

Miikka Veijonen

# Varmuuskopiointiratkaisu PK-yritykselle

Suunnittelu, toteutus ja testaus

## **Alkulause**

Tämä insinööri työ käsittelee varmuuskopiointijärjestelmän suunnittelua, rakentamista ja testausta PK-yritykselle. Työ tehtiin TAG Systems Finland Oy:lle. Työn ohjaajina toimivat Metropolian puolesta yliopettaja Janne Salonen ja TAG Systemsin puolesta vanhempi järjestelmäasiantuntija Jukka Kangas.

Haluan osoittaa kiitokseni työni ohjaajille, työnantajalleni ja kaikille kollegoilleni. Lisäksi haluan kiittää siskojaani Maaritia ja Marianneaa, jotka auttoivat minua työn tekstiosuudessa. Lopuksi haluan sanoa myös kiitokset tyttöystävälleni Irinjalle, joka on tukenut ja kannustanut minua opinnoissani sekä insinööri työni tekemisessä.

Helsingissä, 25.5.2012

Miikka Veijonen

Tekijä(t) Otsikko	Miikka Veijonen Varmuuskopiointiratkaisu PK-yritykselle
Sivumäärä Aika	36 sivua + 5 liitettä 25.5.2012
Tutkinto	Insinööri (AMK)
Koulutusohjelma	tietotekniikka
Suuntautumisvaihtoehto	tietoverkot
Ohjaajat	Yliopettaja Janne Salonen Vanhempi järjestelmäasiantuntija Jukka Kangas
<p>Tämän insinööriyön tarkoituksena oli rakentaa varmuuskopiointijärjestelmä PK-yritykselle. Työ tehtiin TAG Systems Finland Oy:lle ja se koostui varmuuskopiointitekniikoihin tutustumisesta, järjestelmän suunnittelusta, toteuttamisesta ja lopuksi sen testauksesta.</p> <p>Ympäristö, johon varmuuskopiointijärjestelmä toteutettiin, sisälsi työasemia sekä palvelimia. Työasemista löytyi kolme eri käyttöjärjestelmää, ja palvelimia oli sekä fyysisiä että virtuaalisia. Virtuaaliset palvelimet pyörivät VMware-ympäristössä.</p> <p>Työasemista tuli ottaa sekä täydellisiä että tiedostotason varmuuskopioita siten, että loppukäyttäjä pystyi palauttamaan tarvittaessa yksittäisiä tiedostoja. Palvelimet piti varmuuskopioida kokonaisuudessaan siten, että katkoa ei palveluissa syntynyt. Virtuaalisesta tiedostopalvelimesta tuli normaalin virtuaalipalvelinvarmuuskopion lisäksi ottaa myös tiedostotason varmuuskopioita ja säilyttää niitä mahdollisimman pitkään. Tämä toteutettiin hyödyntäen modernia versioivaa Btrfs-tiedostojärjestelmää.</p> <p>Työn tuloksena syntyi toimiva varmuuskopiointijärjestelmä, johon pystyi lisäämään tarvittaessa uusia työasemia ja palvelimia. Työssä saavutettiin sille asetetut tavoitteet.</p>	
Avainsanat	Varmuuskopiointi, VMware, Btrfs

Author(s) Title	Miikka Veijonen IT Backup solution for small business
Number of Pages Date	36 pages + 5 appendices 25 May 2012
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Data Networks
Instructors	Janne Salonen, Principal Lecturer Jukka Kangas, Senior Systems Engineer
<p>The purpose of this project was to build a backup solution for a small business. The project was done for TAG Systems Finland Ltd, and it consists of getting acquainted with different backup techniques, building the actual backup infrastructure and testing the final system.</p> <p>The environment in which the system was built contained workstations and servers. There were three different operating systems running on those workstations and there were both physical and virtual servers. Virtual servers were running on VMware virtualization environment.</p> <p>The backup of the workstations must include full and filesystem level backups. End users had to have access to filesystem level backups so they could restore files on their own. The servers had to be backed up in a way so that there were no interruptions with the service provision. The virtual file server had to have a filesystem level backup alongside the normal virtual machine backups. These filesystem level backups had to be stored for as long as possible. This feature was implemented using the modern versioning filesystem named Btrfs.</p> <p>The result of this project was a fully functional backup infrastructure, to which new workstations or servers could be added easily. The project achieved all its goals.</p>	
Keywords	Backup, VMWare, Btrfs

