisesti toimiva SDRS ehdottaa käyttäjälle tapoja suorittaa halutut toimenpiteet eli esimerkiksi uuden virtuaalikovalevyn luomisen yhteydessä. SDRS esittää ehdotelmansa levyn sijoituspaikasta, sekä kysyy käyttäjältä mikäli levyjen kuormitusta voitaisiin järkevästi tasata Storage vMotion -ominaisuudella. Automaattisesti toimivan kuormantasaajan aggressiivisuutta voidaan myös tarkentaa kuten vSphere DRS -ominaisuuden tapauksessa. Asetuksissa voidaan määrittää myös halutaanko kuormantasauksella vaikuttaa levyn- vai I/O-käyttöön. Ominaisuuksia on myös mahdollista edelleen hienosäätää. SDRS-säännöillä voidaan määrittää haluttujen levyjen yhteenkuuluvuutta tai erottaminen kuten aiemmin mainittiin. Asetuksissa ei voi määrittää suositeltua datavarastoa, mutta asetuksilla voi mahdollistaa, että saman virtuaalikoneen levyt pidetään aina yhdessä, vaikka niitä siirrettäisiin datavarastojen välillä. (Lowe 2011, 619, 620, 622, 623, 625, 627.)

10 Ympäristön pystytys

Kirjoittamisen lomassa suoritettiin käytännön kokeiluja yhdellä fyysisellä tietokoneella virtualisoituna. Hyvin nopeasti kävi kuitenkin ilmi, että yhden työaseman muisti ei millään riitä kokonaisuuden koeistamiseen ja lopulta opinnäytetyön tilaajan kanssa käydyn palaverin jälkeen päätettiin toteuttaa käytännönosuus kahdella fyysisellä työasemalla. Tätä mallia olisi myös helppo käyttää kursseilla, joilla työn materiaalia käytettäisiin.

Tilaajan puolesta käyttöön annettiin kaksi 64-bittistä Windows 7 -työasemaa, joissa molemmissa oli kaksi gigabitin verkkokorttia, 12Gt RAM-muistia ja Intelin Core i7 920 -prosessori. Kokeiluvedoksen perusteella vCenter-palvelin ja levyjärjestelmä virtualisoitaisiin toisella koneella ja ESXi-palvelimet toisella työasemalla. Työasemat kytkettäisiin toisiinsa verkkokaapelilla, jättäen toisen verkkokortin hoitamaan muuta verkkoliikennettä. Alla yksinkertainen ympäristön suunnittelukuva kuviona 15.



Kuvio 15. Suunnittelukuvio testiympäristöstä

Virtuaalikoneet päätettiin hajauttaa kuvion esittämällä tavalla, jotta työasemien muisti riittäisi ylläpitämään kaikkia palveluita. Alustavissa kokeiluissa vCenter-palvelin otti käyttöönsä niin paljon muistia kuin koneella vain kehtasi antaa. vCenter-paketin asennus vaatii koneelta 4 GB RAM-muistia, mutta tuolla määrällä muistin käyttö oli lähes maksimissa koneen ollessa lähes jouten. Tämä näkyi ajoittaisena hidasteluna ja jopa 6 GB RAM-muistilla päästiin muistinkäytössä lähelle sataa prosenttia. Tosin tällä nostetulla muistinmäärällä päästiin eroon ajoittaisista hidasteluista, joten 6 GB päätettiin jättää varsinaiseen ympäristöön vCenter-palvelimen muistin määräksi. Samalle työasemalle haluttiin myös sijoittaa iSCSI-palvelin, koska kyseinen palvelin ei vaadi liikoja resursseja. Näin luotiin tasapainoa virtualisoinnin kannalta.

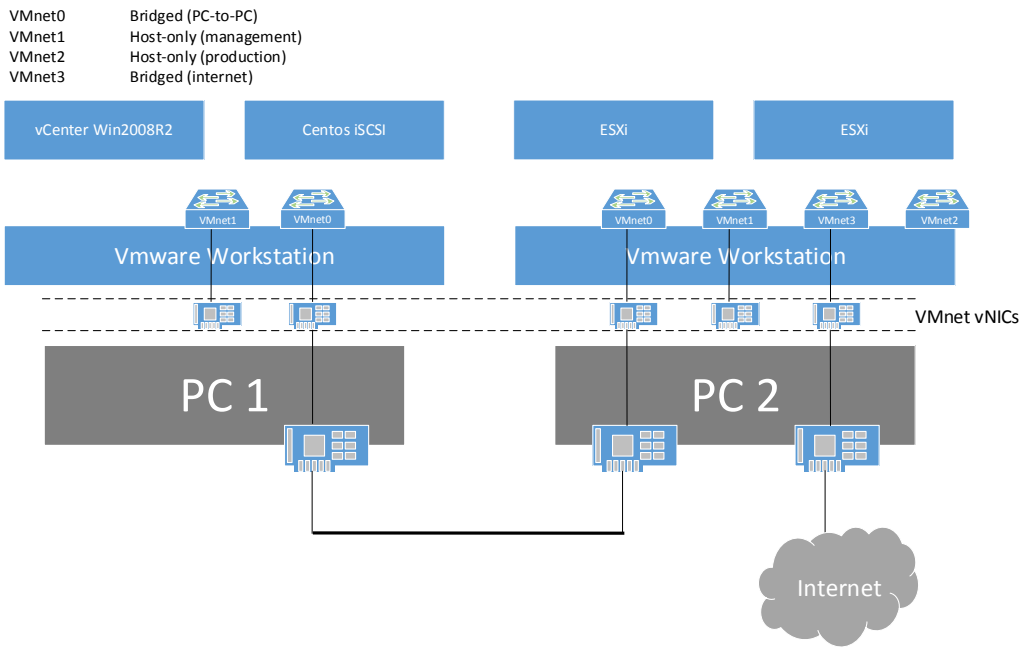
10.1 VMware ja Workstation

VMware luottaa ihmisten haluun päästä itse kokeilemaan työkaluja ennen niiden ostamista ja sen vuoksi tarjoaa kokeilulisenssejä eli 30-/60-vuorokauden evaluation-linsenssejä halukkaille. Halukkaalta riittää yksinkertainen rekisteröinti sähköpostiosoitteen kera, jonka jälkeen oman VMware-tilin turvin voi ladata haluamistaan ohjelmista kokeiluversiot ja tarvittaessa aktivoida ne saadulla evaluation-linsessinumerolla. Tarvittaessa kuka tahansa voi aloittaa kokeilut tässä opinnäytetyössä testatuilla VMwaren tuotteilla. Tätä opinnäytetyötä tehtäessä käytettiin oppilaitoksen omaa linsenssiä VMwaren Worsktation 9 -ohjelmistosta. VMware vSphere -tuotteet otettiin käyttöön mainitulla evaluation-lisenssillä.

Asentaminen vaatii tietysti aina pääkäyttäjän oikeudet työasemaan, mutta myös VMware Workstation -ohjelman network editor-ominaisuuden käyttö antaa ruudulle Windowsin UAC-

ilmoitusviesti. Oppilaitoksen AD-ympäristössä tämä tarkoittaa sitä, etteivät normaaleina käyttäjinä olevat opiskelijat pääse itsenäisesti vaikuttamaan Workstationin VMNet-rajapintoihin, vaan järjestelmävalvojien tulee asettaa ne ennakkoon. Valmiiksi luotujen rajapintojen ominaisuuksien muuttamiseen riittää tietyiltä osin oikeudet myös opiskelijatunnuksilla.

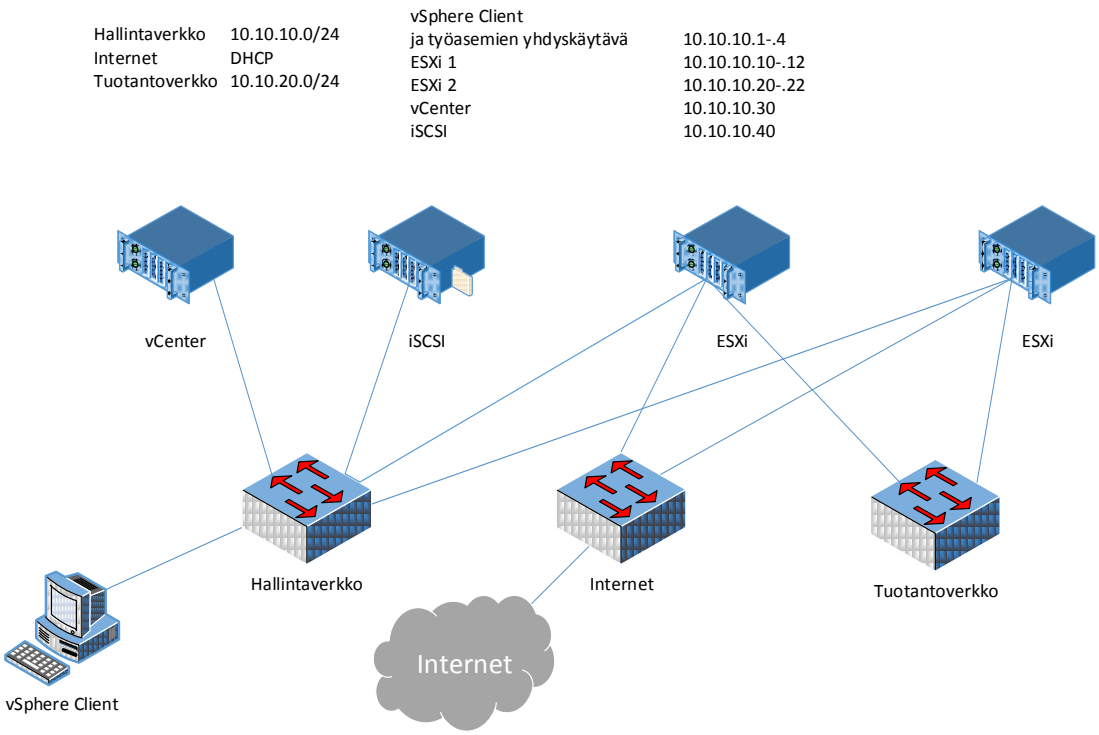
Workstationin osalta työskentely alkoi tarvittavien verkkorajapintojen luomisella. Oleelliseksi kohdaksi topologiamietinnässä muodostuikin työasemia yhdistävä verkkorajapinta. Kyseisen gigabitin ethernet-väylän läpi kulkisi kaikki vCenter-palvelimelta tulevat käskyt ja muu kanssakäyminen ESXi-palvelimien kanssa, mutta myös ESXi-palvelimien ja iSCSI-levyjärjestelmän välinen liikenne. Tätä liikennöintiä varten molempiin Workstation-ohjelmiin luotiin VMNet, joka asetettiin siltaamaan liikenne työasemien kakkosverkkokortteihin. vCenter-palvelimen käyttäminen vaatii lisäksi VMware vSphere Client-ohjelman, joten yhteydellisyys virtualisointikerroksen ja fyysisen verkkokerroksen väliin piti myös järjestää. Tätä varten luotiin erillinen sisäinen VMNet, jolle annettiin työasemien verkkosovittimien asetusten kautta hallintaverkon IP-osoitteet. Tätä VMNet-rajapintaa käytettiin lisäksi muodostamaan suora verkkoyhteys ESXi-palvelimien välille. Näillä toimenpiteillä hallintaverkon perusteet saatiin valmiiksi. Hallintaverkon lisäksi luotiin vielä PC2-työasemalle sisäinen VMNet ESXi-alustoilla pyörivien virtuaalikoneiden välisiä yhteyksiä varten, sekä yksi sillattu VMNet, jolla saataisiin tarvittaessa käytettyä työasemille osoitettua verkkoyhteyttä myös virtualisointikerroksilla. Tätä verkkojärjestelyä on kuvattu kuviossa 16.



Kuvio 16. VMware Workstation -ohjelman verkkorajapinnat

10.2 IP-verkko-osoitteiden suunnittelu

Osoitesuunnittelu pidettiin hyvin yksinkertaisena ja käyttöön otettiin A-luokan 10.0.0.0/8 osoitelohkosta kaksi C-luokan osoitelohkoa. 10.10.10.0/24-lohko osoitettiin hallintaverkolle ja siihen liittyviin verkkokomponentteihin. Hallinnointiliikenteen lisäksi tähän osoitelohkoon liitettiin lisäksi iSCSI-levyjärjestelmän liikenne. Toinen lohko 10.10.20.0/24 osoitettiin ESXi-palvelimien virtuaalikoneiden keskinäistä liikennöintiä varten eli niin sanottu tuotantoverkko. Tätä verkkoa varten Workstationin sisällä asetettiin käyttöön DCHP-asetus, jotta koneet saisivat osoitteen tarvittaessa myös itse. Kuviossa 17 on yksinkertaistettu topologiakuva verkon rakenteesta ja osoitteistuksesta.



Kuvio 17. Verkon fyysinen topologiarakenne ja osoitteistus

10.3 Järjestelmävaatimukset

Ennen ohjelmistojen asentamista VMware Workstationin päälle, täytyy varmistua, että pystymme ylipäätään virtualisoimaan haluttuja ohjelmia. VMwaren verkkosivuilta löytyykin listaus ESXi 5.1-ohjelmiston vähimmäisvaatimuksista. Prosessorin osalta suurin kompastuskivi voi olla prosessorin bittisyys, sillä ESXi asentuu vain 64-bittiselle alustalle, jolla on vähintään kaksi loogista prosessoria. Tämän lisäksi prosessorin tulisi tukea rautavirtualisointia (Intel VT-x tai AMD RVI). Muistin osalta vähimmäismuistin määrä on 2GB RAM-muistia, mutta dokumentoinnissa ehdotetaan vähintään 8 GB RAM-muistia, jotta kaikista ominaisuuksista saataisiin suurin hyöty. Verkkoon liittymisen kannalta vähimmäisvaatimukset haluavat yhden tai

useamman Gigabitin tai 10Gb verkkokortin. Lisäksi tarvitaan vielä joko paikallinen levy, jolle järjestelmä asennetaan, tai verkkolevyjärjestelmä. (Minimum system requirements for installing ESXi/ESX (1003661) 2013.)

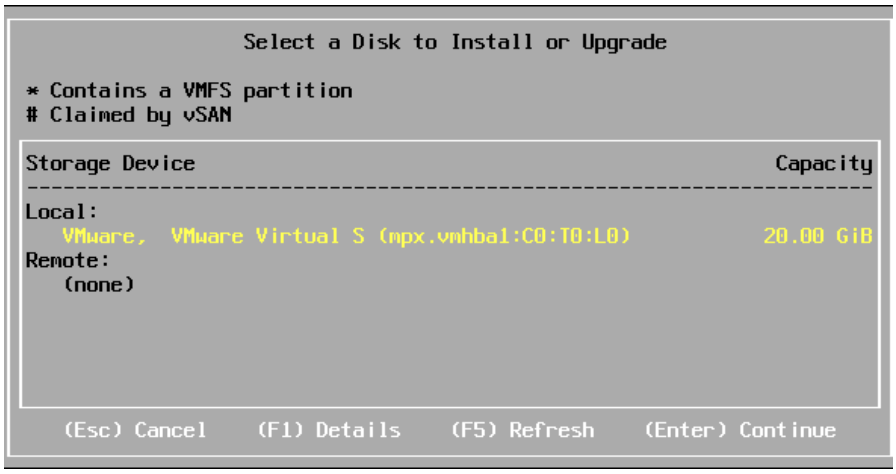
VMware vCenter -palvelin voidaan asentaa joko fyysisenä koneena tai virtualisoituna. Windows-tuen lisäksi vCenter-palvelimesta löytyy myös siis valmis Linux-jakelu. Versiosta riippumatta palvelimelle halutaan vähintään kahden loogisen prosessorin suoritin, joka on nopeudeltaan vähintään 2GHz. RAM-muistia palvelin vaatii vähintään 4GB. Muistintarve kasvaa vielä entisestään, mikäli vCenterin tarvitsema tietokanta asennetaan samalle koneelle. Lisäksi, koska palvelin on niin kriittisessä asemassa koko klusterin toimintaan nähden, halutaan verkkokortin olevan vähintään gigabitin verkkorajapinta. vCenter Simple Sign-On -asennus tarjoaa tietokannan asennuksen palvelinohjelman asennuksen yhteydessä ja oletukseltaan se on Microsof SQL Server 2008 R2 Express. Mikäli halutaan käyttää jotain toista tietokantaa, voi yhteensopivuuden selvittää VMwaren verkkosivuilta. Uusimman 5.x-version asennus vaatii, että alustana oleva järjestelmä on 64-bittinen. (Minimum system requirements for installing VMware vCenter Server (1003882) 2013.)

Molemmat aiemmin mainituista tuotteista vaativat useita loogisia prosessoreita toimiakseen. Loogisen prosessorin voi helposti mieltää, että koneessa pitäisi olla kaksi tai useampi fyysinen prosessori, mutta näin ei onneksi tarvitse olla. VMware määrittää Workstation-ohjelmansa dokumentaatiossa, että usean loogisen prosessorin voi saavuttaa joko yksittäisellä prosessorilla, jolla on hyperthreading-ominaisuus käytettävissä tai usealla ytimellä varustetulla prosessorilla. Lisäksi tilanne missä käytössä on todellakin kaksi fyysistä prosessoria kelpaa tähän käyttöön ilman useaa ydintä tai hyperthreading-ominaisuuttakin. (Selecting the Number of Processors for a Virtual Machine, 2012) Koska ESXi sekä vCenter asennetaan Workstationin päälle, täytyy prosessorituessa katsoa pakan alinta prosessoria eli työasemilla olevaa fyysistä prosessoria. Tässä tapauksessa työasemat on varustettu Intelin Core i7-920 prosessorilla, josta löytyy hyperthreading-ominaisuus sekä neljä ydintä. Käytännössä tämä tarkoittaa kahdeksalla loogisella prosessorilla varustettua suoritinta, koska hyperthreading ominaisuutena mahdollistaa kahden suoritteen ajamisen yhdessä ytimessä. Lisäksi prosessori tukee Intelin virtualisointitekniikkaa (Intel VT-x) sekä edistyneempää Intel VT-x with ETP (Extended Page Tables). Näillä ominaisuuksilla on hyvä jatkaa. (Intel Core i7-920 Processor 2013.)

10.4 ESXi-palvelimien asennus

Palvelimien asennus alkoi määrittämällä virtuaalikoneiden laitteisto Workstation-ohjelmassa. Jotta palvelimissa olisi edes vähän potkua, määritettiin molemmille palvelimille kaksi suoritita neljällä ytimellä ja 5GB RAM-muistia. Muistin määrä määriteltiin sillä perustein, että työasemien muistin ollessa 12GB, jäisi varsinaiselle käyttöjärjestelmälle 2-3GB, vaikka molemmat ESXi-palvelimet olisivat muistinkäyttönsä äärirajoilla. Laskentaa sekoitti entisestään Workstationin ominaisuus, joka ei millään olisi halunnut antaa virtuaalikoneille enempää kuin 9GB RAM-muistia käyttöön fyysisen käyttöjärjestelmän toimintojen turvaamiseksi. Paikallinen kovalevy voitiin jättää hyvin pieneksi, sillä varsinainen asennettu ESXi-palvelin vie levytilaa vain 5,2GB VMFS osion kanssa, josta 1 GB on varsinaista asennusta ja 4 GB VMFS levytilaa varten. Ennen asennusta on vielä asetettava vähintään yksi verkkokortti tälle virtuaalikoneelle tai muuten asennus keskeytyy verkkoasetuksia tarkastellessa.

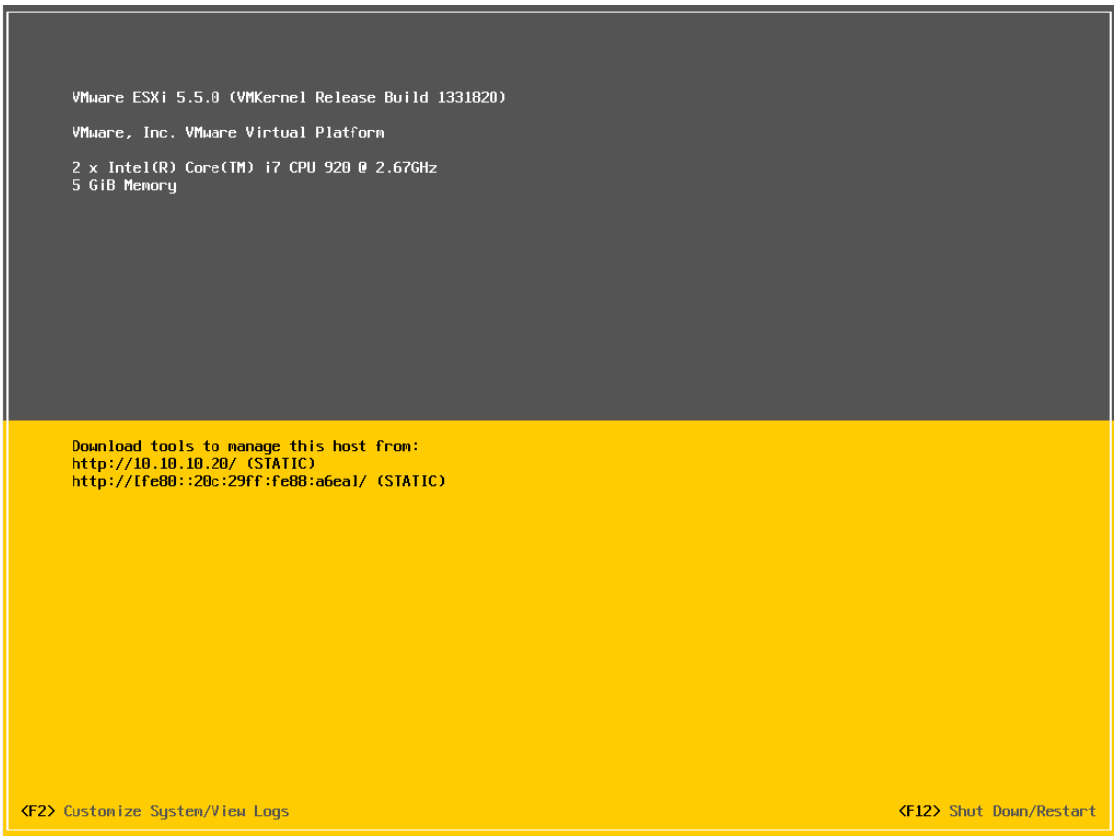
Varsinainen asennus on hyvin yksinkertainen. Tässä tapauksessa virtuaaliseen CD/DVD-asemaan asetettiin asennustiedosto, jolta järjestelmä asetettiin käynnistymään virtuaalikoneen virtoihin laittamisen jälkeen. Asennuksen kulku on pitkälti lyhyiden ohjeruutujen lukemista ja seuraava-funktiolla olevien näppäinten painamisia. Kuviossa 18 on esimerkiksi kuvankaappaus asennusmedian valitsemisesta.



