Ilkka Siuruainen

VIRTUAALISEN YMPÄRISTÖN VARMISTAMINEN

Opinnäytetyö
Kajaanin ammattikorkeakoulu
Luonnontieteiden ala
Tietojenkäsittely
22.5.2012

KAJAANIN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ
TIIVISTELMÄ

Koulutusala Luonnontieteiden ala	Koulutusohjelma Tietojenkäsittely
Tekijä(t) Ilkka Siuruainen	
Työn nimi Virtuaalisen ympäristön varmistaminen	
Vaihtoehtoiset ammattiopinnot Järjestelmän ylläpito	Ohjaaja(t) Tarja Karjalainen
	Toimeksiantaja Kajaanin ammattikorkeakoulu
Aika 22.5.2012	Sivumäärä ja liitteet 31

Tämän työn tilaajana oli Kajaanin ammattikorkeakoulu ja opinnäytetyön tavoitteena oli toteuttaa toimiva varmuuskopiointijärjestelmä Kajaanin ammattikorkeakoulun tietojärjestelmälaboratorioon ja vastata kysymyksiin miten toteutetaan varmuuskopiointijärjestelmä ja miten virtuaalisen opetusympäristön varmistus hoidetaan.

Opinnäytetyön käytännön osuus tehtiin Kajaanin ammattikorkeakoulun tietojärjestelmälaboratoriossa. Ensimmäiseksi testattiin miten ohjelman asennus ja käyttöönotto etenee ja tämän jälkeen aloitettiin varmuuskopiointi- ja palautustestit, joilla selvitettiin ohjelman toimintaa käytännössä. Testien jälkeen tehtiin lopullinen asennus tuotantokäyttöön.

Ensimmäinen asennus tehtiin virtualisoituun palvelimeen. Tällä asennuksella testattiin miten virtuaalikoneen varmuuskopiointi ja palautus toimii. Testeissä testattiin myös yksittäisen tiedoston palautusta varmuuskopiosta. Kaikki testit saatiin suoritettua onnistuneesti, vaikkakin pieniä ongelmia ilmeni virtuaalikoneen palautuksen kanssa.

Testien jälkeen varmistusjärjestelmä asennettiin fyysiselle palvelimelle, jossa oli runsaasti resursseja järjestelmän ajamiselle. Ohjelman asennuksen jälkeen ohjelmaan tehtiin tarvittavat säädöt ja palvelin liitettiin verkkolevyyn, jotta kiintolevytila ei lopu kesken. Valmista varmistusjärjestelmää tullaan käyttämään Kajaanin ammattikorkeakoulun tietojärjestelmälaboratorion konesalissa ajettavien virtuaalikoneiden varmentamiseen ja tätä järjestelmää tullaan kehittämään edelleen tulevaisuudessa.

Kieli	Suomi
Asiasanat	virtualisointi, varmuuskopiointi, varmistaminen, virtuaalinen ympäristö, disaster recovery
Säilytyspaikka	☒ Verkkokirjasto Theseus ☒ Kajaanin ammattikorkeakoulun kirjasto

KAJAANIN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

THESIS ABSTRACT

School Business	Degree Programme Business Information Technology
Author(s) Ilkka Siuruainen	
Title Backing Up A Virtualized Environment	
Optional Professional Studies System Administration	Instructor(s) Tarja Karjalainen
	Commissioned by Kajaani University of Applied Sciences
Date 22.5.2012	Total Number of Pages and Appendices 31

The topic of this thesis is backing up a virtualized environment in Kajaani University of Applied Sciences (=KUAS) datacenter. The object of this thesis was to create a backup system for virtual machines running in the KUAS data center.

The practical part of the thesis was conducted in the KUAS data center. First, the installation and the introduction of the backup software was tested. At this stage, tests were run to determine how easy it is to back up and restore virtual machines in different ways. After the tests, the installation for production use was done on a physical server.

The first installation was conducted on a virtual machine and this was used to test how backing up and restoring virtual machines work. Restoring a single file from backup was also tested. All tests were successful, even though there were some small problems with restoring the full virtual machine.

After the tests were run, the backup software was installed on a physical server, which had a lot of resources to run the software. After the installation was done, the server was connected to network storage, so it will not run out of hard drive space and the settings were tweaked to match KUAS needs. The completed backup system will be used to back up virtual machines in the KUAS data center.

Language of Thesis	Finnish
Keywords	virtualization, backup, virtual environment, disaster recovery
Deposited at	☒ Electronic library Theseus ☒ Library of Kajaani University of Applied Sciences

SISÄLLYS

SYMBOLILUETTELO

Disaster-recovery	Katastrofista palautuminen. Palautumisprosessi sisältää palautus-suunnitelman, joka on tehty katastrofien varalle.
Domain	Toimialue, joka yhdistää joukon tietokoneita.
Dublikaatti	Kaksoiskappale, sama tiedosto useassa paikassa.
ESXi	VMware:n kehittämä palvelinkäyttöjärjestelmä virtualisointikäyttöön.
IQN	iSCSI Qualified Name. iSCSI:n tarvitsema osoite. Sisältää tekstin iqn, verkko-osoitteen, päivämäärän sekä tallennustilan nimen, esim. iqn.2001-04.com.example:storage.tape1.sys1.xyz.
IP-osoite	Numerosarja, joka yksilöi jokaisen Internet-verkkoon kytketyn tietokoneen
iSCSI	Internet Small Computer System Interface. Standardi tiedon välittämiseen tietokoneen ja oheislaitteiden välillä. Perustuu SCSI-standardiin.

RAM-muisti	Random Access Memory. Työmuistia, johon käyttöjärjestelmän ohjelmat, suoritettavat sovellukset sekä näiden tarvitsemat tiedot latautuvat. Tyhjenee, kun tietokoneesta katkaistaan virta
Resource Pool	Resurssivaranto. Joukko asetuksia, jotka asettavat rajat ESXi:ssä ajettaville virtuaalikoneille.
Vcenter	VMware:n kehittämä ohjelmisto ESXi-palvelinten keskitettyyn hallintaan.

1 JOHDANTO

Kajaanin ammattikorkeakoululla oli tarve varmentaa tietojärjestelmälaboratoriossa olevat virtuaaliset koneet ja tätä varten ammattikorkeakoulu hankki varmistusjärjestelmän tietojärjestelmälaboratorion konesaliin. Varmistusjärjestelmää käytetään konesalissa ajettavien virtuaalikoneiden varmuuskopiointiin. Projektin aihe oli ajankohtainen, sillä yritykset ovat ottamassa virtualisointia enemmän ja enemmän käyttöön. Ennen tätä opinnäytetyötä, ammattikorkeakoulun opetuskäytössä olevassa konesalissa pyöriviä virtuaalikoneita ei varmuuskopioitu ollenkaan, joten työn lopputulos oli tärkeä, jotta tiedostot saadaan palautettua vahingon sattuessa. Järjestelmä tuli sisältämään vähän erittäin kriittistä ja paljon ei kriittistä dataa.

Projektin tavoitteena oli luoda toimiva varmuuskopiointijärjestelmä, joka tarkistaa virtuaalikoneiden tiedostot ja poistaa täysin identtiset tiedostot ja näin ollen säästää tilaa levyjärjestelmässä. Virtuaalikoneiden tiedostot varmuuskopioidaan talteen päivittäin riippuen virtuaalikoneelle annetusta tärkeysjärjestyksestä. Järjestelmä toimii ammattikorkeakoulun tietojärjestelmälaboratorion konesalissa. Opinnäytetyö tulee vastaamaan seuraaviin kysymyksiin; miten toteutetaan varmuuskopiointijärjestelmä ja miten virtuaalisen opetusympäristön varmistus hoidetaan?

Projekti toteutettiin keväällä 2012 ja projektin aihe rajattiin virtuaalisen ympäristön varmentamiseen ja duplikaattitiedostojen poistoon kyseisessä ympäristössä sekä katastrofista palautumiseen, jossa tutkittiin miten nopeasti järjestelmät saadaan palautettua ylös ja menetetäänkö dataa palvelukatkoksen aikana. Projektin aihe liittyi Kajaanin ammattikorkeakoulun konesali-projektiin. Projektin tarkoituksena oli rakentaa toimiva konesaliympäristö opetusympäristöksi opiskelijoille sekä tuotantoympäristöksi ammattikorkeakoulun palvelimille.

2 VARMUUSKOPIOINTI

Luvussa käsitellään erilaisia menetelmiä tiedostojen ja virtuaalikoneiden varmuuskopiointiin. Käydään läpi eri valmistajien ohjelmistoja sekä otetaan selvää miten katastrofista palautuminen toimii.

2.1 Mitä varmuuskopiointi on?

Varmuuskopiointi on digitaalisen tiedon tallentamista digitaaliselle tallennusmedialle, kuten CD/DVD-levylle, USB-muistitikulle, perinteiselle nauha-asemalle tai verkkokiintolevylle. Tallentaminen voi tapahtua paikallisesti koneella tai verkon yli. Varmuuskopiointia on manuaalista sekä automaattista ajastettua kopiointia. Suurin osa yrityksistä varmuuskopioi tiedot yöllä nauha-asemalle, josta ne voidaan tarvittaessa palauttaa. (Tampereen ammattikorkeakoulu 2011.)

Manuaalinen kopiointi on ylläpitäjän käsin tekemää kopiointia, jota tehdään itse koneella työskennellen. Automaattinen, ajastettu kopiointi taas tapahtuu automaattisesti, esimerkiksi yöaikaan. Ylläpitäjä on määrittänyt asetukset johonkin ohjelmaan, joka sitten hoitaa kopioinnin näiden asetuksien mukaan, ilman että ihminen olisi koneen edessä valvomassa työn etenemistä. (Tampereen ammattikorkeakoulu 2011.)

Tiedostot kannattaa varmuuskopioida, koska tekniikka ei ole aukotonta ja laiterikkoja tapahtuu harva se päivä, aiheuttaen tiedostojen tuhoutumista tai korruptoitumista. Inhimilliset virheet ovat myöskin mahdollisia ja tiedostoja poistetaan vahingossa tai tahallisesti ja näin aiheutetaan vahinkoa kohteelle. Jotta tiedostojen häviämiseltä vältyttäisiin, tiedostot kannattaa varmuuskopioida manuaalisesti. Suurin osa yrityksistä hoitaa varmuuskopioinnin automaattisesti. Toinen syy miksi tiedostot voivat hävitä ovat virukset ja muut haittaohjelmat, jotka voivat olla suunniteltu poistamaan tiedostoja ja näin ollen aiheuttamaan vahinkoa. (PC911 2011.)