# Sisällys

Alkulause

Lyhenteet ja käsitteet

1	Johdanto	1
2	Varmuuskopiointi	2
2.1	Loogiset tekniikat	3
2.1.1	Yksinkertainen varmuuskopiointi	3
2.1.2	Täydellinen varmuuskopiointi	4
2.1.3	Inkrementaalinen ja differentiaalinen varmuuskopiointi	5
2.2	Laitteisto	9
2.2.1	Perinteiset ulkoiset & sisäiset tallennusmediat	9
2.2.2	Magneettinauhat	9
2.2.3	Dedikoitu laitteisto	10
2.3	Online- ja offline-varmuuskopio	11
3	Järjestelmän suunnittelu	12
3.1	Vaatimukset	12
3.2	Varmuuskopiointiratkaisut	14
3.2.1	Työasemat	14
3.2.2	Palvelimet	15
3.2.3	Laitteisto	16
4	Järjestelmän toteutus	17
4.1	Työasemat	17
4.2	Palvelimet	21
4.2.1	Fyysiset palvelimet	21
4.2.2	Virtuaaliset palvelimet	22
4.2.3	Tiedostopalvelimen tiedostojaot	22
5	Järjestelmän testaus	25
5.1	Yksittäiset tiedostot	25

5.2	Täydellinen palautus	29
5.2.1	Työasema	30
5.2.2	Palvelin	31
6	Yhteenveto	33
	Lähteet	35
	Liitteet	
	Liite 1. Skripti 1	
	Liite 2. Skripti 2	
	Liite 3. Skripti 3	
	Liite 4. Skripti 4	
	Liite 5. Skripti 5	

## Lyhenteet ja käsitteet

AFP-protokolla	Apple Filing Protocol. Applen kehittämä tiedonsiirtoprotokolla.
Bash	Komentotulkki Unix-tyyppisille käyttöjärjestelmille.
Bash-skripti	Bash-komentotulkin ajotiedosto, johon voidaan kirjoittaa peräkkäin ajettavia komentoja.
BAT-skripti	DOS / Windows-ympäristöön tarkoitettu ajotiedosto, jossa on peräkkäin ajettavia komentoja.
Btrfs	B-tree File System. GNU/Linuxissa käytettävä moderni Copy-On-Write-tiedostojärjestelmä.
CD	Compact Disc. Optinen tallennusmedia, jonka kapasiteetti on usein 650-700 Mt.
CIFS-protokolla	Katso SMB.
Copy-on-Write	Tiedostojärjestelmien käyttämä termi tekniikalle, joka mahdollistaa tilannekuvat tiedostojärjestelmässä.
CoW	Katso Copy-on-Write.
Cron	Työkalu Unix-pohjaisille käyttöjärjestelmille, jolla voi ajastaa tehtäviä ajautumaan automaattisesti haluttuna ajankohtana.
DVD	Digital Versatile Disc. Optinen tallennusmedia, jonka kapasiteetti on usein n. 4,5 Gt.
GNU/Linux	Avoimeen lähdekoodiin perustuva, usein täysin ilmainen Unixin kaltainen käyttöjärjestelmä.

IP-osoite	Tietokoneen yksilöivä numerosarja tietoverkossa.
Linux	Virallisesti GNU/Linuxin ydin (kerneli), mutta usein Linux-nimellä viitataan myös koko GNU/Linux-käyttöjärjestelmään. Katso GNU/Linux.
Metatieto	Kuvailevaa tietoa jostakin tiedosta tai tietokokonaisuudesta.
Macintosh / Mac	Applen tietokonemalli.
Mac OS X	Applen kehittämä Unix-pohjainen käyttöjärjestelmä sen Macintosh-tietokoneisiin.
NAS	Network Attached Storage. Tietoverkkoon liitetty kiintolevy, johon pääse käsiksi erilaisilla verkkoprotokollilla. Tyypillisesti vähän USB-kiintolevyä suurempi laite, joka vaatii myös oman virransyötön.
NFS	Network File System. Yleensä Unix-ympäristöissä käytetty tiedonsiirto- ja jakokokonaisuus.
NTFS	Microsoftin kehittämä tiedostojärjestelmä, jota käytetään oletuksena mm. Windows XP:ssä ja Windows 7:ssä.
OS X	Katso Mac OS X.
RAID	Redundant array of independent disks. Tekniikka, jolla voidaan kasvattaa kiintolevyjen vikasietoisuutta tai luoda monesta levystä yksi suuri looginen osio.
Solaris	Alunperin SUN Microsystemsin kehittämä Unix-käyttöjärjestelmä. Nykyisin kaupallisesta kehityksestä vastaa Oracle.



