KYMENLAAKSON AMMATTIKORKEAKOULU
Elektroniikan koulutusohjelma / Tietoliikenne

Ville Ahola

PALVELINKLUSTERI JA VERKKOLEVY

Opinnäytetyö 2010

TIIVISTELMÄ

KYMENLAAKSON AMMATTIKORKEAKOULU

Elektroniikka / Tietoliikenne

Ahola, Ville	Palvelinklusteri ja verkkolevy
Opinnäytetyö	46 sivua
Työn ohjaaja	Martti Kettunen
Toimeksiantaja	Kymenlaakson ammattikorkeakoulu
Maaliskuu 2010	
Avainsanat	iSCSI, verkkolevyt, SimuNet, blade server, blade-palvelin

Tämän opinnäytetyön aiheena oli palvelinklusteri, tiedontallennukseen tarkoitettu iSCSI-verkkolevy ja tietojen hankkiminen suurempien tietomassojen käsittelystä. Työn tavoitteena oli rakentaa Kymenlaakson ammattikorkeakoulun ICTLAB-opetusympäristön SimuNet-opetuslaboratorioon tietoverkko-operaattorin palvelimia kuvaava VMware-käyttöjärjestelmää hyödyntävä virtuaalipalvelinalusta. Toisaalta tavoitteena oli pohtia suurempien palvelinklusterikokonaisuuksien toimintaa ja massiivisten tietovarastojen ylläpitoa.

Klusterin tekemiseen hankittiin kaksi niin sanottua blade-palvelinta ja iSCSI-verkkolevyjärjestelmä. Palvelimet sijoitettiin eri laitekaappeihin kuvaamaan niiden sijoittumista maantieteellisesti eri paikkoihin, joskin yhden kaupungin sisällä. Klusterista tuli virittää vikasietoinen korkean saatavuuden järjestelmä. Toteutettujen virtualisoitujen palvelimien kaikki data tallennetaan itsenäiselle verkkolevylle, josta se on kaikkien klusterin palvelimien käytettävissä.

Korkean saatavuuden saavuttamiseksi kaikki klusterin verkkoyhteydet kahdennettiin ja klusterin sisäinen liikenne eristettiin kokonaan muista tietoverkoista tälle asialle varattuihin verkkoportteihin. Muista verkoista eristäminen toteutettiin tietoturvasyistä. Klusterin hallinta liitettiin ICTLAB-oppimisympäristön tuotantoverkkoon, jotta palvelimien hallinta helpottuisi ja ne voitaisiin liittää omaksi kokonaisuudekseen laboratorion jo olemassa olevaan palvelinhallintaan.

Tuloksena valmistui SimuNet-opetuslaboratorioon sijoitettu hyvin toimiva, helppokäyttöinen ja vikasietoinen virtuaalipalvelinalusta simuloimaan tietoverkko-operaattorin palvelinjärjestelmiä.

ABSTRACT

KYMENLAAKSON AMMATTIKORKEAKOULU
University of Applied Sciences
Electronics / IT telco.

AHOLA, VILLE	Server Cluster and Network Data Storage
Bachelor's Thesis	46 pages
Supervisor	Martti Kettunen, Principal Lecturer
Commissioned by	Kymenlaakson Ammattikorkeakoulu oy KyAMK University of Applied Sciences
March 2010	
Keywords	blade server, iSCSI, server cluster, virtual servers

This paper discusses the Blade server cluster and iSCSI data storage for the KyAMK University of Applied Sciences SimuNet laboratory. Besides the Bachelor's thesis work documentation, this paper contains theoretical considerations about much larger-scale Cluster networks. The whole SimuNetLAB simulates the Internet service provider's network and servers. So, security, redundancy and high availability is also at high priority.

The goal of this thesis work was to provide a redundant virtual server base for SimuNetLAB, information on how it was built and background information about larger-scale server clusters with virtual servers and network data storing.

The Server cluster servers and The iSCSI data storage where delivered to SimuNetLAB and after that it was just hands on work to assemble the server network. The server cluster was the result of numerous trials mainly because the information about the subject is not public anywhere to begin with. Yet, testing for errors and fault tolerance was of high priority and tests from them where frequent.

The result of this Bachelor's thesis work was a blade server cluster with iSCSI data storage for virtual servers. The cluster works like a charm and it keeps on working even if one third of the network connections are down. the control of the Cluster and iSCSI is incorporated into ICTLAB network. The ICTLAB is suggested that someone would look further into the matter of massive data storages and then one day duplicate the iSCSI data storage for redundancy.

SISÄLLYS

LYHENNELUETTELO

Eth-portti	Ethernet-portti, verkkoportti, yleensä rj45
Blade palvelin	englanniksi Blade server; kehikkokaappiin sijoitettavaksi suunniteltu palvelintietokone
VLAN	virtuaalinen fyysisessä tietoliikenneverkossa toimiva lähiverkko
Gbit	Gigabitti eli 1000 megabittiä
WLAN	Wireless local area network; langaton lähiverkko
iSCSI	internet Small Computer System Interface, yksinkertainen tietokoneohjattu järjestelmä Internetissä, yleensä verkkolevyjärjestelmä
.IP	Internet protocol; käytäntö, jonka osoitteilla tietokoneet tunnistetaan Internetistä ja tietoverkoista
IPv6	Internet protocol version 6; vanhan osoitekäytännön uusittu versio, jolla estetään osoitteiden loppuminen maailmasta
RAID	redundant array of independent disks; järjestelmä, josta on useita versioita ja jossa jokaisessa yksittäiset levyt varmuuskopioivat automaattisesti osan toistensa tiedoista itselleen.
CAM	Common Array Manager, yleinen hallintaohjelma Sunin verkkolaitteille, käytetään muun muassa iSCSI-verkkoelvyjärjestelmän hallintaan
CHAP	Challenge-Handshake Authentication Protocol.Seuraavalla tavalla toimiva tunnistautumis käytäntö: Haaste kohteelle, vastaus kohteelta ja hyväksytty/hylätty yhteyden muodostus.

1 JOHDANTO

Tämä työ keskittyy palvelinklustereihin, palvelimien virtualisointiin ja verkkolevyjärjestelmän käyttöön tiedon tallennuksessa klusterityyppisellä virtuaalipalvelinalustalla. Virtuaalipalvelimen ja palvelimen eron on siinä, että virtuaalipalvelin on ohjelmistollisesti simuloitu fyysisen palvelimen tavoin toimiva palvelin, joka on käynnissä fyysisellä palvelimella. Yksi palvelin siis ylläpitää useampaa virtuaalista palvelinta ja virtuaaliset palvelimet näyttävät niitä käyttäville ihmisille aivan tavallisilta palvelimilta. Tähän virtualisoinnin ideaan siis työssä keskitytään vahvistettuna klusteroinnin idealla. Klusteroinnin idea on, että useampi fyysinen palvelin toimii koordinoidusti yhdessä ohjelmien, myös virtuaalipalvelimien, alustana. Työn pääajatus on tehdä palveluntarjoajan käyttämiä palvelinratkaisuja kuvaava tehokas klusterialusta virtuaalipalvelimelle hyvin vikasietoisessa verkossa, jossa tiedot tallennetaan iSCSI-verkkolevyjärjestelmälle.

1.1 Työn rajaus

Tässä työssä keskitytään tarkastelemaan palvelinklusteria, palvelimien virtualisointia ja iSCSI-verkkolevyjärjestelmän käyttöä tiedon tallenukseen. Työstä on rajattu ulos varsinaisen verkkotekniikan osa-alue, johon kuuluvat IP/MPLS-, L2VPN- ja L3VPN-ratkaisut, joita klusterin tietoverkkoverkko käyttää tiedonsiirrossa

1.2 SimuNet-hanke

SimuNet-hanke, EAKR (Euroopan Aluekehitysrahasto), on hanke, jossa ovat mukana Kymen Puhelin Oy, Optimiratkaisut Oy, Haminan Energia Oy, Loviisan Puhelin Oy ja Cursor Oy. Myös Otsakorven Säätiö on rahoittanut hanketta. Siinä on tavoitteena rakentaa todellisen palveluntarjoajan tuotantoverkon kaltainen T&K-verkko, joka edustaa uusinta tietoverkkotekniikkaa. SimuNet-verkkoon liitetään tässä työssä kahdennetut palvelinratkaisut ja iSCSI-verkkolevyjärjestelmä. SimuNet-verkkoon liitetään kahdennetut palomuuriratkaisut sekä simuloituja asiakkaiden yritysverkkoja, mutta niiden käsittely ei sisälly tähän opinnäytetyöhön.

SimuNet-verkon avulla on tarkoitus simuloida niitä Internet-palveluntarjoajan haasteita, joita uusien tekniikoiden sisällyttäminen tuotantoverkkoon aiheuttaa. Tavoitteena on rakentaa SimuNet-verkosta etäkäytettävä kokonaisuus. SimuNet-verkkoa on tarkoitus hyödyntää perusopetuksessa, projektiopinnoissa, erikoistumis opinnoissa ja yrityksille tarjottavissa kursseissa. SimuNet-verkon avulla on tarkoitus toteuttaa työelämälähtöisiä projekteja ja opinnäytetöitä, jotka liittyvät verkkoratkaisujen käytettävyyteen, luotettavuuteen, tietoturvaan tai palvelun laatuun. (1, 9.)

2 BLADE PALVELIMET

Blade-palvelin (blade server) itsessään tarkoittaa modulaarista palvelinta, joka on optimoitu viemään mahdollisimman vähän energiaa ja tilaa. Joten se sopii kehikkokaappiin (rack chassis, ”räkkikaappi” joka on usein lukittava), johon lisättäville laitteille kiinnitetään kiskot. Tässä työssä käytetyt palvelimet vievät 1U:n standartin mukaisen tilan kehikkokaappista. 1U on: Rack Unit: 19" [48 cm] leveä ja 1,75" [4,45cm] korkea. (6)

2.1 Tekniset ominaisuudet

Blade-serverin valmistaja on Sun Microsystems. Sen malli on Sun Fire X2200 M2 ja prosessorina on Quad-core AMD Opteron(tm) processor 2376 (4-ytiminen prosessori, jossa jokaisen ytimen teho on 2,311 Ghz). Kiintolevytilaa serverillä itsessään on 134,75 GB. Gbit Eth -portteja (ethernet-portti eli verkkoportti) on 6 kpl (4 alkuperäistä ja 2 ylimääräisellä verkkokortilla [network interface card eli NIC]) lisättynä, Virtalähde, USB 2.0 -portteja 4, COM-portteja 1 ja VGA-portteja 1.

Palvelimissa ei ole optista asemaa, joten OS (käyttöjärjestelmä, opereting system) täytyy asentaa joko verkon ylitse, käyttäen ulkoista optista USB-asemaa tai OS:in voisi myöskin asentaa bootaavalta USB-massamuistilta esimerkiksi USB muistitikulta. Tässä työssä käytettiin ulkoista optista USB-asemaa, koska OS:in virallinen toimitettu asennusmedia oli DVD levy.

Palvelimissa ei ole kahdennettua virtalähdettä, joten virtalähteen hajoaminen sammuttaa palvelimen aina. Tällainen yksityiskohta heikentää serverien saatavuusarvoa. Virtalähteitä ei ole varastossa ylimääräisiä ja uuden tilaaminen ja saaminen vie aikaa, eikä kyseinen virtalähde ole myöskään kovin helppo tai nopea vaihtaa fyysisesti.

2.1.1 Verkkokortit

Verkkokorttien portit toimivat maksimissaan 1000 Mbps nopeudella. Nopeudet 10Mbps ja 100Mbps voivat toimia joko Half Duplex tai Full Duplex -moodissa. 1000 Mbps nopeudella toimiessaan portti ei voi olla kuin Full Duplex -moodissa.

Verkkokorttien Eth -porteista kaikki eivät ole käytössä, ja taulukossa 1 on esitetty, kuinka ohjelmiston asetuksissa esiintyvien verkkokorttien Eth -portit sijoittuvat fyysisesti palvelimen takana. Taulukon numerot viittaavat palvelimen **Configuratio/network adapters** -kohdan ”vmnic1” -nimeämismallin nimen numero-osaan. Klusterin sisäisen liikenteen kaapelit ovat vihreitä (taulukko 2.) siksi että ne erottuvat muista verkkokaapeleista, joka puolestaan auttaa verkon fyysistä hahmottamista.

Taulukko 1: Porttien sijoittuminen palvelimien taakse

2	**3**	**4**	**5**
1			**0**

Taulukko 2. Kaapeleiden värit klusterin palvelimissa

Portti	käyttötarkoitus	Kaapelinväri
1	Klusterin sisäinen liikenne	vihreä
2	Hallintayhteys	harmaa
3	Klusterin sisäinen liikenne	vihreä
4	Asiakasportti	harmaa
5	Ei käytössä	
0	Ei käytössä	

2.2 Ohjelmiston asennus palvelimelle ja palvelimen hallinta

Palvelimien perus -OS:iksi asennettiin VMware ESX 4.0, ja kuten palvelimien perus omaisuuksissa viitattiin, asennusmedia oli fyysinen DVD-levy.

