Marko Vuorinen

Palvelinvirtualisointi pienyrityksessä

VMware vSphere 4.1 ja Veeam Backup & Replication 5.0

Metropolia Ammattikorkeakoulu
Insinööri (AMK)
Automaatiotekniikka
Insinöörityö
24.11.2011

Metropolia

Tiivistelmä

Tekijä Otsikko Sivumäärä Aika	Marko Vuorinen Palvelinvirtualisointi pienyrityksessä 31 sivua + 1 liitettä 24.11.2011
Tutkinto	insinööri (AMK)
Koulutusohjelma	automaatiotekniikka
Suuntautumisvaihtoehto	kappaletavara-automaatio
Ohjaajat Ohjaava opettaja	toimitusjohtaja Johan Kinnula toimitusjohtaja Pekka Väisälä datanomi Marko Tarvainen lehtori Jukka Pirinen

Tässä opinnäytetyössä oli tarkoitus luoda pienyritykselle virtualisoitu palvelinkeskus- ja tiedonvarmistusratkaisu. Palvelinkeskuksen tuli vastata yrityksen operatiivisten tietojärjestelmien toimivuudesta sekä palvella ohjelmistokehitysympäristönä, joten sen käytettävyyden tuli olla erittäin korkeata tasoa. Tiedonvarmistusratkaisulla tuli pystyä aina palauttamaan vähintään edellisen päivän tilanne, mikäli palvelinympäristössä havaittiin vakava vikatilanne.

Palvelinkeskus toteutettiin kahdella palvelimella ja kolmella levyjärjestelmällä. Palvelinkeskuksen virtualisointiohjelmistona käytettiin VMwaren vSphere 4.1 essentials -tuotetta. Tietojenvarmistus toteutettiin Veeam softwaren Backup & Replication 5.0 -ohjelmistolla. VMwaren vSphere-ohjelman ominaisuudet ovat alansa huippuluokkaa, vaikka tässä työssä ei kaikkia ohjelman tarjoamia ominaisuuksia hyödynnettykään. Varmuuskopiointiohjelmiston käyttöönotto oli erittäin helppo ja nopea toimenpide. Varmuuskopioiden laatiminen ja niiden testaus havaittiin helpoksi ja yksinkertaiseksi.

Työn lopputuloksena luotiin pienyritykselle toimiva virtualisoitu palvelinkeskus. Palvelinkeskuksen käytettävyys yrityksen tuotantoympäristössä on osoittautunut erittäin hyväksi. Ohjelmistokehityksessä testausympäristöjen luonti on havaittu helpoksi ja auttanut ratkaisemaan ohjelmisto-ongelmia. Tiedonvarmistus on todettu hyväksi ratkaisuksi, jolla on saatu pelastettua käyttäjän vahingossa poistamaa tietoa.

Jatkokehityskohteena nähdään yrityksen palvelinkeskuksessa varmuuskopioiden testauksen kehittäminen.

Avainsanat	VMware, Veeam, virtualisointi, varmuuskopiointi

Metropolia

Abstract

Author Title Number of Pages Date	Marko Vuorinen Server Virtualization in Small Business 31 pages + 1 appendix 24 November 2011
Degree	Bachelor of Engineering
Degree Programme	Automation Technology
Specialisation option	Manufacturing Automation
Instructors Supervisor	Johan Kinnula, CEO Pekka Väisälä, CEO Marko Tarvainen, Vocational Qualification in Business Information Technology Jukka Pirinen, Senior Lecturer

The aim of this thesis was to create virtualized datacenter and data recovery solution for a small business. The datacenter would be responsible for corporate operative information systems and serve as programming development environment, so its usability should be very high. Data recovery solution should be able to recover at least previous day's situation, in case datacenter suffers serious malfunction.

The datacenter was created with two data servers and three disk arrays. VMware vSphere 4.1 Essentials product was used to create virtualized datacenter. Veeam software's Backup & Replication 5.0 software was used to create data protection enviroment. The features of VMware's vSphere software are state-of-the-art, even if all features were not implemented in this work. Data protection software implementation was easy and fast operation. Backup testing and backup making was easy and simple.

The result of this thesis was a functioning virtualized datacenter for small business. Datacenter's usability has proven to be very high. In software development the creation of test environments has proven simple and helped solving software problems. Data protection has also proven to be a good solution, which has been used to save users accidentally removed information.

Further development focus on the company's datacenter would be improvements in the testing of the backups.

Keywords	VMware, Veeam, virtualization, backup

Sisällys

Lyhenteet

AD Active Directory, aktiivihakemisto ylläpitää Windows-verkon käyttäjätietokantaa ja hakemistopalvelua.
CBT Changed Block Tracking, muuttuneiden tietolohkojen seuranta vSphere-palvelimessa.
DNS Domain Name System, nimipalvelu, joka ylläpitää IP-osoitteisiin liitetyt nimet.
DHCP Dynamic Host Configuration Protocol, verkkoprotokolla, joka jakaa IP-osoitteet.
DRS Distributed resource scheduler, automaattinen kuormantasausominaisuus.
HA High availability, korkea käytettävyys luodaan kahdennetulla palvelinympäristöllä, jossa vikatilanteessa viallinen palvelin poistetaan käytöstä.
I/O Input/Output, tulo- ja lähtökanava.
IP Internet Protocol, internetprotokolla.
iSCSI Internet Small Computer System Interface, tallennusverkoissa käytetty protokolla.
LACP Link Aggregation Control Protocol, on tekniikka, jonka avulla pystytään yhdistämään useampi portti vikasietoisuuden tai nopeuden kasvattamiseksi.
MTU maximum transmission unit, verkkosanoman maksimipituus.
NAS Network Access Storage, verkkokovalevy.
NBD Network Block Device, on protokolla, joka siirtää tiedon lohkotasolla palvelimesta.
RAID Redundant Array of Independent Disks, tekniikka, jolla kiintolevyjä yhdistetään yhdeksi loogiseksi yksiköksi varmuuden kasvattamiseksi.
SAN Storage area network, tallennusverkko.
SNMP Simple Network Management Protocol, verkonhallintaan tarkoitettu protokolla.
SQL Structured Query Language, standardoitu ohjelmointikieli tietokantojen käytössä.
TCPIP *Transmission Control Protocol / Internet Protocol,* verkkoliikenteessä käytettävä protokolla.
TLB Translation Lookaside Buffer, käännöshakutaulu, josta haetaan muistin sisältöä.
UPS Uninterruptible Power Supply, jännitelähde, joka ylläpitää käyttöjännitettä lyhyiden virtakatkojen aikana.
VLAN Virtual LAN, virtuaalinen lähiverkko.
VMM Virtual Machine Monitor, virtuaalikone eli hypervisor.
VSS Volume Shadow Copy Service, palvelu, joka määrää käyttöjärjestelmän kirjoittamaan kaiken tiedon levylle, jolloin levystä voidaan ottaa levynkuva talteen.
WWN World Wide Name identifier, tallennusjärjestelmissä yksilöllinen laitetunniste.

1 Johdanto

Informa Oy (jäljempänä Informa) on etiketöinti- ja merkintäratkaisuihin keskittynyt suomalainen pienyritys, joka on perustettu vuonna 1989. Yrityksen palvelutarjontaan kuuluvat merkintälaitteet, ohjelmat ja tulostusmateriaalit. Yrityksen tuotteet on tarkoitettu yrityskäyttöön. Yrityksen palveluksessa on tällä hetkellä 32 henkilöä.

Aikaisemmin Informassa oli toinen liiketoimintahaara, joka keskittyi tiedonkeruu- ja työajanseurantajärjestelmiin. Tämä liiketoiminta eriytettiin omaksi yhtiökseen, joka lopulta myytiin. Informan palvelimet oli jo tällöin virtualisoitu VMwaren Infrastructure 3 standard -ohjelmistolla. Yrityksen irtautumisen aikaan sovittiin, että palvelimet ja virtualisointiohjelmistot siirtyvät yrityskaupan mukana uuteen yritykseen. Tämän seurauksena Informan palvelinratkaisut jouduttiin pikaisesti miettimään uudelleen. Tällöin päädyttiin siihen, että hankittiin yksi palvelin ja sille virtuaalinen levyjärjestelmä. Palvelimen ohjelmistoksi otettiin käyttöön ilmainen virtualisointialusta ESXi 3 hypervisor, josta on karsittu ominaisuuksia, esimerkiksi varmuuskopiointi. Tämä ESXi 3 hypervisor -versio ei tue uudempia käyttöjärjestelmiä.

Työn tavoitteena oli päivittää nykyinen virtualisointialusta ESXi 3 uudistuneeseen vSphere 4-ympäristöön. Tällöin saadaan osa ohjelmiston ominaisuuksista takaisin tuotantokäyttöön. Lisäksi luodaan edellytykset sille, että tarvittaessa tuotantopalvelimen virtuaalikoneet pystytään siirtämään varapalvelimelle, jolloin käytettävyys kasvaa ja mahdollisten ongelmatilanteiden aiheuttamat kustannukset pienenevät.

Virtualisointialustan päivitys antaa samalla mahdollisuuden erilaisten testiympäristöjen luomiseen ohjelmistojen asennuksia ja testauksia varten, jolloin päästään eroon vanhoista palvelimista, joita on aikaisemmin käytetty siihen tarkoitukseen. Työssä on samalla tarkoitus laatia toimiva ratkaisu tietojen varmuuskopioinnista. Lisäksi luodaan toimivat rutiinit palvelimien varmuuskopioinnin suorittamiseen ja varmistetaan mahdollisessa ongelmatilanteessa palvelinympäristön palauttaminen mahdollisimman pienin tuotantokatkoin.

2 Virtualisointi

2.1 Yleisesti

Virtualisoinnilla tarkoitetaan teknologiaa, joka piilottaa fyysisen laitteiston piirteet virtualisointikerroksen alle. Virtualisointi sallii useiden käyttöjärjestelmien yhtaikaisen suorittamisen yhdellä laitteistolla. Virtualisointi abstraktoi käyttöjärjestelmät ja sovellukset laitteistosta. Virtualisoidusta palvelinkeskuksesta on alettu käyttää termiä pilvi (cloud). Puhuttaessa yrityksen sisäisestä virtualisoidusta palvelinkeskuksesta tästä käytetään nimitystä oma pilvi (private cloud).