SFTP-protokolla	SSH:n yli tapahtuva tiedonsiirtoprotokolla. Tiedonsiirto tapahtuu salattuna.
SMB-protokolla	Windows-levyjakoihin käytettävä tiedonsiirtoprotokolla.
SSH	Secure Shell. Etäterminaaliympäristö, jonka verkkoliikenne on salattua.
Unix	Käyttöjärjestelmä tai käyttöjärjestelmäfilosofia, joka kehitettiin vuonna 1969. GNU/Linux on Unix-filosofiaan perustuva Unix-variantti.
USB	Universal Serial Bus. Sarjaväyläarkkitehtuuri, joka mahdollistaa oheislaitteiden liittämisen tietokoneeseen.
VMware ESXi	VMWare Inc:n kehittämä ja kaupallistama tietokonevirtualisointiin tarkoitettu käyttöjärjestelmä.
VMware vSphere Client	VMware ESXi:n hallintatyökalu.
ZFS	Zettabyte File System. Alun perin SUN Microsystemsin kehittämä Copy-On-Write-tiedostojärjestelmä Solaris Unixille. Nykyään kaupallisesta kehityksestä vastaa Oracle.

## 1 Johdanto

Tämä insinööri työ käsittelee varmuuskopiointijärjestelmän suunnittelua, toteuttamista ja testausta PK-yritykselle. Työ tehtiin kokonaisuudessaan Vantaalla loppuvuodesta 2011 ja alkuvuodesta 2012 TAG Systems Finland Oy:lle. TAG Systems on kansainvälinen älykorttituotantoon keskittynyt yritys, jolla on tuotantoa myös Suomessa. Työssä ei kerrota turvallisuussyistä TAG Systemsin tuotantoon liittyvistä asioista, eikä siihen olisi ollut tarvetta, sillä tietoverkot tuotannon ja toimistopuolen välillä ovat täysin eriytyneet, ja tämä työ koskee vain TAG Systemsin toimistopuolen varmuuskopiointijärjestelmää.

TAG Systems uusi laitekantansa toimistoonsa syksyllä 2011. Vanhaa varmuuskopiointijärjestelmää ei ollut järkevää hyödyntää uusissa laitteissa, sillä suuri osa uusista palvelimista oli virtualisoituja ja työasemissa pystyttiin hyödyntämään käyttöjärjestelmiin sisäänrakennettuja varmuuskopiointiominaisuuksia. Tämän vuoksi erillisiä ohjelmistohankintoja ei tarvinnut tehdä.

Työ sisältää myös tietoa erilaisista varmuuskopiointimenetelmistä ja -tekniikoista, sillä niihin tuli tutustua laajasti työn suunnitteluvaiheessa. Kaikki työssä esiintyvät skriptit ja koodiesimerkit ovat osa työtä, ja ne laadittiin sitä varten, ellei toisin mainita.

Työn tavoitteena oli suunnitella ja toteuttaa TAG Systems Finland Oy:lle toimiva varmuuskopiointijärjestelmäkokonaisuus yrityksen toimistossa työskentelevän henkilöstön työasemille ja palvelimille. Toteutuksen yhteydessä järjestelmä tuli testata toimivaksi. Yksi työn tavoitteista oli myös tietoteknisen ammattitaidon kasvattaminen varmuuskopiointitekniikoissa.

## 2 Varmuuskopiointi

Varmuuskopiointilla tietotekniikassa tarkoitetaan tietokoneen levyillä olevan tiedon varmentamista. Se on tärkeä osa yrityksen tietoteknisen infrastruktuurin rakennetta, vaikka yleensä sitä hyödynnetään vain esimerkiksi levyrikon tai vahingossa poistettujen tiedostojen palauttamisen yhteydessä. Monesti tästä syystä erityisesti pienissä yrityksissä varmuuskopiointiin ei resursoida tarpeeksi ja tietokoneisiin saatetaan luottaa liian sokeasti, kunnes joku poistaa vahingossa pysyvästi hakemistollisen tärkeitä tiedostoja tai virtapiikki mykistää tärkeän tiedostopalvelimen kaikki kiintolevyt. [1, s. 25; 2.] Siksi yrityksen on hyvä tehdä suunnitelma, kattava dokumentointi ja käyttää riittävästi resursseja varmuuskopiointia varten.