Asennuksen jälkeen palvelin nostaa siihen asennuksessa määriteltyyn IP-osoitteeseen verkkosivun, jolta voi ladata VMware vSphere client –asiakasohjelman, jolla palvelinta hallitaan toisella koneella. Palvelinta voi myös hallita suoraan konsolilta, mikäli Linux tuntemus riittää, tietämys joka Linux-pohjaisen palvelinjärjestelmän kasaamisessa ja ylläpidossa on erittäin suuri apu vikatilanteissa. Konsolin käyttäminen vaatii näytön ja näppäimistön kytkemistä palvelimeen: kytkentä joka ei fyysisesti ole helppo, koska palvelimet ovat - kuten aiemmin mainittua - kehikkokaapissa olevia blade-palvelimia ja tiukasti muiden laitteiden välissä. Kaapin taakse ei myöskään sovi kytkentöjä tekemään, näin ollen konsolin käyttö on tässä tapauksessa viimeinen vaihtoehto kun palvelimeen ei muuten saa enää yhteyttä.

Taulukko 3: Palvelimien hallintaosoitteet

Serveri	IP osoite
Server 1	193.167.58.15
Server 2	193.167.58.16

Palvelimet vastaavat VMware vSphere clientille yllälistatuista osoitteista.

Osoitteet ovat kiinteät ja ne kuuluvat KyAMK:in ICTLAB:in verkkoon joten jokaiselta koneelta ja koneelta joka on ict.kyamk.fi WLAN (wireless local area network, langaton lähiverkko) palvelimia voi hallita. Kummasta tahansa IP-osoitteesta myöskin löytyy myös verkkosivu joka toimii kaikilla yleisillä selaimilla kuten Firefox, Internet Explorer ja Opera, ja sivulta voi ladata VMware vSphere client ohjelman jolla palvelinta hallita.

Sisäänkirjautumistunnukset: käyttäjänimi: *root* salasana: *XXXXXXX* (huom. isojen ja pienten kirjainten ero). Nämä tunnukset ovat yksittäisien palvelimien admin-tunnukset (järjestelmänvalvoja, korkeimman asteen käyttäjä), eikä niillä ei pääse koko klusteria hallitsemaan. Kuva 1:ssä on, miltä sisäänkirjautuminen palvelimelle näyttää.

kuva 1. Sisäänkirjautuminen vSphereen (4)

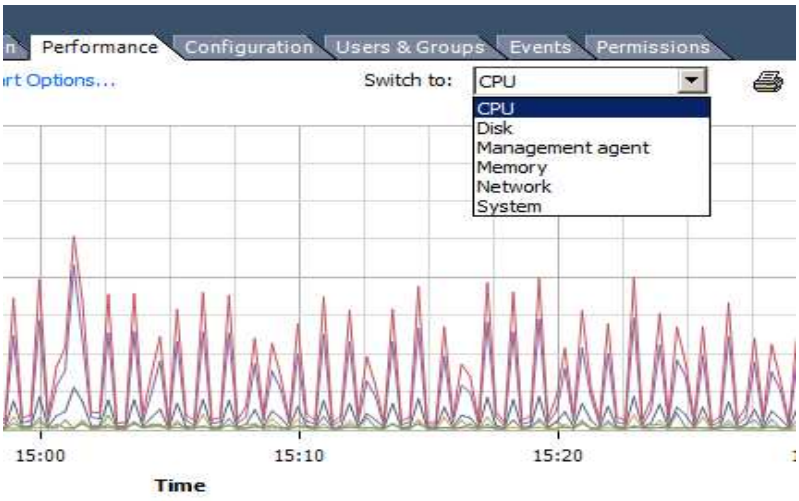
.

2.2.1 Käyttöjärjestelmän ominaisuudet

VMware ESX 4.0 on Linux-pohjainen käyttöjärjestelmä ja alusta virtualisoiduille palvelimelle. Virtualisoitu palvelin tarkoittaa sitä, että fyysinen palvelinkone sisältää ohjelmistollisesti luotuja oikean palvelinkoneen tavoin toimivia palvelimia, joissa on omat itsenäiset käyttöjärjestelmänsä ja ne näkyvät palvelujen ja palvelimien käyttäjille ainoastaan oikeina fyysisinä palvelimina verkossa. VMware ESX 4.0 alustaa hallitaan kuten aiemmassa asennus- ja hallintaosiossa kerrottiin. Kaikki tästä eteenpäin käsiteltävät palvelimien omaisuudet ja asetukset ovat hallittavissa ja löytyvät vSphere clientillä palvelimelle kirjautumisen jälkeen.

VMware ESX 4.0 -alusta tukee seuraavia käyttöjärjestelmiä virtuaalipalvelimissaan: kaikki Windows versioita Windows 3.1:stä Windows 7:ään ja Windows Server 2008 R2 versioon (64-bit), pois lukien Windows Millenium Editionin. Linux-versiosta tuettujenlistalla ovat Red Hat Enterprise Linux 2 -versiosta ylöspäin olevat jakeluversiot, Suse Linux Enterprise 8/9 -versiosta (32-bit) Enterprise 11 -versioon, Open Enterprise server, Asianux 3, Debian GNU/Linux -versiot 4 ja 5, Ubuntu Linux ja muut Linux versiot. Muut käyttöjäjestelmät: Novel NetWare 5 ja 6.x -versiot, Solaris versiot 8 - 10.

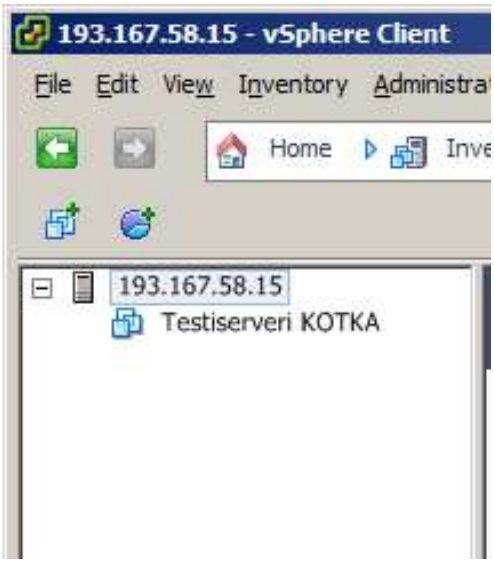
Palvelimen arvoja, kuten muistin ja prosessorin kuormitusta voidaan seurata Performance kohdasta (kuva 2).



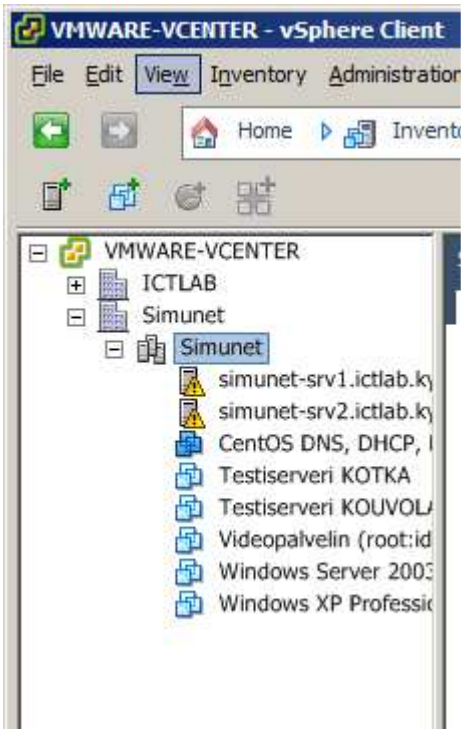
kuva 2: VMware palvelimen kuormituyksen seuranta (4)

2.2.2 Uuden virtuaalipalvelimen luonti

Uusi virtuaalipalvelin luodaan samoin sekä klusteriin että yhdelle yksittäiselle koneelle. Klusteri-näkymässä, sen sijaan että valittaisiin yksi tietty palvelin alustaksi jolle palvelin luotaisiin, valitaankin klusteri. Klusterin valitessa käytössä ovat koko klusterin resurssit, ei vain palvelimen omat resurssit. Kuvat 3 ja 4 havainnollistavat klusteri- ja palvelinnäkymien eroja käytännössä.



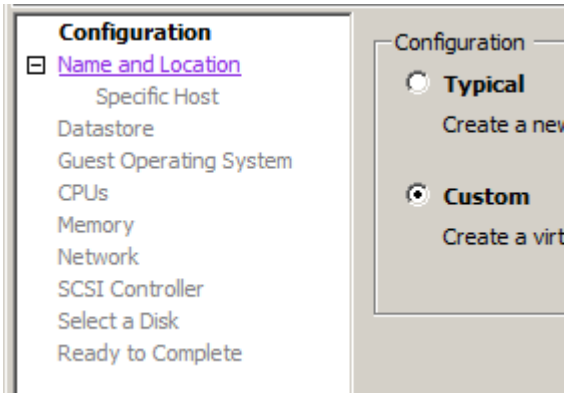
Kuva 3: serveri näkymä (4)



Kuva 4: Klusterinäkymä (4)

Kuvista saa jo tässä vaiheessa käsitystä siitä mitä, termi klusteri tarkoittaa. Kuvan 4 palvelin 193.167.58.15 on sama laite kuin SimuNet-klusterissa oleva simunet-srv1-itclab.ky(amk.fi). Kuten palvelinnäkymästä näkee, server1 ”kotka” (193.167.58.15) käytännössä pyörittää klusterin virtuaalipalvelin ”testiserveri KOTKA”:a fyysisesti.

Uuden palvelimen luonti tapahtuu ”Getting Started” sivulta. Sivu on ensimmäinen sivu joka aukeaa, kun palvelimelle tai klusteriin on kirjautunut sisälle, ja se löytyy myöhemmin välilehdiltä getting started -nimellä samalla tavalla kuin performance kuvassa 2. Painamalla Create new virtual machine aukeaa virtuaalipalvelimen luonti ja asetusten määrittely -ikkuna. Ikkunat eroavat hieman toisistaan riippuen siitä, onko palvelin vai klusterinäkymä lähtökohtana.



Kuva 5: Virtuaalipalvelimen luontia klusteriin (4)

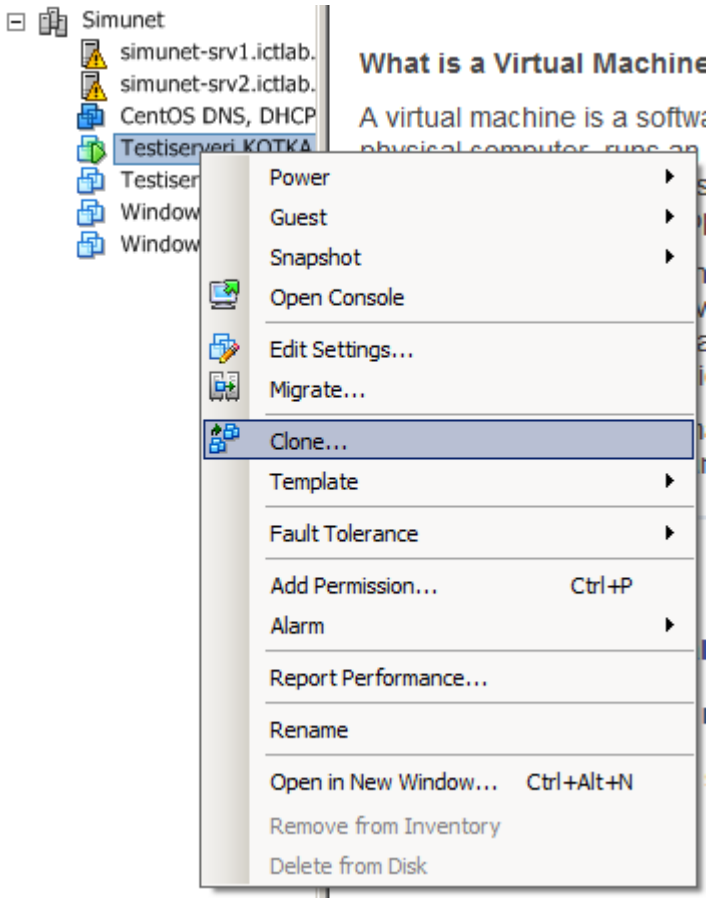
Kuva 5 esittää miltä uuden virtuaalikoneen luonti-ikkunan päävalikko näyttää klusterinäkymässä. Kuvassa 5 luodaan custom-palvelin (enemmän ja tarkempia asetusmahdollisuuksia) jolloin voidaan valita virtuaalipalvelimelle Eth-portti, jota käytetään, kuten myös voidaan valita, paljonko virtuaalipalvelimelle annetaan tallennustilaa, muistia ja prosessoritehoa. Palvelinnäkymässä ”Specific Host” -kohtaa ei ole, mutta klusterinäkymässä tässä kohdassa valitaan, mitä fyysistä palvelinta käytetään. Datastore-kohdassa valitaan, minne virtuaalikone tallennetaan. Tallennuspaikka SimuNet-ympäristössä on Sun iSCSI-verkkolevy, josta on asiaa tässä työssä myöhemmin.

Virtuaalipalvelin käynnistetään luomisen jälkeen valitsemalla se kuvan 4 esittämältä listalta. Kuvasssa 4 on valittuna SimuNet, virtuaalipalvelimen valitsemisen jälkeen

aukeaa palvelimen ”Getting Started” sivu, jolta löytyy kohta ”Power on the virtual machine”. Virtuaalipalvelinta hallitaan vSpherellä hyvin samalla tavallan kuin yksittäistä varsinaista palvelinta. Sen sijaan, että hallittaisiin ja seurattaisiin virtuaalipalvelimia hallitaan itsensä virtuaalipalvelimen, tapahtumia ja sille annettujen resurssien käyttöä. Virtuaalipalvelin ei voi ylittää sille palvelimen määrittelemiä resurssirajoja. Virtuaalipalvelin on yhteydessä verkkoon sille määritellyn 'Virtual Machine Port Groupin' kautta.