2.2 Historia

Virtualisoinnin kehitys on käynnistynyt jo 1959, jolloin Christopher Strachey Oxfordin yliopistosta julkaisi artikkelin, jossa hän esitti time sharing -tekniikan. Hän itse kutsui sitä moniajoksi. Tämä tarkoitti sitä, että toinen käyttäjä pystyi kehittämään ohjelmaa samaan aikaan kun toinen käyttäjä testasi omaa ohjelmaansa. (1, s. 33.)

Ensimmäinen supertietokone, joka osasi hyödyntää näitä tekniikoita, kehitettiin Manchesterin yliopistossa, ja sitä kutsuttiin Atlas-tietokoneeksi. Atlas osasi myös hyödyntää virtuaalimuistia ja muistin sivutusta, kuten myös jaettuja oheislaitteita. Atlas oli aikansa nopein tietokone. Atlaksen suuri nopeus oli saavutettu osittain siitä syystä, että sen ohjelmat oli jaettu kahteen erilliseen osaan. Nämä osat olivat käyttöjärjestelmän ”prosessi”, jota kutsuttiin supervisoriksi, ja ”suorittaja”, joka suoritti varsinaiset käyttäjän laatimat ohjelmat. Supervisor hallitsi kaikkia avainresursseja, kuten prosessointiaikaa ja sille välitettiin erikoiskomentoja, jolla se hallitsi käyttäjän ohjelmaympäristöä. Tämä virtuaalikoneen tarkkailija oli todellisuudessa hypervisor eli virtualisointialusta. (1, s. 33.)

IBM kehitti Atlasta vastaavan projektin M44/44X. M44/44X koostui siten, että siinä oli päätietokone IBM 7044 (M44) ja useita simuloituja 7044 (44X) virtuaalikoneita, jotka käyttivät laitteistoa, ohjelmistoa, virtuaalista muistia ja moniajoa. Tämä arkkitehtuuri oli ensimmäinen, josta alettiin käyttää nimitystä virtuaalikone. (1, s. 33.)

1960-luvun lopussa IBM kehitti ensimmäisen täysin virtualisoidun käyttöjärjestelmän, joka perustui täysin virtualisoituun laitteistoon CP-40. Tämä johti tuotekehitykseen, jonka tuloksena julkaistiin VM/370, joka pystyi käyttämään useita virtuaalikoneita, suuremmalla virtuaalisella muistillaan. Tätä kaikkea hallitsi virtual machine monitor (VMM). (1, s. 34.)

Virtualisointi jäi taka-alalle 1980- ja 1990-luvuilla, jolloin asiakas-palvelinohjelmistot (client-server) valtasivat alaa. Lopulta Windows- ja Linux-palvelinohjelmistot valtasivat yritysmaailman. Kuitenkin 1990-luvun lopussa havahduttiin siihen, että palvelimien käyttöaste oli alhainen ja niiden määrä kasvoi kasvamistaan. Tämä taas lisäsi käyttökustannuksia, ja mahdolliset ongelmatilanteet lamaannuttivat tietojärjestelmät täysin. Näihin ongelmiin VMware kehitti ensimmäisen x86-koneille tarkoitetun virtualisointialustan. (2.)

2.3 Miksi virtualisoida

Perinteisellä tavalla toteutettujen palvelimien käyttöaste on ollut keskimäärin 10 %, ja tällöin loppukapasiteetti on ollut tyhjäkäynnillä. Palvelimien laskentakapasiteetti on kasvanut nopeasti viime vuosina, jolloin käyttöaste on entisestään pienentynyt. Isoissa palvelinkeskuksissa yksittäiset palvelimet vievät runsaasti tilaa, ja koska virtualisoinnilla voidaan vähentää palvelimien lukumäärää, sillä saavutetaan myös suoria kustannussäästöjä. Laitteiden määrän vähentyessä niiden jäähdytys on yrityksille edullisempaa. Voidaan ajatella, että virtualisointi on myös ekologinen teko, koska laitteiden lukumäärän pienentyessä ne käyttävät vähemmän sähköä. Järjestelmän ylläpidon katsotaan myös helpottuvan huomattavasti. (3, s. 5-6.)

2.4 Virtualisoinnin edut

Virtualisoinnilla saavutetaan useita etuja verrattuna perinteiseen palvelinarkkitehtuuriin. Perinteiset palvelimet käyvät keskimäärin 10 %:n käyttöasteella, jolloin saman tehoiseen virtualisoituun palvelimeen voidaan asentaa esimerkiksi kymmenen virtualisoitua palvelinta. Tästä käytetään usein termiä konsolidointi. Laitteiden fyysinen tila pienenee vastaavasti, jolloin laitteet mahtuvat pienempään tilaan. Yksi merkittävistä seikoista on myös sähkönkulutuksen ja laitteiden jäähdyttämiseen tarvittavan energiamäärän pieneneminen. (3, s. 3-6.)

Laitteiston fyysinen ylläpito on helpottunut, kun virtualisoidut palvelimet voidaan siirtää toiselle palvelimelle huoltotöiden ajaksi. Palvelimien huoltotöistä ei aiheudu mitään tuotantokatkoksia. Fyysisten palvelinresurssien lisääminen virtuaaliseen ympäristöön onnistuu hyvin helposti. (3, s. 3-6.)

Järjestelmä pystytään palauttamaan edelliseen toimintatilaansa nopeasti, kun käytetään snapshot-toimintoa. Tämä tarkoittaa, että järjestelmästä otetaan senhetkinen levynkuva talteen ja siihen on mahdollisuus palata jälkikäteen. Palvelimen kaikki muuttuvat tiedot kirjoitetaan tämän jälkeen uuteen tiedostoon. (1, s. 48.)

Ohjelmiston testaus on helpottunut, kun virtualisoiduista käyttöjärjestelmistä pystytään tekemään uusia klooneja eikä koko käyttöjärjestelmää kaikkine päivityksineen tarvitse asentaa alusta lähtien uudestaan. Virtuaalikone voidaan lisäksi määritellä palautuvaksi alkutilaan uudelleenkäynnistyksen yhteydessä, mikä nopeuttaa ongelmien ratkaisua. (1, s. 49.)

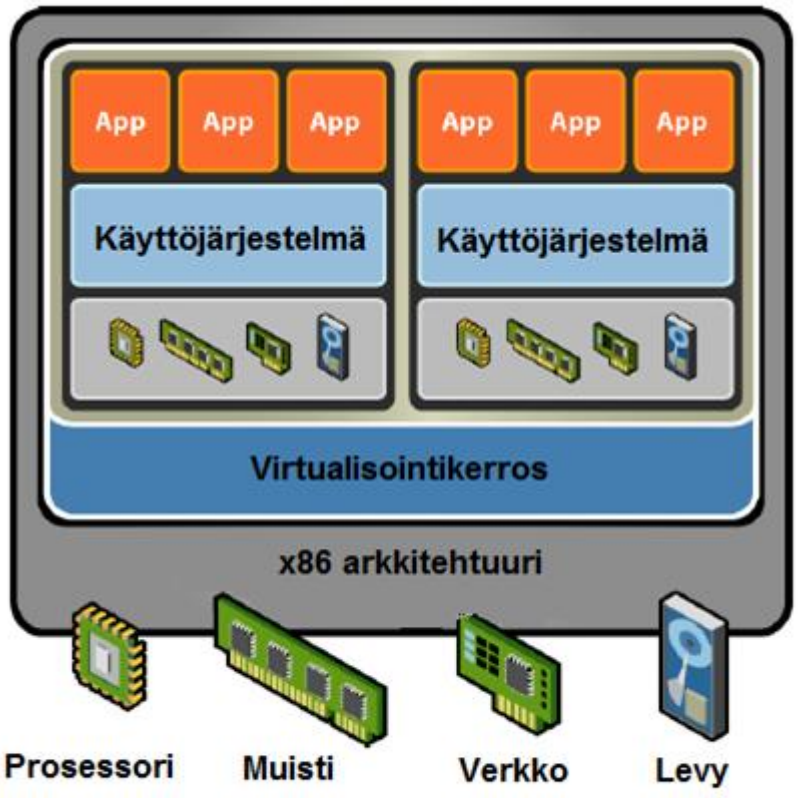
Yhtenä tärkeimpänä piirteenä voitaisiin pitää vikatilanteesta toipumista. Aikaisemmin palvelimen rikkoontuessa siitä toipuminen saattoi kestää päiviä. Nyt palvelin voidaan saada toimintakuntoon minuuteissa. Tämä kuitenkin edellyttää, että tiedot ovat tallennettuna tallennusverkkoon (SAN), josta toiset palvelimet pääsevät tiedot lukemaan. (1, s. 49.)

Tällä tekniikalla koko IT-infrastruktuuri pystytään ulkoistamaan palveluksi, joka hankitaan palveluntarjoajalta. Tästä käytetään termiä infrastructure as a service (IaaS). Palveluntarjoaja huolehtii palvelimista, tallennuslaitteista ja verkoista. Palvelussa palvelimien rakennetta ja ominaisuuksia pystytään muuttamaan käyttötarpeiden mukaan. Tällaisessa palvelussa maksetaan vain käytetyistä resursseista. (1, s. 10.)

2.5 Miten virtualisointi toimii

Virtualisointi on teknologia, joka muuttaa laitteiston ohjelmistoksi. Virtualisointikerros lisätään fyysisen laitteiston ja käyttöjärjestelmän väliin. Tämä abstraktoi fyysisen laitteiston virtuaalikoneita varten. Tämä kerros osoittaa dynaamisesti fyysiset resurssit, kuten prosessorin, muistin, verkon ja levyjärjestelmän kaikille virtuaalisille käyttöjärjestelmille. Virtualisointikerros mahdollistaa useiden käyttöjärjestelmien

samanaikaisen suorituksen yhdellä laitteistolla. Kuva 1 havainnollistaa virtualisoitua palvelinympäristöä. (6, s. 5.)