Kuvio 18. Asennuksessa voi valita paikallisen tai ulkoisen levyn asennukselle

Asennuksessa hyväksytetään ehdot, valitaan asennusmedia, valitaan näppäimistön kieliasetukset, asetetaan pääkäyttäjän salasana, skannataan järjestelmä yhteensopivuusongelmien löytämiseksi (puuttuva verkkokortti keskeyttää asennuksen tässä vaiheessa), kysytään käyttäjältä varmistus asennuksesta ja suoritetaan virallinen asennus. Asennus itsessään ei tee varsinaisia määrityksiä itse, vaan esimerkiksi hallintaosoitteet asetetaan vasta asennuksen jälkeen. Asennus loppuu ruutuun, jossa pyydetään poistamaan asennusmedia koneesta en-

nen uudelleenkäynnistystä. Järjestelmän latautumisen jälkeen aukeaa käyttäjälle hyvin pelkistetty DCUI (Direct Console User Interface), josta kuvankaappaus kuviossa 19.

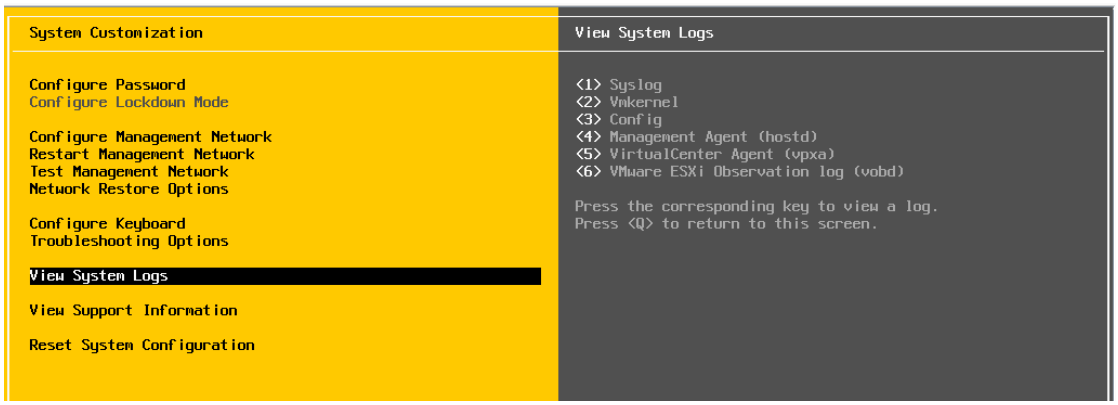


Kuvio 19. ESXi-palvelimen oma graafinen käyttöliittymä ja sen aloitusnäkymä

DCUI aloitusnäkymästä näkee prosessori- ja muistitietojen lisäksi verkosta saadun IP-osoitteen. Kuvion 19 tapauksessa palvelin on saanut IPv4-osoitteen manuaalisen konfiguroinnin avulla ja sen lisäksi palvelin on itse määritellyt staattisen IPv6-osoitteen hallinnan muodostamista varten. Kumpikin näistä osoitteista kelpaa hallintayhteyden muodostamiseksi.

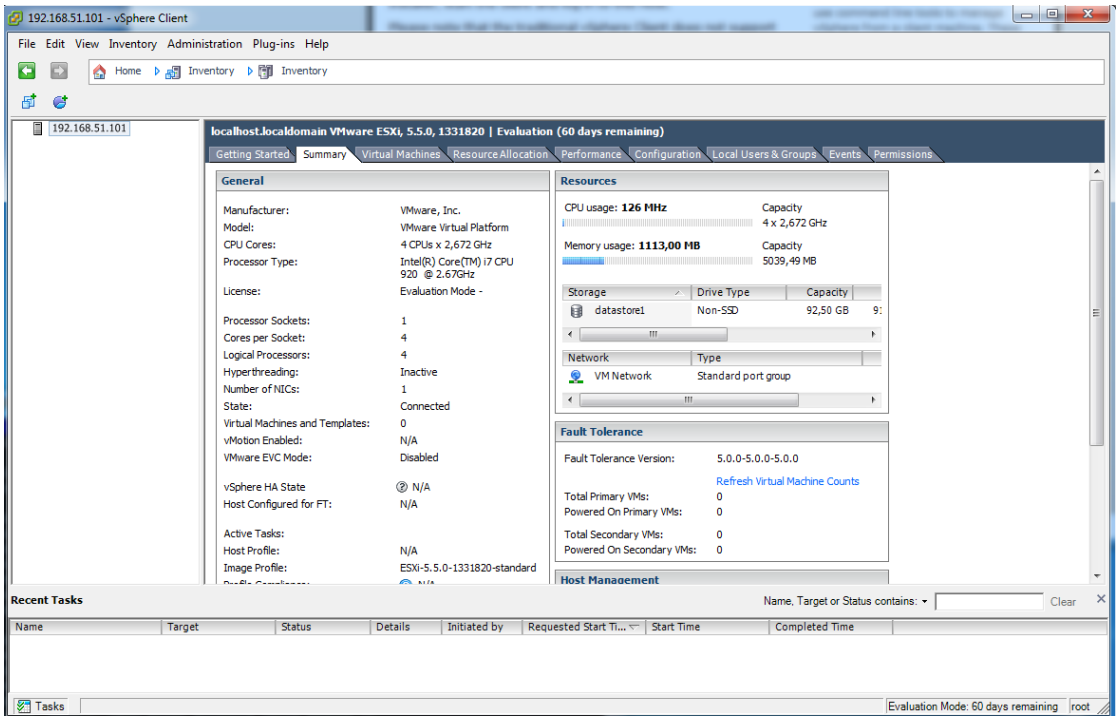
IPv4-osoitte täytyy määrittää käsin. Tätä varten tulee mennä System Customize -näkymään, joka on esitetty kuvankaappauksena kuviossa 20. Kohdan Configure Management Network kautta voidaan manuaalisesti määrittää käytettävät verkkokortit ja hallintaverkon osalla osoitteet, maskit, yhdyskäytäväosoitteen sekä DNS-palvelimien osoitteistuksen. Tässä vaiheessa on hyvä muistaa, että edes staattinen IP-osoite ei ole fyysiselle rajapinnalle tuleva IP-osoite. Asennuksessa palvelin luo oletuksena yhden virtuaalikytkimen (vSwitch0), johon kytkettyyn VMkernel-porttiin asetetaan tämä hallinnointiosoite. Joka tapauksessa tätä hallinnointiosoitetta käytetään myöhemmin palvelimen hallintaan ja liittämiseen osaksi klusteria. Samassa verkossa olevalta tietokoneelta voi internet-selaimen kautta yhdistää tähän osoit-

teeseen joko ladatakseen VMware vSphere Client-ohjelman tai aloittaa verkkosivupohjaisen hallinnoinnin käytön.



Kuvio 20. ESXi-palvelimen asetusvalikko on myös hyvin yksinkertaistettu

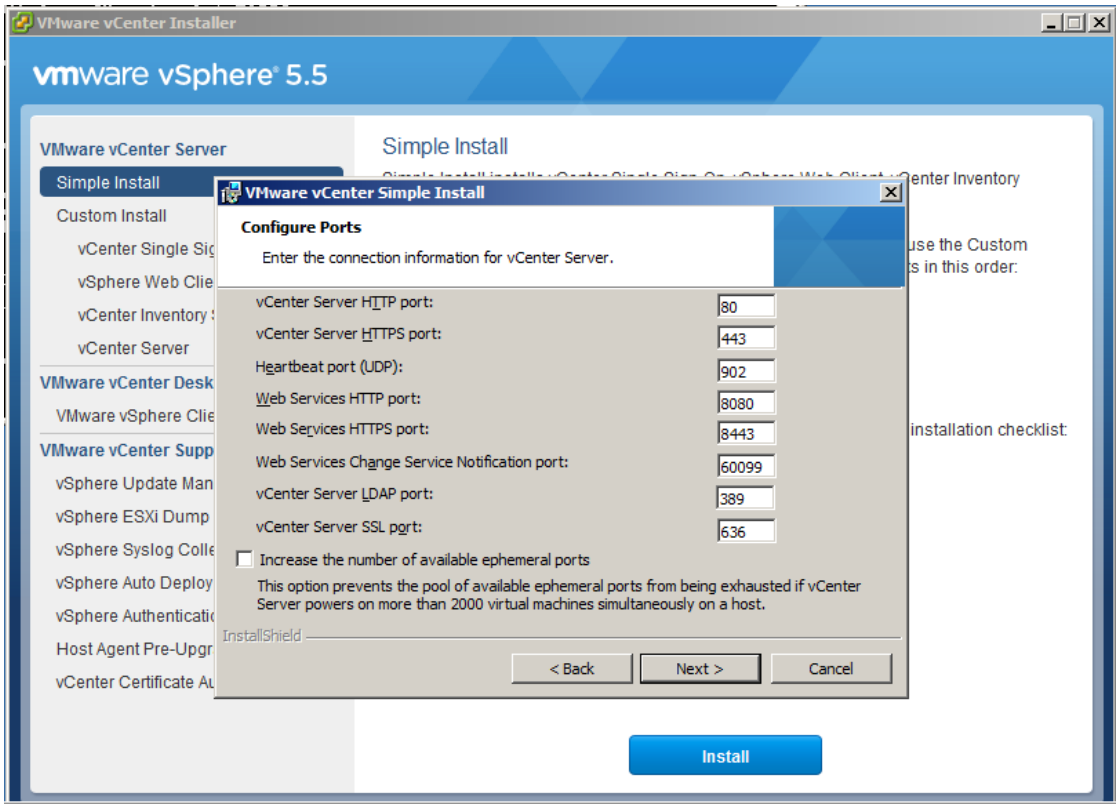
Verkkosivupohjaisen käyttöliittymän ollessa osaltaan riisutumpi versio, päädyttiin käyttämään tarkoitusta varten tehtyä vSphere Client -ohjelmaa. Kuviossa 21 on kuvankaappaus vSphere Client -ohjelman aloitusnäkymästä ESXi-palvelimeen yhdistämisen jälkeen. Kuvankaappauksen tapauksessa virallista hallintaosoitetta ei ole vielä määritelty.



Kuvio 21. Hallintayhteys tyhjään ESXi-palvelimeen

10.5 vCenter-palvelimen asennus

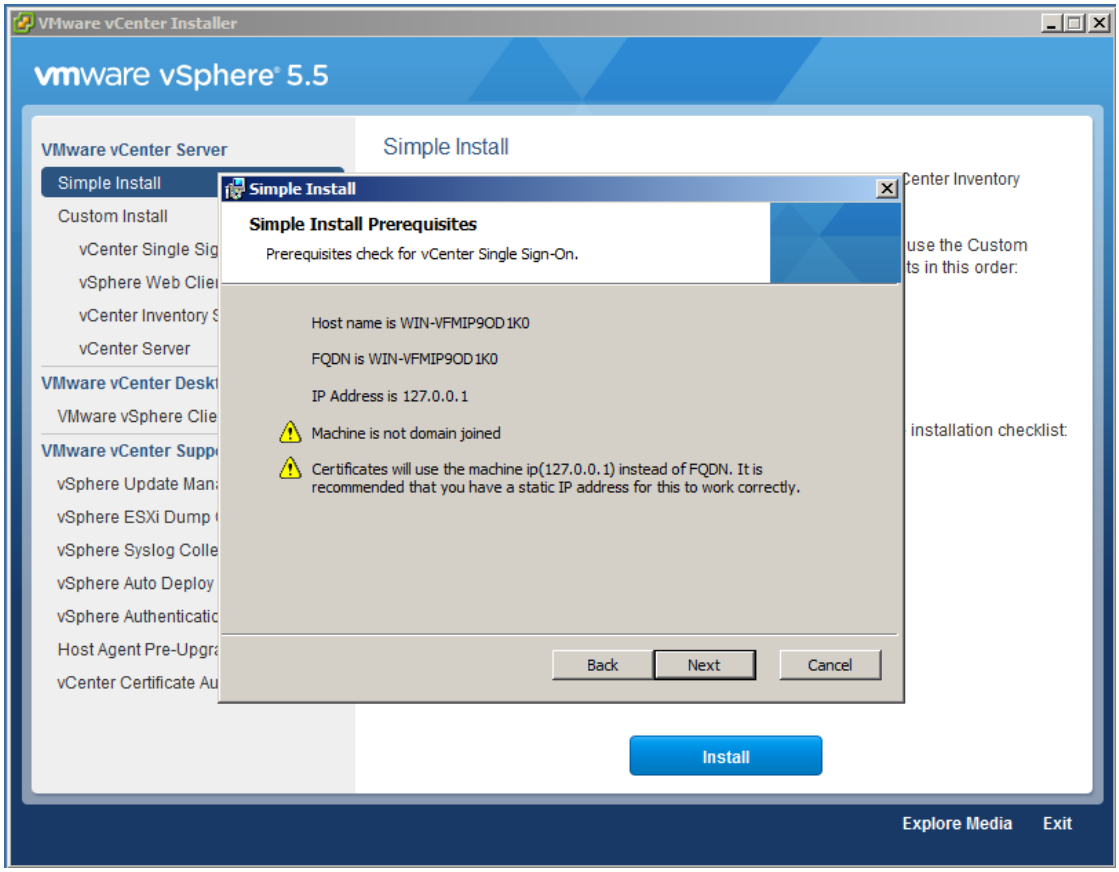
vCenter-palvelimen alustaksi valittiin Windows 2008 R2 Server -käyttöjärjestelmä laajemman ominaisuustuen ansioista. Palvelin asennettiin oppilaitoksen lisenssillä, eikä siihen tehty mitään asetuksia tai muutoksia ennen vCenter-palvelun asentamista. Windows-palvelin tarvitsee useaa lisäosaa, jotta vCenter-ominaisuus voidaan asentaa. Näitä ovat jo useaan kertaan mainittu SQL-tietokanta, mutta esimerkiksi myös .NET Framework -lisäosa. Lisäosat voidaan asentaa toki erikseen ja konfiguroida käsin, mutta koko paketti kaikkinensa on mahdollista asentaa kerralla niin kutsutun Simple Sign-On -paketin asennuksella. Tietyllä tapaa Single Sign-On on suositeltavampi, koska normaalisti esimerkiksi .NET Framework -lisäosan asennus asentaa myös IIS-verkkosivupalvelimen. Tämä ottaa käyttöön palvelimen portin numero 80, jonka myös vCenter haluaisi oletuksena itselleen http-liikennettä varten. Kuviossa 22 onkin asennusvaiheesta otettu kuvankaappaus, jossa näkyy vCenter-palvelimen haluamat oletusportit.



Kuvio 22. vCenter-palvelimen oletusportit

Varsinaisen asennuksen alussa käy erittäin nopeasti ilmi, että vCenter haluaisi kaverikseen jo konfiguroidun Microsoft Windows AD -ympäristön DNS- ja FQDN-palveluilla. Tätä kautta esimerkiksi hallinnointiin käytettävät tunnukset tulisivat suoraan AD-asetusten ryhmä- ja käyttäjähallinnoinnista. AD-ympäristön pystyttämisellä ei kuitenkaan nähty varsinaista lisäar-

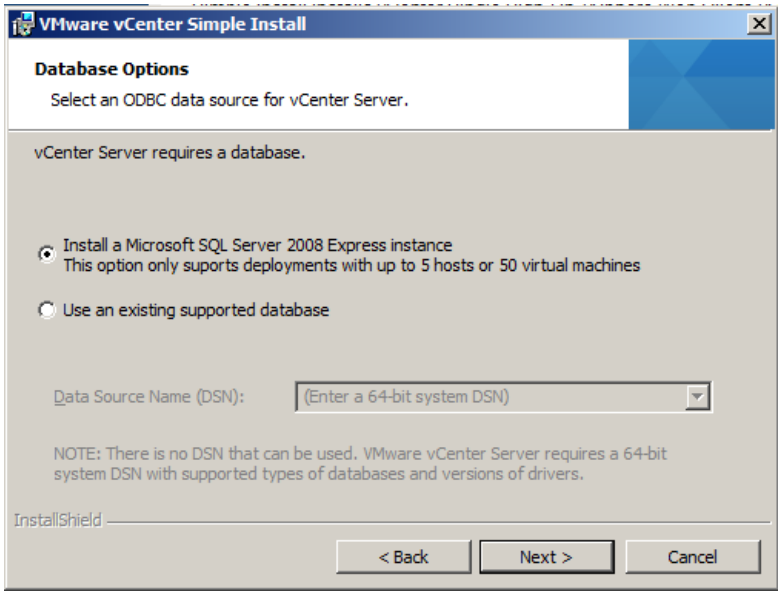
voa ainakaan tässä vaiheessa, joten asennuksen alustavaan tarkasteluun jouduttiin hyväksymään muutama huutomerkki. Kuviossa 23 on kuvankaappaus asennuksen alkuvaiheesta, jolloin asennus vielä muistuttaa käyttäjää domain liitoksista, osoitteista ynnä muusta. Kyseisellä hetkellä palvelimeen ei vielä oltu liitetty verkkokorttia, jonka vuoksi osoite on muotoa 127.0.0.1.



Kuvio 23. vCenter-palvelimen asennuksessa ilmenee ristiriitoja Windows AD -ympäristön puuttumisen vuoksi

Koska Windows-palvelinta ei oltu liitetty valmiiseen domainiin, halusi asennus luoda omansa. Oletuksella tämän domainin nimeksi tulee vsphere.local ja vCenter-palvelun pääkäyttäjän tunnukseksi Administrator. Näitä asetuksia ei voi itse muokata asennuksessa. Domainin ja pääkäyttäjätunnuksen lisäksi asennus kysyy pääkäyttäjälle salasanaa, jolle asennus on määrittänyt tietyn monimutkaisuuden. Salasanassa täytyy olla vähintään kahdeksan merkkiä, vähintään yksi iso ja pieni merkki, numero ja erikoismerkki. Käyttäjäasetusten jälkeen luodaan ensimmäinen klusterin puurakenteen nimi tai englanninkieliseltä nimeltä oleva Site. Asennus on myös varautunut Windowsin omaan palomuurin ja se kysyykin asennuksessa portin numeroa HTTPS-liikenteelle, jolle avataan kulkutie palomuurin läpi. Tämän jälkeen vCenter-palvelun asennus on valmis.

Asennus kuitenkin jatkuu seuraavaksi tietokannan asentamisella sekä määrittämisellä. Mikäli tietokantaa ei asenneta samalle palvelimelle vCenter-ominaisuuden kanssa, täytyy ympäristöstä löytyä DNS-palvelu. Ilman sitä asennus ei anna valita toiselle palvelimelle asennettua tuettua tietokantaa. Yksinkertaisuuden vuoksi tietokanta asennettiin Simple Sign-On -asennuksen yhteydessä. Kuviossa 24 on kuvankaappaus tietokannan valinnasta.



Kuvio 24. Tietokannan valinta vCenter-palvelinta varten

Viimeisinä toimina asennus kysyy tarkennuksena summittaista klusterin kokoa, jolla määritetään maksimi koko JVM-muistille. vCenter-palvelin käyttää muutamia Java-ohjelmointikielellä toteutettuja palveluita, kuten VMware VirtualCenter Management Web-services, Inventory Services ja Profile-Driven Storage Services. JVM-muistin maksimi määrää osaltaan näiden palveluiden toimivuutta. Opinnäytetyön kokeiluja varten riitti 1GB Small -asetus, sillä sekin kattaa 100 ESXi-palvelinta tai 1000 virtuaalikonetta. Asennus on tätä myöten valmis ja vCenter etäkirjautumista vaille valmis käytettäväksi. Jatkon osalta huomio kiinnittyi pitkään käynnistysaikaan. Mikäli palvelimen joutuu käynnistämään kokonaan, kesti lähemmäs kymmentä minuuttia ennen kuin palvelimeen pystyi ottamaan yhteyttä vSphere Client -ohjelmalla.