Yrityksessä hyvin toteutettu varmuuskopiointi on lähes huomaamaton ja täysin automatisoitu toimenpide. Sen tulisi näkyä käyttäjälle ja IT-ylläpidolle vain ilmoituksina virhetilanteista tai varoituksina siitä, että on kulunut liian pitkä aika viimeisestä varmistuksesta. Lisäksi yrityksessä käyttäjille voidaan antaa koulutusta yksittäisten tiedostojen omatoimisesta palauttamisesta työasemaan.

Varmuuskopiointi-termiä käytetään joskus virheellisesti tilanteissa, joissa todellisuudessa on kyse palvelun saatavuuden varmentamisesta. Esimerkiksi palvelimen kiintolevyjen konfiguroinnista RAID-pakkaan ei voida puhua varmuuskopiointista [3.], vaan sillä varmistetaan vain, että yhden tai useamman levyn rikkoutuessa tietoa ei menetetä ja palvelin jatkaa toimintaansa lähes normaalisti. Toinen esimerkki on tilanne, jossa palvelimen tietokantaa tai tiedostoja replikoidaan toiseen identtiseen järjestelmään. Tällä saavutetaan se etu, että ensisijaisen laitteiston hajotessa on mahdollista saada palvelut lähes reaaliajassa saataville toissijaiselta palvelimelta. Usein juuri näitä toissijaisia palvelimia saatetaan kutsua virheellisesti ”backup-palvelimeksi”. Oikeaoppisesti ”backup-palvelin”-termiä tulisi käyttää palvelimesta, jonka pääasiallinen tehtävä on varmuuskopioiden säilyttäminen tai niiden ottaminen [4].

Varmuuskopiointia on monenlaista ja siinä voidaan hyödyntää useita eri tekniikoita. Yksinkertaisimmillaan varmuuskopiointi voi olla tärkeiden tiedostojen kopioimista työasemalta USB-muistitikulle, mutta toisaalta taas suurissa palvelinfarmeissa varmuuskopiointiin saatetaan käyttää hyvinkin monimutkaisia menetelmiä.

Kuten tietotekniikassa yleensä, voidaan varmuuskopiointimenetelmätkin jakaa loogiseen ja fyysiseen puoleen. Loogisella puolella käsitellään, sitä miten varmuuskopiointi tapahtuu teoria- tai ohjelmistotasolla. Fyysisellä puolella käsitellään sitä laitteistosta, johon varmuuskopiot fyysisesti tallennetaan.

## 2.1 Loogiset tekniikat

### 2.1.1 Yksinkertainen varmuuskopiointi

Aikaisemmin luvussa kaksi mainittiin, että yksinkertaisimmillaan varmuuskopiointi voi olla tärkeiden, ennalta määrättyjen tiedostojen kopioimista USB-muistitikulle. Toinen esimerkki yksinkertaisesta varmuuskopioinnista voi olla Microsoft Windowsissa "My Documents" -hakemiston tai koko C:\ -osion kopioimista kaikkine tiedostoineen NAS:lle tai toiselle työaseman kiintolevyille. Jos tiedostoista otetaan joskus uudestaan kopioita vanhan päälle, niin vanhempi varmuuskopio katoaa ja tiedostoista jää jäljelle vain ne versiot, mitä ne olivat kopioinnin aikana. Tämä tarkoittaa sitä, että tekniikka ei ole versioiva varmuuskopiointimenetelmä. Yleensä tällä tekniikalla saavutetaan varmistus siitä, että tietokoneen levyn rikkoutuessa voidaan tiedostot kopioida takaisin, mutta se ei säästä käyttäjää mahdolliselta käyttöjärjestelmän uudelleenasetukselta.

Yksinkertaisessakin varmuuskopioinnissa on varmuuskopioitavat tiedostot kopioitava aina fyysisesti eri levyille tai laitteelle kuin mistä tiedostoja kopioidaan. Ei ole mielekäästä kopioida tiedostoja fyysisen levyn sisällä hakemistosta tai levyosiosta toiselle, koska levyn rikkoutuessa hyvin todennäköisesti kaikki levyllä olevat tiedot menetetään.