Kuva 1. Virtualisoitu palvelinympäristö (9).

Virtualisoidussa palvelinympäristössä on oleellista, että käyttöjärjestelmät eivät pysty kirjoittamaan toistensa muistialueisiin tai käyttämään prosessoria toisen koneen suorittaessa jotain toimintoa. Tämä on toteutettu siten, että virtualisointikerros on asennettu käyttämään prosessorin suojaustasoa 0 ja tietyiltä osin myös suojaustasoa 1 ja käyttöjärjestelmä käyttää suojaustasoa 1, mutta laajennetuin valtuuksin ja sovellukset suojaustasoa 3. Mikäli prosessorissa on tuki virtualisoinnille, tällöin virtualisointikerrosta ajetaan suojatummalla tasolla -1 ja käyttöjärjestelmää tasolla 0. Näillä suojaustasoilla määritellään, mitä toimintoja prosessorilla pystytään suorittamaan. Mikäli jokin käyttöjärjestelmä antaisi vaikka uudelleenkäynnistyskomennon prosessorille, tämä komento estettäisiin ja uudelleen käynnistettäisiin vain kyseinen virtuaalikone, jolta komento tuli. (6, s. 5.)

Muistin virtualisoinnissa fyysinen muisti jaetaan virtuaalikoneille dynaamisesti. Virtualisoidulla käyttöjärjestelmällä ei ole suoraa yhteyttä fyysiseen muistiin, vaan VMM huolehtii muistin käsittelystä. Muisti sivutetaan niin sanottuna varjosivutuksena (shadow paging), jolloin virtuaalikone käyttää normaalia muistin osoitteenhakua välimuistin avulla ja hakee tiedon käännöshakutaulusta (TLB) normaalisti. Tällä vältetään se, että muistia ei tarvitse siirtää kahdesti eri muistipaikkaan virtuaalikonetta varten. Muuttaessaan muistin sisällön sijaintia virtuaalikone päivittää vain varjosivutustaulukon tiedon, jolloin muistin sisältö on taas haettavissa. (6, s.7.)

Lisälaitteiden ja I/O:n virtualisoinnissa reititetään I/O-pyyntöjä virtuaalisen laitteen ja fyysisen laitteen välillä. Ohjelmallisella I/O-virtualisoinnilla pystytään luomaan täysin suora yhteys laitteen ja virtuaalikoneen välille. Tällöin voidaan esimerkiksi yhdistää useampi verkkokortti yhdeksi verkkokortiksi ja luoda siten vikasietoisempi ympäristö. (6, s. 7.)

Perinteisessä palvelinarkkitehtuurissa levyjärjestelmä on ollut suoraan kiinni palvelimessa SCSI-ohjaimen avulla (DAS). SCSI on palvelimien käyttämä tiedonsiirtoprotokolla oheislaitteille. Virtualisoinnissa DAS-tekniikan käyttö on ollut hieman haastavaa ja epäkäytännöllistä, koska virtuaalikoneita ei pystytä siirtämään koneelta toiselle, jos palvelin vioittuu. Levyjärjestelmän virtualisointi tapahtuu käyttämällä erillistä tallennusverkkoa (SAN) tai (NAS). Tallennusverkoissa on käytössä kahta erilaista tekniikkaa, ensimmäinen on kuitukanava (Fibre Channel) ja toinen iSCSI. iSCSI on tallennusverkoissa käytetty protokolla, jossa SCSI-komennot on kapseloitu IP-sanomaan (1, s. 53.)

Verkon virtualisointi tapahtuu käyttämällä IEEE 802.1Q -standardin mukaisia laitteita, jotka osaavat käsitellä virtuaalisia paikallisverkkoja (VLAN). Tässä tekniikassa paketin kehykseen lisätään käytettävän verkon VLAN-tunnus, jota kaikki samassa VLANissa olevat laitteet kuuntelevat. Tällä tavalla toimivassa verkossa pystytään eristämään VLANien verkkoliikenne, vaikka ne olisi kytketty samaan fyysiseen verkkoon. (1, s. 54.)

2.6 Erilaiset virtualisointitekniikat

Palvelimien virtualisointitekniikat voidaan jakaa kolmeen erilaiseen virtualisointitapaan, jotka ovat täysvirtualisointi eli natiivi virtualisointi, paravirtualisointi ja käyttöjärjestelmävirtualisointi (1, s. 51–52).

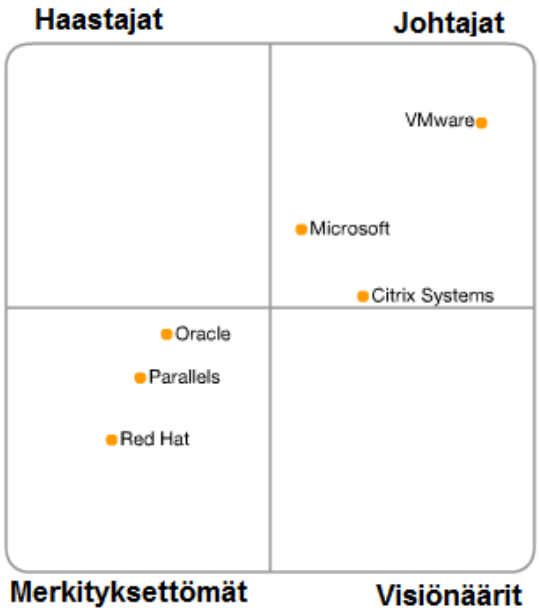
Täysvirtualisoinnissa simuloidaan virtuaalinen laitteisto täysin samanlaiseksi kuin käytössä oleva fyysinen laitteisto. Tällöin kaikki ohjelmistot, jotka pystyvät toimimaan tuossa laitteistossa, pystytään ajamaan tässä ympäristössä. Tällä tekniikalla on kaikista suurin käyttöjärjestelmien tuki, ja käyttöjärjestelmät pystytään asentamaan ilman ylimääräisiä lisäohjelmia. Tällä saavutetaan isäntäkoneen prosessorien ja muistin hyödyntäminen lähes alkuperäisellä tehokkuudella. Virtuaalikoneet ovat täysin eristetyt toisistaan. Haittapuolina voidaan mainita, että täysvirtualisoinnilla ei pystytä kaikkia laitteita käyttämään, koska jokainen laite tarvitsee oman ajurin. Laitevalintojen suhteen on oltava tarkkana, ja sitä varten ohjelmistotoimittajilla on omat luettelonsa yhteensopivista laitteista. (1, s. 51–52.)

Paravirtualisoinnissa lähinnä emuloidaan isäntälaitteistoa, jolloin jokaista käyttöjärjestelmää kohden tarvitaan oma pieni ohjelmisto, joka toimii limittäin käyttöjärjestelmän kanssa. Ohjelmisto muuttaa käyttöjärjestelmää siten, että tietyt prosessorikomennot ohjataan virtualisointikerrokselle. Näistä kutsuista käytetään nimitystä hyperkutsu. Paravirtualisoinnin hyviä puolia on laitteiston laaja tuki, koska paravirtualisointi ei sisällä mitään laiteajureita. (3, s. 14.)

Käyttöjärjestelmävirtualisoinnissa käyttöjärjestelmiä ajetaan olemassa olevan käyttöjärjestelmän päällä. Tällä tavalla virtualisoitu käyttöjärjestelmä ei näe isäntäkoneen resursseja virtualisoituna vaan fyysisinä resursseina. Näin virtualisoidut käyttöjärjestelmät on eristetty osin tai kokonaan isäntäkäyttöjärjestestelmästä. Käyttöjärjestelmävirtualisoinnin hyviä puolia on virtuaalikoneen nopeus, joka vastaa lähes isäntäkoneen nopeutta, ja kaikki käyttöjärjestelmät toimivat tässä ympäristössä ilman laitteisto-ongelmia. (1, s. 67.)

2.7 Erilaiset palvelinvirtualisointiohjelmistot

Alan johtavaa markkina-asemaa ylläpitää VMware Inc. arviolta 80–90 %:n markkinaosuudella VMware vSphere-ohjelmistolla. Microsoft Corporation on lanseerannut oman palvelinvirtualisointiohjelmiston Hyper-V, josta julkaistaan pian versio 3.0. Citrix Systems on julkaissut täysin avoimen Xen Server -tuotteen. Muiden pienempien toimijoiden markkinaosuus on merkityksetön, kuten Gartner on viimeisessä raportissaan todennut. (4.)



Kuva 2. Gartnerin SWOT-analyysi palvelinvirtualisointiohjelmistojen toimittajista (4).