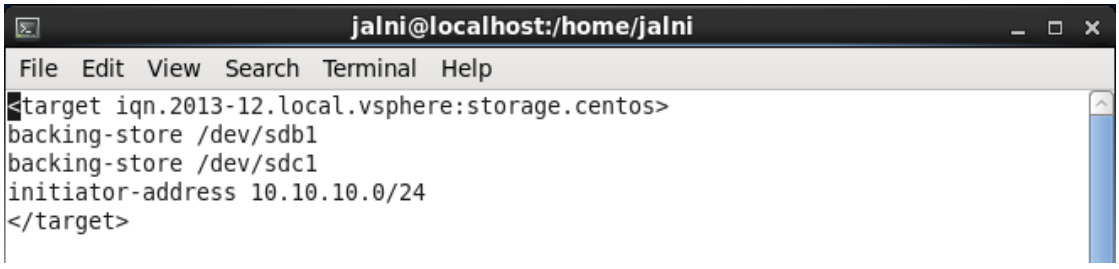
10.6 CentOS iSCSI-palvelimen asennus

Windows-palvelimien ollessa jo itsessään hivenen raskaampia ylläpitää, otettiin iSCSI-palvelimen virkaa suorittamaan Unix-käyttöjärjestelmäjakelu nimeltään CentOS. Kyseinen jakelupaketti on mukana tämänhetkisessä opetuksessakin, joten valintana tämä oli järkevä. Tämän lisäksi CentOS-koneen valjastaminen hoitamaan iSCSI target -palvelimen roolia käy

kohtalaisen helposti. iSCSI-palvelimeen ei haluttu kiinnittää liikaa huomiota, koska se jää lähinnä passiiviseksi klusterin resurssiksi.

CentOSin ollessa Unixin jakelupaketti, tarjotaan tästäkin useaa kokonaisuutta palvelimen asentamiseen. Tarjontaa on tässäkin tapauksessa neljä eri versioita: LiveCD, DVD, minimal ja netinstall. Eroja näiden pakettien osalla on lähinnä asennettujen ohjelmistopakettien määrässä, minkä huomaa jo lataustiedostojen koossa. Versioiksi valikoitui 6.5 sen ollessa tuorein ja latauspaketiksi LiveCD sen ollessa kohtalaisen pienikokoinen asennuspaketti graafisellakin käyttöliittymällä. Graafisuus ei kuitenkaan ollut pääosassa, koska asetukset tehtiin joka tapauksella terminaalilla.

Virtuaalikoneen ollessa valmis käyttöön asennuksen jäljiltä, luotiin koneelle kaksi ylimääräistä kiintolevyä. Nämä virtuaalilevyt osioitiin tarvittavalla tavalla, jotta /dev hakemistossa näkyisi kaksi jakoon kelpaavaa levyä sdb1 ja sdc1. Molemmista tehtiin 100GB levyosiot, jottei harjoitustila loppuisi aivan heti kesken. Tämän jälkeen haettiin koneelle levyjärjestelmää varten asennuspaketit käyttäen yum nimistä paketinhallintaohjelmaa. Tarvittavan paketin löytää nimellä scsi-target-utils. Paketinhallintaohjelman tehtyä asennus, täytyy seuraavaksi tehdä tarvittavat, asetukset ohjelman konfiguraatiotiedostoon. Tiedosto löytyy hakemistosta /etc/tgt/ ja tiedoston nimi siellä on targets.conf. Kuviossa 25 on kuvankaappaus asetuksista, joilla yksinkertaisimmillaan saadaan palvelin jakamaan levyjä verkolle. Ensimmäisen rivin alussa aloitetaan konfiguraatio <target-sanalla. Ensimmäisellä rivillä on myös kyseisen verkkojaon nimi. Seuraavilla riveillä kerrotaan järjestelmälle, mitkä levyosiot otetaan käyttöön ja mitkä laitteet saavat käyttää jakoa. Initiator-koneita voitaisiin tietysti tunnistaa myös yksittäisten osoitteiden perusteella tai käyttää lisänä käyttäjätunnusta ja salasanaa tunnistautumiseen. Viimeinen rivi päättää kyseisen jaon konfiguraatiot.



Kuvio 25. iSCSI-asetukset konfiguraatiotiedoston alussa

Asetusten jälkeen palvelu käynnistetään komennolla /etc/init.d/tgtd start, sekä chconfig-komennolla annetaan riittävät oikeudet palvelulle käynnistyä palvelinkoneen yhteydessä. Koska CentOS asettaa oletuksena iptables-palomuurin, päätettiin palomuuriin tehdä kulku-

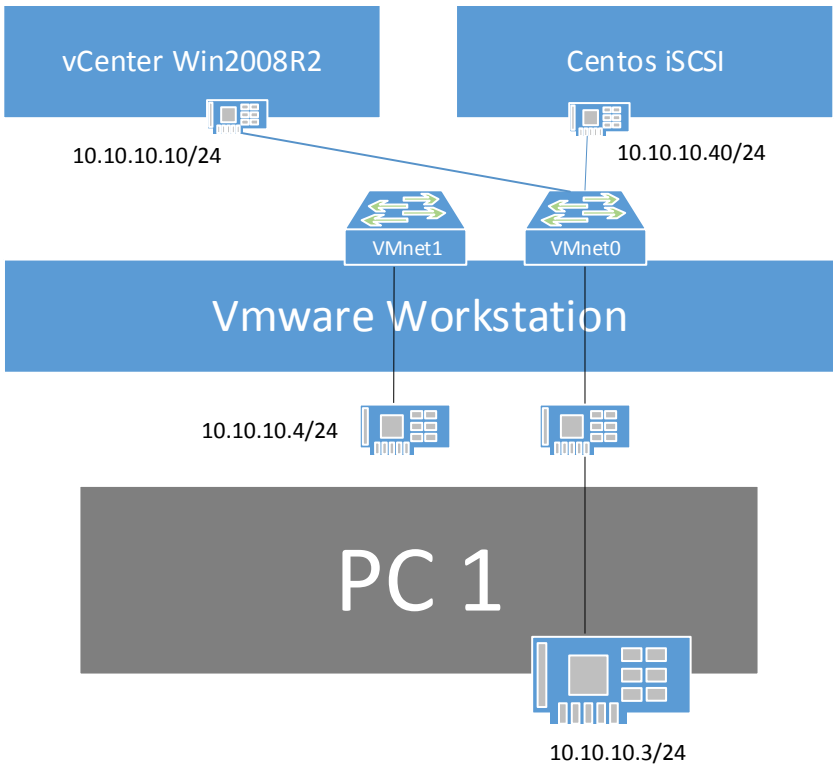
reitti iSCSI-liikennettä varten. Kuviossa 26 on kuvankaappaus, jossa oletusrivien yhteyteen on lisätty rivi, joka sallii TCP-liikenteen portin 3260 kautta. Näillä toimenpiteillä saadaan aikaan valmis palvelin odottamaan initiator-koneiden yhteydenottoja.

Kuvio 26. CentOS-palvelimen palomuurisäännöstö

10.7 Hallintaverkon luominen Workstation-ohjelman tasolla

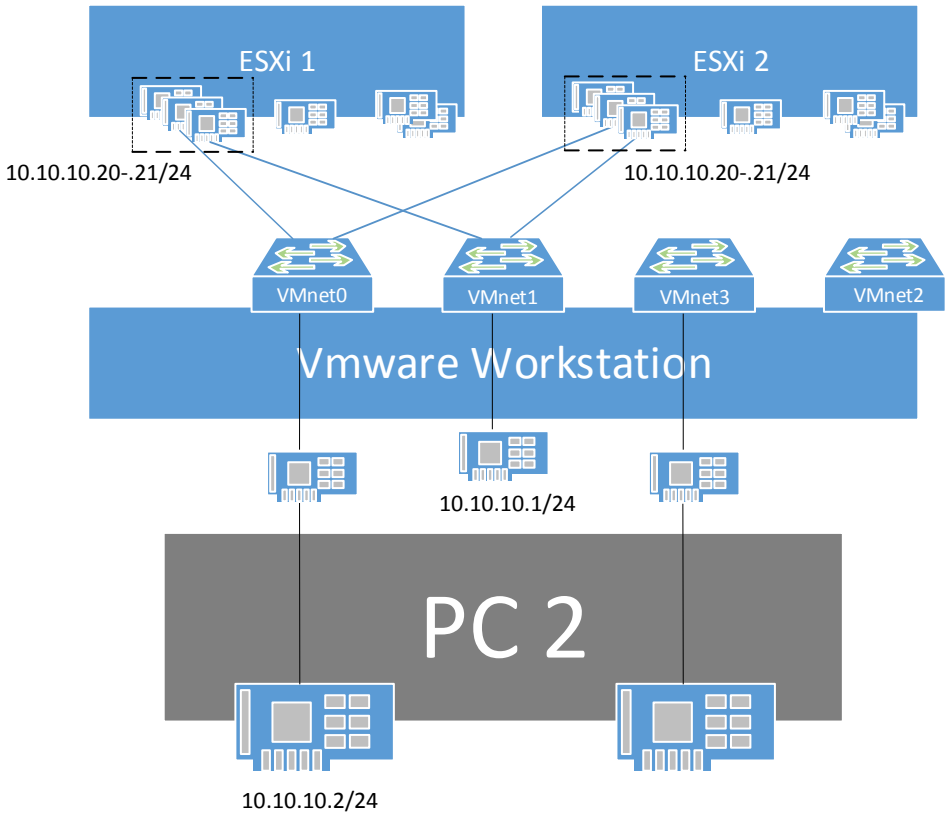
Opinnäytetyön alkupuolella puhuttiin virtuaaliverkkojen ohessa aihetta sivuten redundanttisesta ja vikasietoisesta verkosta. Käytännössä tämä tarkoittaa, että linkit, verkkokortit, kytkimet ja muut verkon laitteet kahdennetaan. Tällä halutaan estää syntymästä pisteitä, joissa yhden komponentin rikkoutuminen lamaannuttaa koko verkon tai sulkee pois osan laitteista. ESXi-palvelimien tapauksessa tietyt ominaisuudet vaativat kahdennetun verkon luomista, mutta vCenter- ja iSCSI-palvelimen tapauksessa kahdennuksia ei todettu tarpeelliseksi. Tämä siksi, että työasemia yhdistää vain yksi gigabitin väylä ja palvelimet ovat virtualisoituna. Pisteet, joissa verkko voisi vikaantua, vaikuttaisivat joka tapauksessa kriittisesti koko verkon toimintaan. Lisäksi iSCSI-palvelimen toimintaa ei pysty nopeuttamaan lisäämällä useaa gigabitin verkkokorttia, kun käytössä on vain yksi gigabitin väylä työasemien välillä.

Yksinkertainen oli siis käytännöllisin ratkaisu ja tätä on kuvattu PC1 osalta kuviossa 27. Kuvioon on lisätty myös hallintaverkon osoitteet. Koska VMnet0 ainoastaan siltaa liikennettä, ei sille tarvita omaa IP-osoitetta. VMnet1 on olemassa PC1-koneella ainoastaan siksi, että myös tältä koneelta voitaisiin muodostaa vSphere Client -ohjelmalla yhteys vCenter-palvelimeen. IP-osoite tälle sovittimelle täytyy laittaa työaseman verkkosovittimien asetusten kautta VMnet1-verkkoadapterille.



Kuvio 27. PC1-työaseman osoitteet ja verkkorajapinnat

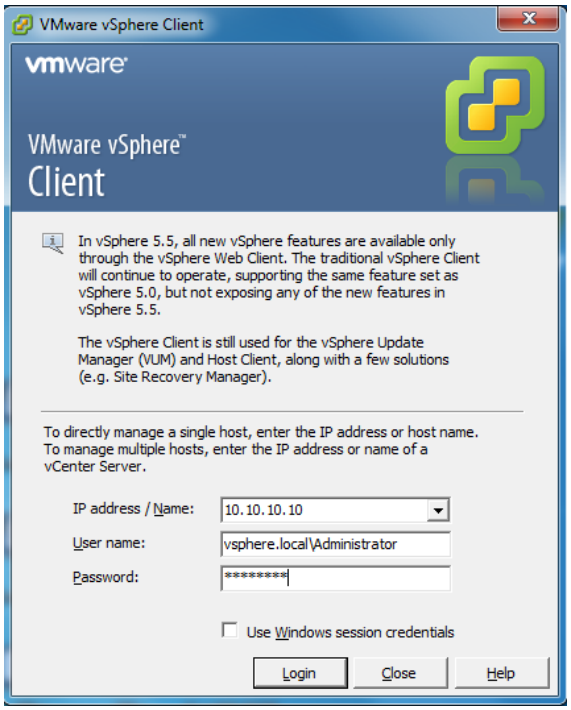
PC2-työaseman osalla verkko onkin jo monimutkaisempi. Kumpaankin ESXi-palvelimeen laitettiin lopulta kuusi verkkokorttia, jotta vaihtoehtoja olisi riittämiin. Lopullisena hahmotelmana kolme näistä päätyi yhdistymään hallintaverkkoon ja loput jäivät odottamaan virtuaalikoneita. PC1-työaseman tapauksessa VMnet0 jaVMnet1 olivat piirroksessakin erillisiä, vaikka kuuluivatkin samaan osoitealueeseen ja ovat lopulta kytkeytyneet toisiinsa ohjelman kautta. ESXi-palvelinten työaseman kanssa tehtiin hiukan eri tavoin, kuten kuvion 28 tapauksesta voi nähdä. Kaksi näistä verkkokorteista liitettiin siltaavina VMnet0 kautta fyysiseen verkkokorttiin ja kolmas yhdistettiin VMnet1-rajapintaan. Alunperin hallintaa hoitivat vain nämä siltaavat verkkokortit. Yhteys oli kahdennettu, jotta korkean käytettävyyden asetukset saataisiin käyttöön. Palvelimien suora yhdistäminen VMnet1-rajapinnan kautta tuli ajankohtaiseksi vikasietoisuus (Fault Tolerance) ominaisuuksien päälle kytkemisen yhteydessä, sillä ominaisuus vaatii varmasti suoran väylän ESXi-palvelimelta toiselle.



Kuvio 28. PC2-työaseman osoitteet ja verkkorajapinnat

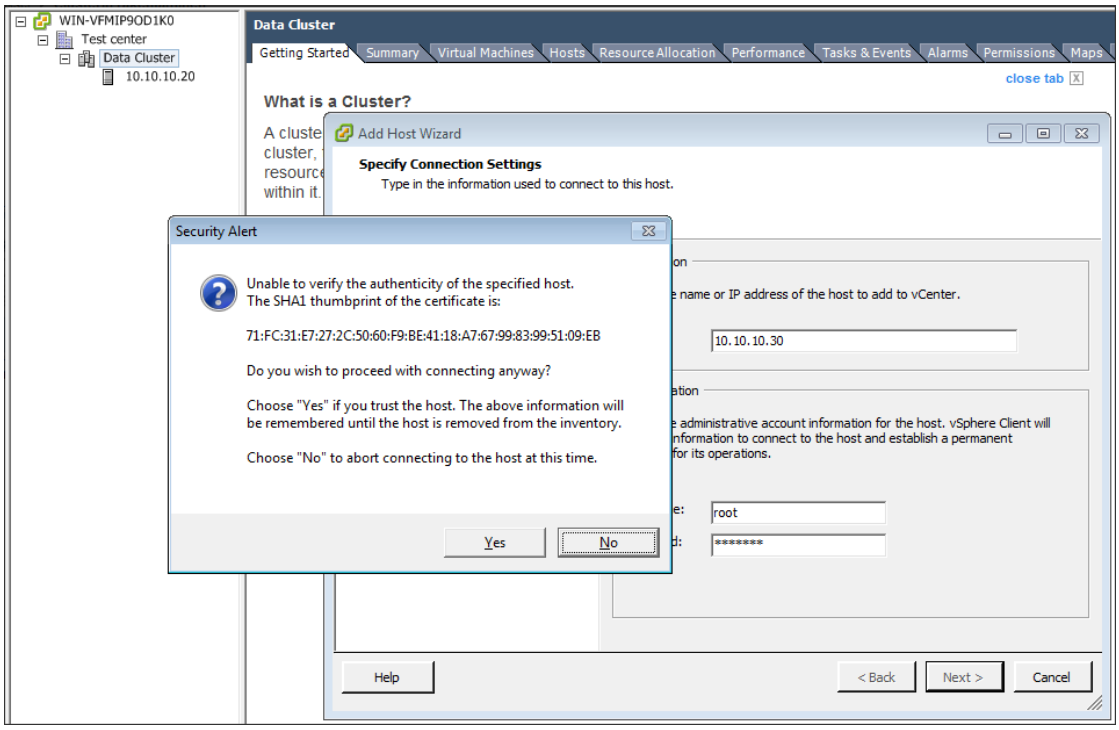
10.8 Ensimmäinen hallintayhteys, ESXi-hallintaverkko ja iSCSI

Kun tarvittava määrä verkkorajapintoja on yhdistettynä palvelimiin, voidaan avata hallintayhteys vCenter-palvelimeen. Tämä voidaan tehdä kummalta työasemalta tahansa avaamalla vSphere Client -ohjelma. Ohjelman avautuessa täytyy täyttää tiedot kirjautumista varten, eli palvelimen osoite, domain ja käyttäjätunnus, sekä salasana. Kirjautumisesta otettu kuvankaappaus on esitettynä kuviossa 29. vCenter-palvelimen asennuksen yhteydessä luodaan domain, ja koska olemassa olevaa Windows AD -ympäristöä ei ole olemassa, täytyy luotua domainia käyttää myös sisään kirjautumisen yhteydessä yhdessä käyttäjätunnuksen kanssa.



Kuvio 29. vSphere Client -ohjelman kirjautumiseen käytetään tunnusten ja salasanan lisäksi domainin nimeä

Yhdistämisen jälkeen avautuvasta valikosta kannattaa ensitöikseen navigoida Hosts and Clusters -näkymään. Avautuvasta valikosta voi joko suoraan lisätä ESXi-palvelimet luotuun klusteriin tai lisäyksen voi tehdä vasemman sarakkeen kautta näkyvästä puurakenteesta. Add Host -valinnnan perusteella aukeava valikko kysyy lisättävän ESXi-palvelimen IP-osoitetta sekä käyttäjätunnusta ja salasanaa. Näiden antamisen jälkeen ruudulle ilmestyy vielä turvahälytys, jossa ilmenee ESXi-palvelimen uniikki sormenjälki. Hyväksymisien jälkeen ESXi-alusta ilmestyy vasemman sarakkeen puurakenteeseen. Kuviossa 30 on vielä kuvankaappaus toisen alustan lisäämisen tuottamasta turvailmoituksesta. Kuviossa on myös nähtävillä klusterin puurakenne.

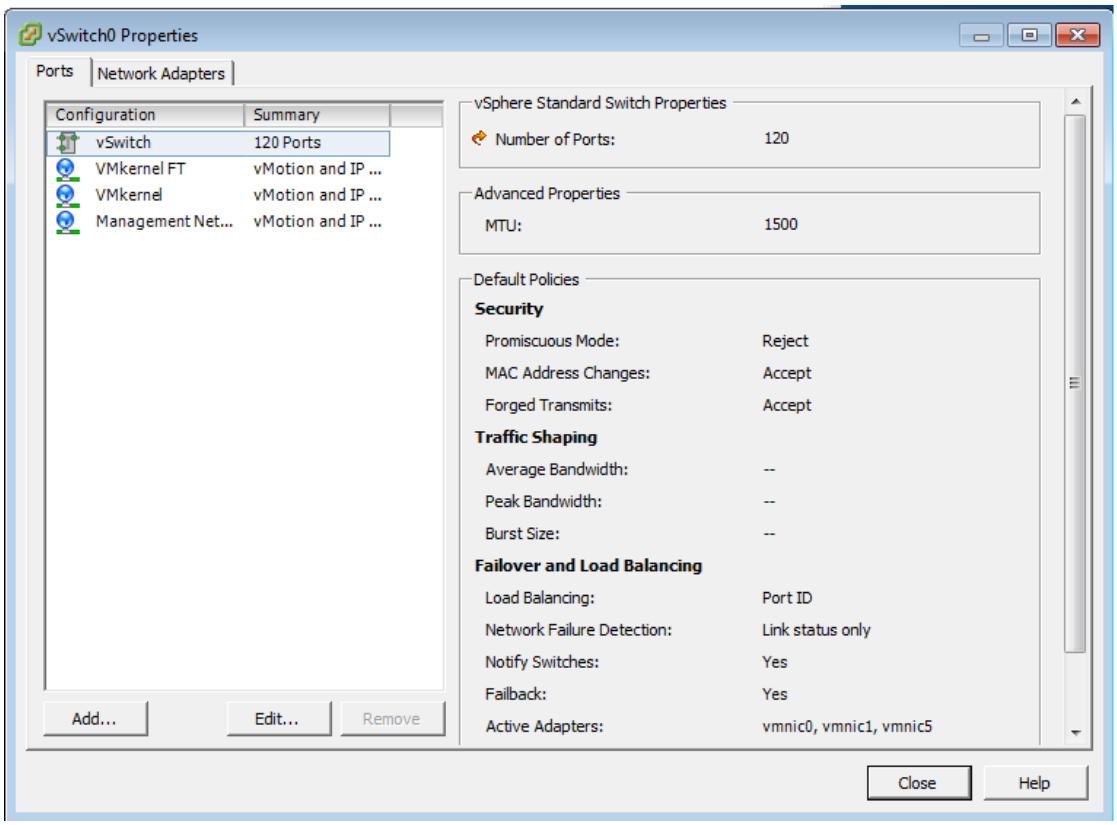


Kuvio 30. Toisen ESXi-palvelimen tuottama turvahälyytys klusteriin liittämisen seurauksena

Molempien palvelimien lisäämisen jälkeen voidaan kutakin palvelinta hallita suoraan vCenter-palvelimeen muodostetun hallintayhteyden kautta. Seuraavaksi siirrytään muokkaamaan palvelimien verkkoasetuksia valitsemalla palvelin puurakenteesta ja siirtymällä Configuration-välilehdelle ja valitsemalla välilehdeltä Networking. Näkymä näyttää ainoastaan yhden Standard Switch -virtuaalikytkimen, jolla on yksi VMkernel-portti ja yksi tai useampi fyysinen adapteri, riippuen ESXi-palvelimelle tehdyistä asetuksista sen oman DCUI-hallinan kautta. Properties-valikon kautta avautuu eteen virtuaalikytkimen tiedot. Network Adapters -välilehden kautta lisätään halutut fyysiset adapterit tähän kytkimeen. Ports-välilehdellä voidaan tarkastella kytkimen ja porttienasetuksia ja luoda uusia portteja. Työssä päädyttiin pitämään vSwitch0 hallintakytkimenä ja luomaan lopulta kaksi VMkernel-porttia tälle kytkimelle. Lisäksi fyysisiä adaptereita jätettiin kolme.