2.2.2.1 Virtuaalipalvelimen kopiointi

Yksi suurimmista virtualisoinnin hyödyistä on palvelimien helppo kopiointi. Kun halutaan nopeasti käyttöön palvelin esimerkiksi uudelle asiakkaalle niin nopein tapa on ottaa palvelimen raakaversio tietopankista ja säätää sen asetukset kohdalleen. Sen sijaan että virtuaalikone luotaisiin alusta alkaen uudelleen jolloin käydään sama prosessi läpi kuin fyysisen normaalin palvelimen tapauksessa. Virtuaalipalvelin kopiointi on yhtä helppoa kuin windows ympäristön leikkaa liimaa toiminto. Perinteisien palvelimien tapauksessa käytettiin käyttöjärjestelmälevyjen kuvia (image tiedostoja) jotka sisältävät täydellisen kopion jonkin tiedosto tallennusmuodon sisällöstä . Kuten kovalevyn kuva sisältää kaiken kovalevyn tiedon täydellisenä kopiona ja cd tai dvd levyn image sisältää kaiken tiedon, jopa kopiosuojat levystä. Virtuaalipalvelimen tapauksessa mitään erillisiä ohjelmia ei tarvita käyttöjärjestelmän kopiointiin ja itse asiassa Virtuaalipalvelimesta ei kopioida vain ainoastaan ohjelmistopuolta vaan koska palvelin on kokonaan virtualisoitu eli datamuodossa sen simuloidut sähköiset ominaisuudetkin voidaan kopioida. Kopioidun Virtuaalipalvelimen käyttöön ottoon liittyy serverin uuden nimen asettaminen, serverin sijoituspikka eli fyysinen serveri ja tallennusmuoto. Kopiointityökalu (clone) löytyy virtuaalipalvelimen työkaluvalikosta (kuva 6).



Kuva 6: virtuaalipalvelimen kopinti (clone)(4)

2.2.2.2 VMwaren verkko-ominaisuudet

VMware ei määrittele palvelimen Eth-portille porttikohtaisia IP asetuksia, vaan IP asetukset määritellään yhteystyyppiryhmälle. Yhteystyyppejä on kolme: Virtual machine, Vmkernel ja Service console. Yhteystyyppiryhmät puolestaan määritellään Vmwaren vSwitch (Virtual Switchin, virtuaalinen kytkin) alle ja vSwitch on sitten sidottu yhteen tai useampaan fyysiseen Eth-porttiin.

Virtuaalikytkin toimii käytännössä samoin kuin normaali kytkin, se on vain täysin ohjelmistopohjainen yhteydenjakotapa, johon virtuaalipalvelimet kytketään kiini. Virtuaalikytkimessä portteja tai tässä tapauksessa paikkoja virtuaalipalvelimille on 24, 56, 120, 248, 504, 1016, 2040 tai 4088. Virtuaalikytkin on multilayer-kytkin (toimii useammalla kerroksella osi-mallissa; Open Systems Interconnection model) joten se ei

ole rajattu vain yksinkertaiseen yhteyden jakamiseen. Virtuaalikytkin osaa jakaa tietoliikennekuorman - mikäli mahdollista – useamman fyysisen portin kesken, sen sijaan että se lähettäisi paketteja vain yhdestä portista. Tämä kuormanjako-ominaisuus keventää yhden portin kuormitusta, tilanteessa jossa esimerkiksi kahdessa fyysisessä portissa on kiinni kenties satoja paljon käytössä olevia virtuaalipalvelimia. Tällainen tietovirta saattaisi aiheuttaa jopa yhden Gbit Eth-portin tukkeutumisen ja suurta packet lossia (tietopakettien häviäminen verkossa), joka näkyy käyttäjille pätkivänä ja hidastuvana yhteytenä.

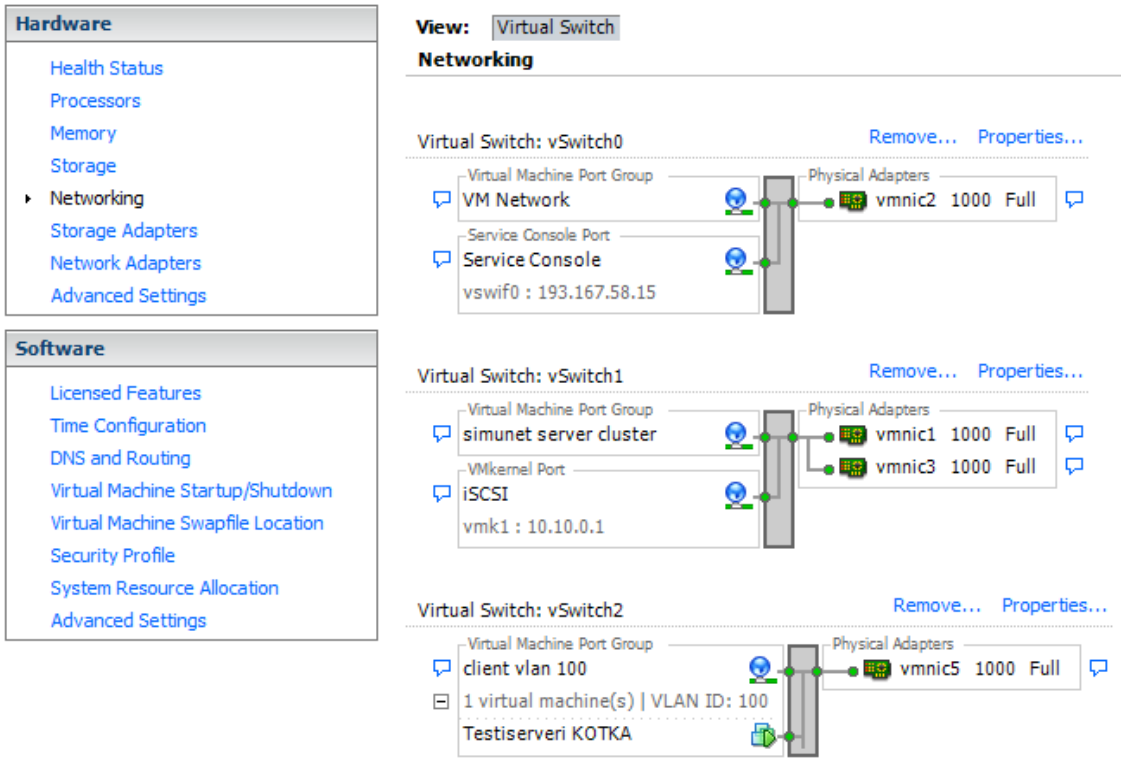
Virtuaalikytkin osaa käsitellä fyysisestä Eth-portista tulevan trunk-yhteyden (runko yhteys), joka kuljettaa kaikkia VLAN:eja (Virtual Local Area Network, virtuaalinen lähiverkko). Ominaisuus on välttämätön, koska jokainen kolmesta yhteystyypistä voidaan tagata (merkitä) kuuluvaksi johonkin VLAN:iin. Koska virtuaalikytkin osaa käsitellä fyysiseen porttiin tulevaa trunk yhteyttä, niin yhdestä Eth-portista voidaan ohjata ulos salattuja VLAN-yhteyksiä. Esimerkiksi palvelmien hallintayhteys ja klusterin sisäinen liikenne voidaan tagata vlaniin ja näin ollen erottaa ja salata muusta liikenteestä tehokkaasti.

Virtual machine Network on virtuaalipalvelimien yhteyksille tarkoitettu yhteysryhmätyyppi. Jokainen virtual machine network-tyyppiä käyttävä yhteysryhmä on hyvä tagata johonkin VLAN:iin, koska tällöin palvelin voidaan erottaa eri aliverkkoihin, ja samassa fyysisessä portissa toimivista palvelmista toinen voi olla Internetiin palveluntarjoava, toinen suljettuun sisäverkkoon.

Vmkernel port -yhteystyyppiryhmä on käytössä VMware koneiden välisessä kommunikoinnissa ja tiedonsiirrossa lukuun ottamatta vCenterin ja vSpheren ohjausta. Vmkernel yhteyden reduntanttisuus on erittäin suositeltavaa ja sen reduntanttisuuden puuttumisesta klusterin HA -ominaisuus (high availability, korkeansaatavuuden) huomauttaa heikkona kohtana verkossa. Tälle yhteystyypille kuten muillekin VLAN tagaus on hyvä idea, samaten kuin yhteydelle kannattaa varata kokonaan oma fyysinen portti. Mikäli Vmotiontionia käyttävä yhteys joutuu jakamaan raskaasti liikennöidyn portin, niin on mahdollista, että vCenter, joka hallinnoi klusteria, komentaakin palve-

linta lataamaan toisen kadonneen palvelimen ylläpitämän virtuaalipalvelimen itselleen verkon läpi. tästä voi seurata, että ennestään ruuhkainen portti voisi väliaikaisesti jopa tukkiutua. Kokonaisen virtuaalipalvelinmen kopiointi verkon yli on hyvin suuri tietopaketti ja se tieto pitää saada nopeasti siirrettyä ja käynnistymään. Palvelimen palvelujen saatavuuskin kärsii jos tiedonsiirto tukkeutuu. Toisien sanoen palvelujen saatavuus kärsii sekä pätkimisestä että siitä, jos jonkin toisen palvelun uudelleen käyttöön saaminen hidastuu vikatilanteessa. VMkernel-portin osoitteet ovat SimuNetin sisäisen palvelinklusteriverkon osoitteet eli 10.10.0.1 ja 10.10.0.2. VMkernel-portteja fyysisesti ovat Eth-portit 1 ja 3

Servevice console (hallinta konsoli) on vCenterille ja vSpeherelle palvelimen hallintaan tarkoitettu yhteysryhmätyyppi. Hallinnan kannalta tämän yhteystyypin reduntanttisuus on hyvin oleellista, mikäli hallittavat palvelimet ovat maantieteellisesti kaukana. Palvelin toimii kyllä, vaikka tämä yhteys katkeaisi, mutta palvelimen asetuksia ei pääse muuttamaan. Mikäli ainoa service konsoli -portti hajoaa palvelimen asetuksiin ei pääse enää muuten vaikuttamaan kuin fyysisesti palvelimen konsolilta. Joskin konsolin käyttö vaatii jonkin verran Linux-osaamista ja käsitystä siitä, miten VMware ESX 4.0 toimii ei-graafisessa ympäristössä. Service -konsolin IP-osoitteet ovat taulukossa 3. Service console -yhteyden katkeaminen myös irroittaa palvelimen klusterista. Service konsoli -yhteyden reduntanttisuuden puuttuessa VMware HA (high availability, selvitystä klusterin omaisuuksista) huomauttaa asiasta heikkona kohtana klusterissa.

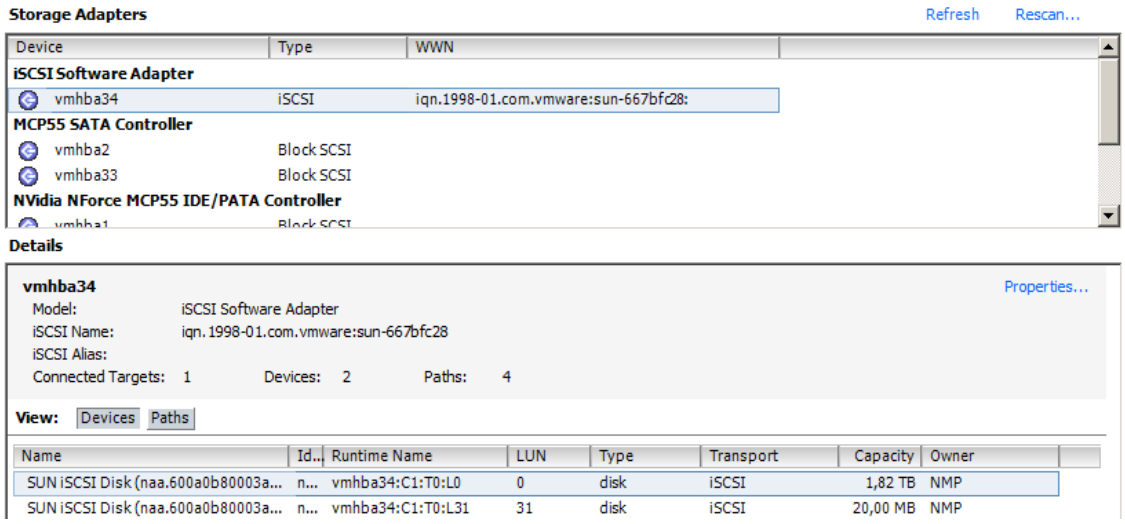


kuva 7: VMwaren verkkoasetusten näkymä (4)

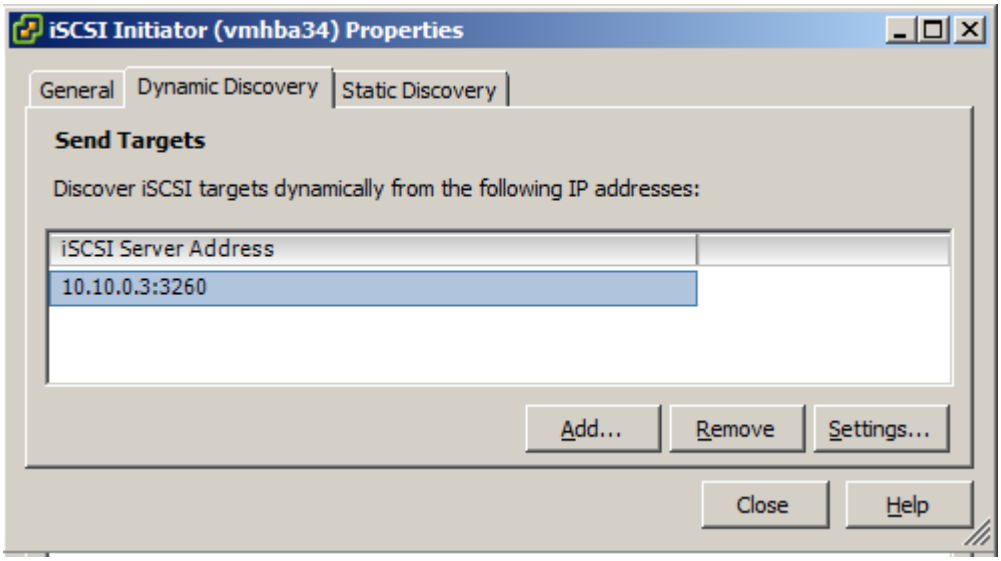
Edellä olevassa kuvassa 7 on esitetty miltä VMwaren verkkoasetukset näyttävät käytännössä. Kuvassa myöskin havainnollistaa sitä, miten eri yhteystyyppien ryhmät näkyvät asetusten kokonaisnäkymässä.