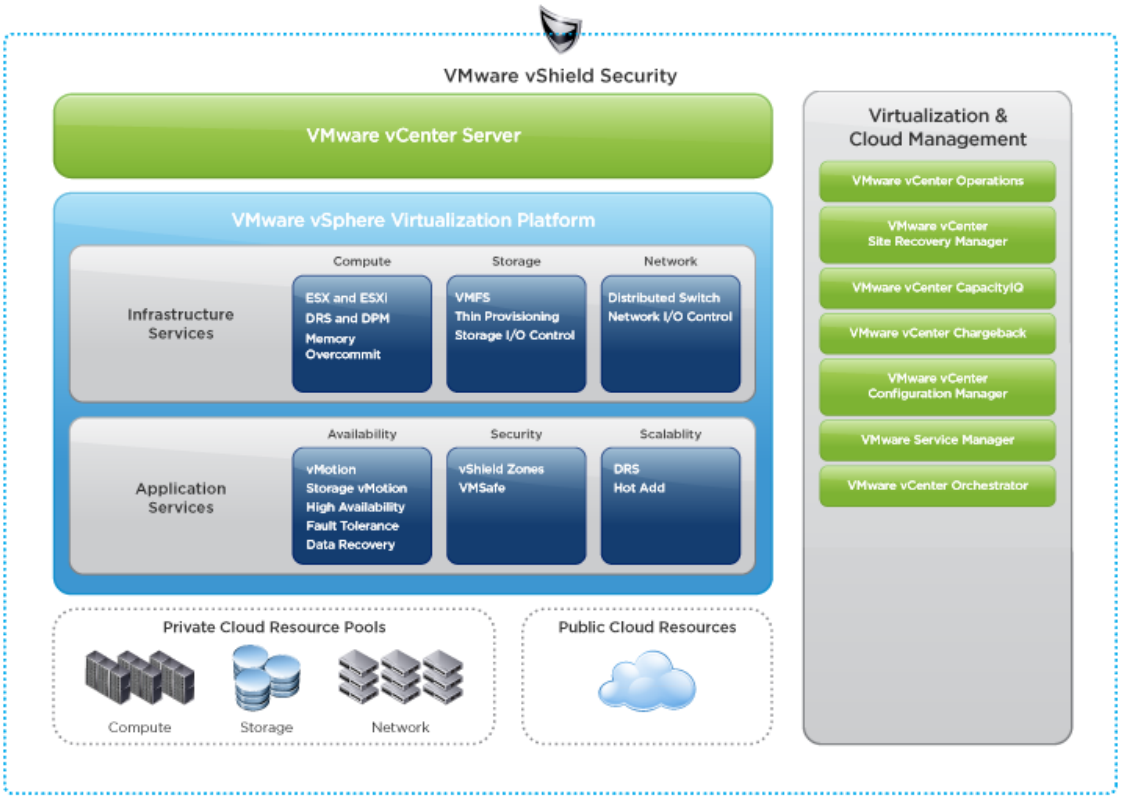
Microsoft on onnistunut Hyper-V:n avulla kasvattamaan markkinaosuuttaan, erityisesti pienemmissä virtualisointihankkeissa, johtuen tuotteen edullisesta hankintahinnasta ja myös uusista ominaisuuksista, joita Hyper-V-ohjelmistoon on tehty. Vuoden 2010 analyysissä Microsoft oli vielä haastajan roolissa. (4.)

3 VMware vSphere

3.1 vSphere

vSphere on VMwaren pilvilaskentaohjelmistopaketti, johon kuuluu useita ohjelmistoja. Tästä käytetään usein termiä oma pilvi (private cloud). Kuvassa 3 on havainnollistettu vSphere-tuoteperhettä. Pakettiin on mahdollista hankkia lisäksi erillisiä

hallintasovelluksia, joilla pystytään muun muassa nostamaan automaatioastetta tai raportoimaan tarkasti palvelinkeskuksen tapahtumista tai suorittamaan varmuuskopiointia.



Kuva 3. VMwaren datakeskustuotteet (10).

3.2 Bare Metal hypervisor

ESX ja ESXi ovat Bare Metal -hypervisoreita eli virtualisointikerros, joka asennetaan suoraan x64-arkkitehtuurin omaavaan järjestelmään ilman isäntäkäyttöjärjestelmää. Bare Metal hypervisorilla tarkoitetaan arkkitehtuuria, jolla on suora yhteys isäntälaitteiston fyysisiin resursseihin. ESX ja ESXi abstraktoivat fyysiset resurssit virtuaalikoneille. ESX on paljon suurempi ohjelmisto ja sisältää oman hallintakonsolin, jolla sitä pystytään hallitsemaan. ESXi omaa vain erittäin pienen virtualisointikerroksen, jota voidaan ajaa esimerkiksi USB-muistitikulta. ESXin hallinta tapahtuu käyttämällä erillistä komentokehotetta (vCLI) tai bios-tyyppistä (Basic Input-Output System) konsolia. (7, s. 26-31.)

3.3 vCenter

vCenter on keskitetty hallintaohjelmisto kaikille ESX- ja ESXi-virtuaalipalvelimille. Ohjelman perustoimintoja ovat resurssien jaot, ajastetut tehtävät, statistiikan keräys, hälytysten ja tapahtumien hallinta sekä virtuaalikoneiden asetukset. Update manager -ohjelmistolla suoritetaan olemassa olevien ESX- ja ESXi-palvelimien ohjelmistopäivitykset, kuten myös näissä sijaitsevien virtuaalikoneiden päivitykset. Ohjelman tietovarastona toimii Microsoftin tai Oraclen tietokanta. Ohjelmiston mukana toimitetaan Microsoftin SQL-server express -tietokantamoottori. (7, s. 4.)

Lisäksi vCenter-ohjelmisto tarjoaa kehittyneitä ominaisuuksia, kuten VMware VMotion, VMware Distributed resource scheduler (DRS) ja VMware High availability (HA). Vmotion-ominaisuudella pystytään siirtämään virtuaalikoneita eri palvelimien sekä tallennuslaitteiden välillä. Distributed resource schedule -ominaisuudella ohjelmisto pystyy automaattisesti päättelemään, miten eri virtaalikoneet kannattaisi jakaa palvelimien kesken, jotta ne kuormittuisivat tasaisesti. High availability -ominaisuudella pystytään luomaan kahdennettu palvelinympäristö, jolloin kaikki tieto virtuaalipalvelimesta kopioidaan toiselle virtuaalipalvelimelle. Ongelmatilanteen sattuessa toinen virtuaalipalvelin aktivoituu automaattisesti ja viallinen palvelin poistetaan tuotantoympäristöstä. (7, s. 4-8.)

3.4 vSphere client

vSphere client on vCenter-, ESX- ja ESXi-palvelimen hallintaan tarkoitettu graafinen käyttöliittymä, jolla kaikki virtuaaliympäristöön tehtävät toiminnot hoidetaan. Työkalu on tarkoitettu virtuaaliympäristön hallinnasta vastaavalle. (7, s. 10-11.)

3.5 vSphere Web Access

vSphere Web Access -käyttöliittymällä pystytään hallitsemaan virtuaalikoneita ja niiden resursseja. Työkalu on tarkoitettu lähinnä loppukäyttäjälle, jolla hän pystyy hallitsemaan omien virtuaalikoneidensa käynnistykset, sammutukset, snapshotit ja resurssit. Virtuaalikoneen etäkäyttö on myös mahdollista vSphere Web Access -käyttöliittymän kautta. (7, s. 11.)

3.6 vSphere converter

vSphere converter-ohjelmistolla pystytään konvertoimaan fyysisiä tai virtuaalisia palvelimia virtuaaliseksi palvelimeksi, joita ajetaan ESX- tai ESXi-palvelimissa. Palvelimet voivat olla joko Windows- tai Linux-pohjaisia. Konversio voidaan suorittaa joko kylmänä (cold migration) tai kuumana (hot migration). Kylmänä tehty konversio tehdään koneeseen, joka ei ole tuotantokäytössä, ja vastaavasti kuumana tehty konversio tehdään tuotantokäytössä olevaan palvelimeen. (5, s. 251-255.)

4 Palvelinjärjestelmä

4.1 Fyysinen laitteisto

Työssä käytettiin kahta palvelinta, pääpalvelinta ja toissijaista palvelinta. Niiden ominaisuudet on kuvattu seuraavassa. Pääpalvelimena toimii Dell PowerEdge R805, jonka suorittimina toimii kaksi kuusiytimistä AMD Opteron™ -prosessoria. Muistia laitteistossa on 64 GB ja verkkoyhteytenä toimii kuusi gigabitin nopeuteen pystyvää verkkokorttia. Toissijaisena palvelimena toimii Dell PowerEdge R310, jonka suorittimena toimii Intel Xeon -prosessori. Muistia laitteistossa on vain 16 GB ja verkkoyhteytenä toimii neljä gigabitin verkkokorttia. Kaikki verkkoliikenne on kytketty Ciscon 2960-sarjan kytkimeen.

Tallennuksessa on käytetty kolmea eri tallennuslaitteistoa. Ensisijaisena tallennuslaitteistona toimii Dell PowerVault MD3000i -levyjärjestelmä. Levyjärjestelmässä tallennuskapasiteetti on 600 GB ja levyvarmistus on toteutettu RAID-10 tasoisena. Levyjärjestelmä on varustettu vain yhdellä ohjaimella. Toissijaisena tallennuslaitteistona toimii Synologyn DS411, jonka tallennuskapasiteetti on 2 GB. Levyvarmistus on toteutettu RAID-5-tasoisena ja yhdellä varalevyllä. Kolmantena levyjärjestelmänä toimii Synologyn RS2211+, jonka tallennuskapasiteetti on 6 GB. Levyvarmistus on toteutettu RAID-1-tasoisena. Tätä levyjärjestelmää käytetään ensisijaisena varmuuskopiosijaintina. Lisäksi varmuuskopiointeja varten tiedot tallennetaan kahteen verkkokovalevyyn vuoroviikoin sekä perinteisenä nauhavarmistuksena nauhojen kierrolla.

4.2 Ohjelmisto

Virtualisointiohjelmistona käytetään VMWaren Vsphere 4.1 Essentials -ohjelmistoa, jonka toimitti Moonsoft Oy. Tiedon varmistukseen käytetään Veeam Backup & Replication 5.0 -ohjelmistoa, jonka toimitti IT-voimala Oy. Molempiin ohjelmistoihin ostettiin lisäksi erillinen ylläpitosopimus, jolla varmistetaan ohjelmistojen päivittäminen uusimpiin versioihin sekä tukipalvelu mahdollisten ongelmatilanteiden selvitystä varten.

5 Asennus ja käyttöönotto

5.1 ESXi-päivitys

Järjestelmän päivitys aloitettiin päivittämällä ensin vanha ESXi 3. Palvelimelta sammutettiin kaikki virtuaalikoneet ja asetettiin palvelin huoltotilaan. Asennus pyrittiin ensin suorittamaan päivityksenä, mutta päivitysvaiheessa ohjelmaa ei pystytty asentamaan, vaan se pysähtyi virheeseen. Asennuksessa saatu virheilmoitus oli seuraavanlainen: ”patching this host is not supported by utility”. Käytännössä tämä tarkoitti sitä, että ohjelmistoa ei pystytä päivittämään, vaan oli tehtävä täysin uusi asennus.