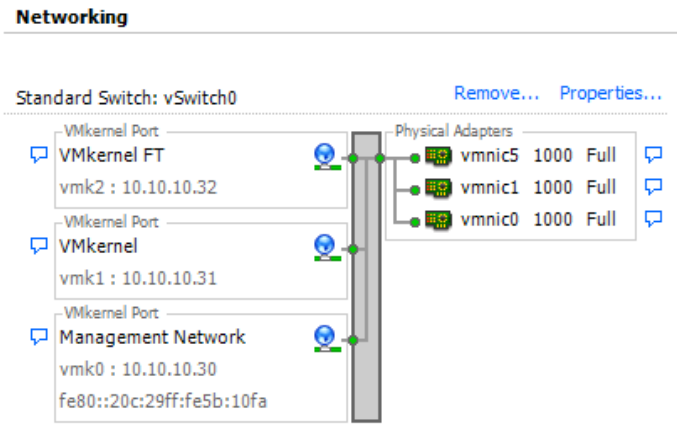
VMkernel-portteja olisi voinut olla enemmänkin, koska osoitejako antoi 10 IP-osoitetta per ESXi, mutta toimiva ratkaisu saatiin aikaan myös kolmella hiukan yhdistellen. Kuviossa 31 on kuvankaappaus virtuaalikytkimen asetusvalikosta, jossa nähtävissä luodut portit. VMkernelFT-portin tehtäväksi jätettiin pelkästään vikasietoisuuden vaatima suora palvelinyhteys ja verkkokortti viisi osoitettiin sen fyysiseksi rajapinnaksi. Management Network - ja VMkernel-portit asetettiin hoitamaan vMotion-toiminnan, hallinta- ja iSCSI-liikenteen välittämisen ja käyttämään verkkokortteja nolla ja yksi. Tilanteen olisi voinut myös ratkaista tekemällä kaksi porttia hallinta-, kaksi iSCSI-, yksi vMotion- ja yksi FT-liikenteelle. Näin olisi tuhlattu IP-

osoitteita ja saatu selkeä jako porttien välille, mutta lisätty taas konfiguroinnin määrää. Adaptereita ei olisi tarvinnut lisätä.



Kuvio 31. vSwitch0-asetuksista voi lisätä portteja ja fyysisiä rajapintoja, sekä muokata niiden asetuksia

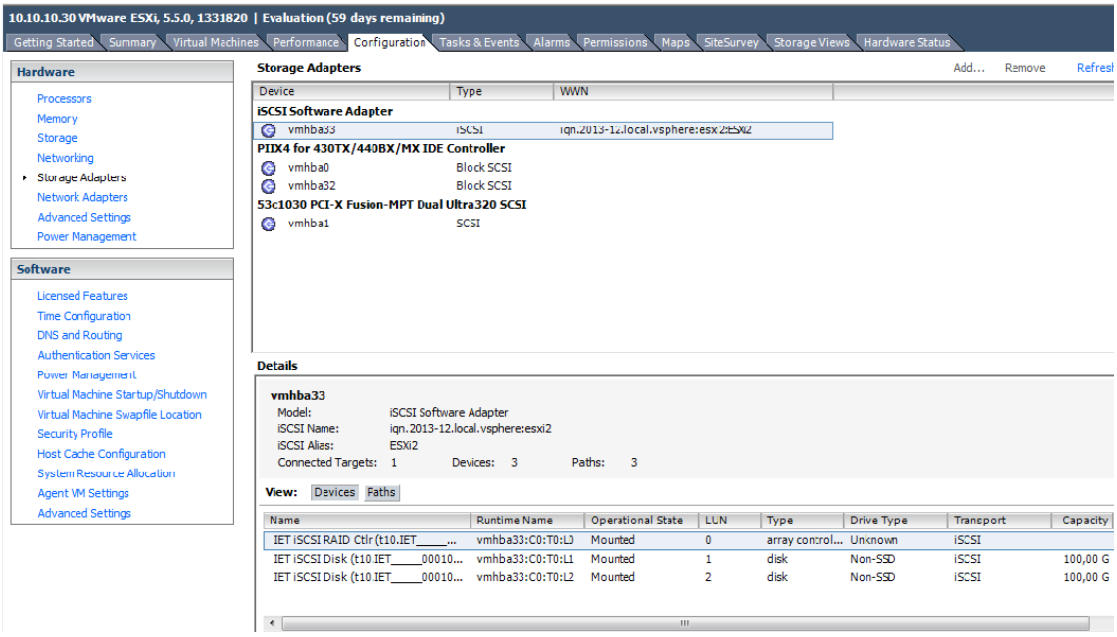
Kuviossa 32 on kuvankaappaus valmiista hallintakytkimestä porttien osoitteiden kanssa. Samat toimenpiteet toistetaan tietenkin myös toisella ESXi-palvelimella, jotta verkkoasetukset olisivat identtiset, mutta eri osoitteilla.



Kuvio 32. Valmis virtuaalikytkin Configuration-välilehdellä

Hallintaverkon lisäksi molemmille ESXi-palvelimille luodaan oma virtuaalikytkin sisäistä liikennöintiä varten, sekä kytkin ulkoverkkoon pääsemiseksi. Uuden kytkimen luominen onnistuu saman Configuration-välilehden Networking-osiosta, jossa muokattiin hallintaverkon kytkintä. Koska järjestelmään lisätään uusi kytkin, tapahtuu toimenpide näkymän oikean ylälaidan Add Networking... -painikkeella. Aukeavasta ikkunasta valitaan VMnetwork ja liitetään halutut fyysiset uplink-rajapinnat. Näin luodaan vSwitch1, jonka avulla virtuaalikoneet voivat liikennöidä VMware Workstation -ohjelman VMnet-verkon yli toistensa kanssa ja vSwitch2, johon yhdistetyt virtuaalikoneet pääsevät tarvittaessa ulkoverkkoon hakemaan esimerkiksi asennuspaketteja.

Verkkoasetusten jälkeen siirrytään liittämään aiemmin luodut iSCSI LUN -verkkolevyt klusterin käyttöön. Kuten teoriaosuudessa mainittiin, täytyy verkkoasetusten perään luoda adapteri iSCSI-levyjärjestelmää varten. Tämä tapahtuu Configuration-välilehden kautta kohdasta Storage Adapters. Adapteri täytyy luoda kumpaankin ESXi-palvelimeen erikseen. Luomisen jälkeen adapterin asetuksissa annetaan iSCSI-yhteyttä varten molemmille ESXi-palvelimille annettiin oma iqn-nimi, jonka runkona toimi aiemminkin mainittu iqn.2013-12.local.vsphere. Rungon perässä olevaan uniikkiin nimiosaan laitettiin esxi1 ja esxi2. Verkkoadaptereista valitaan tämän jälkeen iSCSI-liikenteelle varattu portti ja dynaamiseen etsintään annetaan IP-osoitetieto Target-palvelimesta. Asetusten jälkeen järjestelmä pyytää uudelleen skannaamaan adapterit, jonka jälkeen välilehden alareunaan Details-kohtaan tulee näkyviin jaossa olleet LUN-levyt, kuten kuvion 33 kuvankaappauksessa on nähtävissä. Adapterin lisäys suoritetaan molemmilla alustoilla erikseen.



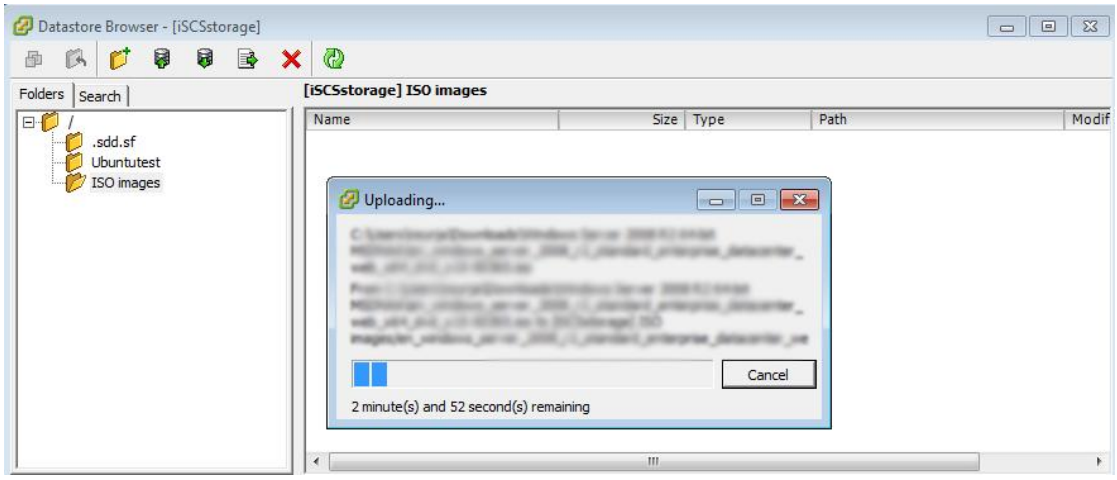
Kuvio 33. Lisätyn adapterin kautta saadaan näkyviin levyjärjestelmän kovalevyt

Onnistuneet iSCSI-yhteydet voi myös tarkastaa Target-palvelimelta kuten kuvion 34 kuvankaappauksessa. Kuviossa palvelinta on pyydetty näyttämään siihen liittyneet initiator-koneet.

```
[root@localhost jalni]# tgtadm --mode target --op show
Target 1: iqn.2013-12.local.vsphere:storage.centos
    System information:
        Driver: iscsi
        State: ready
    I_T nexus information:
        I_T nexus: 1
            Initiator: iqn.2013-12.local.vsphere:esxi1
            Connection: 0
                IP Address: 10.10.10.20
        I_T nexus: 2
            Initiator: iqn.2013-12.local.vsphere:esxi2
            Connection: 0
                IP Address: 10.10.10.30
```

Kuvio 34. Target-palvelimelta saadut tiedot iSCSI initiator -laitteista

Lisättyjä levyjä voidaan tarkastella esimerkiksi Configuration-välilehden Storage-linkin kautta tai siirtyä yläpalkin "osoiterivin" kautta Home->Inventory->Datastores and Datastore Clusters. Browse Datastore -valinta avaa yksinkertaisen tiedostoselaimen koskien yksittäistä levyä. Jotta virtuaalikoneita pääsee lopulta asentamaan, kannattaa tarvittavat asennustiedostot siirtää jollekin LUN-levylle. Siirto onnistuu suoraan vSphere Client -ohjelmaa käyttävältä työasemalta tiedostoselaimen Upload-painikkeen avulla. Kuviossa 35 on kuvankaappaus tilanteesta, jossa Ubuntu-virtuaalikoneita varten siirretään lokaalilta tietokoneelta iSCSI-levyn ISO images -kansioon vSphere Client -ohjelman kautta.

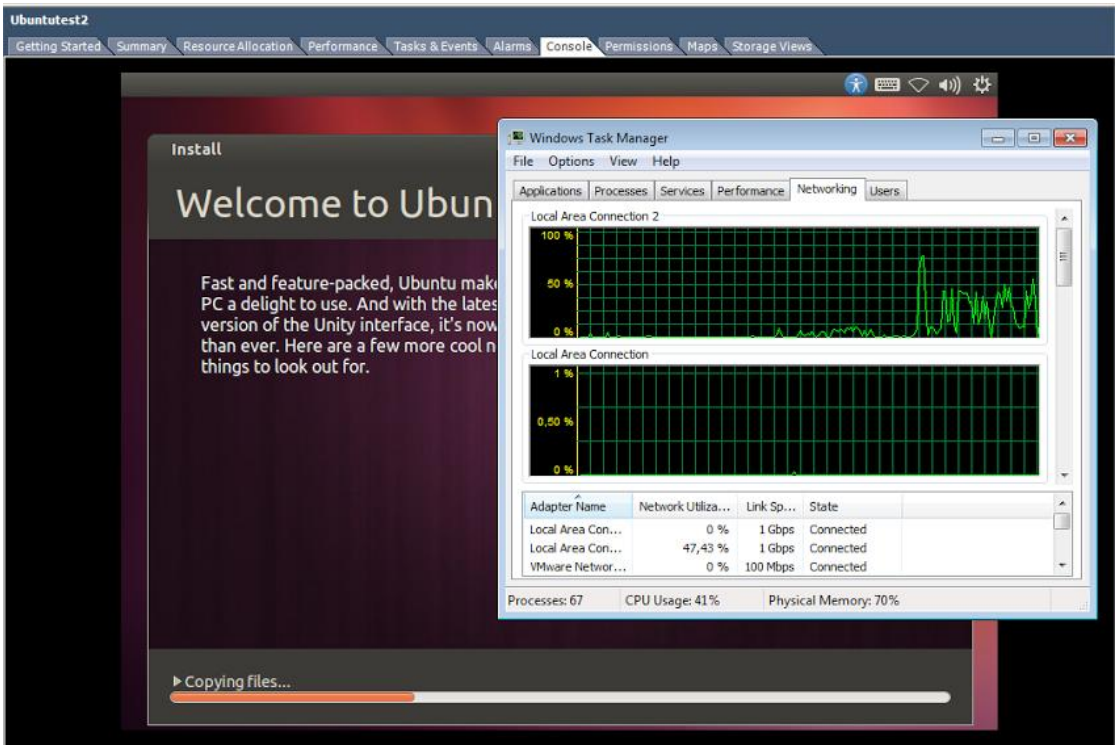


Kuvio 35. Tiedostojen siirto onnistuu myös lokaalin koneen tiedostoista

10.9 Ensimmäiset virtuaalikoneet

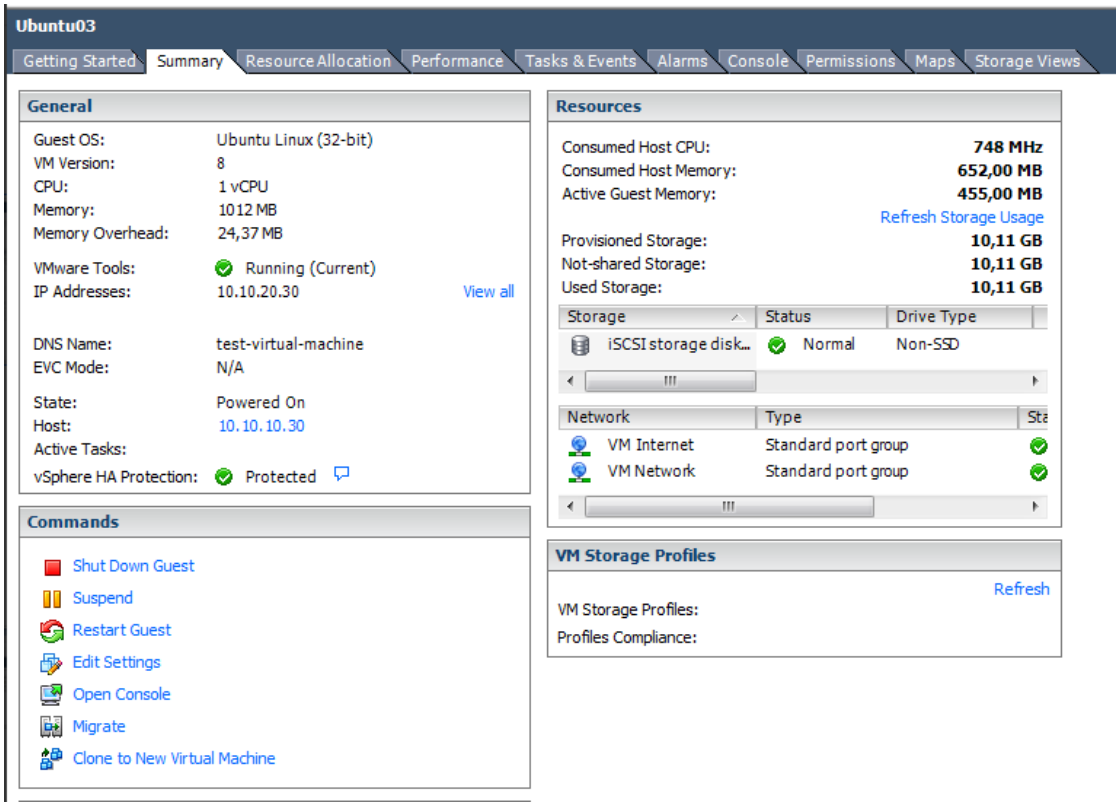
Virtuaalikoneita asennettiin aina tarpeen vaatiessa ominaisuuksien koestamista varten. Rajallisten resurssien vuoksi suurin osa koneista asennettiin käyttämään Ubuntu 13.10 käyttöjärjestelmää käyttäen yhtä prosessoria ja 512Mb tai 1Gb RAM-muistia. Kovempaa rasitusta varten asennettiin myös kokeeksi yksi tyhjä Windows Server 2008 -kone.

Koneiden määrittäminen kulkee kuitenkin samalla kaavalla, kuten luvussa seitsämän oli puhetta. Testiympäristön puitteissa helpoin tapa saada asennusmedia liitettyä tyhjään virtuaalikoneeseen on osoittaa tiedosto iSCSI-levyjärjestelmästä. Fyysinen työaseman levyasema olisi ollut järkevä ainoastaan tapauksessa, jossa käytössä olisi ollut fyysisiä asennuslevyjä ja ESXi-palvelimessa oleva virtualisoitu fyysinen levyasema olisi aiheuttanut mahdollisia komplikaatioita myöhemmissä vaiheissa. Jokainen käyttöjärjestelmä asentuu omalla kaavallaan, eikä niihin haluta tässä työssä ottaa kantaa. Mielenkiintoista oli kuitenkin seurata verkkoliikenteen määrää, jota käyttöjärjestelmän asentaminen sai aikaan. Kuviossa 36 on kuvankaappaus Ubuntu-koneen asennuksesta ja kuvassa näkyvä Windows Task Manager näyttää työaseman fyysisessä verkkorajapinnassa kulkevaa dataa. Vihreä käyrä osoittaa hyvin kuinka paljon kaistaa yksin yhden virtuaalikoneen asennus voi viedä liikennekäyrän noustessa keskimäärin 400Mbps nopeuksiin. Kuvion ottohetkellä ei tehty muita toimenpiteitä järjestelmässä.