2.3 iSCSI-verkkolevyjärjestelmä & VMware

ISCSI-verkkolevyjärjestelmän asetukset ovat tämän työn seuraavassa kohdassa joka käsittelee iSCSI-verkkolevyjärjestelmää tarkemmin.



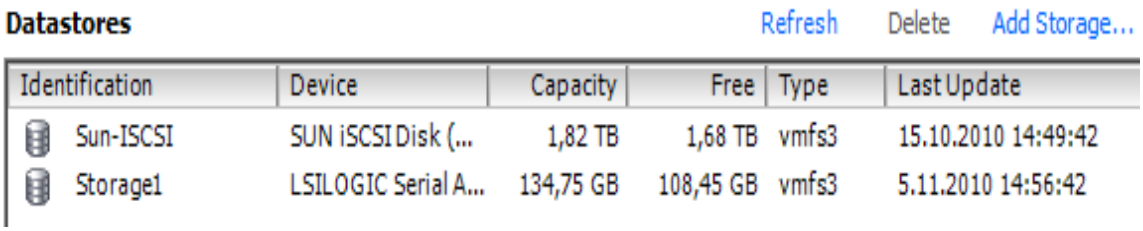
kuva 8: iSCSI VMwaren listalla (4)



kuva 9: iSCSI:n lisääminen VMwareen (4)

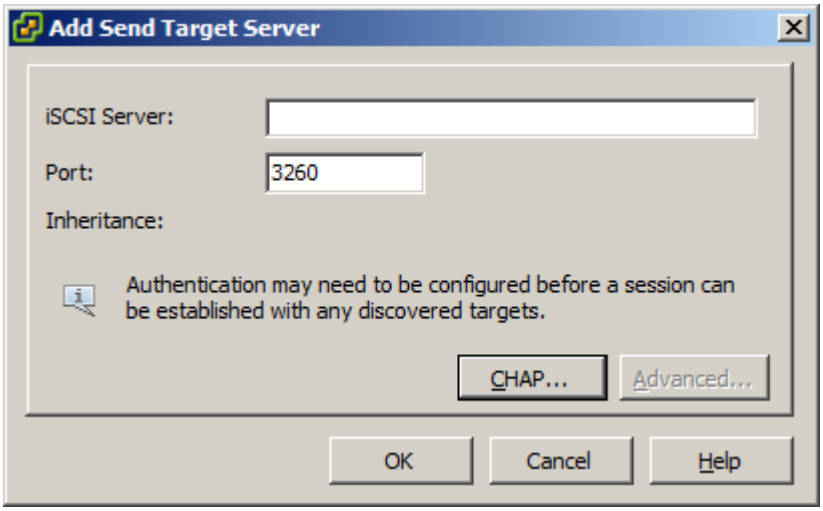
Kun VMwaren verkkoasetuksiet on lisätty porttiin, johon iSCSI-verkkolevyjärjestelmä on kytketty, VMkernel port ilmestyy Storage Adapters -asetussivulle ohjelmistollinen sovitin iSCSI-laitteille (kuva 8). Uuden iSCSI verkkolevyjärjestelmän lisäämiseksi avataan kohta 'vmhba34' valitsemalla se edellämainitulta listaltaja painamalla sen tietosivulta - joka näkyy kuvassa alempana - yläkulman 'properties' tekstinappulaa. Yksinkertaisin tapa etsiä laite tässä tapauksessa on dynamic discovery, koska kuten iSCSI kohdassa tulen tarkemmin kertomaan, laitteella ei

ole suljetussa verkossa suojauksia, jotka sen estäisi. IPv6-verkossa koko verkon tutkimis prosessissasaataisi mennä kauan (mahdollisia IP-osoitteita on hyvin paljon enemmän), joten kohteen staattinen etsintä on siinä tapauksessa hyvinkin suositeltavaa. Mikäli iSCSI-verkkolevyjärjestelmä on suojattu, se ei vastaa dynaamisen etsinnän kyseilyihin, ja se on näin ollen yleisesti näkymätön laite. Mikäli iSCSI-verkkolevyjärjestelmä on suojattu se täytyy etsiä sille määritellyn IP-osoitteen perusteella ja haun tietoihin määritellä CHAP (kuva 10).



kuva 10: iSCSI VMwaren listalla (4)

Kuvasta 11 nähdään, että iSCSI-verkkolevyjärjestelmä on VMware palvelimen tietovarastolistalla, joka löytyy: configuration/hardware/storage/Datastores. Listauksesta nähdään laitteen nimi, kokonaistila, vapaanaoleva tila, levyn tyyppi ja milloin laitteen tietoja on viimeksi päivitetty. Tiedot päivittyvät joka kerta kun tietovaraston tila muuttuu, esimerkiksi kun palvelimelle lisätään uusi virtuaalipalvelin.



kuva 11: iSCSI:n haku IP-osoitteella (4)

3 ISCSI -VERKKOLEVYJÄRJESTELMÄ

Kovalevyt iSCSI-verkkolevyjärjestelmässä on lähes poikkeuksetta RAID:attu (käsite, joka tulee sanoista redundant array of independent disks), joka tarkoittaa, että useamman kovalevyn ryppäästä jokaisesta kovalevystä on tallennuskapasiteetin osa käytetty muiden ryppään levyjen varmuuskopioihin. Levyjärjestelmän kovalevyt ovat joko hot swappable -levyjä tai hot spare -levyjä eli joko levyn voi sen hajotessa vaihtaa virtoja katkaisematta uuteen samankokoiseen levyyn (hot swap) tai järjestelmässä on valmiiksi tyhjälevy toisen levyn vioittumista varten odottamassa ja ottamassa viallisen paikan (hot spare). Hot spare levyä käytettäessä ylläpidolla ei ole kiire vaihtaa levyä hyvän toimivuuden ja saatavuuden ylläpitämiseksi.

Lyhenne iSCSI tulee sanoista Internet Small computer System Interface, joka tarkoittaa IP:lla toimivaa tietopankkien yhteysverkkostandardia. Lyhyesti ilmaistuna tietoverkossa toimiva se on kovalevyjärjestelmä tiedonvarastointiin. ISCSI-verkkolevyjärjestelmiä käytetään kaiken kokoisissa tietoverkoissa tiedon tallentamiseen, yleensä sijoitettuna paloturvallisiin ja suojattuihin tiloihin keskitetysti esimerkiksi yrityksien tietokantoja ja tärkeitä varmuuskopiota varten.

3.1 Käyttöönotto ja tekniset ominaisuudet

Sun StorageTek ™ 2510 iSCSI -verkkolevyjärjestelmä. 2 virtalähdettä, 1 hallinta Eth -portti, 2 tiedonsiirto Eth -porttia, 12 paikkaa kovalevyille, koko: 2U ja 1 konsoliportti (vanhanmallinen sarjaportti). Kovalevypaikat ovat ulosvedettäviä kehikkokelkkoja jotta Hot swap on mahdollista vikatilanteessa ja levyjen asennus helpottuu. Kovalevypaikoista 5 on käytetty ja jokaisessa on 500 Gb:in kovalevy, loput paikat ovat tyhjiä. Kun verkkolevyjärjestelmä otetaan käyttöön ja liitetään verkkoon, se lähwttää ensimmäiseksi kyselyn verkon DHCP-palvelimelle (nimipalvelin, joka jakaa IP-osoitteet verkkoon) ensimmäisestä vapaasta IP-osoitteesta ja mikäli DHCP-palvelua ei ole se antaa itselleen 10.0.0.1-osoitteen. Ongelmaksi muodostui alkuun että verkkolevyjärjestelmän itse itselleen antama IP-osoite hallintaa varten ei toimi kunnolla (mahdollisuus toimia oli noin 10 %) joten aloituskonfiguraation tekemiseksi

hallintaan käytetylle tietokoneelle täytyi käynnistää nimipalvelu, jolla annettiin yksi tietty IP-osoite verkkolevyjärjestelmälle.

3.2 Hallinta ja asetukset

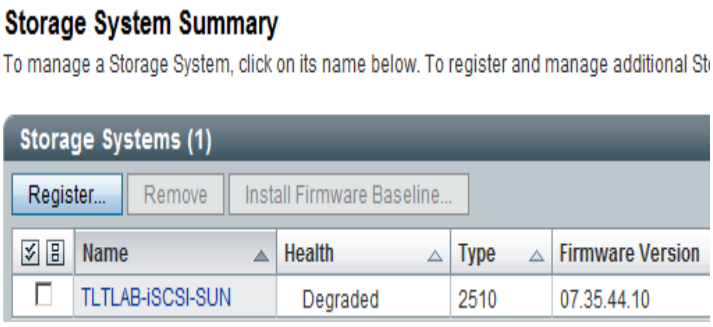
Verkkolevyjärjestelmän käytetään Sun StorageTek ™ CAM:ia (common array manager), jonka vanhan version saa ladattua verkkolevyjärjestelmän IP osoitteessa sijaitsevalta verkkosivulta ja uudemman käytössä olevan CAM:in asennustiedoston entisen tlt lab:n luumupalvelimen share/u-kansiosta. Kuitenkaan jotta nyt valmiiksi konfiguroitua verkkolevyjärjestelmää pääsisi muokkaamaan ja tutkimaan ei tarvitse CAMia asentaa millekään koneelle, vaan se on asennettu ICTlabin Omena-palvelimelle. CAM:in asennuksessa on otettava huomioon että siinä ei ole tukea muun muassa Windows XP home alustalle, koska CAM käyttää kirjautumistietoinaan sen käyttöjärjestelmän käyttäjäprofiileita kuin mihin se on asennettu. Esimerkiksi XP home editionin käyttäjätiedot eivät ole samassa paikassa tai samanlaiset kuin XP professional editionissa, jota CAM kylläkin tukee. CAM:ia ei ole tarkoitettu käytettäväksi koneelta, jolle se on asennettu, ja se ei ole käynnistettävä ohjelma, vaan se on koneessa aina päällä oleva sovellus. CAM-sovellus on tarkoitettu asennettavaksi hallintapalvelimelle josta sitä käytetään tietystä osoitteesta. Mikäli palvelinkäyttöjärjestelmä, jolle CAM on asennettu, hakee käyttäjätunnukset esimerkiksi active directory -palvelusta verkosta, niin tunnuksiksi kelpaavat sieltä listalta löytyvät varsinaisesti käytettyä palvelinta koskevat järjestelmänvalvojan tunnukset.