Jos tiedostoja ei varmuuskopioitaisi, yrityksille tulisi huomattavia tappioita tärkeiden tiedostojen häviämisen takia, ja joissain tapauksissa tämä voi johtaa jopa konkurssiin. Nykypäivänä suurin osa yrityksistä ja organisaatioista käyttää tietokoneita toimintansa pyörittämiseen ja suurimmalla osalla on tallennettua kriittistä tietoa, jonka pitää säilyä tietokoneella. (TopTenReviews 2011.)

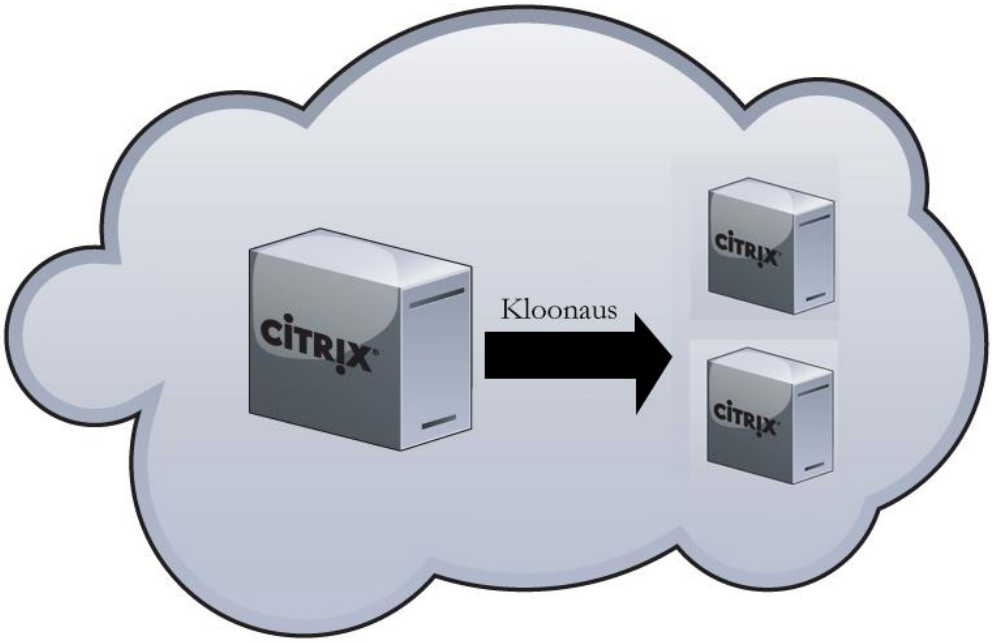
Yksityisen käyttäjän kannattaa varmuuskopioida muutamia erityyppisiä tiedostoja useaan eri paikkaan. Yksityiset käyttäjät kopioivat heille tärkeät tiedostot, kuten valokuvat, Internetselaimen suosikit, pelien tallennukset, musiikkitiedostot ja kaiken muun mikä on tärkeää heille. Yritykset kopioivat yleensä kaiken tiedon mitä heidän kiintolevyillään on nauha-asemille tai verkon yli levyjärjestelmään tai tekevät varmuuskopioita kokonaisista koneista. (PC911 2011.)

2.2 Varmuuskopiointimenetelmät

Varmuuskopiointimenetelmiä on monenlaisia; on kloonausta, tilannevedoksia ja virtuaalikoneiden kohtelua fyysisinä laitteina sekä lähiverkon yli tapahtuvaa varmuuskopiointia (Hess 2008). Opinnäytetyön käytännön osuudessa on käytetty lähiverkon yli tapahtuvaa varmuuskopiointia. Käytännön osuudesta lisää luvussa kolme.

2.2.1 Kloonaus

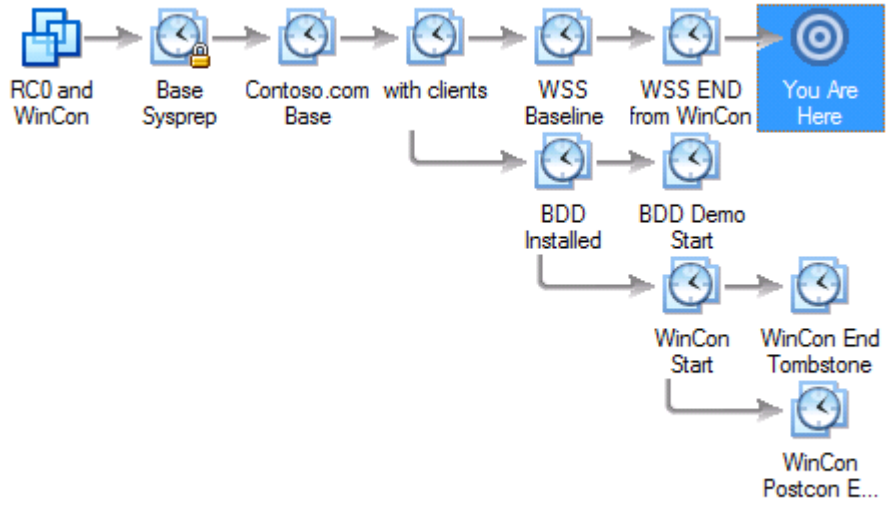
Klooni on täydellinen kopio toimivasta virtuaalikoneesta. Alkuperäistä virtuaalikonetta kutsutaan nimellä ”parent of the clone”. Kuviossa 1 on näytetty, miten kloonaus toimii. Kloonattu virtuaalikone on täysin erillinen virtuaalikone, mutta se voi jakaa virtuaalisen kiintolevyn alkuperäisen virtuaalikoneen kanssa, tästä käytetään nimitystä ”linked clone”. Kyseinen kloonityyppi vaatii isäntävirtuaalikoneen käynnissä olon, muuten kloonattu kone ei lähde käyntiin. Linkitettyjen kloonien hyvänä puolena on nopeus. Linkitetyt kloonit ovat nopeita tehdä, koska virtuaalikoneen kiintolevyä ei tarvitse luoda uudestaan. Täydelliseen kloonaukseen menee enemmän aikaa, koska virtuaalikoneen jokainen osa täytyy kloonata. (VMware 2011 a.)



Kuvio 1. Kloonaus luo kopion alkuperäisestä virtuaalikoneesta (OpenSourceRack, 2010. Mukaillen lähdettä)

2.2.2 Snapshot

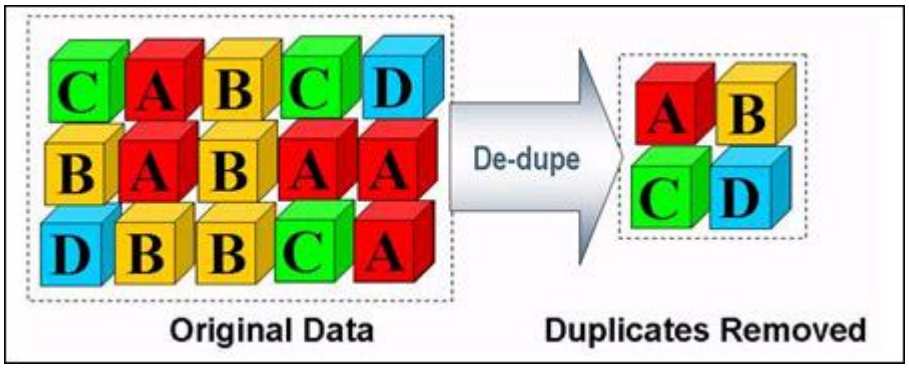
Tilannevedos (snapshot) on kuvaus virtuaalikoneen tilasta snapshotin tekohetkellä ja useasta snapshotista muodostuu lineaarinen polku. Snapshot sisältää virtuaalikoneen kiintolevyn, tilan ja RAM-muistin. Jos jokin menee vikaan virtuaalikoneessa, käyttäjä voi palata snapshotin avulla hetkeen, jolloin virtuaalikone toimi oikein. Kuviossa 2 näkyy snapshottien luoma lineaarinen polku, jonka avulla aikaisempaan vaiheeseen on helppo palata. Snapshot ei kuitenkaan ole 100% vikasietoinen, eikä sitä tule käyttää ainoana varmuuskopiointikeinona, koska snapshot tallennetaan samaan sijaintiin kuin virtuaalikone. Snapshotin voi ottaa silloin kun virtuaalikone on käynnissä, suljettuna tai pysäytetty-tilassa. Snapshot on hyvä ottaa ennen uuden ohjelman tai ajurin asennusta, jos ei ole varma kyseisen asennuksen onnistumisesta. (VirtualizationAdmin 2008.)



Kuvio 2. Kuvaruutukaappaus eri tilanteista otetuista snapshoteista (Cornelius, 2008)

2.2.3 Deduplikointi

Deduplikointi on samanlaista datan pakkaamisen kanssa, mutta deduplikointi tarkistaa isojen tietomäärien tarpeellisuutta. Deduplikoinnissa verrataan bittiryhmiä toisiinsa ja jos löytyy toinen samanlainen ryhmä, ohjelma hylkää datan ja säilyttää vain yhden bittiryhmän kiintolevyllä ja viittaa aina tähän kyseiseen ryhmään. Käyttäjät ja muut ohjelmat eivät näe deduplikointiominaisuutta, vaan kaikki tapahtuu ohjelman sisällä. Kuviossa 3 näkyy, miten tiedon määrää pienennetään karsimalla samanlaiset bittiryhmät pois. (Datadomain, 2011.)



Kuvio 3. Deduplikointi käytännössä (Poelker, 2009)

Deduplikoinnista saatu hyöty tulee parhaiten esille levyjärjestelmän hinnassa. Deduplikoinnilla varmistettu virtuaalikone kuluttaa vähemmän levypintaa kuin perinteisesti täysin varmistettu virtuaalikone mistä johtuen levyjärjestelmään ei tarvitse niin suurta kapasiteettia. Suurissa ympäristöissä tällä voidaan saavuttaa huomattaviakin taloudellisia säästöjä. Myös verkon kuormitus vähenee, kun tiedostoja ei tarvitse varmuuskopioida useaan kertaan, vaan yksi kerta riittää. Palautettavan datan vähentymisen myötä varmuuskopioidun virtuaalikoneen palauttaminen nopeutuu, koska on vähemmän dataa jota palauttaa. (Datadomain, 2011.)