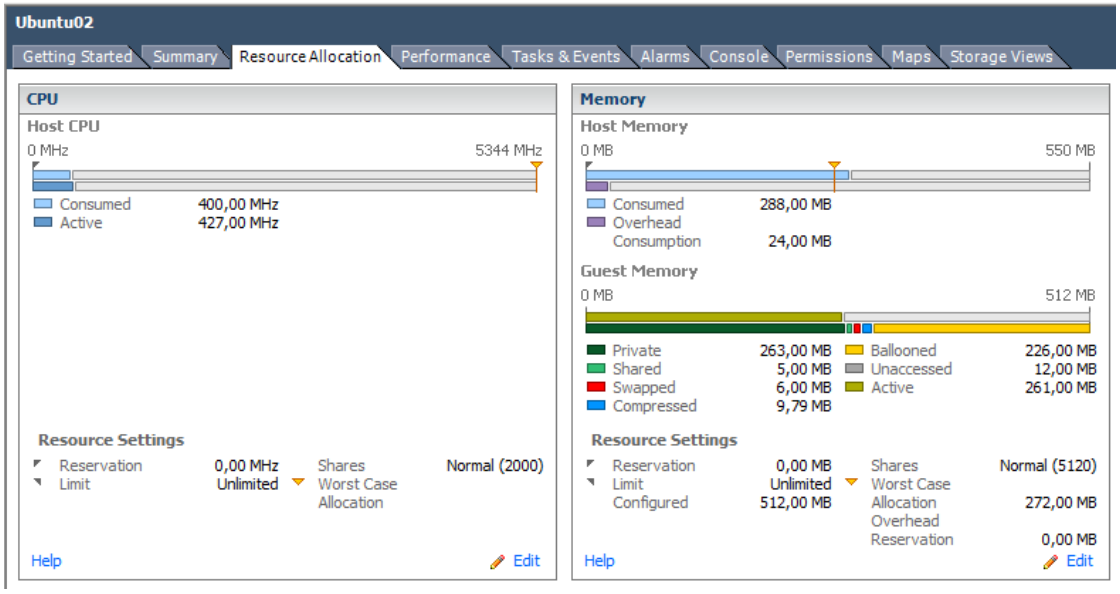
Kuvio 36. Ubuntu-koneen asennuksen aiheuttama verkkoliikenne nähtävissä Windows Task Manager -ohjelmalla

Asennettu kone vaatii VMware Tools -paketin asennuksen ja tämä eroaa Windows- ja Linux-jakeluissa toteutustapansa mukaan. Kuitenkin asennettuna paketti antaa käyttöön koneen Summary-välilehdelle enemmän tietoja. Kuviossa 37 on kuvankaappaus käynnissä olevasta Ubuntu-koneesta, johon Tools-paketti on jo asennettuna. Välilehti näyttää General-osiossa yleistiedot koneesta ja Tools-paketin myötä osaa jopa näyttää koneelle asetetun IP-osoitteen.



Kuvio 37. Virtuaalikoneen Summary-välilehdeltä näkee koneen perustiedot ja komennot

Summary-välilehden lisäksi tietoja koneen resurssien käytöstä löytyy myös Resource Allocation -välilehdeltä. Sivu näyttää grafiikan ja lukujen avulla tiedot koneen prosessorin ja muistin rasituksen asteesta ja muistin osalta, sen kuinka muisti järjestetään virtuaalikoneelle. Kuvion 38 kuvankaappauksessa on auki tämä edellä mainittu Resource Allocation -välilehti. Kuten kuviosta voidaan todeta, on virtuaalikoneen omasta muistista (guest memory) tuotettu osa tiivistyksenä. Käytössä on myös pieni pala swapped-muistia sekä lähes aktiivisen muistin kokoinen pala ballooned-ajurilla tuotettua muistia.



Kuvio 38. Virtuaalikoneen resurssien käytöstä saa dataa esiin Resource Allocation -välilehdeltä

Virtuaalikonetta pääsee varsinaisesti käyttämään valitsemalla Console-välilehden, jolloin ikkunaan avautuu pienellä viiveellä virtuaalikoneen mahdollinen työpöytänäkymä. Mikäli VMware Tools -pakettia ei ole vielä asennettu ja hiiren osoittimen haluaa irti tästä ikkunasta, täytyy käyttää Ctrl- ja Alt-painikkeiden yhdistelmää irtautuakseen ikkunasta. Tools-paketti mahdollistaa kursorin siirtämisen ikkunan ulkopuolelle jatkamaan oman työpöydän käyttöä ilman näppäinyhdisteitä.

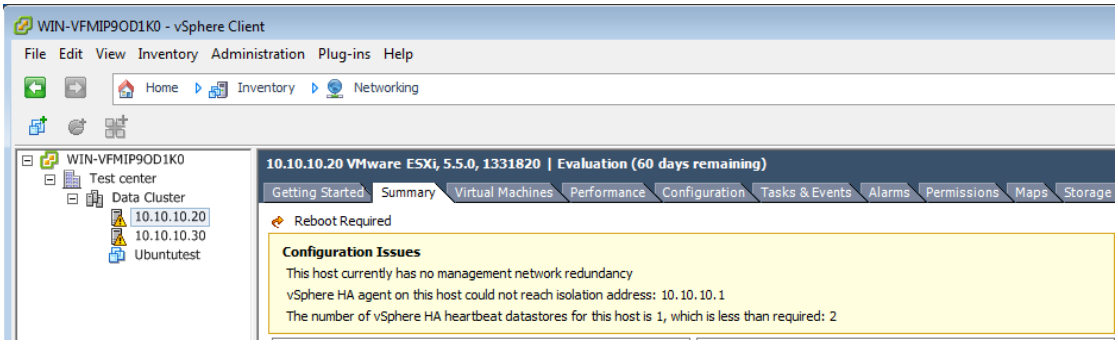
Valmiista virtuaalikoneesta voidaan tarvittaessa luoda templaatti. Tällä ominaisuudella varsinaista virtuaalikonetta ei voida enää käyttää, mutta tätä virtuaalikoneesta tehtyä muottia voidaan käyttää helpottamaan muiden samankaltaisten järjestelmien luomista. Templaatista on mahdollista nimittäin helposti käynnistää uusia virtuaalikoneita, joiden ohjelmisto ja asetukset ovat valmiiksi halutun kaltaiset. Lisäksi luodun templaatin asetuksien kautta voidaan edelleen vaikuttaa koneesta tehtäviin kopioihin. Järjestelmänvalvojan näkökannasta tämä tarkoittaa sitä, että yhdestä valmiista koneesta saadaan nopeasti monistettua klusterin täydeltä koneita. Tarvitaan vain yksi valmiiksi asennettu virtuaalikone halutulla käyttöjärjestelmällä, johon halutut palvelut ja ohjelmat on jo asennettu.

10.10 vSphere HA - ja DRS-ominaisuuksien käyttöönotto

Ennen ominaisuuksien käyttöönottoa täytyy huomioida kaksi asiaa: Isolation Address ja Datastore Heartbeat. Isolation Address on siis osoite, johon palvelin yrittää ottaa yhteyttä, mikäli se ei saa vastausta muilta palvelimilta. Normaaleissa oloissa osoitteena käytetään verkon gateway-osoitetta, joka on esimerkin mukaisessa verkossa 10.10.10.0/24-verkon gateway.

Mikäli sellaista ei ole asetettu, haluaa järjestelmä määrittää gateway-osoitteen HA-toiminnon yhteydessä. Yhdyskäytävän osoitteeksi asetettiin 10.10.10.1, joka siis osoittaa toisen työaseman VMnet1-rajapintaan. Tämä rajapinta ei kuitenkaan kelpaa, sillä kokeilujen perusteella HA ei saanut vastausta tästä rajapinnasta. Näin ollen Isolation Address pitää manuaalisesti määrittää HA-asetusten Advanced-osioon das.isolationaddress parametrilla ja osoittaa esimerkiksi vCenter-palvelimeen. Lisäksi das.usedefaultisolationaddress parametri tulisi asettaa false-tilaan, jolloin kielletään oletusyhdyskäytäväosoitteen olemassaolo. (VMware High Availability cluster reports the error: Could not reach isolation address (1002787), 2011.)

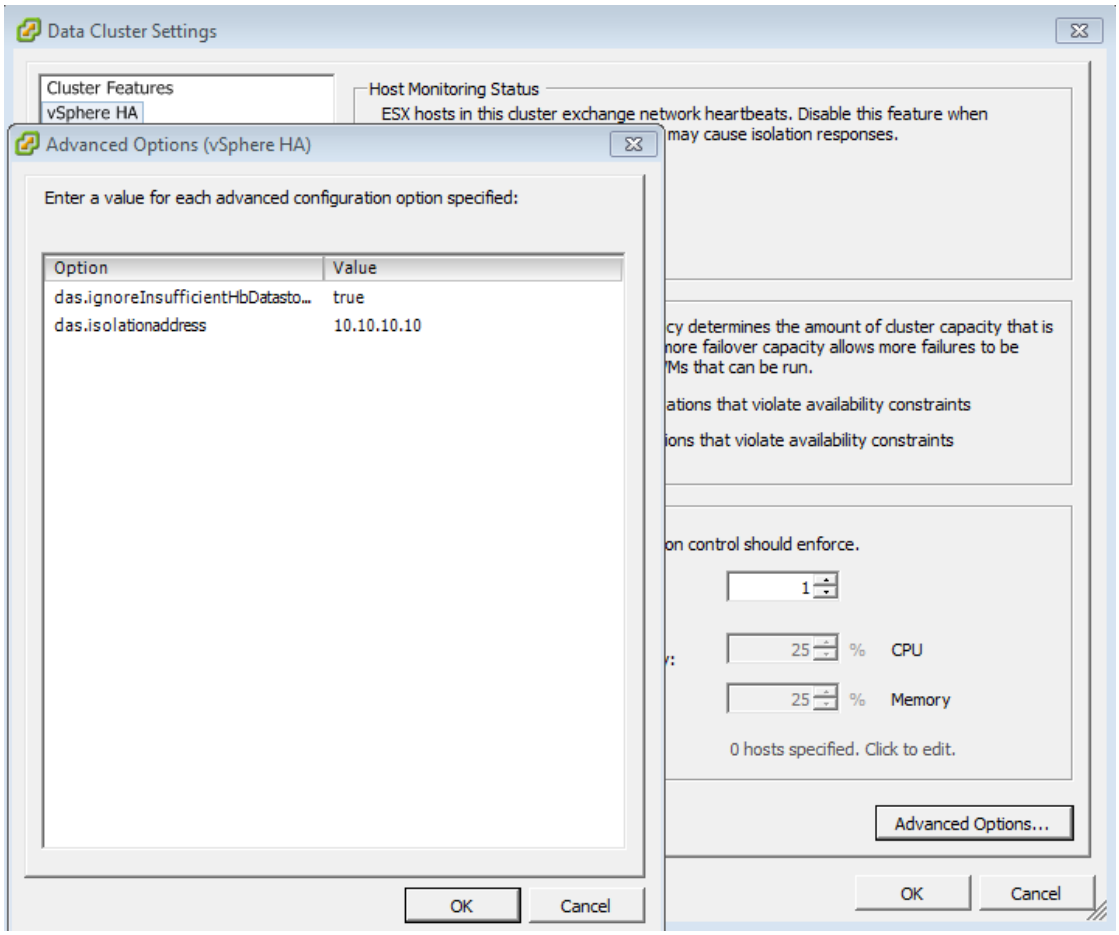
Datastore Heartbeat toiminnon kanssa ei tule ongelmia, mikäli iSCSI Target -palvelimen yhteydessä luodaan vähintään kaksi levyä. HA-toiminto haluaa käytettäväkseen vähintään kaksi erillistä verkkolevyä säilyttääkseen vSphere HA -kansion ja siihen liittyvät tiedostot. Jos datavarastoja on vain yksi, ei HA-ominaisuutta saa päälle. Täysin absoluuttinen tämä ehto ei lopulta ole, sillä HA Advanced -asetuksissa on mahdollista ohittaa tämä vaatimus parametrilla das.ignoreInsufficientHbDatastore ja asettamalla tälle parametrille arvon true. (HA Error: The number of heartbeat datastores for host is 1, which is less than required: 2 (2004739), 2011.) Mikäli nämä kaksi edellä mainittua asiaa eivät ole kunnossa, kaatuu vSphere HA -ominaisuuden käyttöönotto kuvion 39 mukaiseen ilmoitukseen. Ilmoitus valittaa myös kyseisellä hetkellä puuttuvasta redundattisuudesta hallintaverkossa.



Kuvio 39. Epäonnistunut vSphere HA -toiminnon käyttöönotto

Varsinainen käyttöönotto tapahtuu valitsemalla puurakenteesta klusterin kuvake ja editoimalla asetuksia. Avautuvasta valikosta tulee heti näkyviin valinta ottaa vSphere HA käyttöön. Valintalaatikon merkitsemisen jälkeen avautuu vasemman palkin välilehtiin lisää rivejä ja mikäli Advanced-parametreja tarvitsee muokata, onnistuu tämä vSphere HA -välilehden kautta löytyvän Advanced Options... -painikkeen takaa. Kuviossa 40 on kuvankaappaus, josta näkyy tämä mainittu parametrien asetussivu. Kuviossa on myös nähtävillä muutama lisätty

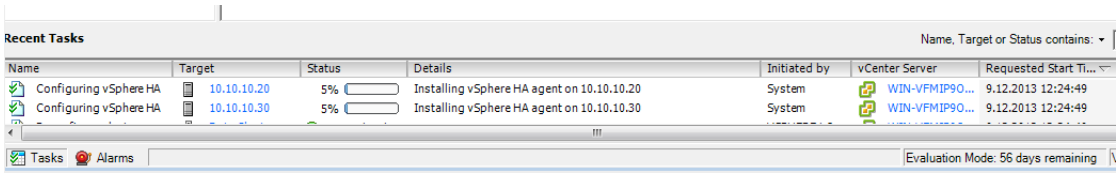
parametririvi asetuksista, jotka mainittiin edellä. vSphere HA -välilehdeltä voidaan myös vaikuttaa monitorointiin ja HA-ominaisuuden varaamaan resurssimäärään, josta puhuttiin kappaleessa 6.3.1 Admission Control -politiikka.



Kuvio 40. Lisäparametrien antaminen vSphere HA -ominaisuuden käyttöönottoa varten

Tarvittavien parametrien ja asetusten määrittämisen jälkeen vSphere HA -käyttöönotto hyväksytään painamalla valikosta löytyvää OK-painiketta. Tämän jälkeen päänäkymän alalaidassa Recent Tasks -valikkoon tulee näkyviin rivit HA-ominaisuuden konfiguroinnille. Konfigurointi kestää kohtalaisen pitkään muun muassa siksi, että klusterin ESXi-palvelimille täytyy asentaa erillinen vSphere HA Agent -lisäosa. Kuvion 41 kuvankaappauksessa on nähtävillä mainittu Tasks-näkymä ja konfiguroinnista ilmoittavat statukset. Onnistuneen konfiguroinnin jälkeen klusterin rakennepuuhun ei ole ilmestynyt varoituskolmioita tai huutomerkkejä ja ESXi-palvelimien Summary-välilehdellä General-osiossa on nähtävissä vSphere HA -tila. Halutessaan HA-asetuksia voi muokata jälkikäteen samaisen Edit Settings -valikon kautta klusterin asetuksista, mutta jokaisen asetusmuutoksen yhteydessä kannattaa kytkeä HA pois päältä ja

uudestaan käyttöön, kun asetukset on tehty.

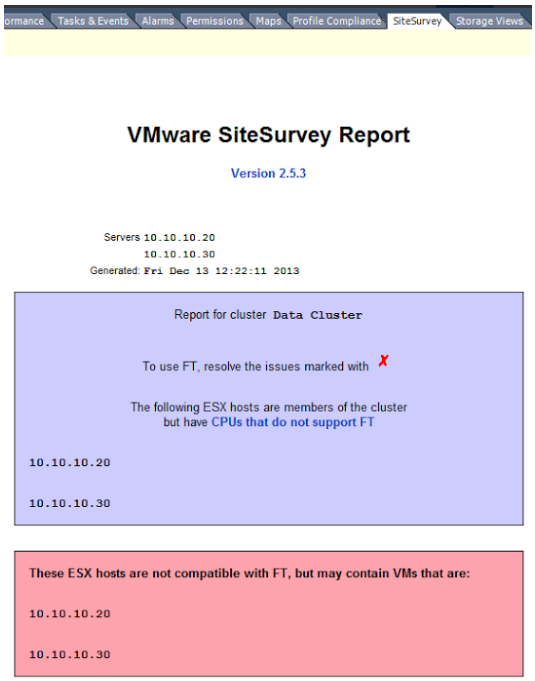


Kuvio 41. vSphere Client esittää klusterissa tapahtuvat työt omassa näkymässään

vSphere DRS -ominaisuuden käyttöönotto sujuu yhtälailla samasta valikosta kuin HA-ominaisuuden, eikä samanlaisia virityksiä tarvita. Ominaisuuden käyttöönoton myötä on mahdollista määrittää DRS-ryhmät virtuaalikoneista, muokata yksittäisiä koneita koskevia asetuksia tai ylipäätään muokata automatisoidun toiminnallisuuden tasoa haluamallaan tavalla.

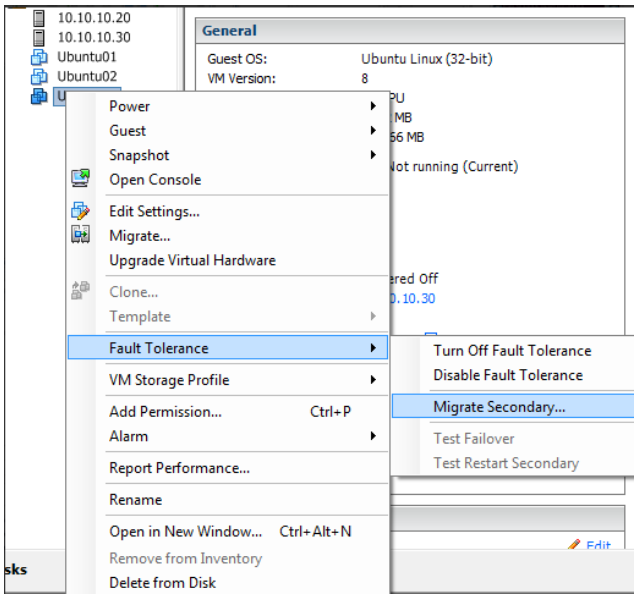
10.11 vSphere FT -ominaisuuden käyttöönotto

vSphere FT -ominaisuuden käyttäminen tulee mahdolliseksi HA-ominaisuuden ollessa käytössä. Kuitenkin on hyvä muistaa erittäin pitkä muistilista, joka mainittiin luvussa 6.4. Opinnäytetyössä isoimpana ongelmana vastaan nousi tuetun prosessorin puuttuminen, kuten kuvion 42 kuvankaappauksessa on nähtävissä. VMwaren verkkosivuja selaamalla löytyi tieto SiteSurvey-lisäosasta, joka helpottaa huomaamaan puutokset omassa klusterissa tai suojattavissa virtuaalikoneissa. Lisäosan saa helposti VMwaren verkkosivuilta ja se asentuu vSphere Client -ohjelman yhteyteen. Asennettua lisäosaa pääsee käyttämään klusterille ja ESXi-palvelimille ilmestyneen SiteSurvey-välilehden kautta. Lisäosa tarkistaa halutun järjestelmän ja antaa käyttäjälle raportin yhteensopivuuksista käyden läpi käytännössä kaikki teoriakappaleessakin mainitut asiat klusterista, palvelimista ja virtuaalikoneista. Asetuksen käyttöönottoa tutkittiin kuitenkin pidemmälle ja se yritettiin saada toimintaan kaikesta huolimatta. (About VMware SiteSurvey, 2013.)



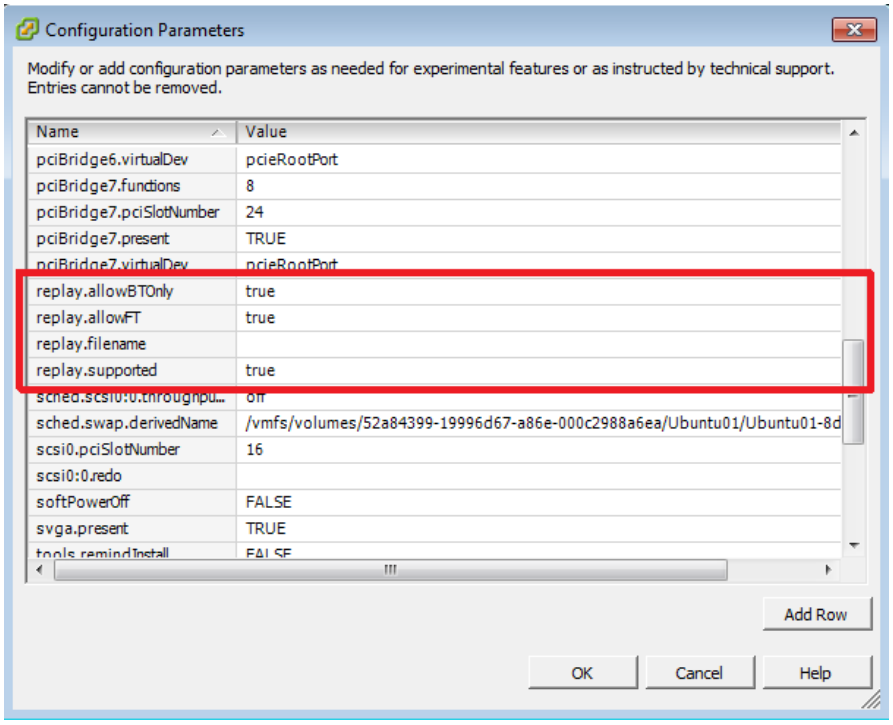
Kuvio 42. VMware SiteSurvey -lisäosa kertoo, ettei klusterin prosessoreista löydy tukea FT-ominaisuudelle

Käyttöönottona Fault Tolerance vaatii siis käytössä olevan HA-toiminteen ja suojattavan virtuaalikoneen. Virtuaalikoneen valikkoon tulee tässä vaiheessa mahdolliseksi vaihtoehdoksi Fault Tolerance -rivi ja sen alta löytyvä Turn On Fault Tolerance. Kuviossa 43 on kuvankaappaus tästä valikosta. Kuvankaappaushetkellä ominaisuus oli saatettuna käyttöön. Kun ominaisuuden ottaa käyttöön virtuaalikoneelle, alkaa järjestelmä kopioida toissijaista konetta varsinaisesta koneesta ja asettaa kopion suorituspaikaksi toista ESXi-palvelinta. Lisäksi järjestelmä käy läpi varmistukset virtuaalikoneen yhteensopivuudesta FT-ominaisuuden kanssa ja keskeytyy hyvin nopeasti, mikäli yhteensopivuus kriittisten osien osalta puuttuu. Mikäli käyttöönotto sujuu ongelmitta, muuttuu kone tummansiniseksi kuten kuvion 43 kuvankaappauksessa näkyvä valittu Ubuntu-kone.