3.2.1 Hallintaan kirjautuminen ja uuden laitteen lisääminen

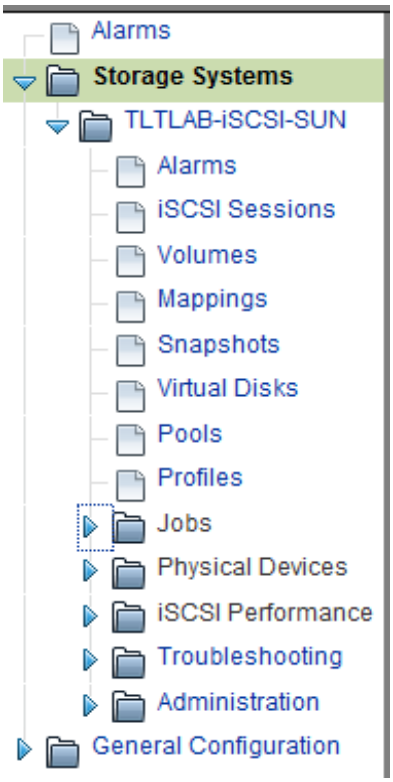
Hallinta tapahtuu kirjautumalla Omena-palvelimelle asennetulle CAM:ille osoitteessa:
https://omena.tlt.kyamk.fi:6789/console/faces/jsp/login/BeginLogin.jsp
Käyttäjätunnus on: ” suniscsi ” salasana: ” ********** ”. (kuva 12)

Kuva 12: CAM:iin kirjautuminen (5)

CAMin käyttö vaatii selaimelta Java tukea, ja se toimii parhaiten yleisimmillä selaimilla kuten Internet Explorer ja Firefox. CAM:iin kirjautumiseen aukeaa selaimeen sivu, jossa on luokat eri sovelluksista: ’Systems’, ’Desktop applications’, ’Storage’, ’Services’ ja ’Other’. Storage kohdassa listalla on ’Sun StarageTek ™ Common Array Manager’: tästä linkistä pääsee CAM sovellukseen. CAM:issa on hallintajärjestelmä puu ja laitelistaa mikäli laitteita on liitetty CAM:iin (kuva 14). Samalla sivulla on lista kaikista laitteista ja tiedot niiden tiloista, sekä laitteiden lisäys että päivitys työkalut (kuva 13).



kuva 13: laitteidenlistaus ja firmwaren päivitys työkalu (5)



kuva 14: Järjestelmäpuu (5)

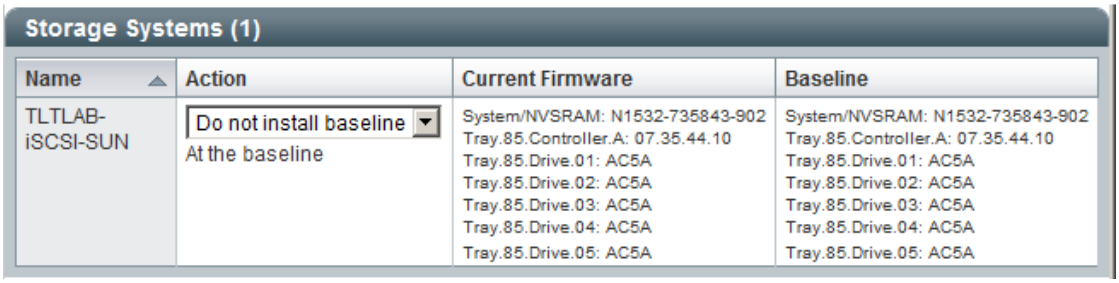
Edellä olleissa kuvissa näkyy tässä työssä käytetty TLTLAB-iSCSI-SUN -verkkolevyjärjestelmä. Uuden laitteen lisäys tapahtuu Register -nappia painamalla. Laitteen lisättäessä uusi laite voidaan joko etsiä tietyllä IP-osoitteella tai koko tieto-verkko voidaan skannata, mikäli ei ole tiedossa, minkä IP-osoitteen verkon DHCP palvelu on uudelle verkkolevyjärjestelmälle antanut. Jos kyseessä on vanha verkkole-vyjärjestelmä, se voi olla suojattu salasanalla, jolloin sen rekisteröinnissä CAM:iin täytyy valita ”use default password”:in sijaan ”Enter password for the discovery”. Tämän työn ympäristössä kyseiselle salasanalle ei ole tarvetta, koska verkkolevyjär-jestelmä on suljetussa verkossa eikä näin ollen siihen voi vaikuttaa ICTLAB:in sisä-verkon ulkopuolelta.

3.2.2 Firmwaren päivittäminen ja asetukset

Sun StorageTek ™ 2510 Firmware (elektroniikan ohjaimien päivitys) on aina sidottu-na CAMin versioon, eli uusin CAM sisältää uusimman firmware-päivityksen ja firm-

waren päivitys onkin suositeltavaa, mikäli CAM päivitetään. ”Install Firmware Baseline” -optioni löytyy Storage Systems yhteenvedosta (kuva 15).

TLTLAB-iSCSI-SUN -verkkolevyjärjestelmän firmware on CAM:in sisältämän firmware päivityksen kanssa samassa versiossa, eli firmware on baseline:ssä samassa versiossa (kuva 15).

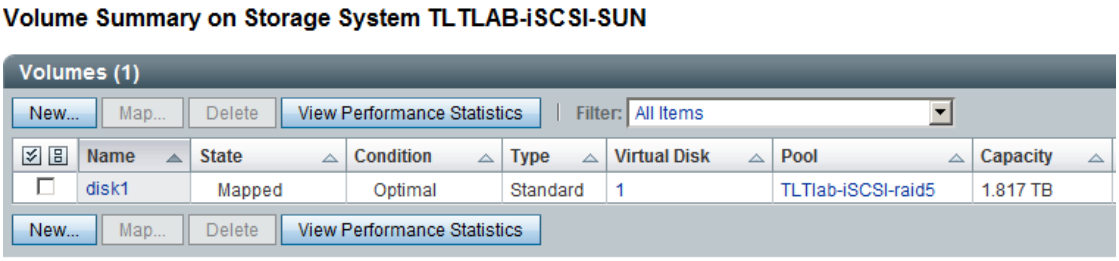


kuva15: Firmwaren päivitys (5)

Kovalevyjen käyttöönotto tämän työn verkkolevyjärjestelmässä tapahtuu Volumes-asetussivulta (kuva 14). Sivulta löytyy listaus käyttöön otetuista kovalevyistä. Uuden kovalevypakan rekisteröinti ja käyttöönotto tapahtuu edellä mainitulta volumes-sivulta new-nappia painamalla.

3.2.3 iSCSI-verkkolevyjärjestelmän yleiset asetukset

ISCSI-verkkolevyjärjestelmässä kovalevyt ovat raidattu reduntanttisuuden parantamiseksi, kuten aiemmin mainittua, ja käyttöönotetut osiot (volumet, osio voi sisältää useammasta kovalevystä tehdyn yhtenäisen esim. RAID-varmistetun tallennustilan) on listattu asetuksien volumes-valikossa (kuva 14). Itse volumes-valikon pääsivulla osiot on listattu oletusarvoisesti nimen mukaan ja jokaisesta osiosta näkee seuraavat tiedot: nimi (name), State (tila), kunto (condition), tyyppi (type), virtuaalilevyn numero (virtual disk), resurssiallas (pool), kokonaiskapasiteetti (capacity) ja maailmanlaajuinen nimi (WWN, world wide name) (kuva 16).



kuva 16: Volumes asetussivu (5)

Tila (state) on joko unmapped tai mapped (kartoitettu) ja tarkoittaa sitä, onko osio merkitty jonkin laitteen käyttöön. Tässä tapauksessa disk1 on kartoitettu ”ESX”-käyttöön, jonka tyyppi puolestaan on palvelin (Host), ja kartoituksella on oikeudet sekä kirjoittaa että lukea levyltä. Kartoituksen tiedot löytyvät ”Mappings”-asetussivulta päävalikosta (kuva 14). Osioista ja osioiden sisällöistä voidaan myöskin ottaa snapshotteja, jotka voidaan myöskin mapata. Tämä tarkoittaa sitä, että kovalevyn sisältö jäädytetään, ja se alkaa jokaisella käyttökerralla aina samasta tilasta. Snapshot-asetuksille on oma asetuksien välilehtensä (kuva 14). Virtual disk (virtuaalilevyt) on RAID:atun useamman fyysisen levyn pakkan osa, tai kkoko raid pakka, joka käytössä näkyy yhtenä levynä. Virtuaalilevyn voi pilkkoa pienempiin osioihin ja osiot voi kartoittaa useammalle palvelimelle.

Pools-asetussivu (resurssialtaat) sisältää listan siitä, miten osiota käytetään ja mihin tarkoitukseen se on optimoitu. Tässä työssä ainoa Storage pool verkkolevyjärjestelmässä on TLTlabiSCSI-Raid5 -resurssiallas ja sen käsittelyn optimointi on high capacity computing eli nopea tiedonkäsittely, joka kuvaa parhaiten sitä että levyltä käytetään VMware virtuaalipalvelimia, jolloin levylle saatetaan jossakin tilanteessa kirjoittaa ja lukea tietotoa nopeasti ja paljon.

ISCSI sessions -kohdasta asetussivulla on listaus kaikista yhteyksistä jotka ovat käynnissä iSCSI-verkkolevyjärjestelmän porteissa. Tältä sivulta näkee ovatko palvelimet yhteydessä verkkolevyjärjestelmään.

3.2.4 ISCSI-verkkolevyjärjestelmän fyysisten laitteiden asetukset

Initiators (aloitteentekijät) physical devices -asetussivun alaiselta sivulta sisältää listauksen niistä laitetunnuksista, joihin iSCSI-verkkolevyjärjestelmä vastaa verkkoon. Iniator sisältää tiedon initatorin nimestä, uniikista tunnuksesta (unique identifier), palvelimesta (host), palvelimen tyypistä (host type) ja tunnistautuminen (Authentication). Tunnistautuminen mikäli sitä käytetään tapahtuu CHAP:alla (Challenge-Handshake Authentication Protocol, lähetetään tunnus palveluun joka, sitten vastaa, kelpaako tunnussana tai lause). CHAP:an tunnuksen tulee olla 12 - 57 merkkiä pitkä merkkijono, mikäli sitä käytetään. Verkkolevyjärjestelmä ei vastaa yhteyttä ottavalle palvelimelle mikäli Initiatorin tiedot eivät täsmää listan tietojen kanssa. Initiators asetuksissa oleva host listaus löytyy. Fyysisten laitteiden asetussivulta Host-välilehdeltä.

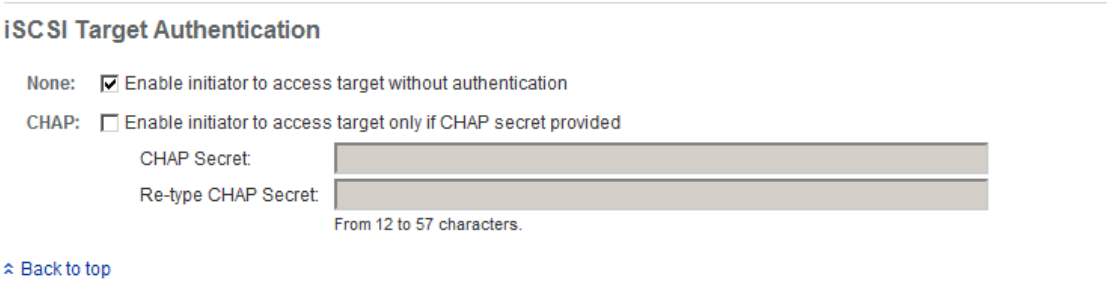
Host-nimeen on sidottu mitä osiokartoituksia käytetään, ja kuten edellisessä kävi ilmi, se liittyy läheisesti initiators-tietoihin. Palvelimia (Host) voidaan myöskin ryhmitellä Host Groups välilehdeltä ja sitten voidaan kerralla mapata osioita kaikille groupeille.

kuva 17: iSCSI kohteen tunnistauminen. (5)

ISCSI kohde (iSCSI Target) asetusvälilehti koskee laitetta itseään. Tämä sivu on yhteyden muodostamisen ja sen sääntöjen kannalta hyvin tärkeä. ISCSI-kohteen tunnistus (target identification) sisältää tiedon iSCSI-verkkolevyjärjestelmän maailmanlaajuisesta uniikista nimestä, ja tälle nimelle voi itse määritellä aliaksen, joka on huomattavasti käyttäjäystävällisempää kuin että alkaisi kirjoittaa tietyissä tapauksissa yhteydenmuodostustilanteessa nimeä: 'iqn.1986-

03.com.sun:2510.600a0b80003acb6b000000004ad6f92c' (kuva17) SimuNetin tapauksessa koska kyseessä on suljettu verkko, iSCSI kohteen alias on sun-iscsi.

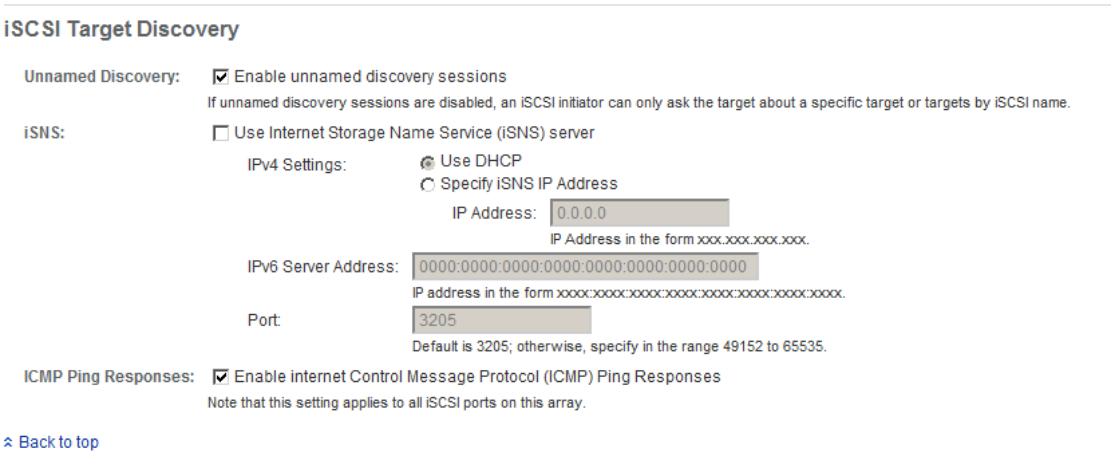
ISCSI kohteen tunnistauminen (target authentication). Kuten VMware osiossa iSCSI-verkkolevyjärjestelmän hakemisessa ja käyttöönotossa kerroin iSCSI voi olla suojattu. Kohteen tunnistauminen on nimenomaan tämä suojaus. Tarkoitukseen käytetään



kuva 18: iSCSI kohteen tunnistauminen. (5)

CHAP mallista tunnistautumista. Tunnus tulee olla 12 -57 merkkiä pitkä. SimuNet verkossa kyseistä ominaisuutta ei ole käytetty koska kyseessä on suljettuverkko ja sen sisällä toimivaan iSCSI-verkkolevyjärjestelmään ei pääse käsiksi ulkopuoliset mitenkään (kuva18).