### 2.1.2 Täydellinen varmuuskopiointi

Täydellisellä varmuuskopiointilla (full backup) tarkoitetaan sitä, että tietokoneesta tai sen levystä otetaan täydellinen kopio, josta yleensä syntyy yksi suuri tiedosto. Näitä tiedostoja kutsutaan usein myös levykuviksi (disk image) ja niihin sisällytetään usein jopa käynnistyssektori. Tämä tarkoittaa sitä, että täydellisen varmuuskopion palauttamisen ja uudelleenkäynnistyksen jälkeen tietokone on siinä tilassa, kuin mitä se oli varmuuskopiota otettaessa. Levykuvatiedostot ovat usein niin suuria, että niiden säilömiseen tarvitaan joko ulkoinen USB-kiintolevy tai NAS. Täydellisten varmuuskopioiden palauttamiseen vaaditaan yleensä tietokoneen käynnistäminen suoraan palautusohjelmistoon. Tällöin tietokone käynnistetään CD- tai USB-käynnistykseällä, joka sisältää ohjelmiston levykuvan palauttamiseen.

Joissakin tapauksissa käyttöjärjestelmän oma varmuuskopiointiohjelmisto voi käyttää ”täydellinen varmuuskopiointi” -termiä, jolloin otetaan kopio kaikesta käyttöjärjestelmän asetuksista, käyttäjän tiedoista, tiedostoista sekä asennetuista ohjelmista. Ohjelmisto ei kuitenkaan todellisuudessa ota kokonaisuutta levykuvakopiota. Tämä varmuuskopio palautetaan heti käyttöjärjestelmän uudelleenasetuksen jälkeen. Yleensä näissä tapauksissa vaatimuksena on kuitenkin se, että uudelleenasetettu käyttöjärjestelmä ja sen versio ovat samoja kuin se, mistä varmuuskopio on aikaisemmin otettu.

Täydellistä varmuuskopiointia voidaan hyödyntää myös virtuaalipalvelimien varmuuskopioimisessa. Tämä tapahtuu siten, että virtuaalikoneesta ja / tai sen levykuvista otetaan tilannekuva (snapshot), jonka jälkeen virtuaalikone ja sen levykuvat kopioidaan kokonaisuudessaan toisaalle. Tilannekuvan ottaminen sallii virtuaalikoneen jatkaa toimintaansa normaalisti varmuuskopiointin aikana. Nyt esimerkiksi virtualisointialustan levyjärjestelmän rikkoutuessa voidaan alustavien korjaustoimenpiteiden jälkeen helposti palauttaa nämä kokonaiset levykuvat ja muu metatieto (metadata) virtuaalikoneesta takaisin virtualisointialustalle. Tämän jälkeen se käynnistetään tilannekuvasta, jolloin tilanne palautuu siihen pisteeseen, jossa se oli ennen varmuuskopiointin alkamista. Jos levytilaa on tarpeeksi, voidaan edelliset virtuaalikoneiden kopiot säilyttää, joka mahdollistaa aikaisempien tilanteiden palauttamisen. Tästä on hyötyä esimerkiksi silloin, kun virtuaalikoneen käyttöjärjes-