5.2 ESXi-asennus

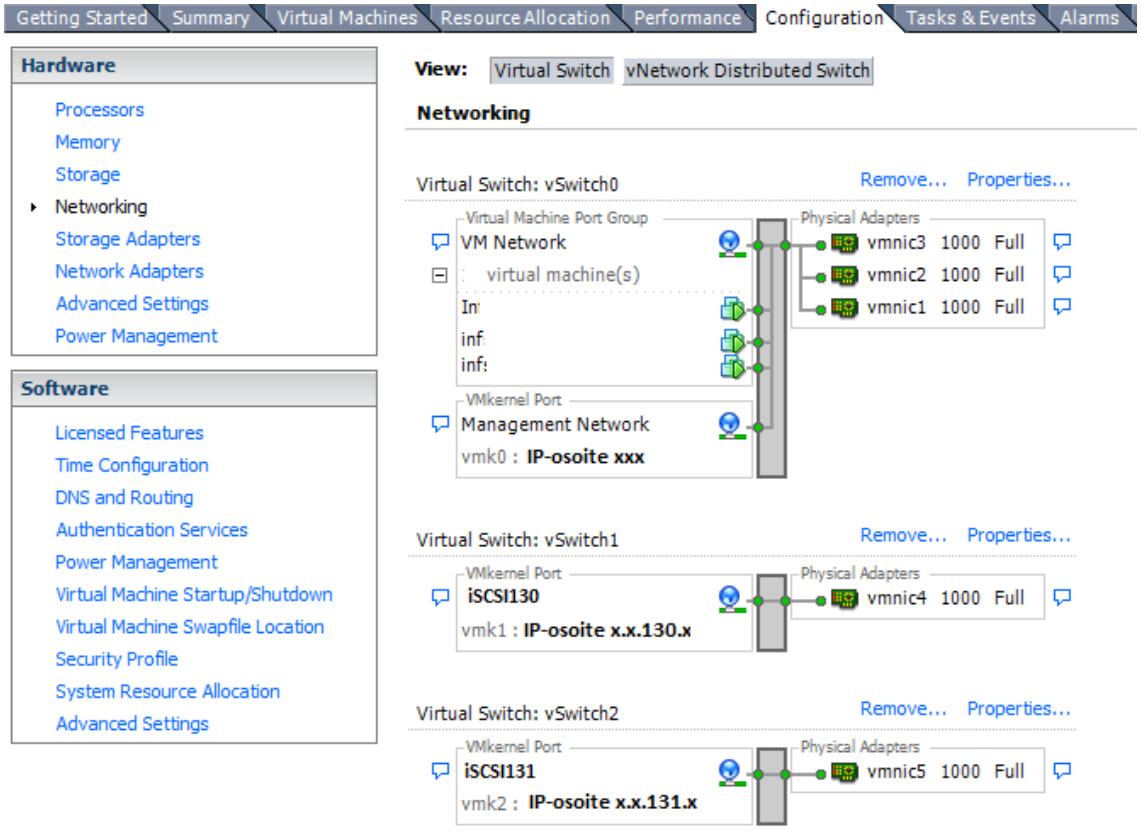
Uusi asennus oli hyvin suoraviivainen. Asennuksessa valittiin uuden asennuksen sijainniksi RAID-1-tasoinen paikallinen kovalevy. Asennuksen alussa hyväksytään ohjelmiston käyttöoikeussopimus, ja tämän jälkeen asennus sujuu automaattisesti. Ensimmäisen käynnistyksen jälkeen asetetaan palvelimen perustiedot. Näitä tietoja ovat salasana, palvelimen nimi, IP-osoite ja DNS. DNS on toimialueen nimipalvelin, jonka tehtävä on ylläpitää toimialueeseen kuuluvien laitteiden nimet ja niiden IP-osoitteet. Yksi näistä Ethernet-porteista määriteltiin varatuiksi palvelimen hallintaa varten. Toinen palvelin asennettiin vastaavalla tavalla.

5.3 ESXi-asetukset

Asetuksien tekeminen aloitettiin asentamalla ensin vSphere client -ohjelmisto omalle kannettavalle tietokoneelle asennus-cd:ltä. Tämän avulla pystyttiin luomaan yhteys oman kannettavan tietokoneen ja ESXin välille. Konfigurointi aloitettiin ottamalla ensin yhteys ESXi-palvelimeen. Palvelimen asetuksien laatiminen tapahtuu ”Configuration”

-välilehdellä. Tärkeimmät asetukset olivat verkon laatiminen ja levypakkojen käyttöönotto. Suurin epävarmuus liittyi siihen, toimisiko vanha levypakka suoraan ja näkyisivätkö jo aiemmin tehdyt virtuaalikoneet järjestelmässä.

Verkon asettelu aloitetaan luomalla virtuaalinen kytkin (vSwitch). Virtuaalisen kytkimen asetuksissa asetellaan ensin virtuaalikoneiden verkkokortit yhdeksi ryhmäksi ja tarvittaessa voidaan asetella käytettävä VLAN-tunniste. Tämän jälkeen lisätään kaksi verkkokorttia, jotka asetellaan VMkernel-tilaan. Näiden verkkokorttien tehtävänä on huolehtia iSCSI-liikenteestä. Tässä tapauksessa näille verkkokorteille annettiin lisäksi oma VLAN-tunnus, jolla erotetaan iSCSI-liikenne muusta verkkoliikenteestä. Verkkoliityntä näkyy kuvassa 4. Verkkoliikenteen pakettien kokoa (MTU) ei pystynyt muuttamaan suoraan käyttöliittymästä. Tämä muutos tehtiin erillisellä VMwaren vMA ohjelmalla, jolla pystyttiin muuttamaan vSwitch1 ja vSwitch2 verkkoliikenteen pakettien (MTU) koko arvoon 9000. Tästä käytetään nimitystä jumbo frame ja tällä saadaan parannettua tiedonsiirron hyötysuhdetta iSCSI-verkossa.



Kuva 4. Verkkokorttien asettelu.

Tallennuslaitteiden asetuksissa määriteltiin adapteriksi ohjelmallinen iSCSI-adapteri. Adapterille annettiin yksilöllinen nimi, jonka perusteella adapteri yksilöidään. Tästä käytetään nimitystä World Wide Name identifier (WWN). Tämän jälkeen aseteltiin kaikkien iSCSI-laitteiden IP-osoitteet ja niiden käyttäjätunnukset. Tätä ennen iSCSI-tallennuslaitteille oli määriteltävä käyttäjätunnus, salasanat ja sallitut osoitteet, joista yhteys voidaan muodostaa. Tämä aiheutti alkuun ongelman, koska PowerVault hyväksyi vain 31 merkkiä pitkät WWN-nimet. Ongelmatilanne korjaantui lyhentämällä tuota nimeä. Kaikki virtuaalikoneet löytyivät ja ne lisättiin ESXin virtuaalikone-hakemistoon. Virtuaalikoneet lisättiin automaattisen käynnistyksen piiriin, jolloin ne käynnistyvät automaattisesti mahdollisten virtakatkojen jälkeen.

5.4 vCenter-asennus

Asennus aloitettiin luomalla ensin virtuaalikone ESXi-palvelimeen. Virtuaalikoneelle määriteltiin resurssit, kuten prosessorien lukumäärä, kovalevy sekä muistin määrä ja aseteltiin CD-aseman sijainniksi oman kannettavan tietokoneen CD-asema. Lisäksi määriteltiin, että asennus tulee olemaan Microsoft Windows Server 2008 R2 -käyttöjärjestelmä.

Microsoft Windows Server 2008 R2 -käyttöjärjestelmän asennuksessa valittiin käyttöjärjestelmäksi sen 64-bittinen standard-versio. Palvelin nimettiin ja liitettiin yrityksen aktiivihakemistoon (AD). Aktiivihakemisto on Windows-verkon käyttäjätietokanta ja hakemistopalvelu. Aktiivihakemisto ylläpitää käyttäjien, laitteiden ja resurssien luetteloa. Lisäksi ohjelmiston vaatimuksena oli kiinteä IP-osoite ja .Net Frameworkin asennus. Verkkokortin ominaisuuksista aseteltiin IP-osoite kiinteäksi ja määriteltiin DNS-osoite. Microsoft .Net Frameworkin asennus tapahtui palvelimen hallintakonsolista valitsemalla lisää piirre toiminnolla.

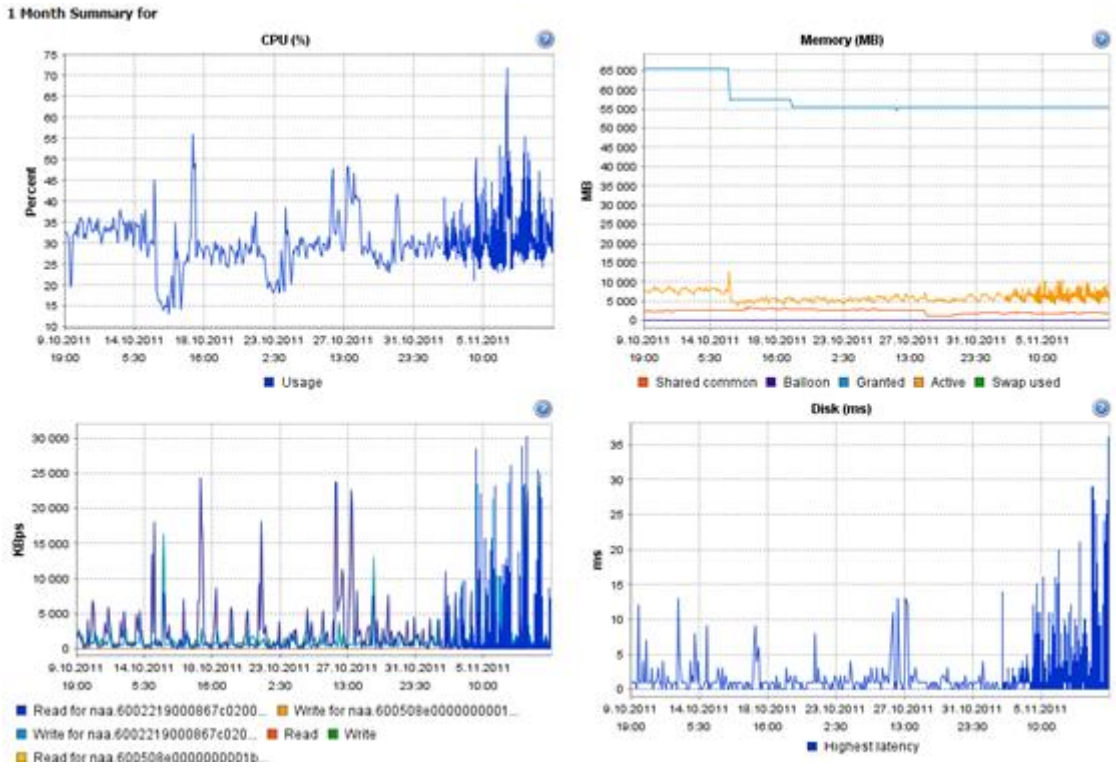
Tämän jälkeen palvelimelle asennettiin vCenter-ohjelmisto. Asennuksen alussa annettiin yrityksen tiedot sekä lisenssiavain. Tietokannaksi valittiin ohjelmiston mukana tuleva Microsoft SQL Server 2005 Express Edition. Valinta perustui siihen oletukseen, että käytettävien virtuaalikoneiden lukumäärä tulee pysymään alle 50 kappaleena. Asennustavaksi valittiin paikallinen asennus. Seuraavaksi määriteltiin käytettävät porttinumerot erilaisille verkkoprotokollille. Lopuksi valittiin, että koneiden lukumäärä tässä datakeskusympäristössä tulee jäämään alle 100 kappaleeseen.