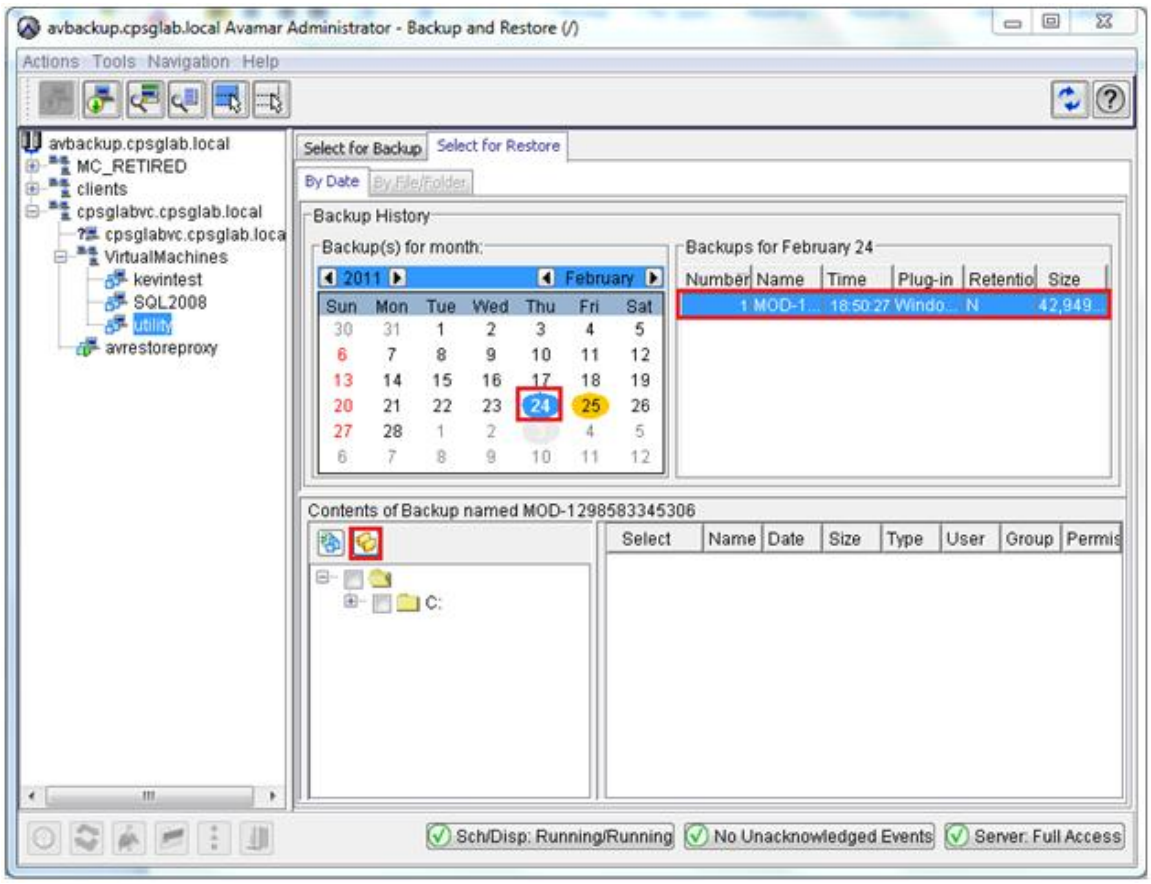
Virtuaalikoneen varmuuskopiointiin on kaksi tapaa. Ensimmäinen tapa varmuuskopioi koko virtuaalikoneen ja luo yhden varmuuskopiotiedoston. Toinen tapa on varmuuskopioida yksittäisiä tiedostoja. Hyvä tapa varmuuskopion luomiseen on luoda täysi perinteinen varmuuskopio virtuaalikoneesta ja tehdä lisääviä (incremental) varmuuskopioita tähän täyteen varmuuskopioon. Lisäävä varmuuskopiointitapa tallentaa vain tehdyt muutokset ja muuttuneet tiedostot. Tämä säästää aikaa ja levytilaa, kun täyttä varmuuskopiota ei tarvitse tehdä joka kerta, kun virtuaalikone varmuuskopioidaan. (Mello Jr., 2009.)

2.3 Varmuuskopiointiohjelmat

Tiedostojen varmuuskopiointiin on useita eri ohjelmistoja eri valmistajilta. Tässä kappaleessa esitellään muutamia yleisesti käytössä olevia tuotteita sekä opinnäytetyön käytännön projektissa käytetty ARCserve Backup -ohjelmisto.

2.3.1 Avamar

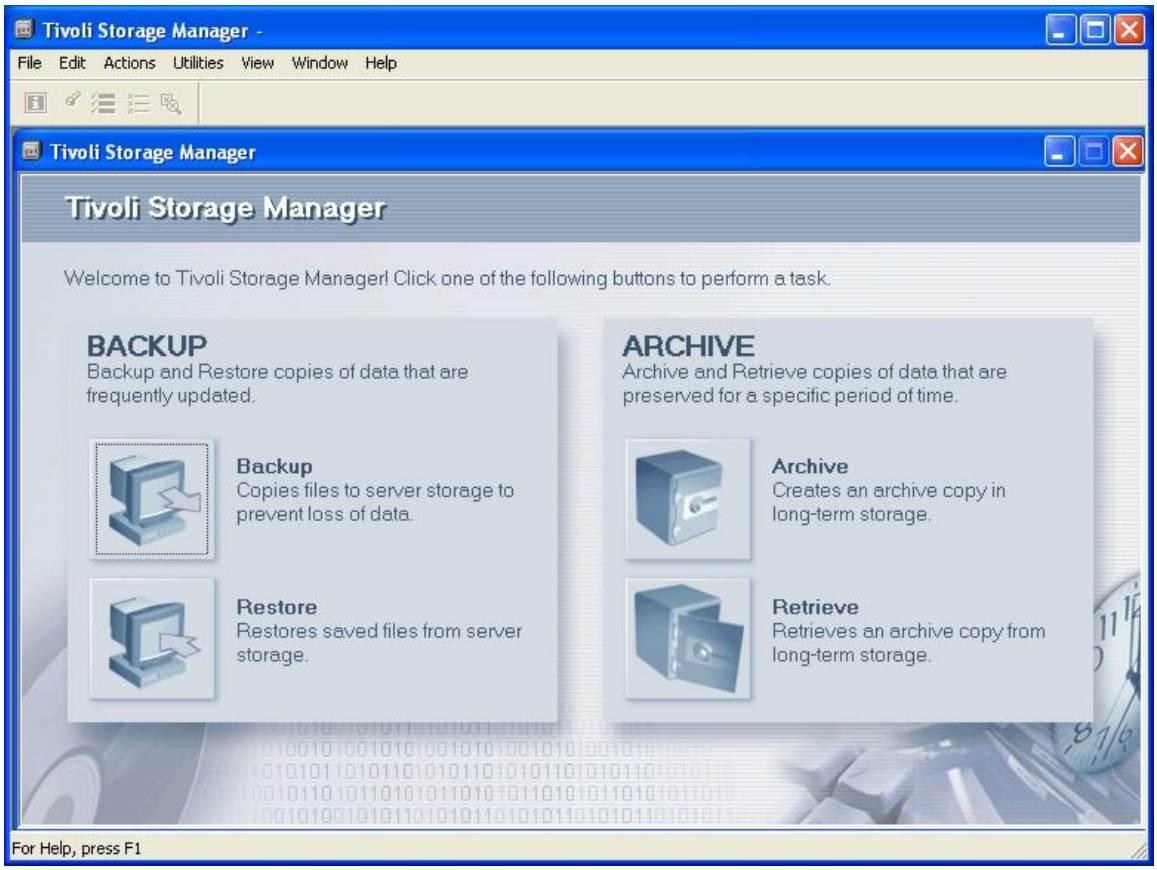
Avamar on EMC:n omistama tuote, joka mahdollistaa tiedostojen, esim. virtuaalikoneiden varmuuskopioinnin VMwaren ESXi-palvelimilta. Kuviossa 4 on esillä Avamarin käyttöliittymää. Avamar sisältää deduplikaatio-ominaisuuden, joka tarkoittaa käytännössä samanlaisten tiedostojen tarkastamisen ja varmuuskopioinnin vain kerran. Deduplikaatio -ominaisuus säästää tilaa levyjärjestelmässä, koska järjestelmä estää identtisten tiedostojen kopioinnin jo palvelimen puolella. Tarpeetonta verkkokuormaakaan ei pääse syntymään, kun tiedostoja kopioidaan levyjärjestelmään tai muuhun varmuuskopiointiin tarkoitettuun mediaan. (EMC 2011.)



Kuvio 4. Kuvaruutukaappaus Avamar-ohjelmasta (Blackburn, 2011.)

2.3.2 Tivoli Storage Manager

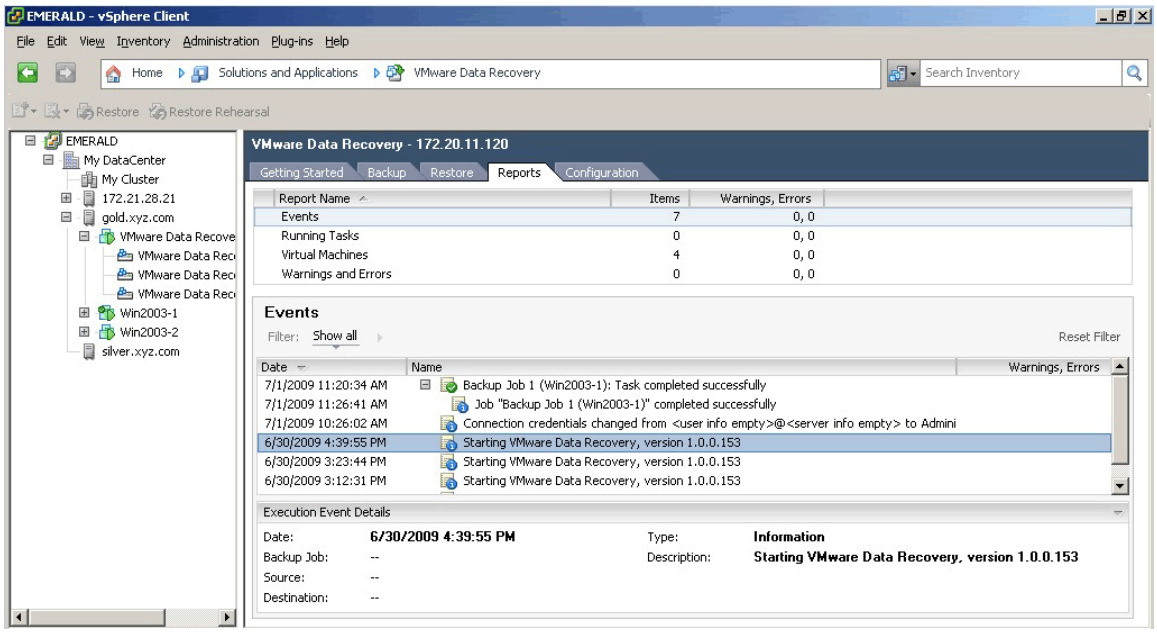
Tivoli Storage Manager on IBM:n ohjelmisto, joka Avamarin tapaan käyttää deduplikointimenetelmää. Tivoli Storage Manager on keskitetty varmuuskopiointiohjelmisto. Kuviossa 5 esitellään Tivoli Storage Managerin käyttöliittymä, josta voidaan valita erilaisia toimintoja varmuuskopiointiin tai palautukseen. Erona Avamariin on virtuaalikoneeseen liittäminen. Avamar liitetään palvelimeen, kuten ESXi-palvelimeen, kun taas Tivoli Storage Manager liitetään jokaiseen palvelimella olevaan virtuaalikoneeseen erillisen asiakasohjelman avulla. (IBM. 2011.)