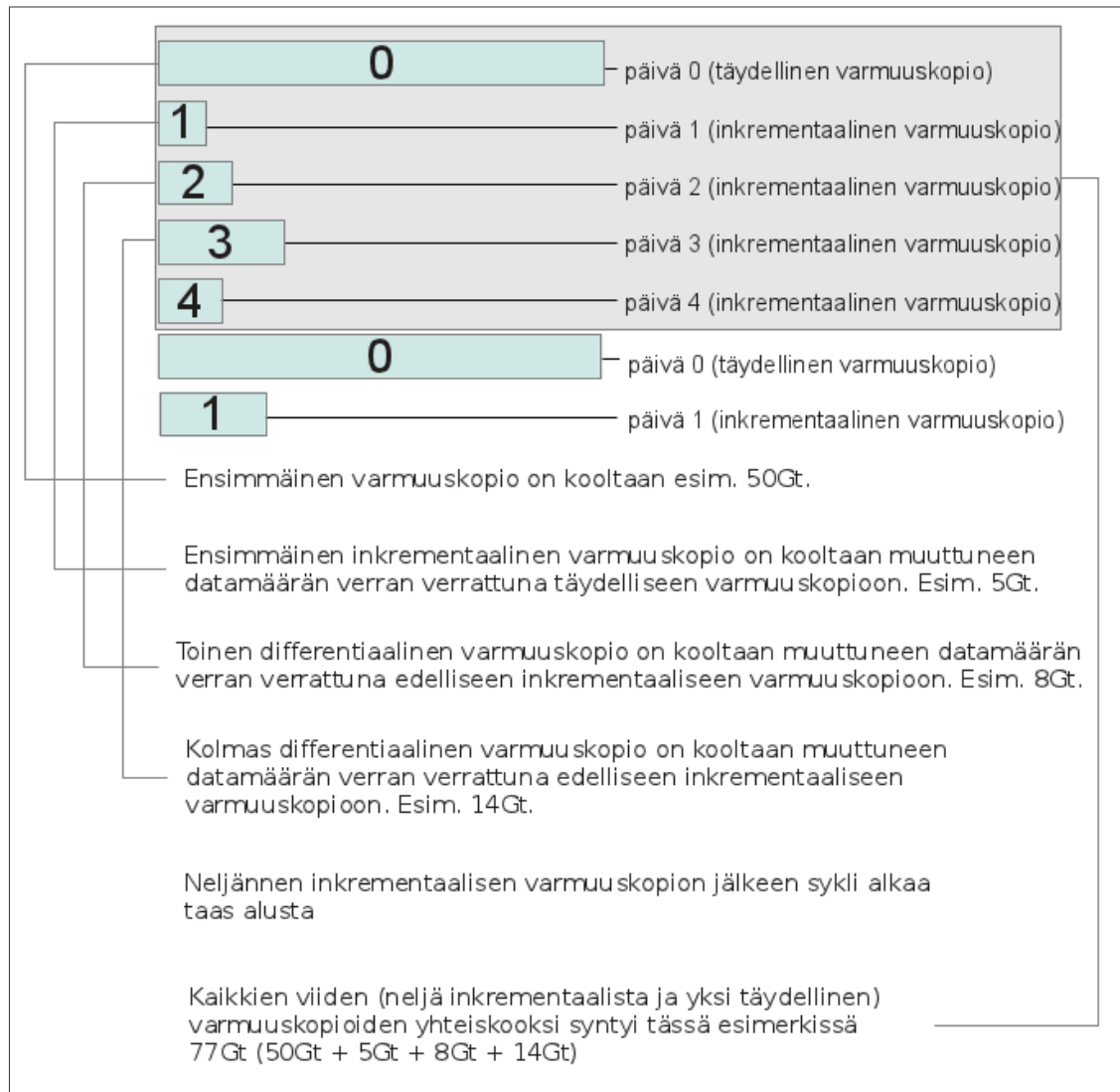
telmään asennetun päivityksen aiheuttama vika huomataan vasta muuttaman varmuuskopiointin jälkeen.