ISCSI-kohteen löytyminen (target discovery). Tämä asetussivu (kuva19) on hyvin oleellinen verkkolevyjärjestelmän verkosta löytymisen kannalta. SimuNetin iSCSI-verkkolevyjärjestelmän kohteen löytyminen on jätetty kaikille näkyväksi, koska laite on ainoastaan verkon suljettuun osaan yhteydessä, joten ulkopuoliset eivät missään ta-



kuva 19: iSCSI kohteenlöytymis asetuskenttä (target discovery) (5)

pauksessa pääse sitä etsimään saati käyttämään. Tietoturvamielessä nimettömillä hakuyrityksilla ei siis ole väliä tässä tapauksessa, ja dynaaminen laitteenhaku verkosta helpottaa iSCSI-verkkolevyjärjestelmän löytämistä. Osaltaan dynaamisen etsinnän mahdollisuus eliminoi palvelimen configuroijan inhimillisistä virheistä johtuvia ongelmia kuten hyvin helposti väärin kopioituja iSCSI-nimiä joista olinkin kertonut aikaisemmin.

Storagetek 2510 iSCSI –verkkolevyjärjestelmä, jota tässä työssä käytetään tukee myöskin IPv6 verkkoratkaisuja ja sen hallintayhteys on valmis IPv6-verkkoon ja hakee IPv6 osoitteen DHCP-palvelimelta välittömästi kun sellainen verkkoon liitetään. (liite 1). Hallintayhteys iSCSI verkkolevyjärjestelmälle on nimeltään controller, kun taas tiedonsiirronportit on merkitty pelkällä port-nimellä. Käytössä on ainoastaan controller A, joka on määritetty iSCSI Eth -portti ykköseen ja tiedonsiirtoportit ovat ETH porteissa 2 ja 3. Kontrollerille eli hallintayhteydelle ei ole määritelty laitteen päästä kiinteää IP-osoitetta. Syynä tähän on se, etteivät kiinteät osoitteet koskaan toimineet kunnolla. Tällä hetkellä ja pysyväksi ratkaisuksi päätyi ICTlabin kalaverkon (laboratorion tuotantoverkko) DHCP-palvelimelle määritelty kiinteä IP-osoite iSCSI-verkkolevyjärjestelmän Eth-portti 1:n MAC osoitteelle.

4 KLUSTEROINTI JA ISCSI

4.1 Klusteroinnin teoriaa ja hyötyjä

Klusteri tulee englanninkielen sanasta cluster, joka tarkoittaa terttua, kimppua ja ryhmää. Rypäleterttu on erinomainen kuvaamaan klusteria. Jokainen palvelin on oma yksikkönsä joka on verkkoyhteydessä keskukseen, samalla tapaa kuin rypäleet ovat tertun rangassa kiinni. Palvelimien tapauksessa koontirunkona toimii vain tietoverkko, ja jotkut palvelimet sitten hallitsevat kaikkien koneiden tehtävänjakoa. Käyttäjälle esimerkiksi Internetissä surfaajalle tai jopa palvelimen vuokraajalle, klusterointi näkyy parempana palvelun saatavuutena, mutta ei millään tapaa ulospäin, vaan kaikki toimii kuin normaalissa palvelimessa.

Klusterointia käytetään monella tavalla: sitä voidaan käyttää reduntanttisuuden parantamiseksi tai laskentatehon keräämiseen. Yliopistot ovat käyttäneet tutkimusprosessin analyysin ja laskemisen nopeuttamiseen vapaaehtoisten tietokoneenkäyttäjien tietokoneita ajatuksella ”anna meille osa koneesi laskentatehosta käyttöön, niin me saamme tämän uuden hienon lääkkeen valmiiksi nopeammin”. Tässä käytetään oikeastaan massiivista pienistä osista koostuvaa klusteria, joka hyväksikäyttää siihen liitetyn koneen laskentatehoa. Myös krakkerit (kutsutaan myöskin virheellisesti nykyään hakkereiksi) voivat periaatteessa käyttää saastuttamiaan tietokoneita – niin sanotut botnetit tai zombikoneet Internetissä klusterin tapaan. Useimmiten krakkerien valtaamat koneet toimivat itsenäisinä yksikköinään samaan aikaan yhden tai useamman kohteen kimpussa koordinoidusti, mutta eivät simuloidusti yhtenä koneena.

Klusteri voi sisältää koneita yli kolmesta satoihin tai jopa tuhansiin. Kolmen koneen tapauksessa yksi kone kolmesta ohjaa kahden muun koneen tehtävänjakoa. Klusteri on hyvin reduntanttinen, koska mikäli yksi kone rikkoutuu tai menettää kaikki verkkoyhteytensä eli siis katoaa muiden koneiden yhteydestä, niin muut koneet ottavat tämän prosessit hoidettavakseen. Samalla tavalla, kun palvelin voi kadota klusterista yllättäen ilman sen suurempia seurauksia, niin palvelimia voidaan lisätä tai

palvelimien omaisuuksia voidaan muokata. Tämä tarkoittaa sitä, että tarvittaessa palvelimeen voidaan lisätä tai vaihtaa uusi prosessori tai koko klusterin farmiin (paljon palvelimina toimivia tietokoneita samassa paikassa) lisätä uusi palvelin palvelujen saatavuuden siitä häiriintymättä. Sen lisäksi, että palvelimet samassa klusterissa ottavat toistensa prosesseja vikatilanteessa, niin palvelimien välillä tapahtuu myös kuormanjakoa; palvelimen load balancingiksi kutsuttua käsittelyä. Jos jokin palvelimista ylikuormittuu esimerkiksi siinä tilanteessa, että tiettyjen palvelujen käyttäjät alkavat käyttää kyseisiä palveluita ja palvelin ei enää ehdi tehdä kaikkea, niin osa sen raskaista palvelusovelluksista siirtyy vähemmän kuormitetulle palvelimelle. Näin edesautetaan sulavaa toimivuutta ja palvelinfarmista saadaan mukautuvampi. VMwaressa näitä kuormanjako ominaisuuksia hoitaa VMware HA (high availability, korkea saatavuus) ja DRS (Distributed Resource Scheduler, jaettujen resurssien hallinta), kun kyseessä on nimenomaan palvelimien prosessointitehon kuormitus, ei tietoliikenneverkon yhteyksien kuormitus.

Hyvin usein klusterien koneet sijaitsevat maantieteellisesti samoilla alueilla kuten vaikka samassa kaupungissa ja vain muutamassa konesalissa. Klusterin osia voi tietysti olla pitkin maailmaa, mutta tehokkaimmin klusteri toimii, kun koneiden väliset linjat ovat nopeita, joko operaattorin runkoverkko tai gigabitin Ethernet (1000 Mbit/s lähiverkko). Vaikkei yhden koneen vikaantuminen olekaan klusterin kannalta kovin kriittistä niin koneiden keskittämisestä on hyötyä niin fyysisen huollon kuin tietoturvankin kannalta. Nopeampaa on korjata vika viereisen rakennuksen kellarikerroksen konesalista kuin yhden koneen vikaa yli 20 kilometrin päästä.

4.1.1 Klusterin tietoturva ja sijoittaminen

Tietoturvan kannalta klusterialusta on kestävä, mutta myös klusterissa tietoturva on yhtä tärkeää kuin perinteisissä palvelinratkaisuissa. Sen lisäksi että klusterin virtuaalipalvelin on hyvä suojata yhtä hyvin kuin perinteiset palvelimet, niiden kaataminen ja niille tunkeutumisen aikana pahanteko ovat käytännössä katsoen hyödytöntä; ellei tarkoituksena ole tiedon varastaminen eikä tuhoaminen. Kuten aiemmin olen kertonut, virtuaalipalvelimista on helppo tehdä varmuuskopioita, jotka

on nopea käynnistää uudelleen. Sen lisäksi että virtuaalipalvelimelle tunkeutuminen voi olla vaikeaa, niin krakkerin on hyvin paljon vaikeampi päästä käsiksi itse fyysiseen palvelimeen, etenkin kun klusterin sisäinen liikenne on rajattu täysin suljettuun sisäverkkoon, josta ei ole avoimia portteja ulospäin. Ainoastaan ulospäin auki olevia portteja ovat ne, jotka on avattu vain virtuaalipalvelin käyttöön. Virtuaalipalvelinporttien kautta ei voi hallinnoida tai edes nähdä palvelinalustaa. Tunkeutuja voi siis päästä virtuaalipalvelimelle, mutta ei itse palvelimelle, joka ylläpitää virtuaalipalvelimia. Tilannetta voisi kuvata niin, että tunkeutuja pääsee saarelle, joka kelluu tyhjyydessä. Eli itse virtuaalipalvelimen voi tuhota ja siellä olevaa tietoa varastaa, mutta eteneminen loppuu siihen, ja milloin vain kyseinen voidaan virtuaalipalvelin korvata toimivalla kopiolla, josta tietoturva-aukko on korjattu. Kun virtuaalipalvelimelle on määritetty tarkat rajat, miten paljon palvelimen resursseja sillä on käytössä, se ei myöskään voi tukkia sitä ylläpitävää fyysistä palvelinta.

Kun klustereista on kyse ja siis mahdollisista suuristakin kokonaisuuksista, niin ei sovi unohtaa ympäristöä, jossa klusteri sijaitsee fyysisesti. Kun klusteri on jaettu maantieteellisesti kahteen tai kolmeen paikkaan, saadaan estettyä koko klusterin vikaantuminen kerralla. Suomessa ympäristön aiheuttamaan vioittumiseen varautumiseen riittävät kahdennetut virransyötöt, UPS:it (uninterrubtable power supply) ja paloturvallinen ympäristö. Rauhattomimmissa maissa pomminkestävät databunkkerit maan alla puolestaan ovat realistinen ratkaisu, niin poliittisesta tilanteesta kuin luonnonmullistuksista johtuen. Maantieteellisellä sijoituksella voi olla muutakin merkitystä kuin yksinomaan saatavuuden turvaaminen. Esimerkiksi suuret konesalit tuottavat valtavasti lämpöä ja käyttävät vielä paljon enemmän sähköä. Näistä ominaisuuksista kertoo yksinkertaisesti se, että suuri palvelinsali voi helposti tuottaa sitä ympäröivälle asutukselle lämmityksen, ja edes vanhan paperitehtaan sähkökaapeloinnit eivät ole riittävät sen sähköntarpeisiin.

Hyvä esimerkki suurista palvelinsaleista ovat Googlen datacenterit, joista yksi muun muassa avataan Haminaan vanhaan tehdaskiinteistöön, koska tehtaan vieressä on joki, jonka vettä voidaan käyttää konesalien jäähdytykseen. Ihanteellisen maantieteellisen

sijainnin lisäksi sijoituspaikka vieläpä sijaitsee kaikin puolin rauhallisessa matalan korruption maassa.

Klusteriin sinänsä ei kuuluvana osana on hyvin usein myöskin verkossa itsenäisinä yksiköinään olevat verkkolevyjärjestelmät. Nämä verkkolevyjärjestelmät, kuten myöskin tämän työn SimuNetin iSCSI –verkkolevyjärjestelmä, ovat yhteydessä kaikkiin klusterin palvelimiin, jolloin yhden tallentama tieto on kaikkien palvelimien käytettävissä ja levyn suurta kapasiteettia voidaan helposti jakaa asiakkaiden tallennuskapasiteetiksi. Kun tieto on tallennettu kaikilta palvelimilta samaan paikaan, se ei pääse vahingoittumaan, vaikka palvelimia hajoaisikin. Tieto on siis aina tallessa ja muiden palvelimien käytettävissä.