Kuvio 5. Kuvaruutukaappaus Tivoli Storage Manager-ohjelmasta (Rensselaer, 2008.)

2.3.3 VMware Data Recovery

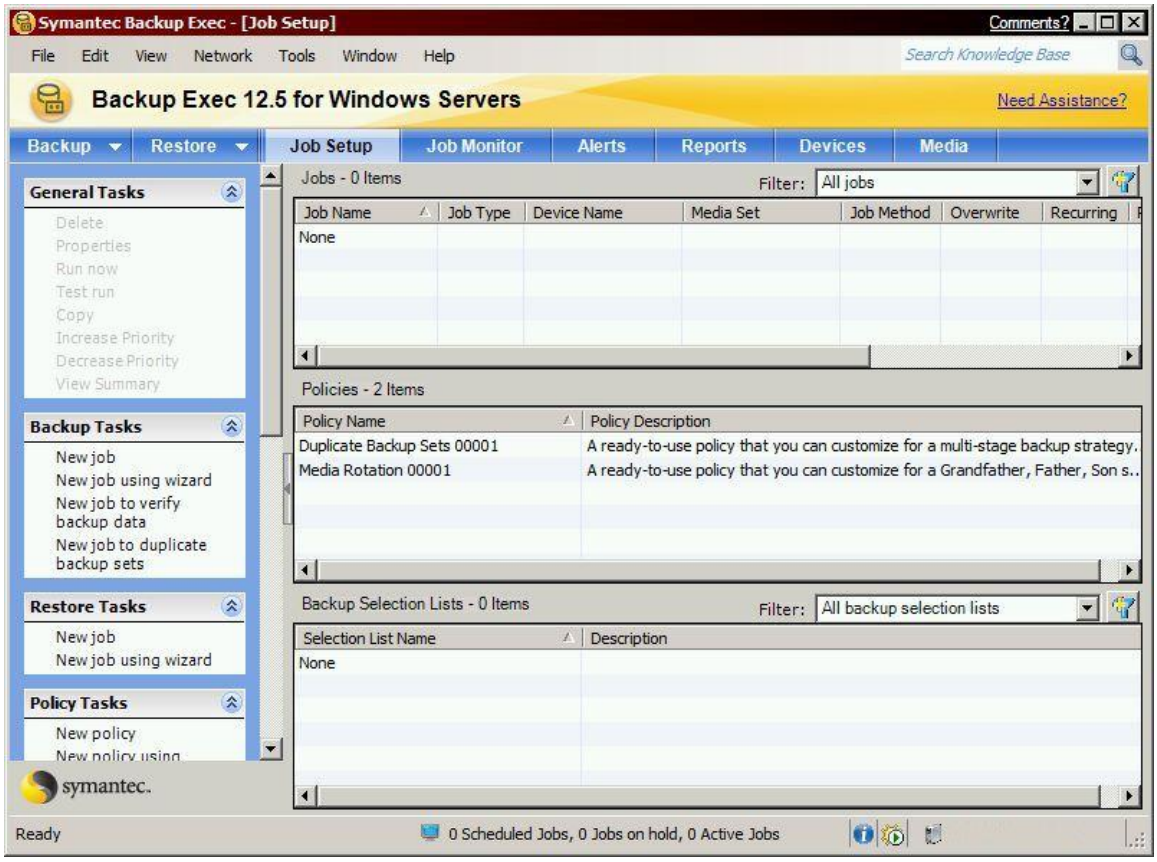
VMware Data Recovery on nimensä mukaan VMware:n kehittämä ohjelmisto. Kuviosta 6 näkee miten ohjelmisto liittyy yhteen vSphere Client -ohjelman kanssa ja ohjelmisto vaatii vCenter Server:in toimiakseen. VMware Data Recovery on tarkoitettu virtuaalisten koneiden ja palvelimien varmuuskopiointiin ja kuten aikaisemmin tässä kappaleessa esitellyt ohjelmistot, Data Recovery sisältää tuen deduplikoinnille. Data Recovery voi palauttaa kokonaisen virtuaalikoneen levykuvan tai yksittäisen tiedoston virtuaalikoneesta. Yksittäisen tiedoston palautus edellyttää, että virtuaalikoneessa ajetaan jotain Microsoftin Windows-käyttöjärjestelmää. (VMware 2011 b.)



Kuvio 6. Kuvaruutukaappaus VMware Data Recovery -ohjelmasta (Seibert, 2009).

2.3.4 Symantec Backup Exec

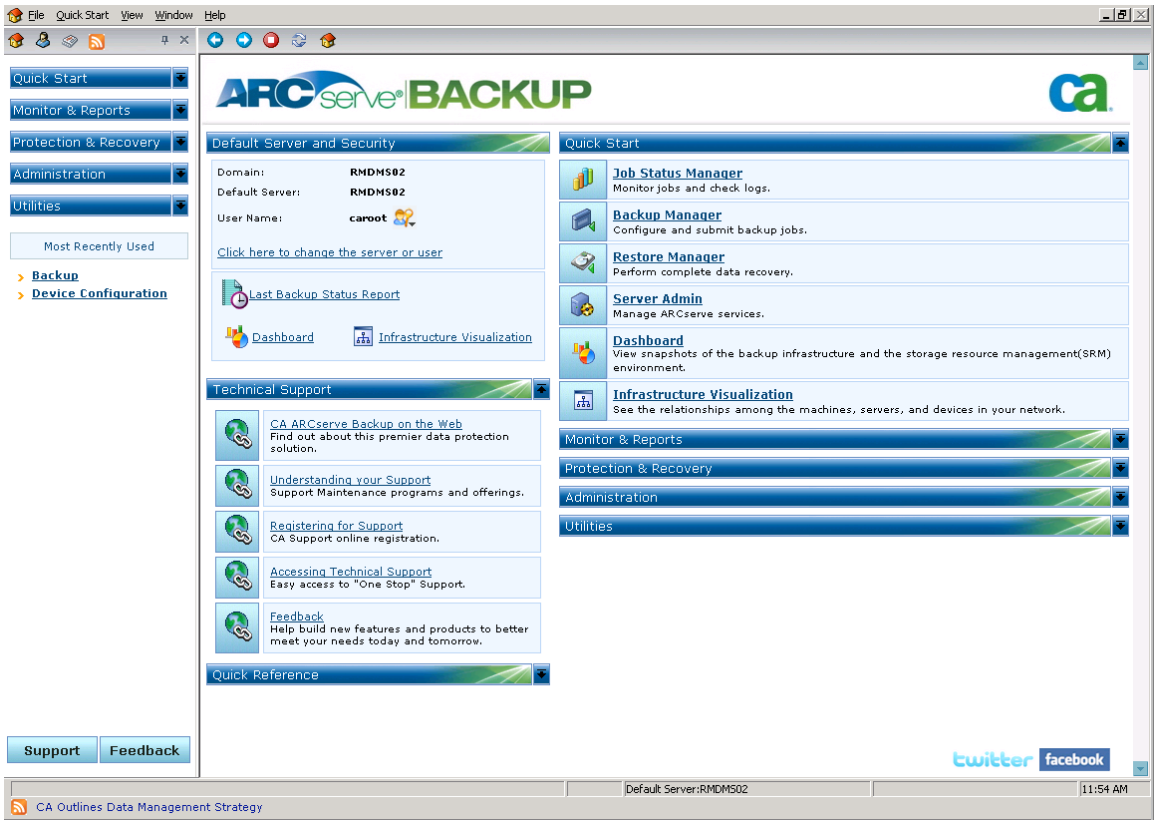
Symantec Backup Exec on Symantec Corporationin kehittämä ohjelmisto, joka vaatii joko Microsoft Windows Server tai VMware ESX -käyttöjärjestelmän palvelimelta, jolla ohjelmistoa ajetaan. Kuten kaikki aikaisemmat ohjelmistot, Symantec Backup Exec sisältää myös deduplikointituen. Kuviosta 7 näkee Symantec Backup Execin käyttöliittymän, jossa voi nähdä työt ja yleiset töihin liittyvät komennot. (Symantec 2011.)



Kuvio 7. Kuvaruutukaappaus Symantec Backup Exec -ohjelmasta (Chirpa, 2009).

2.3.5 CA ARCserve Backup

ARCserve Backup on CA Technologiesin kehittämä varmistusjärjestelmä. ARCservellä voidaan varmistaa molempia; fyysisiä sekä virtuaalisia koneita ja se sisältää deduplikaatiotuen, kuten monet kilpailijansa. Ohjelma tukee myös varmuuskopiointia Amazonin S3-pilveen. Opinnäytetyön käytännön osuus toteutetaan uusimmalla ARCserve-ohjelmistolla, joka on nimeltään ARCserve Backup R16. Käytännön osuudesta lisää luvussa kolme. ARCserven ominaisuuksia voidaan lisätä erilaisilla agenteilla, jotka mahdollistavat esimerkiksi Windows- tai Linux-koneiden varmennuksen. Kuviossa 8 on esillä ARCserven pääkäyttöliittymä, josta pääsee käsiksi ohjelmiston eri alueisiin, kuten varmistukseen ja palautukseen. (CA Technologies, 2012.)



Kuvio 8. Kuvakaappaus ARCserve Backup -ohjelmasta (CA Technologies, 2010)

2.4 Katastrofista palautuminen

Hyväkin laitteisto tai tietojärjestelmäkokonaisuus voi joutua koetukselle inhimillisen erheen tai luonnonkatastrofin, kuten tulvan tai maanjäristyksen takia. Myös tulipaloja ja vesivahinkoja voi tapahtua. Jos tällaisiin ei ole varauduttu varmuuskopioilla tai varalaitteilla, tulee yrityksen liiketoiminta varmasti kärsimään ja jotain tietoa voidaan menettää, eikä menetettyjä tietoja välttämättä saada koskaan takaisin. (The DRG. 2002.)