5.5 vCenter-asetukset

vCenterissä luotiin ensin datakeskus, johon molemmat palvelimet yhdistettiin. Resurssien jakoa varten luotiin omat resurssivarannot, joihin virtuaalikoneet sijoitettiin. Tällä varmistetaan, että kriittiset sovellukset saavat palvelinresursseja aina riittävästi. Aikaisemmin huomattiin, että tietty virtuaalikone saattoi ajan kuluessa varata palvelimesta liikaa resursseja ja se häiritsi palvelimen toimintaa. Lisäksi laadittiin omat käyttöoikeusryhmät eri osastojen toimintoja varten. Tämä käyttöoikeusryhmittely tarvittiin siksi, että pystyttäisiin tekemään tarvittaessa testiympäristöjä ohjelmiston testaukseen ilman, että tuotantoympäristö vaarantuisi missään tilanteessa tai että käyttäjä voisi vahingossa poistaa mitään, mihin hänen oikeutensa eivät riittäisi. Tämän jälkeen annettiin datakeskuksen käyttöoikeus tietyille käyttäjäryhmille tietyin valtuuksin.

vCenter-ohjelmassa pystytään laatimaan hälytysrajoja tietyistä tapahtumista, ja siellä on jo valmiiksi ohjelmoituja yleisiä hälytyksiä. Tämä on erityisen kätevää mahdollisten ongelmatilanteiden ennaltaehkäisemiseksi. Hälytyksen sattuessa ohjelma lähettää sähköpostilla kyseisen hälytyksen tiedot halutuille vastaanottajille. Ohjelmassa voi myös laatia ajastettuja tehtäviä, joilla pystyy esimerkiksi säätämään virtuaalikoneen resursseja ajastetusti tai sammuttamaan palvelimen työpäivän päätteeksi ja käynnistämään sen aamulla uudestaan.

Virtuaalipalvelimien resursseja pystytään helposti seuraamaan lähes reaaliaikaisesta tiedosta pidempiaikaiseen tietoon. Tällöin pystytään helposti havainnoimaan, miten järjestelmiin tehdyt muutokset vaikuttavat palvelimen suorituskykyyn. Tarkasteltavia kohteita ovat prosessori, muisti, levyjärjestelmä ja verkko. Raporteissa pystytään tarkastelemaan kohteita mitattavana suureena tai prosentuaalisena arvona. Kuvassa 5 näkyy palvelimen resurssien käyttöä yhden kuukauden ajalta. Nämä tiedot pystytään viemään myös Excel-raporteiksi mahdollista jatkojalustusta varten.



Kuva 5. Resurssien käytön seuranta.

5.6 ESXi-palvelimien asetuksien tallennus

Palvelimien asetuksista otettiin oma varmuuskopio. Varmuuskopiointi suoritettiin vCLI-komentokehotteella: ”vicfg-cfgbackup.pl --server [palvelimen IP-osoite] --portnumber 443 --protocol HTTPS --username [käyttäjätunnus] --password [salasana] -s E:\BU\ESXibu.bak”. Tällöin kaikki tiedot tallennettiin ulkoiselle USB-muistitikulle. Mikäli palvelimen omat kovalevyt vioittuvat, niin ESXin asetukset pystytään palauttamaan luodusta varmuuskopiosta.

5.7 Synologyn levyjärjestelmien käyttöönotto

Synologyn levyjärjestelmät toimitettiin ilman kovalevyjä. Kovalevyiksi valittiin Western Digitalin SATA-kovalevyt Enterprise-tasoisina, millä tarkoitetaan yrityskäyttöön suunniteltuja kovalevyjä. Kovalevyt asennettiin levyjärjestelmiin ohjeen mukaisesti. Laitteet kytkettiin verkkoon, josta ne saivat IP-osoitteet DHCP:ltä. Levypakkojen saapuessa molempien levypakkojen käyttöjärjestelmistä löytyi jo uudemmat käyttöjärjestelmäversiot. Käyttöjärjestelmät päivitettiin levypakkojen mukana tulevalla

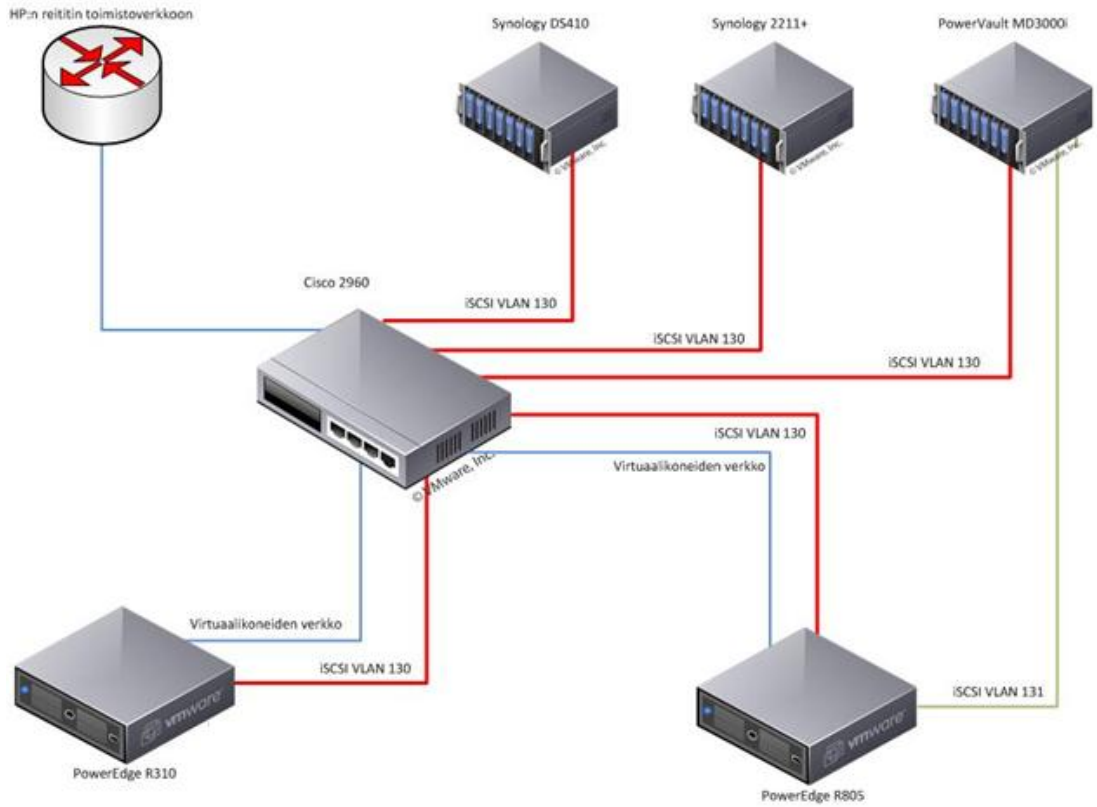
Synology Assistant -ohjelmalla. Päivitystä varten Synologyn kotisivuilta haettiin uusin käyttöjärjestelmän versio.

Laitteiston asettelu tapahtuu selainpohjaisella käyttöliittymällä. Aluksi määriteltiin yleiset ominaisuudet, kuten kiinteät IP-osoitteet ja SNMP-palvelimen osoite sekä aktivoitiin sähköpostihälytykset ja määriteltiin virranhallinta. iSCSI-liityntää varten määritettiin uusi iSCSI-kohde. iSCSI-kohteen tehtävänä on odottaa, että iSCSI-käynnistäjä ottaisi siihen yhteyttä ja pyytäisi siltä tietoja. Tämän jälkeen määriteltiin WWN-nimi ja käyttäjätunnukset. Sitten luotiin uusi LUN (Logical Unit Number), joka on looginen levyalueen yksilöllinen numero, jolla laite näkyy toisille laitteille. Tallennusmuodoksi määriteltiin lohkotyyppinen tallennus. Kovalevyjen RAID-tasoiksi määriteltiin RAID-5 ja RAID-1, jonka jälkeen kovalevyt alustettiin.

5.8 Cisco-kytkimen asennus

Kytkimen asettelu tapahtuu joko merkkipohjaisesti Telnet-ohjelmalla tai graafisella Cisco Network Assistant -ohjelmalla. Työssä kytkin aseteltiin merkkipohjaisesti Telnet-ohjelmalla. Kytkimessä määriteltiin virtuaalikoneiden liityntää varten Link Aggregation Control Protocol (LACP), jonka avulla pystytään yhdistämään useita portteja vikasietoisuuden tai nopeuden kasvattamiseksi. Virtuaalikoneille menevät portit määriteltiin trunk-porteiksi. Trunk-portilla tarkoitetaan porttia, johon kaikkien VLAN-sanomien tiedot välitetään.