Kuvio 43. Virtuaalikoneen suojaaminen FT-ominaisuudella alkaa koneen omasta asetusvalikosta

Muutaman yrityksen jälkeen konfigurointi onnistui 32-bittisellä järjestelmällä ja kopio virtuaalikoneesta ilmesty omaksi koneekseen. Virtuaalikoneen käynnistyksen yhteydessä puuttuva tuki iski vastaan estäen käynnistymisen virheilmoituksella. Virheilmoitus kertoi, ettei ESXi-palvelin tue binäärikäännöstä record/replay-toiminnolla. Tämän kiertämiseen ei toiminut prosessorivirtualisoinnin muutokset VMware Workstationin tasolla. Tietohaulla paljastui, että testiympäristön kaltaisessa Nested-ympäristössä (työpöytävirtualisoituna) oli mahdollista huijata virtuaalikone uskomaan, että tuki record/replay-toiminnolla olisi käytössä. Tämä järjestelmän huijaaminen onnistuu menemällä virtuaalikoneen omiin parametreihin ja muuttamalla sekä lisäämällä muutama rivi. Kuviossa 44 on nähtävillä kuvankaappauksen muodossa oleelliset rivit. Parametrien muokkaamiseen tarkoitettu valikko löytyy virtuaalikoneen Option-välilehdeltä. Välilehdeltä navigoidaan General-osioon ja aukeavasta valikosta valitaan Configuration parameters. Rivit replay.allowFT ja replay.supported löytyvät listauksesta false-arvolla jo valmiiksi, joten ne pitää muuttaa arvolle true. Rivi replay.allowBTOnly täytyy lisätä erikseen. Mikäli käynnistyksessä tapahtuu edelleen virheitä, kannattaa arvot käydä tarkastamassa uudestaan. (Building the Ultimate vSphere Lab – Part 11: vMotion & Fault Tolerance 2011; Testing vSphere 5 FT in a VMWare Workstation lab 2012.)



Kuvio 44. Virtuaalikoneen parametreihin tulee lisätä tuki record/replay-toiminnalle, jotta sitä voi testata

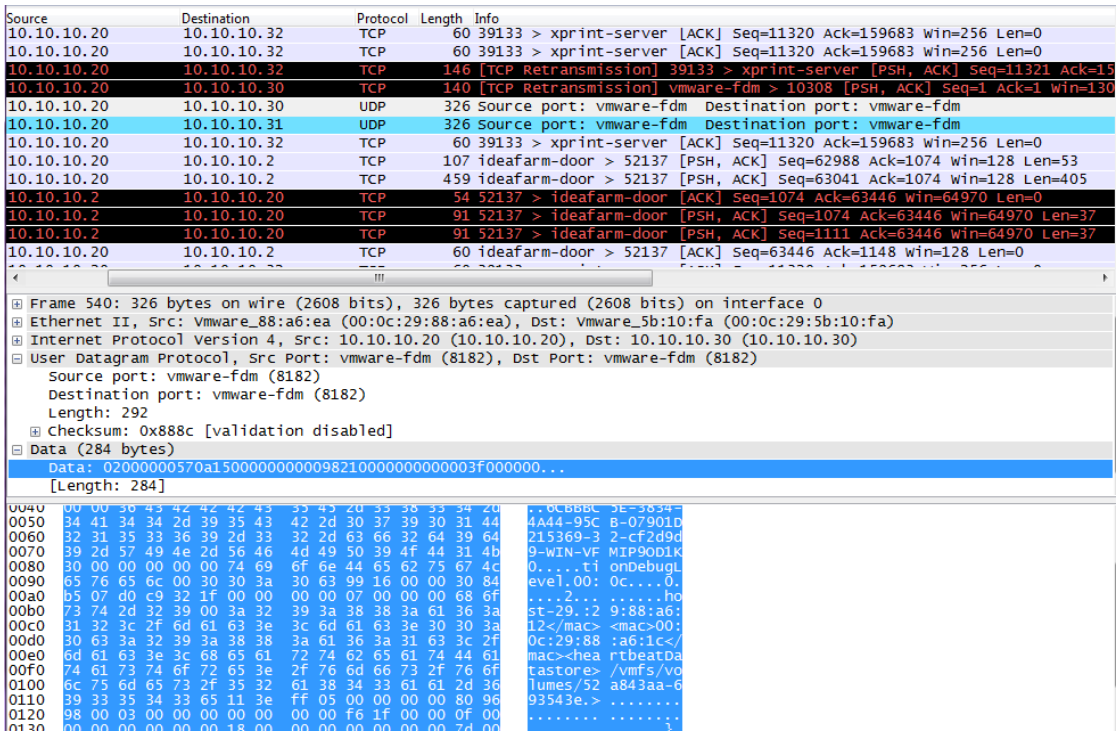
11 Toiminnallisuuden toteaminen ympäristössä

11.1 Verkkoliikenteen analysointi

Toiminnallisuutta testatessa yritettiin ottaa kantaa palvelimien väleillä kulkeviin verkkoviesteihin. Tähän parhaiten soveltuva kolmannen osapuolen sovellus oli avoimeen lähdekoodiin perustuva Wireshark-ohjelmisto. Rajoitteena ohjelmistolla on, että ohjelma seuraa yhden järjestelmässä kiinni olevan verkkorajapinnan läpi kulkevaa toimintaa ja se joudutaan asentamaan olemassa olevan Windows- tai Linux-käyttöjärjestelmän päälle. Näin ollenverkkoliikenteen seuraaminen ei onnistuisi suoraan ESXi-palvelimilta. Ainoaksi järkeväksi seurantapisteeksi muodostui kumpi tahansa työasemia yhdistävistä fyysisistä verkkokorteista, koska niiden läpi kulkisi kaikki vCenter-ESXi -liikenne ja iSCSI-ESXi -liikenne.

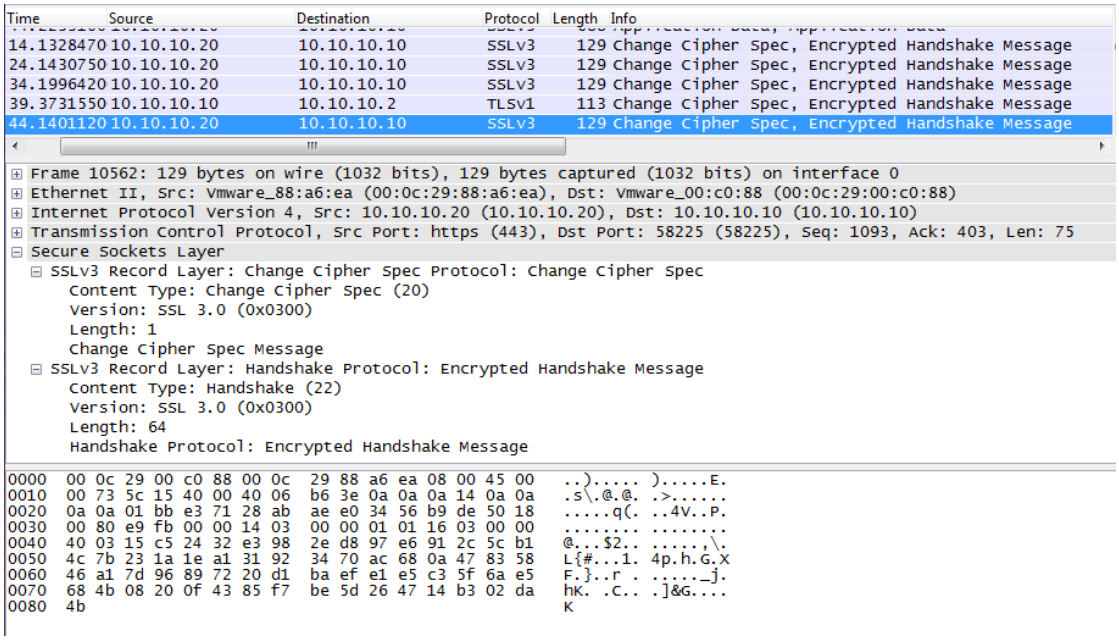
Wireshark-pakettianalysaattoria yritettiinkin käyttää HA- ja FT-ominaisuuksien toiminnan tutkimiseen, mutta tulos jäi laihaksi. Haaviin tarttui ainoastaan muutama ESXi-palvelimen VMware FDM -viesti, jotka yrittivät tavoittaa kaatuneen palvelimen. Teoriaan nojaten vähäinen löydösmäärä johtui Wireshark-analysaattorin sijainnista. Suurin osa HA-toiminnan viestittämisistä kulkee suoraan ESXi-master ja -slave koneiden välillä eli tässä tapauksessa Workstation-ohjelman virtualisointikerroksilla. Fyysisten laitteiden kanssa tutkintaa varten voitaisiin peilata kaikki liikenne halutun kytkimen porteista yhteen porttiin, jossa analysaat-

tori on kiinni, mutta virtualisoinnista johtuen, tämä on testiympäristön osalta mahdotonta. Kuviossa 45 on kuitenkin kuvankaappauksena FDM-paketti tilanteessa, kun 10.10.10.30 kaatui. 10.10.10.20 yrittääkin lähettää kaatuneen palvelimen tunnettuihin hallintaosoitteisiin kuvion alalaidassa avattua heartbeatDatastore-viestiä saamatta kuitenkaan vastausta.



Kuvio 45. Wireshark-ohjelmalla kaapattua liikennettä, jossa näkyvillä vmware-fdm-paketti ja sen sisältämä heartbetDatastore-viesti

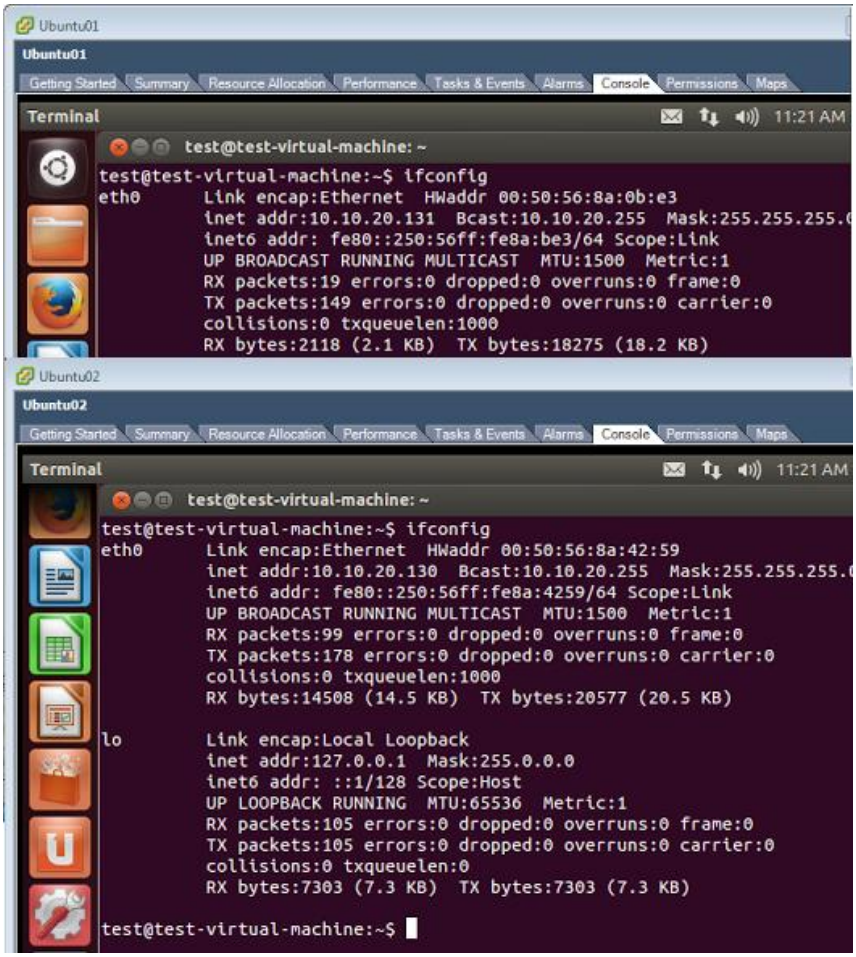
Yleisestä liikenteestä huomionarvoisia asioita oli, että ESXi-palvelimet autentikoivat itsensä vCenter-palvelimen kanssa noin 10 sekunnin välein käyttäen SSLv3-salausta, kuten kuvion 46 kuvankaappauksesta on nähtävillä. Salatun autentikoinnin lisäksi Hello-viestit, joita vCenter-palvelin lähettelee ESXi-palvelimille ovat SSLv3-salattuja, kuin myös application data -paketit. Olettamus on, että application data -paketit sisältävät vCenter-palvelimen lähettämät hallintakäskyt. Salauksista löytyi eroavaisuuksi, sillä vSphere Client -ohjelman ja vCenter-palvelimen välillä kulkevat paketit liikkuvat TLSv1-salattuina. Suurin osa kaapatusta liikenteestä sisälsi iSCSI-paketteja sekä näiden segmentoituja TCP-paketteja.



Kuvio 46. Salattu autentikointikättely näkyy toistuvan kummenen sekunnin välein

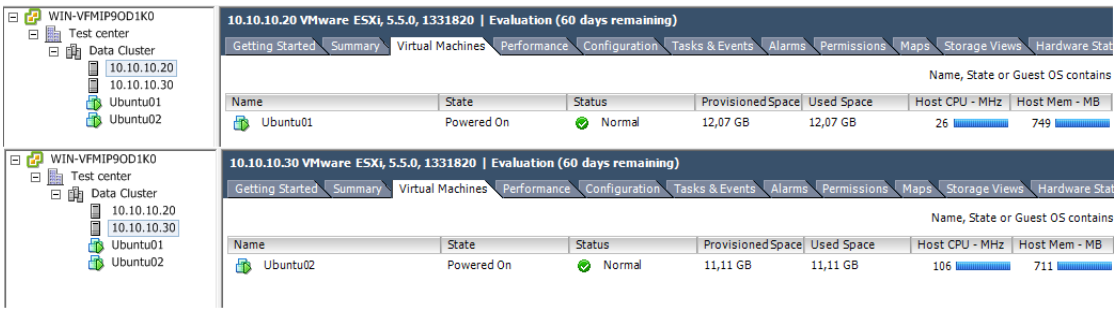
11.2 vMotion

Live migraatiota kokeiltiin siirtämällä suorituksessa ollut Ubuntu-kone alustalta toiselle samalla lähettäen ICMP echo -pyyntöjä toiselta Ubuntu-koneelta. Näin saatiin jonkinlainen suoritusmittari siirron nopeudelle ja katkottomuudelle. Kuvion 47 kuvakaappauksessa on vSphere-järjestelmän päällä olevien kahden virtuaalikoneen konsoli-ikkunat, joissa on nähtävillä molempien koneiden IP-osoitteet. Ubuntu01 sai tässä vaiheessa DHCP-palvelusta osoitteen 10.10.20.131 ja Ubuntu02-kone osoitteen 10.10.20.130.



Kuvio 47. vMotion testissä olleet koneet ja niiden osoitteet

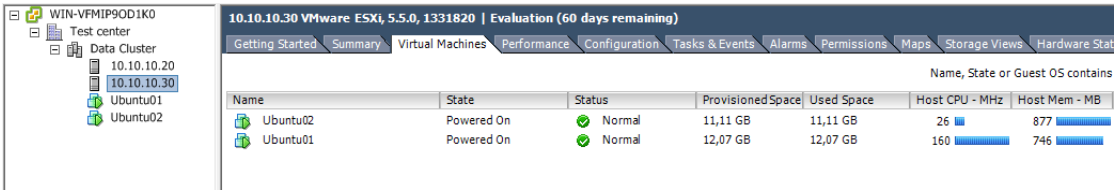
Kuviossa 48 on yritetty todentaa alkutilannetta. Kuvion ylemmässä osassa on avattuna IP-osoitteella 10.10.10.20 olevan ESXi-palvelimen virtuaalikoneet ja alemmassa 10.10.10.30 palvelimen koneet. Kuten kuviosta näkyy, molemmilla ESXi-palvelimilla on suorituksessa vain yksi virtuaalikone ja nämä ovat edellisen kuvion näyttämät virtuaalikoneet.



Kuvio 48. Lähtötilanteessa kumpikin virtuaalikone oli omalla alustallaan

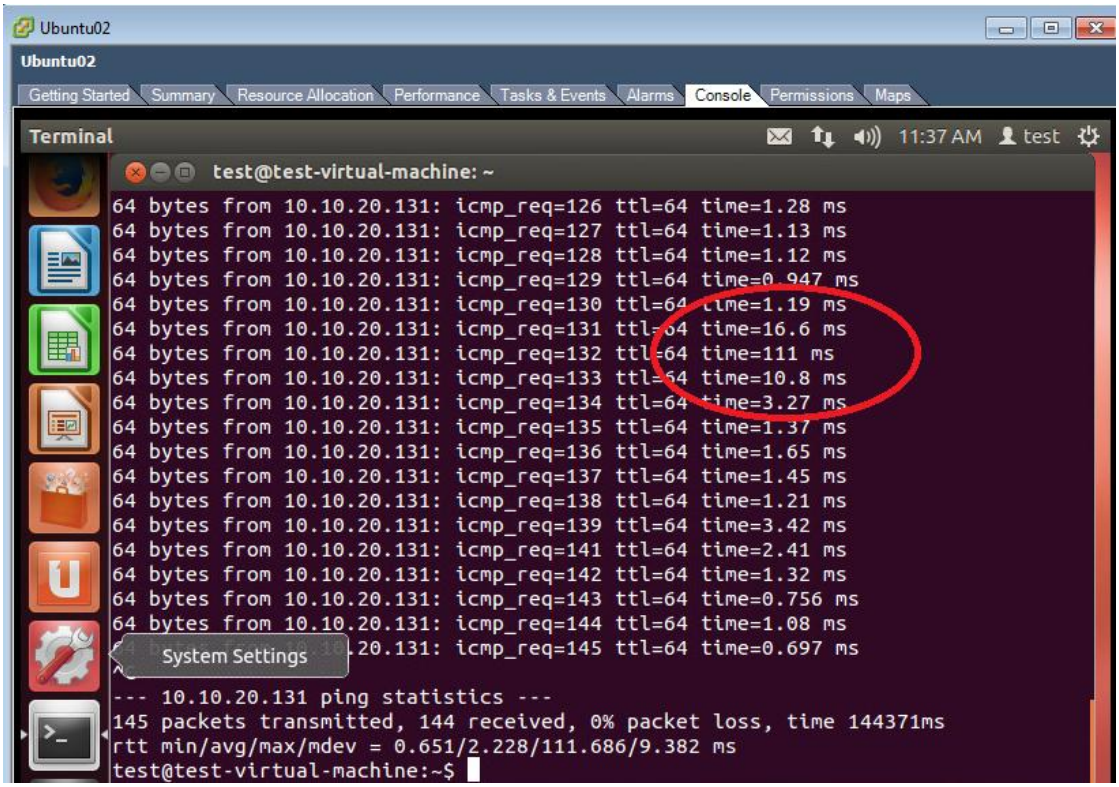
Siirron suorittaminen tapahtuu valitsemalla halutun virtuaalikoneen asetuksista Migrate...-vaihtoehto. Järjestelmä kysyy tämän jälkeen siirretäänkö virtuaalikone, virtuaalilevy, vai mo-

lemmat ja määränpääksi halutun alustan. Tällä kertaa määrityksistä valittiin pelkkä virtuaalikoneen siirto toiselle alustalle. Siirron jälkeen Ubuntu01-koneen suoritus on vaihtunut toiselle ESXi-palvelimelle, kuten kuvion 49 kuvankaappauksesta voi huomata.



Kuvio 49. Onnistuneen vMotion-siirron jälkeen molemmat koneet ovat suoritusessa samalla ESXi-palvelimella

Kuviossa 50 on kuvankaappaus Ubuntu02-koneella tapahtuneesta PING-komennon suorittamisesta. Migraation aiheuttama hetkellinen katkos näkyy yhtenä yli sadan millisekunnin vasteella olevana pakettina. Vasteaikojen perusteella siirron aiheuttamien muutoksien tasaantuminen kestää icmp_req-pakettiin numero 142 asti, jonka jälkeen vasteaika putoaa alle millisekuntiin verkkoliikenteen liikkuessa enää saman ESXi-palvelimen sisällä. Kuvion perusteella voidaankin sanoa, ettei siirto aiheuta palvelua käyttävälle taholle näkyvää katkosta.