Katastrofista palautumista ja tilanteen uhatessa tarvittavia toimia voidaan katsoa kolmelta eri suunnalta; ehkäisevät, paikantavat sekä korjaavat toimet. Ehkäisevillä toimilla pyritään estämään tapaturmia, paikantavilla toimilla havaitaan ei-toivottuja tapahtumia, kuten laiterikkoja. Korjaavilla toimilla taas korjataan tai palautetaan järjestelmää tapaturman jäljiltä. Edellä mainitut toimet tulisi kirjoittaa yrityksen palautussuunnitelmaan, jota noudatetaan tapaturman sattuessa. (StrategyBeach, 2009.)

Edellä mainittu palautussuunnitelma sisältää suunnitelman tehtävistä toimenpiteistä ennen hätää, hädän hetkellä ja hädän jälkeen. Palautussuunnitelma auttaa yritystä valmistautumaan pahimpaan ja voi estää päivien käyttökatkokset palveluissa. Suunnitelma pitää dokumentoida ja suunnitelman toiminta pitää testata, jotta kaikki sujuisi hyvin hätätilanteessa. (Wold, 1997.)

Palautussuunnitelman teossa tarvitaan muutamaa asiaa. Ensinnäkin yrityksen hallinnon pitää olla mukana suunnitelman teossa, koska suunnitelman tekoon pitää antaa riittävästi aikaa ja työvoimaa. Samalla pitää varmistaa, että kaikki näkökulmat tulevat huomioiduiksi. Yrityksen hallinnon pitää myös varmistaa suunnitelman toimivuus käytännössä. Suunnitelmaa tekemässä olevien henkilöiden pitää olla oman osa-alueensa taitajia mahdollisimman hyvän palautussuunnitelman aikaansaamiseksi. (Wold, 1997.)

Suunnitelman tekijöiden kannattaa suorittaa riskianalyysit erilaisista skenaarioista, joissa yrityksen tietojärjestelmät ja tallennettu data on vaarassa tuhoutua. Riskianalyysit kannattaa tehdä ainakin luonnonkatastrofeista, teknisistä ja ihmisten aiheuttamista uhista. Riskianalyysissä kannattaa huomioida arvokkaiden tiedostojen ja rekistereiden turvallisuus ja säilyvyys hädän hetkellä. Yleisesti tulipalot ovat yritysten suurin riski, mutta tahallinen tiedostojen tuhoaminen tulee ottaa huomioon suunnitelmaa tehdessä. Suunnitelma on hyvä tehdä myös pahimman mahdollisen katastrofin, talon tuhoutumisen varalle. Suunnitelmassa on hyvä arvioida seurauksia tiedon tuhoutumisen kannalta. (Wold, 1997.)

Suunnitelma pitää kirjoittaa sovitun standardin mukaisesti, jotta sen päivittäminen tulevaisuudessa on helppoa. Suunnitelman päivittäminen tulee tehdä siinä vaiheessa, kun yrityksen ulkoiset tai sisäiset järjestelmät muuttuvat. Standardin ylläpitäminen on tärkeää, jotta suunnitelman kirjoitustyyli ei muutu kirjoittajan vaihtuessa. Hyvin kirjoitettu palautussuunnitelma säästää aikaa, kun sitä luetaan ja toteutetaan. (Wold, 1997.)

2.5 Virtualisoinnin hyvät ja huonot puolet

Miten virtualisointi vaikuttaa katastrofista palautumiseen? Täydellisesti kloonatun virtuaalikoneen pystytys on helppoa ja nopeaa, sillä ylläpitäjän ei tarvitse pystyttää uutta palvelinta, vaan hän voi vain käynnistää kloonatun virtuaalikoneen. Myöskin rahaa säästyy, kun ei tarvita uusia palvelimia jokaiselle virtuaalikoneelle. Perinteisellä, ns. täydellisellä mallilla jokaisella

palvelimella pitäisi olla varakappale, jos käytössä oleva hajoaa. Tämä malli olisi kallis toteuttaa, koska palvelimet maksavat paljon ja yrityksillä ei ole käytössä loputonta määrää rahaa. Virtualisointi mahdollistaa varakappaleista luopumisen lähes kokonaan. Totta kai yrityksellä pitää olla muutama palvelin varalla, jos käytössä oleva menee nurin, mutta verrattuna täydelliseen malliin, yhtä suurta määrää palvelimia ei enää tarvita. (Mello Jr., 2009.)

Vaikka yritys säästääkin rahaa palvelinkustannuksissa, voi yritys joutua maksamaan enemmän hankkiessaan tallennuskapasiteettia kaikille virtuaalikoneille ja niiden varmuuskopioille. Hankinnoissa voidaan säästää hankkimalla erilaisia, esimerkiksi hitaampia levyjä varmuuskopiointijärjestelmään tai kokoonpanoon, joka käynnistyy tapaturman sattuessa. (Mello Jr., 2009.)

Palvelinten virtualisointiin lukeutuu useita hyviä puolia, mutta joukkoon mahtuu myös muutama huonokin puoli. Virtualisointi vähentää palvelinkustannuksia, koska ei tarvitse ostaa useita palvelimia, vaan yksikin riittää. Tämä näkyy sitten fyysisen tilan vähempänä vaatimuksena sekä alhaisempana sähkönkulutuksena. Virtualisointi luo myös laitteistoriippumattoman ympäristön, jossa virtuaalikoneita voi siirtää fyysiseltä koneelta toiselle ilman, että niissä tulisi yhteensopivuusongelmia. Palvelinten kapasiteettia voi myös muuttaa lennosta, eikä palvelinta tarvitse sammuttaa kiintolevyjen lisäämisen ajaksi, ellei sitten lisätä fyysisiä kiintolevyjä isäntäpalvelimeen. (Keshav 2010.)

Palvelininfrastruktuurista voi tulla vaikeammin hallittava, koska ylläpitäjän on hallittava myös fyysisen palvelimen asetukset, eikä vain virtualisoitujen palvelinten asetuksia. Virtuaalipalvelimet ovat enemmän riippuvaisia fyysisestä palvelimesta ja sen toiminnasta. Jos käytössä ei ole varapalvelinta, fyysisen palvelimen rikkoutuminen voi olla kohtalokasta. Virtualisoidut palvelimet voivat olla myös haavoittuvampia tietomurtojen kohteita. Jos hakkeri pääsee murtautumaan fyysisen palvelimen käyttöjärjestelmään, voivat kaikki palvelimella olevat virtuaalipalvelimet olla vaarassa. (Keshav 2010.)

Virtualisoinnista tai muistakaan ehkäisevistä toimista ei ole apua, jos fyysiset laitteet ja varalaitteet eivät toimi tai hajoavat juuri sillä hetkellä, kun niiden pitäisi toimia. Juuri näin kävi World of Warcaftiin sekä lukuisiin muihin peleihin erikoistuneelle yritykselle, Curse.comille. Yksi SAN-ohjainsolmu hajosi Cursen omistamassa tietokeskuksessa Atlantassa ja tämä ohjainsolmun hajoaminen aiheutti koko Curse-verkon, joka sisältää useita kymmeniä sivustoja

ja keskustelufoorumeita, kaatumisen usean päivän ajaksi. Varalla ollut ohjainsolmu käynnistyi normaalisti, mutta se hajosi asetusten kopioinnin jälkeen. Yrityksen tiedot eivät onneksi olleet vaarassa, koska rikkoutunut osa oli verkkolaitteen ohjainsolmu. (Curse Inc, 2011.)

Mitään virallista tietoa katkon aiheuttamista kustannuksista ei ole, mutta Curse omistaa useita kymmeniä sivuja ja jokaisella sivulla on Cursen omia mainoksia, joten mainostuloissa tullaan näkemään pienoinen pudotus, samoin sivujen kävijämäärissä. Monet sivustojen käyttäjät olivat tuskastuneita Cursen toimintaan katastrofin aikana, vaikka heidän ei olisi pitänyt syyttää ketään. Laitevikoja sattuu eikä niille voi mitään. (Curse Inc, 2012.)

3 PROJEKTI

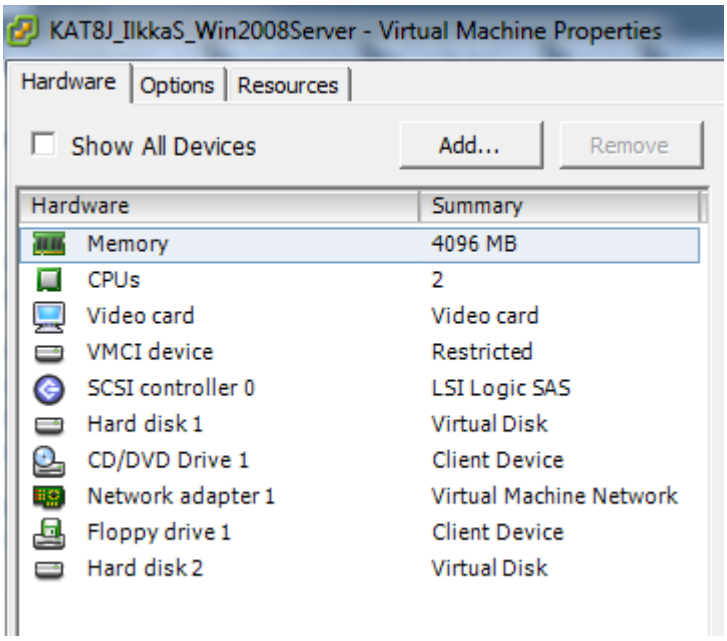
Opinnäytetyön käytännön osuus toteutettiin Kajaanin ammattikorkeakoulun tietojärjestelmälaboratoriossa kevään 2012 aikana. Projektin tavoitteena oli toteuttaa toimiva varmuuskopiointijärjestelmä, jota Kajaanin ammattikorkeakoulu voi käyttää tietojärjestelmälaboratoriossa pyörivien virtuaalikoneiden varmuuskopiointiin. Varmistusjärjestelmä käyttää CA ARCserve Backup -ohjelmistosta löytyvää deduplikaatio-ominaisuutta, joka vähentää varmistuksessa tarvittavaa kiintolevytilan määrää.