Levypakoille menevä iSCSI-liikenne laitettiin omaan VLANiin, jotta se ei häiritse muuta verkkoliikennettä. Lisäksi verkkoliikenteen pakettien kokoa (MTU) muutettiin arvoon 9000. Ciscon 2960-kytkin ei tukenut porttikohtaista määritystä tälle asetukselle, vaan asettelu piti tehdä kaikille porteille käyttäen määritystä ”system mtu jumbo 9000”. Tämä määrittely estää kaikkien 10/100-megabittisten verkkolaitteiden käytön kytkimessä. Toimilaitteet kytkettiin verkkoon kuvan 6 mukaisesti. PowerVault-tallentimen toinen kanava kytkettiin suoraan R805-palvelimelle, jolla kasvatettiin järjestelmän vikasietoisuutta sekä tiedonsiirron kaistanleveyttä.



Kuva 6. Ethernet-verkon kytkentä.

6 Varmuuskopiointi ja tiedonvarmistus

6.1 Veeam Backup & Replication 5.0

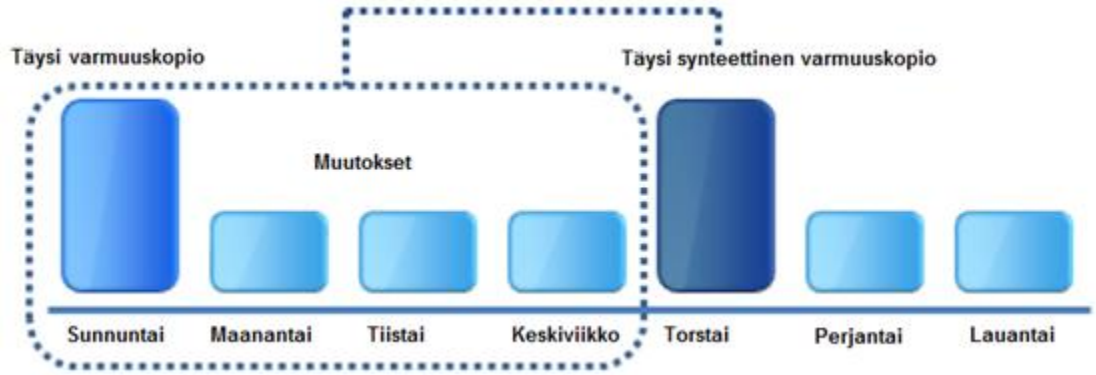
Tiedon varmuuskopiointiohjelmistoksi valittiin Veeam Softwaren toimittama Veeam Backup & Replication 5.0. Tässä työssä en kuvaa ohjelmiston valintaperusteita tarkemmin. Ohjelmistolla on kuitenkin kolme arvokasta piirrettä, joiden takia se lopulta valittiin. Nämä ovat varmuuskopiosta yksittäisen tiedon palautus, varmuuskopion toimivuuden testaus ja varmuuskopioidun palvelimen välitön käynnistys varmuuskopiosta.

Varmuuskopiointitapoja ohjelmassa on kaksi erilaista. Ensimmäinen tapa on Reversed incremental backup, jolloin ensin luodaan täysi varmuuskopio virtuaalikoneesta ja tämän jälkeen kaikki seuraavat varmuuskopiot sisältävät vain virtuaalikoneen muuttuneet tiedot. Varmuuskopioinnin yhteydessä muuttuneet tiedot yhdistetään alkuperäiseen täyteen varmuuskopioon, jolloin käytössä oleva varmuuskopio on aina ajan tasalla. Kuva 7 hahmottaa tätä varmuuskopiointitapaa. Aikaisempaan ajankohtaan

palaaminen on mahdollista, koska ohjelma osaa poistaa muutokset luodusta varmuuskopiosta. Tätä tapaa suositellaan käytettäväksi, kun tallennuslaitteena käytetään kiintolevypohjaista varmuuskopiointiratkaisua. (8, s. 11.)

Kuva 7. Reversed incremental backup (8, s. 11).

Toinen tapa on Incremental backup, joka luo ensin täyden varmuuskopion virtuaalikoneesta ja seuraavat varmuuskopiot sisältävät muuttuneet tiedot. Ohjelma luo tarvittaessa täyden varmuuskopion yhdistelemällä nämä varmuuskopiot, mistä käytetään termiä täysin synteettinen varmuuskopio. Kuva 8 hahmottaa tätä varmuuskopiointitapaa. Tämän tavan etuna on se, että se ei kuormita lainkaan ESXi-palvelinta, koska yhdistely tapahtuu ohjelmallisesti. Tätä tallennustapaa suositellaan käytettäväksi nauhavarmistuslaitteiden kanssa. (8, s. 11-12.)



Kuva 8. Incremental backup (8, s. 11).

Varmuuskopio-ohjelmassa on myös mahdollista luoda aina täysi varmuuskopio virtuaalikoneista. Menetelmän haittapuolena on kuitenkin se, että tämän suorittamiseksi tarvitaan monin verroin enemmän aikaa sekä tallennustilaa. (8, s. 13.)

Ohjelmisto tukee myös Microsoftin Volume Shadow Copy Service (VSS) -palvelua. Tällä varmistetaan se, että jatkuvasti kirjoittavat kriittiset sovellukset, kuten SQL-server ja AD saadaan luotettavasti varmistettua. VSS-palvelu kertoo varmuuskopioitavalle virtuaalikoneelle, että sen pitää tallentaa kaikki kesken olevat I/O-toimet välittömästi ja tällöin käyttöjärjestelmä luo virtuaalikoneesta snapshotin. Mikäli näin ei tehtäisi, niin esimerkiksi SQL-serverin tapahtumatiedoston (Transaction Log) suoritus voisi olla kesken siten, että varsinainen tietokanta saattaisi korruptoitua. (8, s. 23.)

Varmuuskopioita varten virtuaalikoneen tiedot voidaan hakea käyttäen kolmea erilaista toimintatapaa. Ensimmäinen tapa on suora SAN-yhteys (Direct SAN). SAN-yhteyden käyttäminen on mahdollista vain, jos varmuuskopio-ohjelmistoa ajava palvelin on kytketty suoraan iSCSI- tai kuitukanavatallennusverkkoon. Tällöin tieto kopioidaan suoraan tallennusverkosta. Menetelmällä saavutetaan suurin siirtonopeus, mutta vastaavasti se kuormittaa paljon verkkoa. Toinen tapa on hakea tiedot verkkosiirrolla (Network). Tällöin varmuuskopio haetaan ESX-palvelimesta käyttäen verkkoliityntää ja Network Block Device (NBD) -protokollaa, joka siirtää tiedon lohkotasolla palvelimesta. Kolmas tapa on virtuaalinen sovellus (Virtual Appliance), ja tätä voidaan käyttää vain, jos Backup & Replication 5.0 -ohjelma on asennettu virtuaalikoneelle. Tällöin ohjelma lisää varmuuskopioitavan tietokoneen kovalevyn kuvan suoraan omaan virtuaalikoneeseensa ja luo siitä varmuuskopion. Ohjelma pystyy lisäksi salaamaan kaiken tiedon, joka siirretään verkon ylitse. (8, s. 16-17.)

Varmuuskopiointi nopeutuu asettamalla changed block tracking (CBT) -seuranta toimintaan. Tämä tarkoittaa sitä, että vSphere-palvelin ylläpitää tietoa siitä, mitkä tietolohkot ovat muuttuneet tallennuslaitteessa sitten edellisen varmuuskopion. Tämä nopeuttaa paljon varmuuskopion luomista, koska tällöin vain muuttuneet tiedot siirretään. (8, s. 24.)

6.2 Veeam Backup & Replication 5.0 -asennus

Veeam Backup & Replication 5.0 -ohjelmiston asennus tapahtui asennusohjeen mukaisesti samalle palvelimelle, jolle vCenter-ohjelmisto asennettiin. Asennusvaiheessa valittiin aikaisemmin asennettu SQL-Server ohjelmiston tietokannaksi. Sähköpostin

lähetystä varten määriteltiin käytettävä postipalvelin ja osoitteet, joihin mahdolliset hälytykset lähetettäisiin.

6.3 Varmuuskopiointi asetukset

Ohjelmiston asennuksen jälkeen aseteltiin vCenter-palvelimen tiedot, jotta ohjelma pystyy kytkeytymään virtuaalikoneisiin. Tämän jälkeen laadittiin jokaiselle virtuaalikoneelle oma varmuuskopiointiaikataulu ja määriteltiin varmuuskopioasetukset. Varmuuskopiointitavan valinnan jälkeen lisättiin haluttu palvelin varmuuskopioitavaksi ja määriteltiin ajankohta, milloin varmuuskopiointi suoritetaan. Ohjelmaan määritetään lisäksi varmuuskopioitavien koneiden palautuspisteiden lukumäärä. Palvelimien varmistus toteutetaan automaattisesti öisin, viikoittain ja kuukausittain. Päivittäiset varmistukset tallennetaan Synologyn 2211+ -levyjärjestelmään ja viikoittaiset varmistukset tehdään kahdelle NAS-verkkokovalevylle. Varmuuskopioajastukset on kuvattu liitteessä 1. Tämän lisäksi järjestelmästä otetaan nauhavarmistuksella erilliset varmuuskopiot, jotka säilytetään erillisessä paloturvallisessa tilassa.

6.4 Varmuuskopion testaus

Varmuuskopioiden testausta varten luodaan oma virtuaalinen testilaboratorio Veeam Backup & Replication 5.0 -ohjelmalla, jossa niiden testaus tapahtuu. Laboratorion luonnissa määritetään ensin ESX- tai ESXi-palvelin, joilla testaus suoritetaan. Tämän jälkeen annetaan käytettävä levyjärjestelmä ja luodaan välityspalvelin, jonka tehtävänä on ottaa yhteys testattavaan virtuaalikoneeseen. Verkon määrityksessä valitaan joko perus- tai kehittyneet asetukset. Kehittyneiden verkkotoimintojen käyttöä tarvitaan vain, jos testattavan virtuaalikoneen täytyy ottaa yhteyttä johonkin muuhun toimivaan palvelimeen testauksen suorittamiseksi.