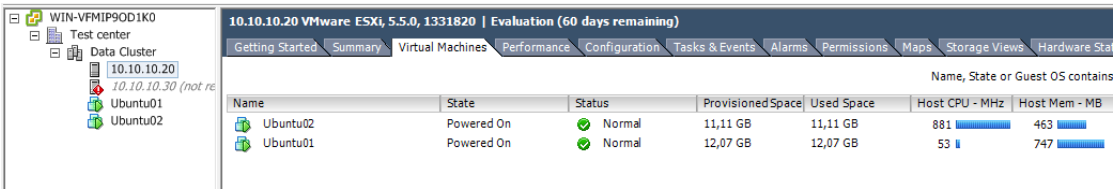


Kuvio 50. vMotion-siirron aiheuttamat muutokset icmp-viestien vasteaikoihin

11.3 HA restart

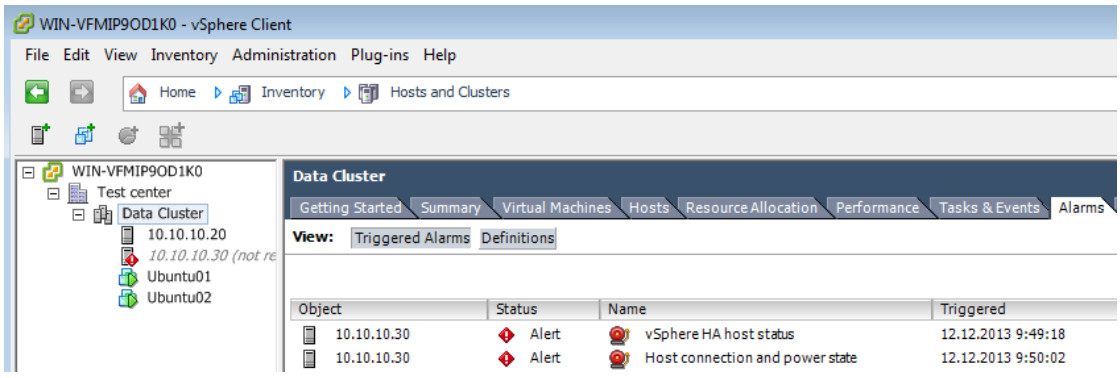
HA-ominaisuuden kytkemisen jälkeen on klusteri koko ajan valmiudessa käynnistää kaatuneen ESXi-palvelimen virtuaalikoneet toisella alustalla palvelujen suojaamiseksi. Tätä samaa suojausta voidaan myös käyttää käyttöjärjestelmien toiminnan monitoroinnin ohella huomaamaan järjestelmän kaatuminen ja huolehtia näin automatisoidusta uudelleenkäynnistyksestä. Perustoimintona kyseessä on siis kylmäkäynnistys, eli palveluun tulee katkos, mutta automatisointi huolehtii koneen uudelleenkäynnistyksestä.

Testiskenaario alkoi samoista lähtökohdista kuin live migraatio, eli yksi käynnissä oleva virtuaalikone per ESXi-palvelin. Alustan vikaantumista ei jääty odottamaan, vaan toinen palvelimista sammutettiin niin kuin sähkönsyöttö olisi katkennut. Automaatio puuttui välittömästi tilanteeseen ja kuten kuvion 51 kuvankaappauksesta näkyy, siirtyi Ubuntu02-koneen suoritus 10.10.10.20-palvelimelle.



Kuvio 51. Rikkoutuneen alustan Ubuntu-kone käynnistyi onnistuneesti toiselle alustalle

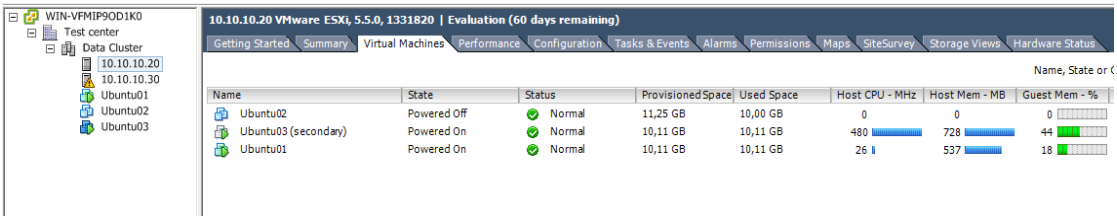
Tiedot tapahtuneesta löytyvät helpoimmin klusterin Alarms- ja Tasks & Events -välilehdiltä. Kuviossa 52 on nähtävillä kuinka automaatio on havainnut palvelimen häviämisen kokonaan resursseista ja antanut hälytyksen aiheesta.



Kuvio 52. Klusterissa aiheutuneet hälyytykset, joiden takia HA restart suoritettiin

11.4 Fault Tolerance

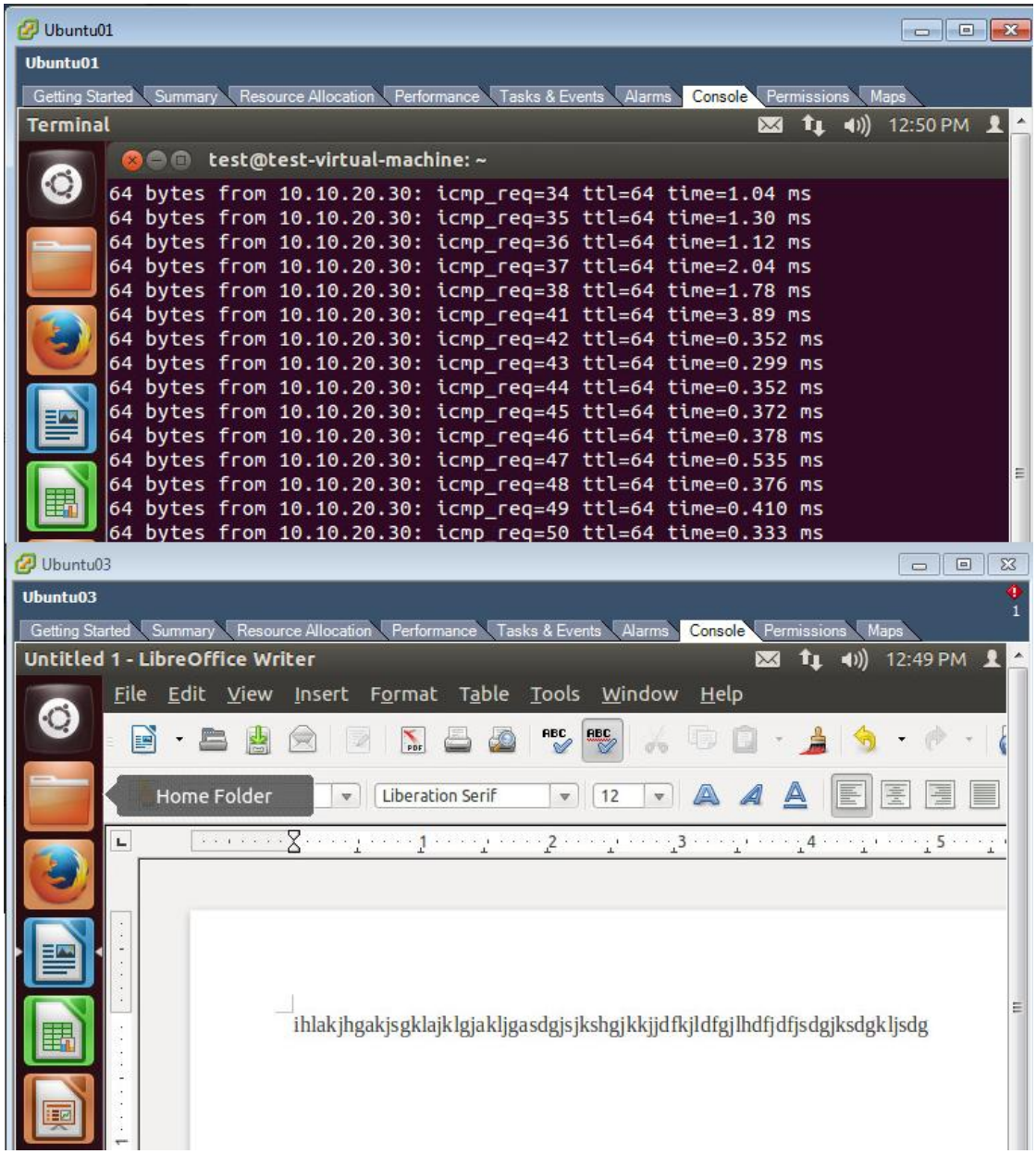
Vikasietoisuusominaisuuden nirsous kävikin jo ilmi aikaisemmissa aihetta käsittelevissä luvuissa, mutta aiheesta ei voi olla kirjoittamatta liikaa. Puuttuva prosessorituki ei siis ole este virtualisoidussa ympäristössä ominaisuuden koestamiseen, mutta kärsivällisyydestä voi nousta este. Toiminnon päälle saaminen tuntui olevan jo sattuman kauppaa. Konfiguroinnin alkaessa ei koskaan voinut olla täysin varma onnistuuko ominaisuuden käynnistäminen vai tuleeko eteen jälleen uusi virheilmoitus. Lisäksi automatiikka tuntui välillä unohtavan kopioida toissijaisen koneen toiselle palvelimelle. Kävi nimittäin niin, että onnistuneen konfiguroinnin jälkeen järjestelmä valitti molempien koneiden olevan odottamassa käynnistystä samalla ESXi-palvelimella. Onneksi Fault Tolerance -valikosta löytyy myös vaihtoehto Migrate Secondary, jolla tilanteen voi korjata. Kuviossa 53 on hienosti nähtävillä onnistuneen käynnistyksen tuottama tilanne, jossa sekundaarikone myös käynnistyi.



Kuvio 53. Onnistuneen FT-konfiguraation jälkeen myös toissijainen kone näkyy omana koneenaan klusterin valikoissa

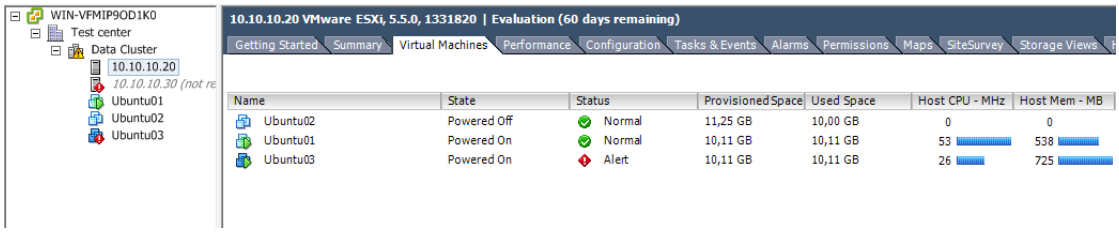
Onnistuneen konfiguroinnin ja suojatun koneen käynnistämisen jälkeen seuraa pitkä odotus. Koneen käynnistymiseen kulunutta aikaa ei mitattu tarkasti, mutta työpöytä tuli käytettäväksi muutaman kymmenen minuutin odottelun jälkeen. Huomio käynnistyksen aikana kiinnittyi virtuaalikoneen prosessorin käyttöön, sillä se oli koko käynnistämistoimenpiteen ajan sadassa prosentissa. Myös yksinkertaisetkin toimenpiteet virtuaalikoneella saivat aikaan prosessorikuorman kovan rasituksen.

Virtuaalikonetta oli kuitenkin mahdollista käyttää. Tästä osoituksena kuvankaappaus kuviossa 54, jossa FT-suojattuun Ubuntu-koneeseen on saatu auki LibraOffice-kirjoitusohjelma ja tekstiä ohjelmaan. Kuviossa on myös juokseva PING-komento seuraamassa suojatun koneen vastaamista vian sattuessa. Ubuntu03-koneen alustana toimivan palvelimen vikaantuminen tapahtui icmp_req-paketin numero 38 paikkeilla, jonka jälkeen seuraa hetken tauko ja paketin 42 kohdalla koneen suoritus ja verkko on siirtynyt onnistuneesti samalle alustalle Ubuntu01-koneen kanssa. Tästä kielii myös lyhentynyt vasteaika, joka putoaa millisekunnista noin millisekunnin kolmasosaan. Vaikka muutama paketti ehti hukkua, on näinkin lyhyt vasteaika merkittävä saavutus vikatilanteessa.



Kuvio 54. Suojatun virtuaalikoneen ja sitä vastauspyynnöillä pommittavan koneen konsoliruudut

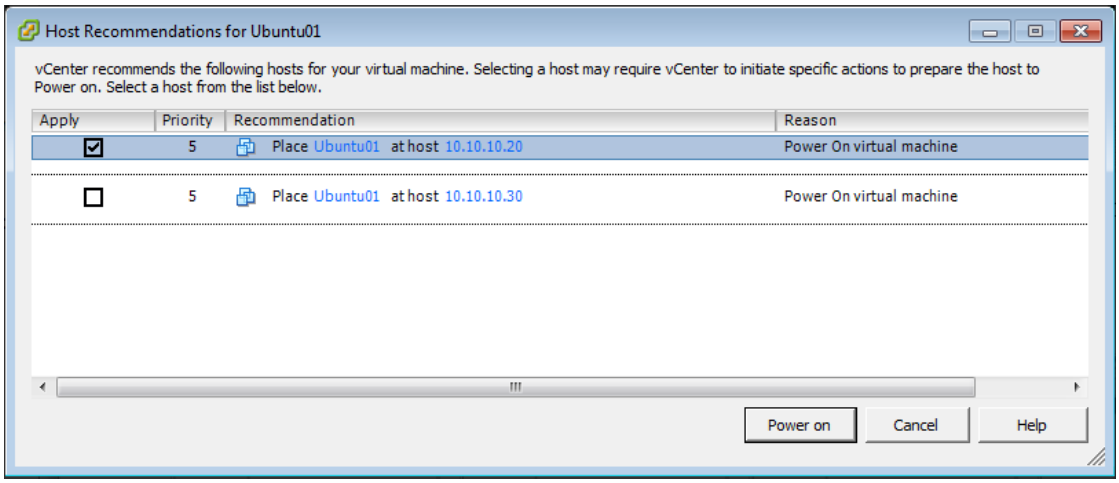
Odottamisesta huolimatta Ubuntu03-koneen konsoliruutu ei suostunut näyttämään mitään siirron jälkeen. Vastaukset PING-paketteihin varmensivat riittävän hyvin koneen toiminnan siirtymisen toiselle alustalle ilman merkittävää käyttökatkosta näinkin yllättävän vikaantumisen takia. Kuviossa 55 on vielä nähtävillä tummansinisenä näkyvän Ubuntu03-koneen suorituksen oleva ehjällä palvelimella. Kone kuitenkin hälyttää, koska siitä ei saada kopioitua toissijaista toiselle palvelimelle klusterin pitäessä sisällään vain kaksi ESXi-palvelinta.



Kuvio 55. Palvelu jatkuu vikatilanteesta huolimatta ja suoritus onkin onnistuneesti ehjällä palvelimella

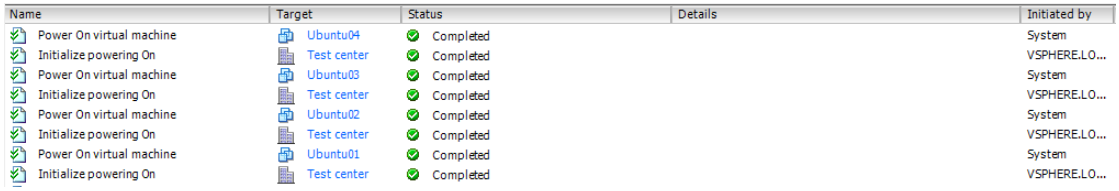
11.5 Distributed Rersource Scheduler

Distributed Resource Scheduler -toiminnon koeistamista varten asetettiin automaatio mahdollisimman passiiviseksi. Tarkoituksena oli saada ohjelma tekemään itse ehdotelmat siirroista ja käynnistämisistä. Ominaisuuden käyttöönoton jälkeen virtuaalikoneiden käynnistämistä seurasi kuvion 56 mukainen ilmoitus alustasta, jolla olisi parhaimmat mahdollisuudet virtuaalikoneen pyörittämiseen. Kyseessä on kuitenkin vain ehdotelma, jota ei välttämättä tarvitse seurata.



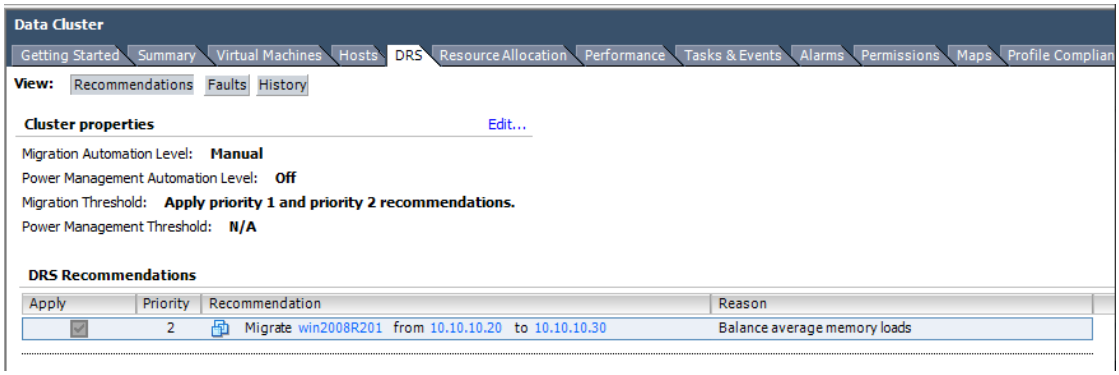
Kuvio 56. Virtuaalikoneen käynnistämisen yhteydessä esiintyvä ehdotelma sopivasta alustasta.

Ominaisuutta kokeiltiin myös automatisoituna. Tällöin neljä virtuaalikonetta oli odottamassa käynnistämistä samalla ESXi-palvelimella. Koneiden käynnistyksen yhteydessä puolet koneista käynnistettiinkin automaatin toimesta toisella alustalla. Tätä on kuvattu kuvion 57 kuvankaappauksessa, jossa virtuaalikoneen käynnistyksen laukaisseet työrivit ovat vsphere.local\administratorin suorittamia, mutta varsinaiset käynnistysrivit olivat järjestelmän itsensä tuottamia.



Kuvio 57. vSphere DRS jakoi neljän koneen käynnistymisen tasan kahdelle alustalle

Virtuaalikoneiden rasittuessa syntyi myös tilanne, jolloin toisen ESXi-palvelimen muisti oli loppumassa. Kyseisessä tilanteessa toisella palvelimella ei ollut työkuormaa. Tällöin klusterin Summary-välilehdelle tuli näkyviin DRS-toiminteen tuomia ehdotelmia klusterin tasapainottamiseksi. Nämä ehdotelmat ovat tarkemmin luettavissa klusterin DRS-välilehdeltä, kuten kuviossa 58 on nähtävillä.



Kuvio 58. Muistin loppuessa ESXi-palvelimelta, tekee DRS ehdotelman tasapainoa tuovasta siirrosta

11.6 Jumbo Frames

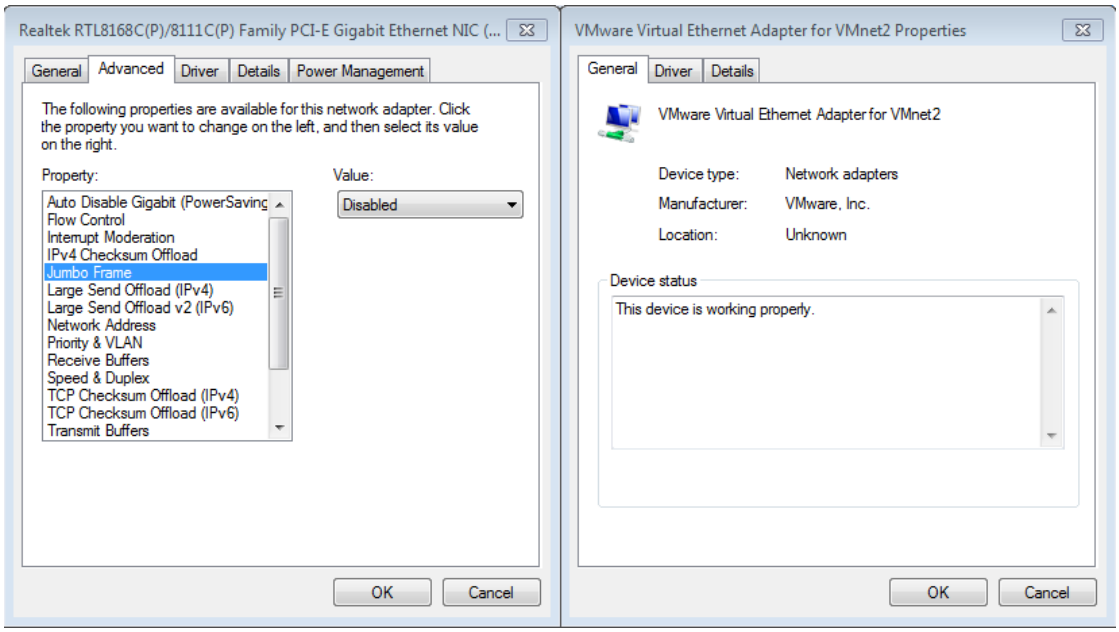
OSI-mallin toisen kerroksen Ethernet-kehykset ovat normaalisti maksimissaan 1500 tavun mittaisia. Tavumäärään sisältyy siirrettävän datan lisäksi myös otsikkotietoja, jotta eri protokollat osaavat hyödyntää paketissa olevia osoitetietoja ja purkaa sen lopulta vastaanottopäässä. Normaalioloissa 1500 MTU (Maximum Transmission Unit) on riittävän suuri kehyskoko käytettäväksi tietoverkoissa ja yleensä paketit ovatkin paljon tätä maksimia pienempiä. Tilanteissa, joissa siirretään paljon dataa isoina paketteina, olisi MTU-arvon parempi olla suurempi. Näin ollen kehykset, joiden MTU on 1501-9000, kulkevatkin nimellä Jumbo Frames. (iSCSI and Jumbo Frames configuration on VMware ESX and VMware ESXi (1007654) 2013.)