Projekti aloitettiin tutustumalla käytettävään ohjelmistoon, ja tällä ohjelmistolla tehtiin muutamia testejä. Testeillä katsottiin kuinka helppo varmuuskopioita oli tehdä ja kuinka nopeasti niiden palautus sujui. Testien jälkeen tehtiin varsinainen asennus tuotantokäyttöön. Varsinaisesta asennuksesta löytyy lisää luvusta 3.3.

Varmuuskopioidut virtuaalikoneet jaettiin kolmeen eri tärkeysjärjestykseen; korkea, keskiväli ja matala. Korkea-taso sisälsi tuotantokäytössä olevat virtuaalikoneet. Nämä varmuuskopioitiin täysinä varmuuskopioina perjantaisin ja lisäävillä varmuuskopioilla keskellä viikkoa sekä siirrettiin taustanauhoille joka päivä. Keskivälin, testi- ja kehitysvirtuaalikoneet varmuuskopioitiin perjantaisin täysinä varmuuskopioina ja lisäävinä varmuuskopioina keskellä viikkoa. Matalan tason oppilaskoneiden varmuuskopiointi oli aika samanlainen kuin medium-tason, erona kuitenkin se, että viikolla ei välttämättä otettu lisääviä varmuuskopioita.

3.1 Varmuuskopiointijärjestelmä

Projektin toteuttamiseen käytettiin CA ARCserve Backup -ohjelmistoa. Ohjelma asennettiin Windows Server 2008 R2 Enterprise -palvelimelle, joka oli virtualisoitu VMwaren ESXi-palvelimelle. Windows Serverille asennettiin Microsoft SQL Server 2008 pyörittämään varmuuskopiointiin tarkoitettua tietokantaa sekä Microsoft .NET Framework 3.5 SP1. Windows-palvelimelle annettiin neljä gigatavua RAM-muistia, 40 gigatavua kovalevytilaa ja kaksi ydintä prosessorilta. Kuviossa 9 näkyy varmuuskopiointipalvelimen asetukset.



Kuvio 9. Varmuuskopiointipalvelimen tiedot

3.2 Varmistusjärjestelmän testaus

Varmuuskopiointijärjestelmän testi suoritettiin VMwaren ESXi-palvelimella, käyttäen Windows Server 2008 R2 -palvelinkäyttöjärjestelmää testijärjestelmänä. Käyttöjärjestelmälle annettiin 40 GB kiintolevytilaa, 4 GB RAM-muistia sekä yksi ydin.

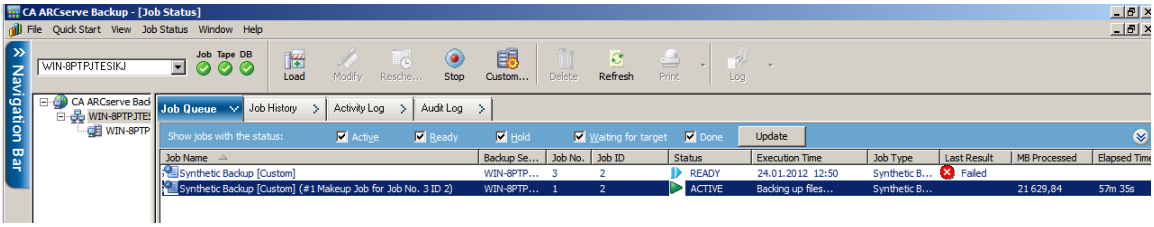
3.2.1 Täyden varmuuskopion ottaminen

Ennen varmuuskopion ottamista, kohdekoneeseen voi asentaa agentin, joka huolehtii varmuuskopioinnista. Agentin asentaminen hoituu ARCserven mukana tulevalla Agent Deployement -työkalulla. Kyseinen työkalu käyttää tietokannassa olevia virtuaalikoneiden isäntänimiä, eikä virtuaalikoneille ESXi:ssä annettuja nimiä. Listasta valitaan koneet, joihin agentit asennetaan ja listassa oleviin kenttiin syötetään järjestelmänvalvojan tunnus ja salasana. Agentin asennuksessa oli hieman ongelmia, koska testikoneessa ollut Windowsin palomuuri esti yhteydenoton verkon yli, mutta palomuurin alasajolla selvittiin tästä ongelmasta. Tuotan-

tokäytössä palomuuriin pitää tehdä aukko, jotta palomuuria ei tarvitse ajaa alas agentin asennusta ja toimintaa varten.

Agentin asennus on tärkeää, jos haluaa mahdollistaa yksittäisten tiedostojen palautuksen varmuuskopioista. Ilman backup agenttia palautuksen voi tehdä vain kokonaisen virtuaalikoneen palautuksen RAW-muodossa tai suoraan ESXi-palvelimelle.

Agentin asennuksen jälkeen varmistusjärjestelmään luotiin kertaluonteinen työ, joka tekee täyden varmuuskopion testikoneesta ja tallentaa varmuuskopion omalle kiintolevylleen. Kuviossa 10 ARCserve loi itselleen toisen työn, joka tekee saman kuin ensimmäinen epäonnistunut työ. Ensimmäinen työ ei onnistunut, koska virtuaalikoneesta, jolle ARCserve oli asennettu loppui kiintolevytila. Ongelma ratkesi lisäämällä virtuaalikoneelle uutta levytilaa ESXi:n asetuksista. Tämän vaiheen jälkeen virtuaalikoneella oli käytössä 120GB kiintolevytilaa.

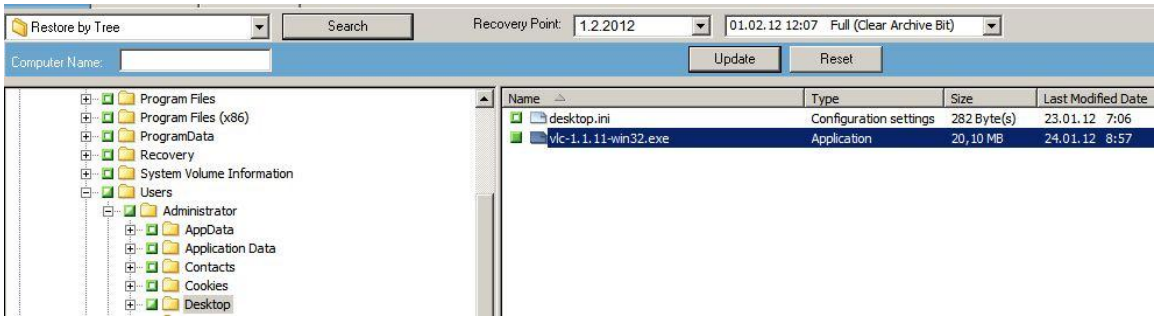


Kuvio 10. Kuvaruutukaappaus varmennustyöstä

Testeissä käytettiin virtuaalikonetta, jolle oli annettu 40GB:n kiintolevy. Valmis varmistustyö tästä koneesta vei 40 GB kiintolevytilaa, koska varmistettavaa dataa ei oltu käsitelty mitenkään. Käsittelyyn on kuitenkin mahdollisuus, jos deduplikaatio laitetaan päälle asetuksista. Deduplikaatiota käyttämällä varmistetun datan määrä kutistui noin 7,5 gigatavuun. Varmistetun datan määrästä huomaa miten suuri hyöty deduplikaatiosta on käytännössä ja varmistukseen käytetty aika lyheni yli 50 prosentilla deduplikaation ansiosta.

3.2.2 Yksittäisen tiedoston palautus

Yksittäisen tiedoston palauttamista testattiin aikaisemmin luodulla täydellä varmistuksella. Täyteen varmistukseen tehtiin lisäysvarmistus, joka varmisti muuttuneet tiedostot. Tämä menetelmä säästää levytilaa, koska tiedostot muuttuvat vain täyden varmistuksen sisällä eivätkä vaadi lisää levytilaa levyjärjestelmästä. Kuviossa 11 näkee, miten helppoa yksittäisen tiedoston valinta on hakemistopuusta, kunhan vain tietää palautettavan tiedoston tarkan sijainnin.



Kuvio 11. Tiedoston palautus varmuuskopiolta

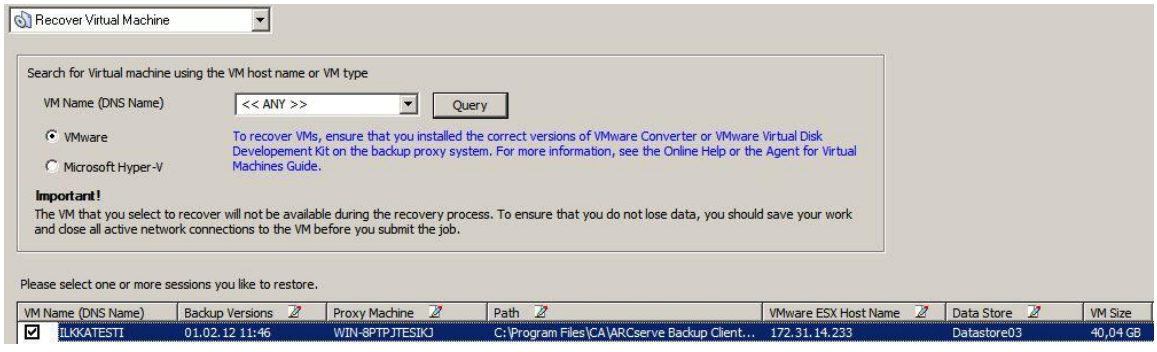
Yksittäisen tiedoston sai palautettua helposti ARCserven Restore-valikosta, josta voi sitten valita virtuaalikoneen ja siitä otetun varmuuskopioin. Tiedoston valinnan jälkeen voidaan valita mihin sijaintiin tiedosto palautetaan. Oletuksena oli tiedoston alkuperäinen sijainti. Tiedoston voi palauttaa myös eri koneeseen kuin mistä se on varmuuskopioitu. Testissä käytettiin 20MB:n kokoista .exe-tiedostoa Järjestelmänvalvoja-käyttäjätilin työpöydällä. Kyseisen tiedoston palautukseen meni aikaa kuusi sekuntia. Kuvio 12 näyttää keskimääräisen tiedonsiirtonopeuden, joka oli 772,50MB/minuutissa palautuksen aikana. ARCserve antaa hyvän raportin jokaisesta työstä, mistä näkee tarkemmin työhön käytetyn ajan sekä tiedonsiirtonopeuden. Isojenkaan tiedostojen palautukseen ei mene kovin pitkää aikaa testin perusteella.

```
Total Size (Disk)..... 59,97 MB
Total Size (Media)..... 64,38 MB
Elapsed Time..... 5s
Average Throughput..... 772,50 MB/min
Totals For..... Job
Total Session(s)..... 1
Total Skip(s)..... 0
Total Size (Disk)..... 59,97 MB
Total Size (Media)..... 64,38 MB
Elapsed Time..... 6s
Average Throughput..... 772,50 MB/min
Restore Operation Successful.
```

Kuvio 12. ARCserve:n raportti tiedoston palautuksesta

3.2.3 Virtuaalikoneen palautus

Virtuaalikoneen palautus toimii melkein kuten yksittäisen tiedoston palautus. Kuviossa 13 näkyvässä Restore-valikosta otetaan valinta Recover Virtual Machine. Tämän jälkeen pitää syöttää salasanat ESXi- ja ARCserve-palvelimille, jotta palautustyön voi luoda.