Seuraavaksi laaditaan testausrutiini, jossa määritellään testattava varmuuskopio. Tämän jälkeen voidaan valita valmiista testausrutiineista testattavat toimenpiteet. Oletuksena on, että koneen käynnistys ja verkkoyhteys tarkistetaan. Lisäksi suoritetaan lisätestauksia, joita ovat muun muassa DNS-, posti- ja SQL-palvelintestaus. Tällöin ohjelma automaattisesti yrittää avata TCP/IP-portin (Transmission Control Protocol / Internet Protocol) ja lähettää paketin sille käytettävälle palvelulle, jota testataan. Tällä tavalla ohjelma tarkastaa, että kyseiset palvelut ovat toiminnassa. TCP/IP on verkkoliikenteessä käytettävä protokolla. Testaustoimintoja pystyy myös itse laatimaan.

Tarvittaessa voidaan käyttää Windowsin PowerShell-komentoja, mutta tällöin ne pitää tehdä varmuuskopioitavaan koneeseen jo valmiiksi. Testauksen suorituksesta voidaan lähettää erillinen sähköpostikuittaus tai SNMP-viesti valvontapalvelimelle. SNMP on verkonhallintaan tarkoitettu protokolla. Lopuksi määritellään testauksen suoritusaikataulu. Tarvittaessa voidaan määrittää, että testattava virtuaalikone jätetään toimintakuntoiseksi, jolloin testaaja käy suorittamassa manuaalisen testin ja lopettaa virtuaalikoneen testauksen.

7 Yhteenveto

7.1 Ongelmat

Työn aikana esiintyi muutama ongelma. Ensimmäinen ongelma liittyi levyjärjestelmän WWN-nimen pituuden käsittelyyn, kun palvelin ei saanut yhteyttä levyjärjestelmään. Ongelma selvisi VMwaren kotisivuilta, koska itse levyjärjestelmä ei antanut mitään virheilmoitusta. WWN-nimen pituus ei saanut ylittää 31 merkkiä. Kun nimi lyhennettiin 31-merkkiseksi, yhteys muodostui välittömästi.

Toinen ongelma tuli esiin siinä vaiheessa, kun levyjärjestelmä lopetti yhteydenpidon palvelimen kanssa. Tämä pysäytti tuotannossa olevat palvelimet välittömästi. Ongelma liittyi palvelimen verkkoasetuksiin. Olin valinnut liikennöintitavaksi Most Recently Used (MRU) -protokollan, jota normaalisti käytetään toimilaitteissa, jotka kytketään tilaan aktiivinen/passiivinen. Tämä tarkoittaa sitä, että toinen verkkokanava on aktiivinen, kunnes se vioittuu, jolloin vaihdetaan toissijaiseen verkkokanavaan. Ensimmäisen aktiivisen kanavan vioituttua se ei enää automaattisesti yritä palauttaa yhteyttä, vaan se täytyy käydä manuaalisesti aktivoimassa.

Vikatilanne aktivoitui siitä syystä, että olin aikaisemmin testannut sitä, miten järjestelmä toimii, kun toinen kommunikointikanava irrotetaan järjestelmästä. Tällöin yhteys oli siirtynyt passiiviselle kulkureitille, joka kulki kytkimen läpi. Yön aikana oli ollut sähkökatko, jolloin kytkimen UPS (Uninterruptible Power Supply) ei ollut pitänyt sitä jännitteellisenä riittävän pitkää aikaa ja kytkin oli sammunut. UPSin tehtävänä on ylläpitää käyttöjännitettä lyhyiden virtakatkojen aikana. Palvelimen ja levyjärjestelmän UPS oli riittänyt pitämään ne toiminnassa siihen saakka, että sähköt palautuivat. Verkkopolku tallennuslaitteelle oli kuitenkin jo vioittunut, eikä mitään tietoa enää

kulkenut levyjärjestelmän ja palvelimen välillä. Tämä ilmeisesti liittyy siihen, että yhteyden alussa annetaan tunnistamistiedot eikä palvelin osannut antaa tätä enää uudestaan. Palvelimen asetuksia muutettiin tämän seurauksena siten, että uusi yhteystapa on Round Robin. Tämä tarkoittaa sitä, että palvelin vuorottelee käytettävien yhteyskanavien välillä.

Kolmas ongelma liittyi käyttäjän virheeseen. Käyttäjälle oli annettu liian suuret oikeudet, ja hän tuhosi vahingossa Synology 411 -levypakan. Levypakalla oli ainoastaan testikoneita, joten ongelma ei aiheuttanut korvaamatonta vahinkoa. Levypakan saaminen taas toimintakuntoon vei muutaman viikon, sillä kiintolevyn osiointi (partition) oli tuhoutunut ja sen korjaus voitiin tehdä ESXi-palvelimen tech support -tilassa. Kuvassa 9 on esitetty komennot, jotka suoritettiin osioinnin korjaamiseksi. Osioinnin korjauksen jälkeen kaikki virtuaalikoneet toimivat normaalisti.

```
~ # fdisk /dev/disks/naa.6001405d77abd1ed7afbd3298da568dc
The number of cylinders for this disk is set to 81458.
There is nothing wrong with that, but this is larger than 1024,
and could in certain setups cause problems with:
1) software that runs at boot time (e.g., old versions of LILO)
2) booting and partitioning software from other OSs
   (e.g., DOS FDISK, OS/2 FDISK)
 Command (m for help): n
Command action
   e   extended
   p   primary partition (1-4)
p
Partition number (1-4): 1
First cylinder (1-81458, default 1): Using default value 1
Last cylinder or +size or +sizeM or +sizeK (1-81458, default 81458): Using default value 81458
 Command (m for help): t
Selected partition 1
Hex code (type L to list codes): fb
Changed system type of partition 1 to fb (VMFS)
 Command (m for help): x
 Expert command (m for help): b
Partition number (1-4): 1
New beginning of data (63-1308622769, default 63): 128
 Expert command (m for help): w
The partition table has been altered!
```

Kuva 9. Osioinnin korjaus.

Neljäs ongelma oli kovalevyn hajoaminen Dell PowerVaultissa. Levyjärjestelmä toimi RAID-10-tilassa, joten yhden levyn rikkoontuminen ei aiheuttanut tuotannolle mitään ongelmia. Dell toimitti uuden kovalevyn seuraavana päivänä, ja sen paikalleen laiton jälkeen levypakka kopioi automaattisesti toimivalta levyltä tiedot siihen ja järjestelmä toimi taas RAID-10-tilassa.

7.2 Saavutetut tavoitteet

Palvelinkeskuksen käytettävyys tuotantoympäristössä on osoittautunut erittäin hyväksi. Nyt jo lähes vuoden tuotantokäytössä olleessa ympäristössä on ollut yksi kriittinen vikatilanne, joka on kuvattu kohdassa 7 (Ongelmat). Virtualisoitujen palvelimien päivitys käynnistyi kesällä 2011 ja vSphere-ympäristön mahdollistama palvelimien kopiointiominaisuus nopeutti uusien palvelimien käyttöönottoa. Automaattisesti toimivat varmuuskopioinnit varmistavat yrityksen jatkuvuuden kannalta tärkeät tiedot, mikäli datakeskus joskus kärsisi vakavasta ongelmasta. Lisäksi palvelinkeskuksen virheiden ja mahdollisten ongelmatilanteiden automaattiset hälytykset antavat reaaliaikaista kuvaa sen tilasta. Ohjelmistotestauksen kannalta virtualisoitu ratkaisu on ollut hyvin toimiva. Uudet testikoneet syntyvät minuuteissa aikaisemmin valmiiksi luoduista pohjista (template). Tämän työn seurauksena vanhat testipalvelimet poistettiin testauskäytöstä.

Edistyneempiä palveluita, kuten korkean käytettävyyden (HA) ja kuorman automaattista tasausta (DRS), en työssä päässyt tutkimaan. Nämä ovat ohjelmiston lisäominaisuuksia, jotka eivät kuuluneet työssä käytetyn ohjelmistolisenssin piiriin.

Jatkokehityskohteena näkisin varmuuskopioiden testauksen edelleen kehittämisen. Tällöin ehkä pystyttäisiin varmistamaan se, että kaikkien varmuuskopioitujen virtuaalikoneiden sovellusohjelmat toimisivat suunnitellusti, jos niitä jouduttaisiin vikatilanteen takia ottamaan tuotantokäyttöön.

Lähteet

1 David Rule & Rogier Ditter, 2007. The Best Damn Server Virtualization Book Period. Syngress Publishing Inc.

2 Historia VMware. <http://www.vmware.com/virtualization/history.html>. Luettu 10.9.2011

3 Bernard Golden, 2007. Virtualization For Dummies. Wiley Publishing, Inc.

4 Gartner-raportti x86-palvelinten virtualisoinnista Q2 2011 <http://www.gartner.com/technology/media-products/reprints/microsoft/vol2/article8a/article8a.html>. Luettu 23.10.2011

5 2010 VMware, Inc . VMware vSphere 4.1:Install, Configure, Manage ESX 4.1, ESXi 4.1, and vCenter Server 4.1. Student Manual — Volume I Revision A.

6 Understanding full virtualization, paravirtualization and hardware assist. <http://www.vmware.com/files/pdf/VMware_paravirtualization.pdf>. Luettu 29.10.2011

7 Scott Lowe, Jason W. McCarty & Matthew K. Johnson. 2010. VMware vSphere 4 Administration instant reference. Wiley Publishing, Inc.

8 Veeam Backup & Replication 5.0, User Guide. <http://www.veeam.com/files/guide/veeam_backup_5_0_user_guide.pdf>. Luettu 11.11.2011

9 Virtualisoitu palvelinympäristö. <http://capitalhead.com/1146.aspx?VMware>. Luettu 20.11.2011

10 VMware tuotteet.<http://www.vmware.com/products/#productdiagram>. Luettu 20.11.2011

Varmuuskopioinnin ajastusrutiinit