ESXi-palvelimien tapauksessa iSCSI-tiedostonsiirrossa joudutaan lähes poikkeuksetta siirtämään paljon maksimimittaisia paketteja. Koska sama otsikkotieto vaaditaan jokaisen kehyksen toimittamiseen perille, olisikin järkevää saada pakettikokoa suuremmaksi. Näin hyötyda-

tan määrä nousisi suhteessa otsikkodatan määrän. Toimenpide vaatii kuitenkin verkolta tukea toimiakseen. VMware suosittelee nostamaan MTU-yksikön koon 9000 tavuun, jotta tiedostonsiirto nopeutuisi. Tätä yritettiin koestaa myös testiympäristössä. (iSCSI and Jumbo Frames configuration on VMware ESX and VMware ESXi (1007654) 2013.)

MTU-arvon muuttaminen täytyy ESXi-palvelimien tapauksessa tehdä kytkimen asetuksissa muuntamalla koko kytkimen MTU-arvoksi 9000. Koska hallintaliikenne ja iSCSI-liikenne kulkevat ympäristössä samassa IP-verkossa, täytyy myös hallintayhteyksien käyttää suurempaa kehystä. Kuitenkin käytännön testit osoittivat, että palvelimesta kannattaa ottaa Snapshot-palautuspiste ennen kokeiluja tai tehdä toinen erillinen hallintaverkko, jolla palvelimeen pystyy yhdistämään toista kautta.

Kokeiluissa hallintayhteys tuhoutui täysin MTU-arvon muutaamisen vuoksi, eikä asiaa auttanut sekään, ettei Workstation-ohjelman VMnet-rajapintoihin löytynyt asetusta jumbokehyksille. Kuviossa 59 onkin kuvankaappaus, jossa vasemmalla laidalla näkyy normaalin verkkokortin asetusvalikko ja sieltä löytyvä vaihtoehto jumbokehysten aktivoimiseen. Vastaava asetussivu puuttuu kokonaan VMnet-rajapinnan asetusvalikoista. Ongelma hallintayhteyksienkin katkeamiselle johtuu näin ollen rajapintojen MTU yhteensopivuusongelmista.



Kuvio 59. Jumbo Frames -asetusta ei ole valittavissa VMnet-rajapintaan samalla tavalla kuin fyysiseen verkkorajapintaan

VMwaren omia sivuja selaamalla ei löytynyt suoraa vastausta Workstation-ohjelman verision yhdeksän kykyyn hoitaa jumbokehyksiä. Sen sijaan ohjelman versio seitsämän Best Practices -dokumentista (Performance Best Practices for VMware Workstation 2009, 32.) löytyi tieto

ettei kyseinen versio tue jumbokehyksiä. Oppilaitoksen suhteiden kautta laitettiin kyselyä myös VMwaren suuntaan aiheesta, mutta vastaukseksi saatiin vain epämääräinen "ei tuettu"-vastaus. Näin ollen jumbokehysten toimintaa ei ole mahdollista soveltaa Workstation-ohjelman päälle rakennetussa ympäristössä.

12 Yhteenveto

12.1 Työn tuloksien yhteenveto

Opinnäytetyö lähti liikkeelle Jyväskylän Ammattikorkeakoulun tarpeesta saada kattava selonteko VMware vSphere -tuotteesta. Teoriaosuuden selonteon avulla oli myös tarkoitus tuottaa käytännönratkaisu ympäristöstä, jota voitaisiin käyttää mallina oppilaitoksen koulutuskäytössä. Näitä tavoitteita silmällä pitäen keskityttiin VMware vSphere -ohjelmiston ominaisuuksiin, joiden katsottiin olevan oleellisimpia palvelinvirtualisoinnin ymmärtämisen kannalta. Työssä ei esimerkiksi puututtu juurikaan ympäristön tietoturvaan tai sen edistämiseen. Karsiminen kohdistui myös varsinaisiin palvelimiin, sillä työhön ei tässä vaiheessa nähty tuovan lisäarvoa esimerkiksi toimivan AD-ympäristön pystytys vSphere-ohjelmalla virtualisoituna. Käytännön testeihin riittivät erittäin hyvin virtuaalikoneet ilman varsinaisia palveluja.

Teoriaosuudesta muodostui lopulta riittävän kattava ja se sivuaa lähes koko tietoverkkotekniikan insinöörikoulutusohjelmaa käyden läpi tietoverkkoja, palvelimia, virtualisointia, palveluiden jatkuvuutta ja tietokoneiden komponenttien resursseja. Vaikka teoriaosuus kattaakin yli puolet koko opinnäytetyön pituudesta, olisi se voinut ollu laajempi esimerkiksi virtuaalikoneiden luomista käsittelevän luvun osalta. Ajan ja työmäärän puitteissa oli kuitenkin pakko karsia jostain.

Käytännön osuutta oli alkuun hankala hahmottaa toimivana kokonaisuutena, koska jokainen ominaisuus tuntui lisäävän uusia ehtoja alkuperäiseen kokoonpanoon. Asiaa ei auttanut, että ensimmäinen vedos käytännönosuudesta toteutettiin samaan aikaan teoriaosuuden kanssa ja tämän takia törmättiin usein hienoisiin vaikeuksiin saada tarvittavat ominaisuudet toimintaan. Käytännönosuutta oli osaltaan myös rajoittamassa testiympäristön ominaisuudet, joista erityisesti käytössä oleva fyysinen verkko rajoitti käytännön ratkaisua. Tämä myös näkyi verkkoliikenteen tutkimisen hankaluudessa.

Käytännönosuuden perusteella haluttiin luoda alustavat rungot harjoituksille, joita opinnäytetyön pohjalta alettaisiin valmistella. Näiden harjoitusten kuvaukset löytyvät opinnäytetyön Liitteet-osiosta. Harjoituksia varten sanottiin olevan varattu kolme noin kuuden tunnin mittaista sessiota, joten käytäntö pyrittiin jakamaan kolmeen osaan.

12.2 Parannusehdotuksia

Osassa käytännönosuutta kuvaavista todennuksista oli jonkin verran parantamista esimerkiksi kuvioiden kannalta. Todennuskuvat otettiin kuitenkin ennen käytännönosuuden kirjoitusprosessia ja kokeilulisenssin päättymisen jälkeen. Kuvioissa näkyviin kuvankaappauksiin olisikin voinut käyttää enemmän aikaa suunnitteluun ja paremman kokonaisuuden hahmottelemiseen jo etukäteen. Työhön valitut kuviot valittiin kuitenkin mahdollisimman hyvin kaikista otetuista kuvankaappauksista.

Opinnäytetyön kirjoitusprosessi osoittautui myös osittain haasteelliseksi johtuen pitkälti siitä, että kaikki lähteet olivat englanninkielisiä. Tiedon keräämisen lisäksi täytyi tehdä paljon käännöstyötä, ja koska ICT-ala kehittyy niin hurjalla vauhdilla myös termistönsä osalta, ei kaikelle ole järkevää käännöstä. Kirjoittamista vaivasikin jatkuva mietintä siitä, että mitkä osat termistöstä voi ylipäätänstä kääntää. Tästä jäi varmasti näkyviä jälkiä kielellisen sujuvuuden osalta.

Verkkoliikenteen seuraamista varten olisi voitu pystyttää vielä yksi ESXi-palvelin työasemalle, joka pyöritti vCenter- ja iSCSI-palvelimia. Näin ESXi-palvelimien liikennöinnistä olisi saatu kattavampi kuva ja paremmat kaappaukset Wireshark-analysaattorilla. Hallintaverkkoa varten olisi myös voinut tehdä molemmille Workstation-ohjelmille reitittävän Unix-koneen, jotta liikennettä olisi voinut ohjata paremmin. Tämä olisi kuitenkin aiheuttanut entistä suurempaa resurssien käyttöä, mutta olisi myös antanut lisää mahdollisuuksia liikenteen tutkimiselle. Lisäksi ESXi-virtuaalikytkimiä olisi voinut tehdä enemmän, jotta eri ominaisuuksien tarvitsemat VMkernel-portit olisi saatu jaoteltua selkeämmin. Tämä asia haluttiin ottaa paremmin huomioon käytännönharjoituksissa, joita lähdettiin suunnittelemaan opinnäytetyön pohjalta.

Lähteet

About VMware SiteSurvey. 2013. VMwaren tukisivusto SiteSurvey-lisäosasta. 2013. Viitattu 13.12.2013. https://www.vmware.com/support/sitesurvey/help_2_5_2.html

Al-Dabbas, A. 2012. Using VM Workstation for advanced networking. Tekninen verkkoblogi. 19.9.2012. Viitattu 22.10.2013. http://www.trainsignal.com/blog/vm-workstation-advanced-networking

Baroudi, C. 2009. Green IT for Dummies. Indianapolis, Yhdysvallat: Wiley Publishing, Inc.

Building the Ultimate vSphere Lab – Part 11: vMotion & Fault Tolerance. 2011. Beorlowie's Blog -blogikirjoitus. 16.12.2011. Viitattu 14.12.2013. http://boerlowie.wordpress.com/2011/12/16/building-the-ultimate-vsphere-lab-part-11-vmotion-fault-tolerance/

Configuring the VMware vCenter server appliance. 2013. VMware vSphere 5.5 Documentation Center, ohjelmiston dokumentaatiosivusto. 2013. Viitattu 20.10.2013. http://pubs.vmware.com/vsphere-55/index.jsp

HA Error: The number of heartbeat datastores for host is 1, which is less than required: 2 (2004739). 2011. VMware Knowledge Base. 26.10.2011. Viitattu 10.12.2013. http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2004739

Happe, D., Humphrey, G., Muller, A. & Wilson, S. 2005. Virtualization with VMware ESX Server. Yhdysvallat: Syngress Publishing Inc.

High availability in campus network deployments. 2004. Cisco Networkers -esitys. Viitattu 28.10.2013. http://www.cisco.com/networkers/nw04/presos/docs/RST-2514.pdf

Intel Core i7-920 Processor. 2013. Prosessorin tekniset tiedot valmistajan verkkosivuilla. 4.8.2013. Viitattu 11.1.2014. http://ark.intel.com/products/37147/Intel-Core-i7-920-Processor-8M-Cache-2_66-ghz-4_80-gts-Intel-qpi

iSCSI and Jumbo Frames configuration on VMware ESX and VMware ESXi (1007654). 2013. Knowledge base. Verkossa oleva tukisivusto ominaisuuksien käytöstä. 7.10.2013. Viitattu 3.2.2014. http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1007654

iSCSI Naming Conventions. 2013. VMware vSphere 5.5 Documentation Center. 2013. Viitattu 27.1.2014. http://pubs.vmware.com/vsphere-55/index.jsp#com.vmware.vsphere.storage.doc/GUID-686D92B6-A2B2-4944-8718-F1B74F6A2C53.html?resultof=%2522%2569%2573%2563%2573%2569%2522%2520%2522%2569%2571%256e%2522%2520

Jorgenson, P. 2012. Virtual Networking 101: Understanding VMware Networking. Tekninen verkkoblogi. 30.5.2012. Viitattu 22.10.2013. http://www.trainsignal.com/blog/virtual-networking-101-understanding-vmware-networking

Lowe, S. 2011. Mastering VMware vSphere® 5. Indianapolis, Yhdysvallat: John Wiley & Sons, Inc.

Minimum system requirements for installing ESXi/ESX (1003661). 2013. Knowledge base. Verkossa oleva tukisivusto ominaisuuksien käytöstä. 25.1.2013. Viitattu 11.1.2014. http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1003661

Minimum system requirements for installing VMware vCenter Server (1003882). 2013. Knowledge base. Verkossa oleva tukisivusto ominaisuuksien käytöstä. 17.10.2013. Viitattu 11.1.2014. http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1003882

Novak, J. & Simpson, T. 2010. Hands-On Virtual Computing. Yhdysvallat: Course Technology, Cengage Learning

Performance Best Practices for VMware Workstation. 2009. Ohjelmistotuottajan sähköinen kirja. Viitattu 24.10.2013. http://www.vmware.com/pdf/ws7_performance.pdf

Rouse, M. 2011. iSCSI (Internet Small Computer System Interface). Tekninen verkkojulkaisu. Toukokuu 2011. Viitattu 23.1.2014. http://searchstorage.techtarget.com/definition/iSCSI

Rouse, M. 2012. VMware Snapshot - Best practices, tips and tools for VMware virtual recovery and backup. Tekninen verkkojulkaisu. Joulukuu 2012. Viitattu 26.11.2013. http://searchvmware.techtarget.com/definition/VMware-snapshot

Selecting the Number of Processors for a Virtual Machine. 2012. VMware Workstation 9 Documentation Center. 2012. Viitattu 11.1.2014. http://pubs.vmware.com/workstation-9/index.jsp#com.vmware.ws.using.doc/GUID-9745D560-9243-4262-A585-D709D52B1349.html?resultof=%2522%2570%2572%256f%2563%2565%2573%2573%256f%2572%2522%2520

Testing vSphere 5 FT in a VMWare Workstation lab. 2012. Happy SysAdm -blogikirjoitus. 27.2.2012. Viitattu 14.12.2012. http://www.happysysadm.com/2012/02/testing-vsphere-5-ft-in-vmware.html

Using the Virtual Network Editor in VMware Workstation (1018697). 2013. Knowledge base. Verkossa oleva tukisivusto ominaisuuksien käytöstä. 6.9.2013. Viitattu 22.10.2013. http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1018697

Virtualization Overview. 2006. VMware white paper. Valmistajan verkkojulkaisu. 3.6.2006. Viitattu 15.10.2013. http://www.vmware.com/pdf/virtualization.pdf

VMware Compatibility Guide. 2014. VMwaren yhteensopivuushakusivusto. 2014. Viitattu 28.1.2014. http://www.vmware.com/resources/compatibility/search.php

VMware High Availability cluster reports the error: Could not reach isolation address (1002787). 2011. VMware Knowledge Base. 22.9.2011. Viitattu 10.12.2013. http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1002787

VMware Workstation. 2013. VMware Workstation 10 - Taking virtualization to the next level. Tuotekuvaus verkkojulkaisuna. Viitattu 21.10.2013. http://www.vmware.com/products/workstation/

VMware Workstation 5.5 Custom Networking Configurations. 2006. Ohjelmiston tukisivuilla oleva artikkeli. 9.6.2006. Viitattu 30.10.2013.
https://www.vmware.com/support/ws55/doc/ws_net_configurations_custom.html

Benefits of server virtualization. 2013. VMware vSphere -ohjelmiston sisäinen ohjekirja. 2013. Viitattu 20.11.2013.

Liitteet

Liite 1. Harjoitusten kuvaus

Harjoitukset vaativat oppilaitoksen it-tuelta valmistavia toimenpiteitä. Nämä toimenpiteet koskevat lähinnä VMware Workstation -ohjelmaa ja sen verkkosovittimia. Koska opiskelijoilla ei ole riittäviä oikeuksia rajapintojen luomiseen, täytyy jokaiselle harjoituksissa käytettävälle koneelle tehdä työssä mainitut neljä VMnet-verkkoa. Yksi näistä siltaa liikennettä koneita yhdistävään rajapintaan, toinen tarjoaa sisäiset hallintaverkon liitokset, kolmas varataaan ESXi-palvelimien virtuaalikoneiden välistä liikennöintiä varten ilman Windows-koneelle näkyvää adapteria ja neljäs siltaa liikennettä ulkoverkkoon. VMnet-verkkojen lisäksi täytyy työasemia yhdistävät rajapinnat valmistella hallintaverkkoon kuuluvalla IP-osoitteella sekä antaa hallintaverkkoon kuuluvalle sisäisen verkon Windows-rajapinnalle IP-osoite.

Harjoitus 1. Ympäristön perusteet

Tässä harjoituksessa pyritään tarjoamaan teoriapohja kokonaisuuden hamottamiselle. Ryhmä jaetaan pareihin, joille kerrotaan käytännön järjestelyistä työasemien osalta. Näillä toimenpiteillä pyritään varmistamaan perusasioiden ymmärrys siitä, kuinka verkko tulee jatkossa toimimaan ympäristöä käsiteltäessä.

Tämän jälkeen koneille haetaan ja asennetaan VMware Workstation -ohjelman päälle asennettavat käyttöjärjestelmät ja valmistellaan ESXi- ,iSCSI ja vCenter-palvelimet. ESXi- ja vCenter-lisenssejä varten ryhmät joutuvat tekemään tunnukset VMwaren verkkosivuille. Harjoitus katsotaan päättyneeksi, kun ryhmällä on asennettu vCenter-palvelin, hallintaosoitteilla varustetut ESXi-palvelimet ja konfiguroitu iSCSI-target -palvelin yhdellä tai useammalla LUN-levyllä. Koneista otetaan vielä varmuuden vuoksi Snapshot-tallennukset tässä vaiheessa.

Harjoitus 2. Klusterin rakentaminen

Tässä harjoituksessa molemmat ryhmäläiset ottavat hallintayhteydet vCenter-palvelimeen ja aloittavat yhdessä klusterin rakentamisen ensin liittämällä ESXi-palvelimet osaksi klusteria. Tämän jälkeen molempiin palvelimiin luodaan erilliset virtuaalikytkimet hallinta- ja iSCSI-verkkoa varten. Molempiin palvelimiin lisätään myös iSCSI-ohjaimet ja ne liitetään iSCSI-levyjärjestelmään.

Onnistuneen iSCSI-liitoksen jälkeen siirretään asennustiedostot halutuista käyttöjärjestelyistä levyjärjestelmälle ja asennetaan ensimmäiset virtuaalikoneet. Tässä vaiheessa ryhmät voivat tutustua virtuaalikoneita koskeviin hallinta-asetuksiin ja luoda tarvittaessa asennetusta pe-

rusjärjestelmästä templaatin. Valmistuneiden virtuaalikoneiden asentamisen jälkeen luodaan uusi virtuaalikytkin vMotion-ominaisuutta varten ja kokeillaan ominaisuutta käytännössä. Opiskelijat voivat halutessaan pystyttää yksinkertaisen palvelun siirrettävälle virtuaalikoneelle, mitä käytetään siirron aikana. Näin pyritään varmistumaan siirron tehokkuudesta. Harjoitus päättyy vMotion-ominaisuuden tutkimiseen.

Harjoitus 3. vSphere HA - ja DRS -ominaisuudet

Harjoituksessa käydään hiukan teoriaa ominaisuuksien vaatimuksista ja käytännön tekeminen aloitetaan selvittämällä rakennetun klusterin puutokset vSphere HA -ominaisuuden toimintaan saattamisen kannalta. Onnistuneen HA-konfiguroinnin jälkeen tutustutaan HA-asetuksiin hiukan laajemmin ja kokeillaan aiheuttaa vikatilanne, josta klusterin täytyy selvitä. HA-toiminteisiin voidaan syventyä myös käyttöjärjestelmäkohtaisen monitoroinnin saattamiseksi toimintaan ja kokeilemalla itse aiheuttaa käyttöjärjestelmän vikaantuminen.

Tämän jälkeen kytketään vSphere DRS -toiminto päälle ja kokeillaan automaation tuomia uudistuksia klusterissa. Toiminnan todentamista varten kokeillaan virtuaalikoneiden käynnistämista ja pyritään jakamaan ESXi-palvelimien kuormitus epätasaisesti, jotta nähdään ominaisuuden toimintaa. Opiskelijat voivat vielä todentaa affinity-valintaa ja kokeilla mitä anti-affinity-sääntö saa aikaan kahden koneen klusterissa.

Viimeisenä osana opiskelijoiden tulee joko manuaalisesti tietoa hakemalla tai SiteSurvey-lisäosan avulla selvittää klusterin yhteensopivuus Fault Tolerance -ominaisuuden kanssa. Opiskelijoiden tulee myös selvittää, mitä toimenpiteitä virtuaalikoneet vaativat, jotta ominaisuutta voitaisiin kokeilla ilman prosessoritukea. Tämä harjoituksen osa tulee olemaan haastavin kaikista ja edes perusteellisilla ohjeilla sen onnistuminen ei ole varmaa. Harjoitus katsotaan päättyneeksi onnistuneen FT-todennuksen jälkeen tai ajan loppuessa.