Kuvio 13. Virtuaalikoneen palautus

Tässä vaiheessa ongelmaksi muodostui se, että ARCserve ei voinut luoda virtuaalikonetta ESXi-palvelimelle, koska varmuuskopioitu virtuaalikone oli poistettu manuaalisesti palvelimelta ja ARCserve ei voi kirjoittaa poistetun virtuaalikoneen päälle. Seuraavalla kerralla virtuaalikonetta ei poistettu manuaalisesti, vaan annettiin ARCserve:n hoitaa virtuaalikoneen poisto. Se onnistui hyvin, mutta jostain syystä ARCserve ei kyennyt luomaan uutta virtuaalikonetta poistetun tilalle. Ongelmaa koetettiin korjata luomalla virtuaalikone resource pool:in ulkopuolelle, koska palvelimella epäiltiin olevan liian vähän resursseja uuden virtuaalikoneen luontiin. Tämä ei kuitenkaan auttanut, vaan ARCserve antoi edelleen saman, kuviosa 14 näkyvän virheilmoituksen lokitiedostoon.

```
 2/09/12 12:57:28  [39.13] CreateVM Failed with error msg - "Err_code: -113 CreateVM: Exception Raised - No Compute
Resource Found On Specified Host."
```

Kuvio 14. Kuvaruutukaappaus ARCserve:n virhelokista

Varmuuskopioidun virtuaalikoneen palautuksessa ilmennyt No Compute Resource Found On Specified Host ongelma korjautui vaihtamalla palautusasetuksista kohdekoneeksi ESXi-palvelin Vcenter-palvelimen sijaan. Jostain syystä ARCserve ei osaa kommunikoida Vcenter:in kanssa tarpeeksi hyvin, jotta virtuaalikoneen saisi palautettua suoraan Vcenterin kautta ESXi-palvelimelle.

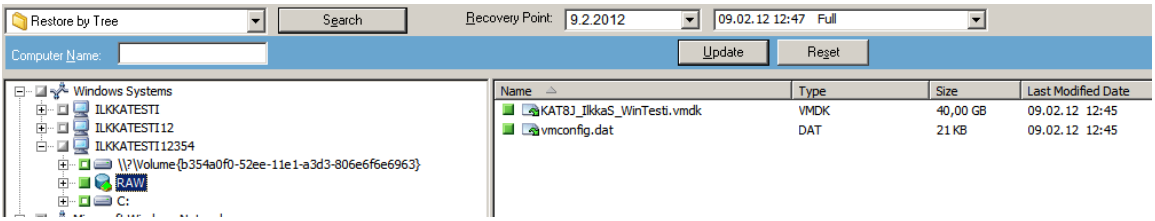
Deduplikaatiolla varmistetun virtuaalikoneen sai palautettua alle 10 minuutissa. Palautuksen jälkeen palautettu virtuaalikone piti siirtää oikeaan resurssipooliin, koska ARCserve palautti sen poolin ulkopuolelle. Kuviossa 15 on esitetty käsittelemättömän ja deduplikoidun virtuaalikoneen palautusraportit. Käsittelemättömän virtuaalikoneen palautuksessa kestää pidempään, koska palautettavaa tietoa on määrältään enemmän. Vanhan virtuaalikoneen korvaaminen (overwrite) on oletuksena päällä palautuksessa, mutta sen saa pois päältä ARCserve:n asetuksista.

```
Total Size (Disk)..... 7,17 GB
Total Size (Media)..... 7,17 GB
Elapsed Time..... 8m 38s
Average Throughput..... 850,97 MB/min

 Total Size (Disk)..... 40,07 GB
 Total Size (Media)..... 40,07 GB
 Elapsed Time..... 42m 31s
 Average Throughput..... 965,16 MB/min
```

Kuvio 15. ARCserve:n raportit deduplikoidun ja käsittelemättömän virtuaalikoneen palautuksesta

VMware ESXi:n luomat image-tiedostot sai palautettua ARCserve-palvelimen kiintolevylle valitsemalla kuviossa 16 esitelty Restore by Tree vaihtoehto ja RAW. Tämä palautustapa on hieman ongelmallinen, koska tiedostot pitäisi saada palautettua levyjärjestelmään, eikä varmistuspalvelimen kiintolevylle. Palautetut tiedostot voi siirtää verkon yli levyjärjestelmään, jos sinne on yhteys koneelta, jonne tiedostot on palautettu. Tiedostot voidaan myös siirtää VMware Workstationiin ja ajaa palvelinta paikallisesti jollain tietokoneella, koska tiedostot ovat VMware:n käyttämässä .vmdk-tiedostomuodossa.



Kuvio 16. Virtuaalikoneen tiedostojen palautus

Vmdk-tiedostot saa palautettua myös valitsemalla Restore by Session vaihtoehto palautusnäkymässä. Valitaan vain tallennusväline ja sieltä sitten istunto, jossa palautettava virtuaalikone on. Istunnot erotellaan toisistaan istuntonumerolla, joten on mahdollista, että siellä on useita

versioita samasta virtuaalikoneesta. Restore by Session palautuksella on myös mahdollista palauttaa yksittäisiä tiedostoja virtuaalikoneista.

3.3 Varmistusjärjestelmän loppuasennus

Varmistusjärjestelmä asennettiin Dell PowerEdge 2950 mallin palvelimelle Kajaanin ammattikorkeakoulun tietojärjestelmälaboratorion konesaliin. Palvelimessa on 52GB RAM-muistia, neli-ytiminen Intel:in 2GHz prosessori ja kiintolevytilaa noin yksi teratavu. Käyttöjärjestelmäksi valittiin 64-bittinen Windows Server 2008 R2, koska se on uusin Microsoft:in kehittämä palvelinkäyttöjärjestelmä tuotantokäyttöön. 64-bittinen versio valittiin palvelimella olevan suuren muistimäärän takia. 32-bittinen käyttöjärjestelmä ei olisi osannut tukea niin suurta määrää muistia.

Palvelimeen asennettiin uusimmat Windowsin päivitykset Windows Update:sta. Varmistusjärjestelmää ei virtualisoitu, koska varmistaminen ja palautus vaativat paljon resursseja koneelta. Virtualisoituna järjestelmä olisi jakanut resursseja muiden virtuaalikoneiden kanssa, ja tästä olisi voinut tulla ongelmia, kun aletaan varmuuskopioida suuria määriä tietoja. Varmistusjärjestelmä vaatii myös SQL-tietokannan. Tähän tarkoitukseen asennettiin virtualisoitu Windows 2008 R2-palvelin, joka ajaa useita SQL-tietokantoja.

Ennen ARCserve:n asennusta palvelimeen piti laittaa oikea staattinen IP-osoite ja siirtää palvelin oikeaan toimialueeseen. Samalla luotiin domain admin-tason käyttäjätunnus, jota ARCserve käyttää. ARCserve asennettiin Primary Server valintaa käyttämällä. Samalla asennettiin Global Dashboard, virtual machine agentti ja Open file agentti.

Global Dashboard mahdollistaa nopean tavan tarkistaa usean ARCserve-palvelimen tila ja seurata varmistustöiden etenemistä. Virtual machine agent mahdollistaa virtuaalikoneiden varmuuskopioinnin sekä yksittäisten tiedostojen varmuuskopioinnin ja palautuksen. Open file agentti taas mahdollistaa avoinna olevien tiedostojen varmuuskopioinnin.

Palvelimelle avattiin yhteys iSCSI-levyjärjestelmään. Tähän tarvittiin palvelimen IP-osoite sekä IQN. Levyjärjestelmästä annettiin yhteensä noin neljä teratavua kiintolevytilaa varmis-

tusjärjestelmän käyttöön. Koska levytila oli kahdella eri levyllä, ne piti yhdistää yhdeksi levyksi palvelimella, jotta kaikki neljä teraa olisivat saman asemakirjaimen alla.

Osa ARCserve:n luomasta datasta varmennuksen aikana tallennettiin paikallisesti palvelimen kiintolevylle. Levyjärjestelmään luotiin paikat, joihin ARCserve voi tallentaa eri varmennustasojen datan sekä viimeisen virtuaalisen nauha-aseman. Tätä virtuaalista nauha-asemaa käytettiin viimeisenä tallennuspaikkana, johon data siirretään deduplikaation jälkeen.

Tarkoitus oli asentaa jokaiseen virtuaalikoneeseen uusin versio VMware Tool:sista, mutta se ei onnistunut, koska sen asennus manuaalisesti noin 260 koneeseen on niin suuri urakka. Samoin agenttien asennuksessa tuli ongelmia. Suurimmaksi ongelmaksi muodostui järjestelmänvalvoja-tilin salasana. Opiskelijat ovat asentaneet koneita ja laittaneet omat salasanansa paikoilleen. Näin ollen, on mahdotonta asentaa jokaiseen koneeseen ARCserve:n agentit, joita tarvittaisiin tiedostotason varmuuskopioiden ottamiseen. Agentti saatiin kuitenkin asennettua muutamaan tuotantokäytössä olevaan virtuaalikoneeseen, koska ne olivat uudessa tuotantoon tarkoitetussa domainissa, johon pääsi kirjautumaan sisään.

ARCserve:en luotiin kaksi erilaista työtä, toinen varmentamaan kriittisiä tuotantokäytössä olevia palvelimia ja toinen varmentamaan opiskelijoiden luomat virtuaalikoneet. Ensimmäinen, kriittisiä palvelimia varmuuskopioiva työ asetettiin ajettavaksi joka ilta. Kriittisistä palvelimista otetaan perjantaisin täysi varmuuskopio RAW- ja tiedostotasolla sekä muuttuneet tiedostot viikolla. Toinen työ joka tehtiin järjestelmään, varmuuskopioi opiskelijoiden luomia virtuaalikoneita perjantaisin. Jos opiskelijan tekemään virtuaalikoneeseen on asennettu ARCserve:n virtual machine agent, koneesta saadaan myös täysi varmuuskopio tiedostotasolla ja RAW-muodossa. Jos kyseistä agenttia ei ole asennettu, virtuaalikoneesta saadaan vain RAW-tason varmuuskopio, jonka katsottiin riittävän opiskelijoiden luomien koneiden varmuuskopiointiin.