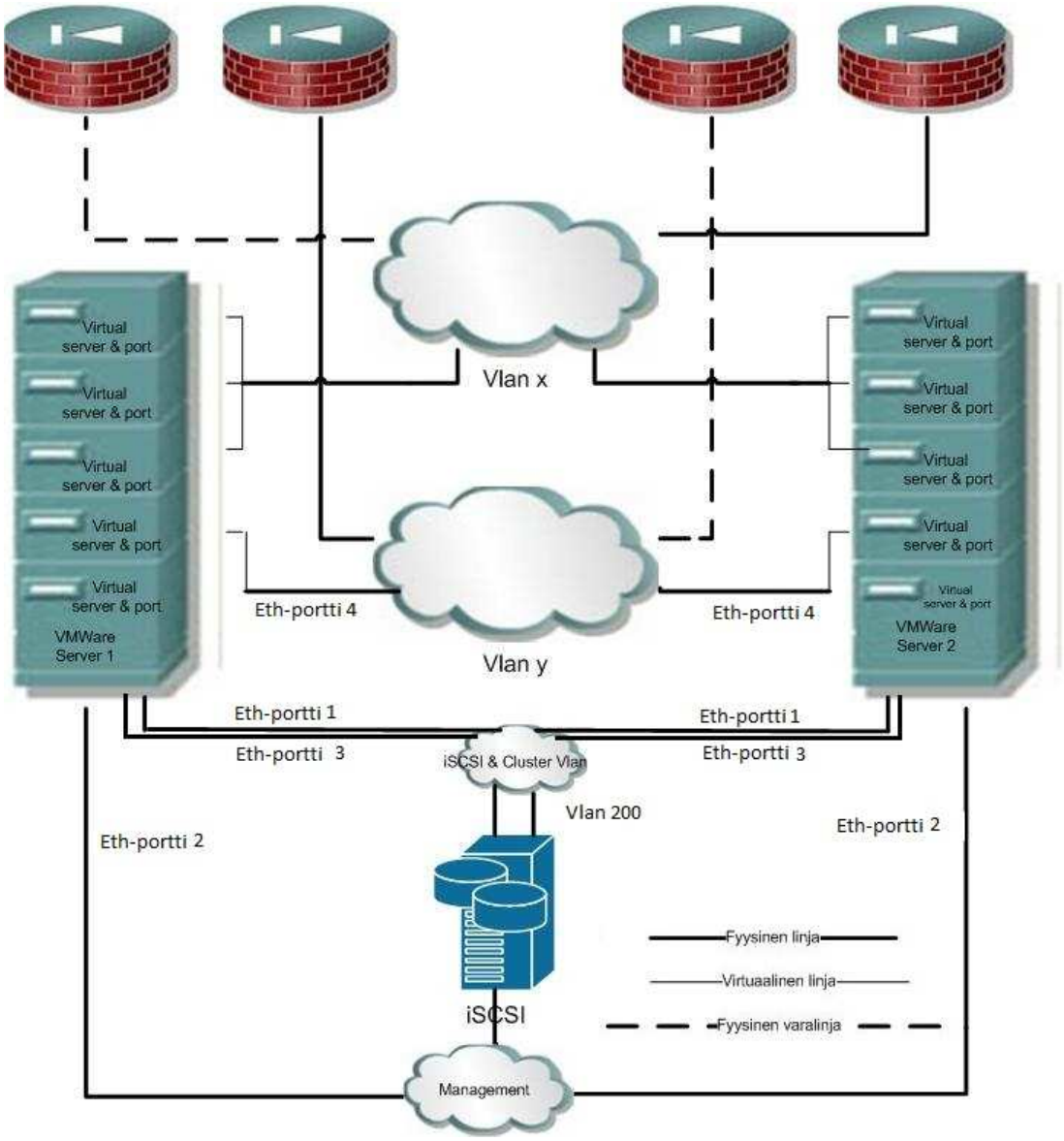
4.2 Klusterin fyysiset kytkennät

Kuten aiemmin jo mainitsin, on hyvä, että klusterin palvelimien väliset linjat ovat mahdollisimman nopeita; eikä pelkästään nopeita, vaan nopeuden lisäksi niiden olisi hyvä olla reduntanttisia (kahdennettuja). Verkkoyhteyksien reduntanttisuudella saadaan aikaan se että yhden fyysisen yhteyden vikaantuminen ei irrota palvelinta klusterista ja kahden tai useamman linjan kesken on mahdollista käyttää kuormanjakoa.

SimuNetin klusterin fyysiset kytkennät (taulukko 2 ja kuva 20) ovat reduntanttiset SimuNetin sisäpuolella tapahtuvan liikenteen osalta. Vihreät kaapelit ovat klusterin sisäiseen liikenteeseen tarkoitettuja ja liitetty vlan 200:an, jotta niiden liikenne ei sekoitu muuhun SimuNetin liikenteeseen ja että ne erottuvat verkkolaitteiden asetuksissa. Klusterin käyttämissä kahdessa portissa palvelinta kohden ajatuksena on, että toinen portti on varattu iSCSI-verkkolevyjärjestelmän liikenteelle, kun taas toinen palvelimien väliseen tiedonsiirtoon. Kummallekin palvelimelle on määritelty iSCSI porteista toinen portti ensisjaiseksi ja toinen toissijaiseksi portiksi. Server1 käyttää pääasiallisesti iSCSI-verkkolevyjärjestelmän porttia 10.10.0.3 ja server2 10.10.0.4. Tämä järjestely auttaa etenkin silloin, kun palvelimille asennetaan uusia

virtuaalipalvelimia ja virtuaalipalvelimien oletustallennuspaikka on iSCSI-verkkolevyjärjestelmä.

.



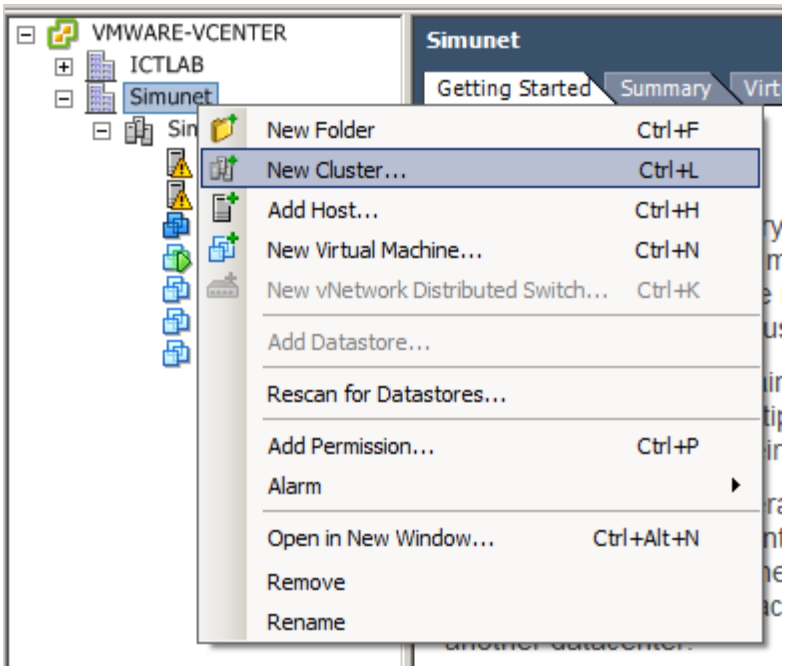
kuva 20: Serverien klusteri ja iSCSI verkon kuva

Kuva 20 esittää sitä miten palvelimet sijoittuvat SimuNetin sisällä ja mitkä portit ovat kiinni missäkin verkossa. Portit 4, 5 ja 0 on varattu asiakasyhteyksille, joskin tällä hetkellä ainoastaan portti 4 on käytössä. Porttien käyttöönotto onnistuu joko klusterin admintunnuksilla tai palvelimien järjestelmänvalvojan tunnuksilla. Mikäli käyttöönotto tehdään klusterin ulkopuolelta, niin asetuksien täytyy kummassakin palvelimessa olla identtiset, jotta portteja käyttävät virtuaalipalvelimet voivat toimia kummassakin palvelimessa vikatilanteessa identtisesti.

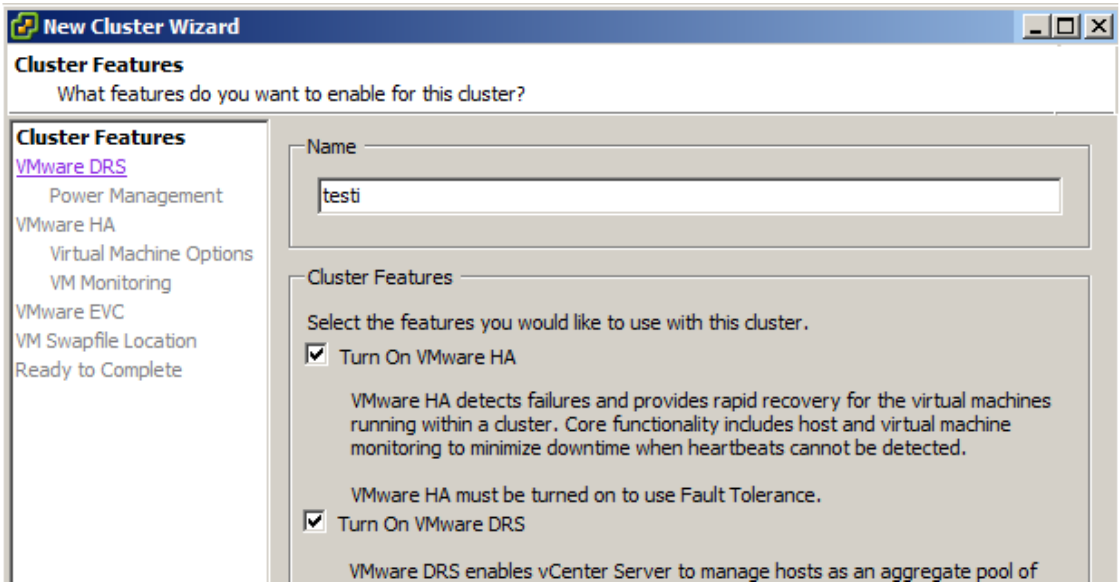
Portista yksi lähtevät harmaat verkkokaapelit päätyvät SimuNetin ulkopuoliseen switchiin (kytkin). Switchi on klusterin ja iSCSI-verkkolevyjärjestelmän hallinnan koontikytkin, jonka 5 porttia on eristetty VLAN-tagauksella muusta mahdollisesta tulevaisuuden kytkimenliikenteestä. Koontikytkin on osa ICTlabin tuotantoverkkoa eli kalaverkkoa, ja tämän switchin kautta ICTlabin vCenter ohjaa klusterin toimintaa. Lisäksi ICTLAB-verkosta tulee hallintayhteys iSCSI-verkkolevyjärjestelmälle Omena-palvelimelta. Kaiken kaikkiaan aktiivisessa käytössä koontikytkimen porteista on neljä: yksi kummallekin palvelimelle, yksi iSCSI:lle ja yksi, joka yhdistää portit kalaverkkoon. Viides portti on käyttämätön, ja siinä on pitkä ethernet-kaapeli kiini ja kerällä verkkolaitteiden päällä. Tämä viides portti on tarkoitettu siihen tilanteeseen, että yhteys jostakin syystä ei toimi laboratorion verkosta palvelimille, jolloin kannettava tietokone on helppo liittää verkon toiseen päähän vianhakua ja korjausta helpottamaan. Klusterin verkkoa kasatessa ICTlabin IP-osoitemuutoksien aikana tämä edellä mainittu varaportti kannettavalle oli aktiivisessa käytössä, koska palvelimien hallinta IP-osoitteet eivät ole dynaamisia, vaan ne on käsin määritelty palvelimien asetuksiin, ja palvelimille käyttöön annetut tuotantoverkon osoitteet vaihtuivat muutamaankin kertaan. Klusterin hallintalinjojen kahdennus olisi hyvä lisä, ja vCenter ilmoittaa siitä klusterin heikkona kohtana mutta tämänhetkisillä laitteilla hallintayhteyden kahdentamisen toteuttaminen ei ole käytännössä järkevästi ja hyvin toimivasti mahdollista. Syy hallinnan kahdentamisen toteutuskelvottumuuteen johtuu siitä että kalaverkko ja SimuNet tulee pitää erillään, ja palvelimissa ei yksinkertaisesti ole Eth-portteja tarpeeksi klusterille, asiakasporteille ja kahdelle hallintaan varatulle portille.

4.3 Klusterin luominen VMware vCenteriin ja palvelimen lisääminen klusteriin

Klusterin luomistyökalu löytyy vCenter:istä datacenterin valikosta (kuva 21). Klusteria luodessa ominaisuuksiin voidaan valita VMware HA, joka tarkoittaa high availability -ominaisuutta eli korkeaa saatavuutta parantavaa ominaisuutta (kuva22). VMware DRS on ominaisuus, jolla klusterin resursseja voidaan jakaa tehokkaammin ja klusteri saadaan itsestään laskemaan esimerkiksi, mille palvelimelle virtuaalipalvelin on paras sijoittaa resurssien optimaalisen käytön kannalta.



kuva 21: Klusterin luominen (4)

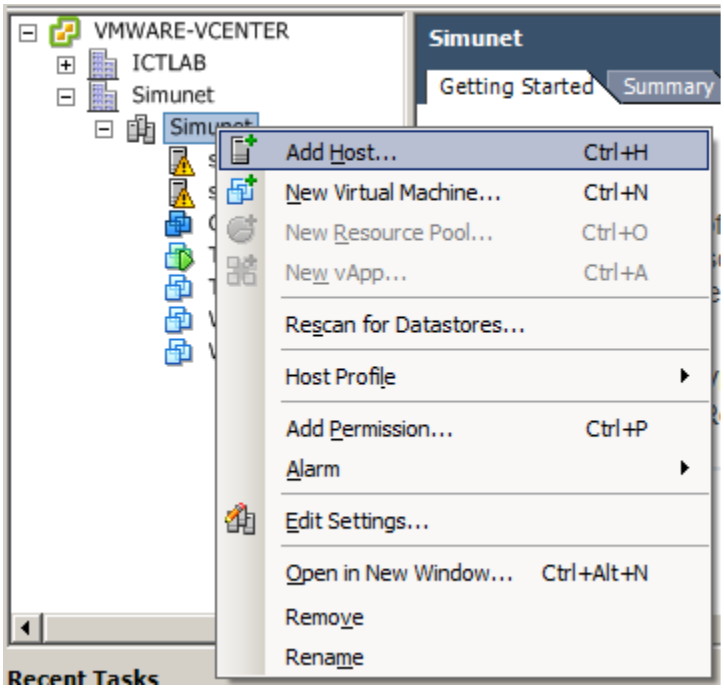


kuva22: klusterin luonnin ominaisuuksia (4)

Oletuksena DRS ja HA eivät ole käytössä, mutta niiden käyttäminen on erittäin hyödyllistä jotta klusteri toimisi mahdollisimman tehokkaasti suuren kuormituksen ja vikatilanteiden tapauksessa. Kyseisien ominaisuuksien oletusasetukset ovat kohdallaan ja järkevät. Klusterin automaattista virtuaalipalvelinmigraatiota ja kuormanjakoa voidaan kyllä säätää aktiivisemmaksi tai passiivisemmaksi, mutta oletuksena se on keskiarvossa. Tämä tarkoittaa sitä että virtuaalipalvelimen fyysinen sijainti muuttuu tarvittaessa, mutta ei heti jos palvelimelle tulee hetkellinen kuormituspiikki.