Varmuuskopioitavat virtuaalikoneet ryhmiteltiin korkean, keskitason ja matalan tärkeystason ryhmiin. Tuotantokäytössä olevat koneet luokiteltiin korkean tason ryhmään ja muut koneet luokiteltiin matalan tärkeystason ryhmään. Virtuaalikoneiden luokitus on muutettavissa parilla hiiren klikkauksella jälkeenpäin ja ryhmittely helpottaa varmennuksen tarkkailua, koska ARCserve:ssä on paikka, josta näkee ryhmitellyt koneet ja niiden varmuuskopio-tilan. Tämä tila kertoo onko konetta varmuuskopioitu ja onko varmuuskopiointi epäonnistunut.

Tässä vaiheessa ilmeni ongelma, joka estää Windows Server 2008 R2 palvelinten varmuuskopioinnin. VMware Tools, joka tulee VMware vCenter-ohjelmiston mukana, aiheuttaa tilannekuvan luonnin epäonnistumisen ja tästä syystä virtuaalikoneista, joissa on tämä kyseinen Windows-käyttöjärjestelmä, ei saada varmuuskopioita. Ongelma korjaantuu tulevaisuudessa, kunhan virtuaalikoneet siirretään uuteen ympäristöön, jossa on käytössä uudempi versio vCenter:istä.

Varmistusjärjestelmän käyttöönottoprojektia jatketaan asentamalla ARCserve D2D. Tämä mahdollistaa disk to disk -varmuuskopioiden ottamisen kriittisistä virtuaalikoneista, kuten tietokantapalvelimesta ja monimutkaisista Windows-palvelimista.

4 POHDINTA

Varmuuskopiointi on loppujen lopuksi aika pieni aihealue, joten opinnäytetyön rajaus syntyi aika selkeästi. Kun aihealue oli selvillä, tiedon haku oli aika helppoa erinäisiltä varmuuskopiointiin erikoistuneilta sivustoilta ja järjestelmäntoimittajien sivuilta. En ollut aikaisemmin tutustunut tämän kokoluokan varmuuskopiointiohjelmiin, joten aika pystymetsästä tähän tuli lähdettyä, mutta oppimista on tapahtunut koko matkan aikana. Koulussa ei opetettu tähän aihepiiriin oikeastaan mitään, joten mitään oppeja ei voinut soveltaa sieltä, vaan piti lukea ja opetella itse käytännön kautta ja soveltaa lukemalla opittua käytäntöön.

Ikävä puoli tämän opinnäytetyön tekemisessä oli se, että aikataulut venyivät rankasti alkuperäisestä arviosta ja työn käytännön osuuden teolle jäi loppujen lopuksi lyhyt aika keväällä. Aikataulut venyivät minusta riippumattomista syistä. Varmistusjärjestelmän hankintaprosessi kesti oman aikansa ja se tapahtui muutama kuukausi myöhässä sovitusta aikataulusta.

Sitten, kun ongelmalistaan lisätään lopullisessa asennuksessa olleet muutamat ongelmakohdat, kuten varmistusohjelman asennuksen ajankohdan sekä keskitetyn tietokantapalvelimen asennuksien viivästyminen, niin kyllähän siinä muutama harmaa hius meinasi ilmestyä.

Myös VMware toolsin asennus kaikkiin valmiisiin virtuaalikoneisiin ja ARCserve backup agentin asennus tuotti päänvaivaa. Ongelmat johtuivat siitä, että opiskelijat eivät olleet asentaneet VMware toolsia itse omiin koneisiinsa, enkä tiennyt salasanoja, joilla olisin päässyt asentamaan backup agenttia kyseisiin virtuaalikoneisiin. Tämä turhautti itseäni hieman, koska backup agentin asennuksen puuttuminen vaikeuttaa varmuuskopiointia, koska yksittäisiä tiedostoja ei tällöin pystytä palauttamaan.

Testatessani virtuaalikoneen palautusta huomasin, että varmuuskopioidun virtuaalikoneen saa palautettua aika nopeasti, joten järjestelmän palautus toimintakuntoon katastrofin sattuessa ei ole kovin aikaa vievä prosessi. Katastrofissa menetetyn tiedon ja työn määrä riippuu siitä, milloin viimeisin varmistus on otettu. Jos virtuaalikoneet varmistetaan joka yö, menetetään alle päivän työ. Jos taas virtuaalikoneet varmuuskopioidaan joka tunti, menetetään vain alle tunnin työ. Yksittäisten tiedostojenkin palautus on helppoa ja suhteellisen nopeaa, joten

tästäkään ei koidu isoja menetyksiä, vaan hommat saadaan toimimaan nopeasti, kunhan oikea tiedosto löydetään varmuuskopiosta.

Käsittelin palautussuunnitelmaa aika paljonkin teoriaosassa, mutta itse käytännön työssä sitä ei näkynyt. Tähän on syynä se, että palautussuunnitelma on tehty kattamaan koko Kajaanin ammattikorkeakoulun tietokoneet, eikä tietojärjestelmälaboratoriolle ole tehty erillistä palautussuunnitelmaa, muuten kuin mitä on sovittu varmuuskopiointitöiden ajankohdaksi ja asetuksiksi.

D2D:n asennuksen poisjättäminen jäi hieman harmittamaan. Olisi ollut kiva nähdä miten se asennetaan ja miten se oikein toimii käytännössä, mutta koska D2D-ominaisuuden selvittäminen, asentaminen sekä konfigurointi (configuration) olisi ollut liian iso urakka tehdä lyhyellä aikajaksolla, ominaisuuden asentaminen oli pakko jättää pois tästä opinnäytetyöprojektista.

LÄHTEET

Blackburn K. 2011. Avamar. http://www.clearpathsg.com/file-level-restores-vm-image-level-backups-using-avamar-and-vmware-vstorage-api (Luettu 10.2.2012)

CA Technologies. 2012. CA ARCserve® Backup Product Features. http://www.arcserve.com/us/products/backup/features-overview.aspx (Luettu 17.1.2012)

CA Technologies. 2010. CA ARCserve® Backup. https://support.ca.com/cadocs/0/CA%20ARCserve%20%20Backup%2015-ENU/Bookshelf_Files/HTML/Online_Help/index.htm?toc.htm?caab_home_page.htm (Luettu 10.2.2012)

Chirpa. 2009. Symantec Backup Exec. http://www.readynas.com/?p=1951 (Luettu 10.20.2012)

Cornelius J. VMWare Snapshot inspirations http://www.cjvandyk.com/blog/Lists/Posts/Post.aspx?List=744536f4%2D127e%2D4c4a%2Dbcff%2Db85408e7e7e5&ID=163&Web=70a3e89c%2Dd7de%2D44f0%2D9cd7%2Dcf99e224b81a (Luettu 15.5.2012)

Curse Inc. 2011. Curse Network Downtime Explanation. http://www.curse.com/news/other/11490-curse-network-downtime-explanation (Luettu 20.9.2011)

Curse Inc. 2012. Curse Inc. http://www.curse.com/ (Luettu 20.2.2012)

Datadomain. 2011. EMC Resources. http://www.datadomain.com/resources/faq.html (Luettu 11.5.2011)

EMC. 2011. Avamar. http://www.emc.com/products/series/avamar.htm (Luettu 8.5.2011)

Hess K. 2008. Virtual Machine Backup and Restore: What's Your Strategy? http://www.linux-mag.com/id/7182/ (Luettu 10.5.2011)

IBM. 2011. IBM Tivoli Storage Manager. http://www-01.ibm.com/software/tivoli/products/storage-mgr/features.html (Luettu 8.5.2011)

Keshav S. 2010. Virtualization: The Good, The Bad, and The Ugly. Web-dokumentti. Saatavilla http://research.microsoft.com/en-us/people/sriram/keshav.ppt (Luettu 15.12.2011)

Mello Jr J. 2009. Virtualization Makes Disaster Recovery Cheaper. http://www.enterprisestorageforum.com/continuity/features/article.php/11570_3832971_2/Virtualization-Makes-Disaster-Recovery-Cheaper.htm (Luettu 13.1.2012)

OpenSourceRack. 2010. Kloonaus. Mukaillen lähdettä. http://www.opensourcerack.com/2010/09/30/cloning-xenapp-in-the-cloud-2/ (Luettu 10.2.2012)

PC911. 2011. Backing up data – why you need to do it. http://pcnineoneone.com/howto/backup1/ (Luettu 7.5.2011)

Poelker C. 2009. How to Leverage Data Deduplication to Green Your Data Center. http://www.eweek.com/c/a/Data-Storage/How-to-Leverage-Data-Deduplication-to-Green-Your-Data-Center/ (Luettu 10.2.2012)

Rensselaer. 2008. Tivoli Storage Manager.

http://helpdesk.rpi.edu/update.do?artcenterkey=277 (Luettu 10.2.2012)

Seibert E. 2009. VMware Data Recovery. http://www.voiceanddata.com.au/articles/34421-Backing-up-virtual-environments-with- VMware (Luettu 10.2.2012)

StrategyBeach. 2009. Disater recovery and data backup solutions. http://www.strategybeach.com/Disaster-Recovery-Data-Back-Up.aspx (Luettu 20.12.2011)

Symantec. 2011. Symantec Backup Exec. http://www.symantec.com/business/backup-exec-for-windows-servers (Luettu 10.5.2011)

Tampereen ammattikorkeakoulu. 2011. Varmuuskopiointi. http://www.cibernarium.tamk.fi/tietoturva2/varmuuskopiointi.htm (Luettu 7.5.2011)

The DRG. 2002. Disaster Recovery Planning Guide http://www.disaster-recovery-guide.com/ (Luettu 4.1.2012)

TopTenReviews. 2011 Why Backup Your Computer Data? http://data-backup-software-review.toptenreviews.com/why-backup-your-computer.html (Luettu 7.5.2011)

VirtualizationAdmin. 2008. What is a snapshot? http://www.virtualizationadmin.com/faq/snapshot.html (Luettu 12.5.2011)

VMware 2011 a. Understanding Clones. http://www.vmware.com/support/ws55/doc/ws_clone_overview.html (Luettu 13.5.2011.)

VMware 2011 b. VMware Data Recovery. http://www.vmware.com/products/data-recovery/features.html (Luettu 10.5.2011)

Wold G, 1997. Disaster Recovery Planning Process.
http://www.drj.com/new2dr/w2_002.htm (Luettu 13.11.2011)