4.3.1 Palvelimen lisääminen klusteriin

Palvelimen lisäys klusteriin tapahtuu klusterin alavalikosta (kuva 23) sekä klusterin aloitussivulta, joka näkyy, kun klusteri on valittuna. Palvelimen lisäämiseen tarvitaan palvelimen IP-osoite ja administrator-tunnukset. Kun vCenter on löytänyt palvelimen, palvelin nimetään uniikisti klusterin listalle, kuten kuvassa 3 nähdään SimuNetin klusterien palvelimien nimeämistavasta.



kuva 23: serverinlisäys klusteriin (4).

4.3.2 Virtuaalipalvelimet klusterissa

Virtuaalipalvelimet ovat klusterin sisällä toimivia prosesseja, jotka toimivat kuten aiemmin klusteritoiminnassa klusterin sisäiset prosessit toimivat. Kun virtuaalipalvelin joko käyttäjän toimesta tai klusterin sisäisen tasapainotuksen johdosta siirtyy toiselle fyysiselle palvelimelle, sitä kutsutaan migraatioksi. Migraatio ei toisaalta ole vain klusterin sisäisten virtuaalipalvelimien fyysisen sijainnin vaihtumista, vaan migraatio käsittää myös klusteriin siirrettävän virtuaalipalvelimen

siirron, kuten myös klusterista klusterin ulkopuoliselle palvelimelle tapahtuvat virtuaalipalvelimen siirron. Sinällään migraatio ei ole siis klusteri sidonnainen tapahtuma eikä käsite, joskin se on hyvin tyypillinen tapahtuma vikatilanteissa ja edellä mainitussa kuormanjaossa. Migraatiota ei pidä ymmärtää virtuaalipalvelimen kopiointina (clone), koska kun virtuaalipalvelin siirretään, sen prosessit ajetaan alas vanhalta serveriltä ja kyseisen virtuaalipalvelimen kaikki datat siirtyvät uudelle varsinaiselle palvelimelle. Myöskään virtuaalipalvelimen nimi tai mitkään muutkaan asetukset eivät vaihdu. Migraatio ominaisuus löytyy clone-työkalun yläpuolelta (kuva 6).

Migraatio on hyvä ominaisuus esimerkiksi tietoturvapalvelimia testatessa, jolloin kontrolloiduissa laboratorio-olosuhteissa voidaan rakentaa ja testata palvelinta liittämättä sitä tuotantoverkkoon. Kaiken ollessa valmista voidaan käynnissä oleva virtuaalipalvelin liittää tuotantoverkkoon kitkatta heti käyttövalmiina. Klusterin sisäinen virtuaalipalvelimen siirto tapahtuu automaattisella migraatiolla, kun esimerkiksi jonkin palvelimista ylikuormittuu.

5 TULOSTEN TARKASTELUA

Palvelinklustereita käsitellessä vikasietoisuus on olennainen hyöty ja tietomassojen tallennus on hyvin tärkeä osa. Tämän työn iSCSI-verkkolevyjärjestelmä on kevytsarjalainen tiedontallennus sarjoissa, ja tiedontallennus on kovaa bisnestä samalla tapaa kuin palvelimien virtualisointi ja ylläpito. Samalla tapaa kuin palvelimien pitää olla käytettävissä 24 tuntia vuorokaudessa 7 päivänä viikossa, on massiivisten datapankkien oltava hyvässä kunnossa ja aina käytettävissä.

5.1 Vikasietoisuus ja virheestä palautuminen

Kuten tässä työssä on jo aiemmin useasti viitattu virhe ja vikatilanteisiin, niin klusterin parhaita puolia on nimenomaan sen vikasietoisuus. SimuNetin klusterin vikasietoisuus tämän työn konkreettisen tekemisen aikana tuli esiin monesti, ja mitä paremmin kokonaisuus alkoi toimia, sitä vakaammaksi klusterin palvelut muuttuivat. Tällä hetkellä, kun klusteri on valmis, sen ylläpitämät virtuaalipalvelimet jatkavat toimintaansa, mikäli edes toinen palvelin on toiminnassa. Suoran palvelinvian simuloimiseksi, kenellekään klusterin käyttäjälle ilmoittamatta, sammutin äkillisesti toisen palvelimen. Äkillinen sammuttaminen tarkoittaa tässä tapauksessa virtojen katkaisua. Muutama käyttäjä huomasi, että palvelimilla esiintyi hyvin lyhyt katkos, mutta hekin pitivät sitä lähinnä palvelimen hallintakoneen jumittumisena, ei niinkään palvelimien ongelmana. SimuNet-klusteri siis kaikesta päätellen on hyvin vakaa järjestelmä.

Verkko-ongelmia sen sijaan ei ole tarvinnut simuloida missään vaiheessa, niitä on riittänyt aivan kylliksi viantestausmielessä, koska SimuNetin tietoverkon asetuksia on ollut muuttelemassa useita ihmisiä, ja monilla on ollut jossain määrin omat näkemyksensä asioista, näkemyksiä, joista toiset ovat olleet toimivampia kuin toiset. Suurin yksittäinen ongelmia aiheuttanut sekaannus oli, kun joku oli käynyt muuttelemassa palvelimien verkkokytkentöjä klusterin sisäisen liikenteen tietoverkkossa. SimuNet-kokonaisuus on suunniteltu niin, että kummallakin palvelimella on oma linjansa toiselle palvelimelle ja oma linja iSCSI:lle (kuva 20). Joku oli vaihdellut johtoja, niin että toinen palvelin oli menettänyt yhteyden iSCSI-

verkkolevyjärjestelmään ja iSCSI oli yhteydessä SimuNetin klusteriverkkoon enää yhdellä kaapelilla. Käytännössä 1/3 verkkoyhteyksistä ei toiminut, mutta silti kaikki virtuaalipalvelimet olivat käynnissä ja toimivat moitteettomasti. Tätä edellä mainittua ongelmaa en olisi edes havainnut, ellen aina välillä varmistaisi, että kaikki laiteet tunnistavat toisensa kun alan parantelemaan kokonaisuutta. Ongelma näyttäytyi niin että palvelimista toinen oli menettänyt 1,82 terabittiä kovalevytilastaan. Vastaisuuden varalle vaihdoin kaikki klusterin sisäisen liikenteen kaapelit tummanvihreiksi ja kerroin ettei niihin pitäisi koskea.

Toinen suurenluokan mysteeri oli miten klusteri toimi, vaikka sen verkko oli ihan väärin konfiguroitu. Potentiaalinen ongelma syntyi siitä, että tietoverkon kasanneet olivat nimenneet verkkolaitteet kasaamisjärjestyksessä. Järjestys sattui oleman oikealta vasemmalle, kun taas varsinaisten asetusten tekijät olivat tehneet asetukset ajatellen, että laitteet olisi nimetty vasemmalta oikealle. Jopa verkon kuvat oli piirretty niin, että laiteet olisi nimetty vasemmalta oikealle. Joka tapauksessa klusteri onnistui luomaan yhteydet, ilmeisesti virtuaalikytkimien kautta ja toimimaan kohtuullisen hyvin. On siis perustelua ilmaista asia näin, että vaikka ongelman pitäisi olla suorastaan koko järjestelmän rampauttavaa luokkaa, niin klusteri mukautuu ja toimii silti niin kauan kun palvelimien asetukset ovat kunnossa.

ISCSI verkkolevyjärjestelmä on koko klusterissa heikoin lenkki. ISCSI toimii kyllä tallennuskapasiteettina todella varmasti, mutta sen hallintayhteydellä on paha tapa muuttua täysin toimimattomaksi täysin tuntemattomasta syystä. Ongelma esiintyy täysin sattumanvaraisesti ainakin sen perusteella, mitä itse olen voinut havainnoida. Voi olla, että yhteys toimii moitteettomasti kuukausia, mutta sitten jostakin syystä yhtenä aamuna yhteys ei enää toimikaan. Ainoaksi ratkaisuksi ongelmaan on löytynyt vain iSCSI-verkkolevyjärjestelmän sähköinen uudelleenkäynnistys, jonka jälkeen hallintayhteyden muodostus taas onnistuu. Ongelman ja ratkaisun luonteesta johtuen epäilen että ongelma on sähköinen, koska laitteen elektroniikka on paljon hienompaa kuin sen sisältämä ohjelmisto.

ISCSI-verkkolevyjärjestelmän hallintaongelmia voi syntyä mikäli myös yhteys ICTLAB:in kalaverkon DHCP-pavelimeen ei toimi. Mikäli iSCSI ei saa DHCP-palvelimeen yhteyttä voidaan verkkolevyjärjestelmää hallita irrottamalla sen hallintayhteys koulun verkosta ja liittämällä se suljettuun pieneen verkkoon, jossa sama kannettava tietokone ylläpitää sekä CAM:ia että DHCP-palvelua. Kannettava tietokone ei ole pakollinen ratkaisu, mutta on huomattavasti helpompi liikutella kuin pöytäkone tai palvelinkone. Täytyy kuitenkin ottaa huomioon, että CAM-ohjelma vaatii, että sitä pyörittävän koneen käyttöjärjestelmä on Windows XP pro tai jokin Windows 2004 serveriä uudempi palvelinkäyttöjärjestelmä.

Klusterin palveluiden palautuminen on käytännössä kiinni kahdesta asiasta: kuinka noopea verkko klusterin osia yhdistää ja kuinka nopeasti virtuaalipalvelimet käynnistyvät uudelleen. Hyvin optimoitu virtuaalipalvelin, jolle on annettu paljon resursseja käyttöön palvelimelta, käynnistyy todella nopeasti uudelleen toisella palvelimella olettaen, että verkko, jonka läpi virtuaalipalvelin siirtyy toiselle palvelimelle, on nopea. Palveluratkaisuissa nopeutta, etenkin vikatilanteissa, ei pidä siis sälyttää ainoastaan klusteripohjan varaan, vaan edelleen palvelimetkin tulee virittää huippuunsa kuten aikaisemminkin. Klusteri ja iSCSI-verkkolevy antavat kyllä erinomaisen pohjan palveluratkaisuille suorituskyvyssä, tiedontallennuskapasiteetissa ja tietoturvamielessä, mutta huonosti suunniteltu virtuaalipalvelin on edelleen huono palvelujen tarjoaja.

5.2 Teoreettista pohdintaa tietomassojen ylläpidosta ja tallennuksesta

Kun on kyse valtavista tietomassoista, kuten tuhat terabittiä eli miljoona megabittiä, on selvää, että tietojen hallinnointi ei olekaan enää Windows-työkalujen hallittavissa. Itse asiassa normaalit pienten järjestelmien työkalut ja etenkin yksityisille tarkoitetut Windows työkalut, ovat hyvin huonoja tämän kokoluokan tietomääriin, ja ne automaattisesti tukehtuvat. Yleensä tiedostot, joita normaalikäyttäjä käsittelee, ovat pieniä, noin sadasta megasta muutamaan gigabittiin, mutta kun katsotaan palvelinpuolen suuria tietovarastoja, niin yksittäiset logitiedostot kasvavat kymmeniin

gigabitteihin. Näin suuria tiedostoja normaalit levyneheytysohjelmat eivät osaa enää edes käsitellä.

Datavaraston ylläpito itsessään on nykyään todellista bisnestä, jossa kokematon ja asiaan perehtymätön ihminen saa hetkessä suurta tuhoa aikaan. Mikäli erehtyy käyttämään liian kevyen sarjan ohjelmaa tietovaraston eheyttämiseen, niin todennäköinen lopputulos on täysin jumissa oleva palvelu joka puolestaan käy nopeasti yritykselle kalliiksi. Esimerkiksi IBM:n tarjoaa Tivoli storage manager palvelua/ohjelmaa, joka on tarkoitettu massiivisien datapankkien kokonaishoitoon. Valitettavasti ohjelmasta itsestään julkista tietoa ovat vain mainokset, ja 5 sivua asiaa sisältävä englanninkielinen tietolehtinen. (3, 1–5)

LÄHTEET

1. Kormu T. 2010. Simunet-testialustan perustaminen ja testitapaustutkimus. Opinnäytetyö, Kymenlaakson ammattikorkeakoulu. Saatavissa: http://papaya.ictlab.kyamk.fi/~amake/SimuNet/opinnayte_Kormu_Tero.pdf [viitattu [14.11.2010].

2. Wikipedia, Free Encyclopedia. 2010. Challenge-Handshake Authentication Protocol. Saatavissa: http://en.wikipedia.org/wiki/Challenge-handshake_authentication_protocol [viitattu 19.11.2010].

3. IBM corporation. 2010. IMB Tivoli Storage Manager Data sheet. Saatavissa: ftp://public.dhe.ibm.com/common/ssi/ecm/en/tsd03066usen/TSD03066USEN.PDF [viitattu 21.11.2010].

4. VMware Inc. 2010. vShere client v4.0. Saatavissa: ICT-laboratorion wlan, ip: 193.167.58.15, Kymenlaakson Ammattikorkeakoulu [viitattu: 10.9.2010].

5. Sun microsystems Inc. 2010. Common Array Manager. Saatavissa: ICT-laboratorion Luumu-palvelin, Kymenlaakson Ammattikorkeakoulu [viitattu: 11.9.2010].

6. Wikipedia, Free Encyclopedia. 2010. Rack Unit. Saatavissa: http://en.wikipedia.org/wiki/Rack_unit [viitattu: 8:12.210].