### 2.1.3 Inkrementaalinen ja differentiaalinen varmuuskopiointi

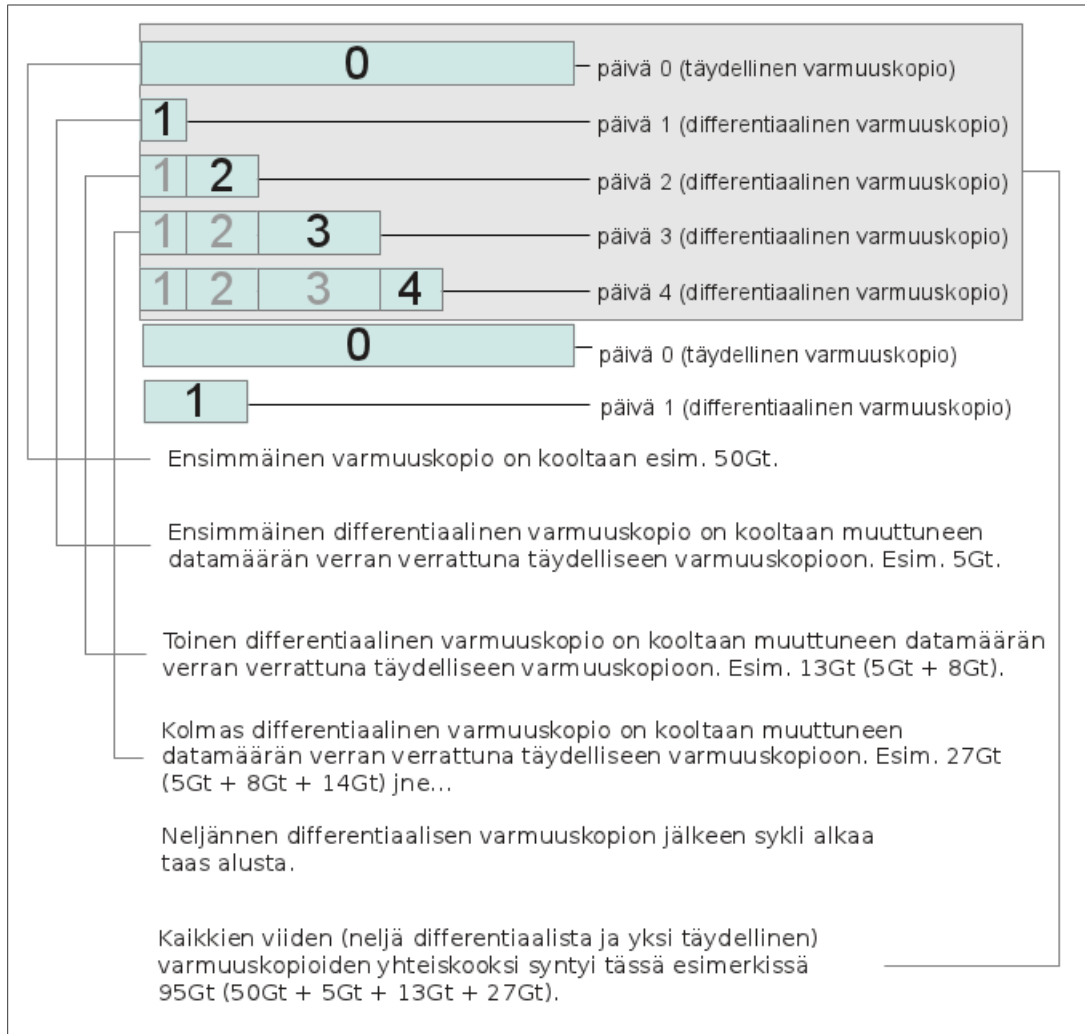
Inkrementaalista ja differentiaalista varmuuskopiointia käytetään usein silloin, jos varmuuskopiointin hoitaa erillinen varmuuskopiointiohjelmisto tai tarpeeksi kehittynyt käyttöjärjestelmään integroitu varmuuskopiointiominaisuus. Näitä varmuuskopiointitekniikoita voidaan kutsua myös versioiviksi varmuuskopiointitekniikoiksi, sillä ne mahdollistavat tiedostoista monen eri version säilyttämisen. Inkrementaalinen ja differentiaalinen varmuuskopiointi perustuu siihen, että aluksi tietokoneesta tai sen tiedostoista otetaan ensin täydellinen varmuuskopio (full backup) ja myöhemmin kopioidaan vain muuttuneet tiedostot tai tiedoston osat. Tyypillisesti tämänkaltaisen varmuuskopiointi tapahtuu usein jonkinlaisessa syklissä, jossa esimerkiksi täydellinen varmuuskopio otetaan kerran viikossa. Muina päivinä otetaan joko inkrementaalisia tai differentiaalisia varmuuskopioita tätä täydellistä varmuuskopiota vasten.

Inkrementaalisen ja differentiaalisen varmuuskopiointin olennainen ero on se, että inkrementaalissa varmuuskopiointissa tiedostojen muutosvertailu tehdään aina edelliseen varmuuskopioon, olipa se sitten toinen inkrementaalinen tai täydellinen kopio (kuva 1). Differentiaalissa varmuuskopiointissa vertailu tehdään aina vain viimeisimpään täydelliseen varmuuskopioon (kuva 2). Tämä kuluttaa enemmän levytilaa kuin inkrementaalinen varmuuskopiointi, mutta se sallii differentiaalisten varmuuskopioiden poistamisen jostakin välistä. Jos inkrementaalissa varmuuskopiointissa välistä poistetaan yksikin varmuuskopio, niin kaikki siitä myöhemmät inkrementaaliset varmuuskopiot korruptoituvat.

Tätäkin varmuuskopiointitekniikkaa koskee nyrkkisääntö, jonka mukaan varmuuskopiot tulee ottaa aina fyysisesti eri levyille tai laitteelle, sillä levyn rikkoutuessa kaikki samalla levyllä olevat tiedostot ja levyosiot hyvin todennäköisesti menetetään.



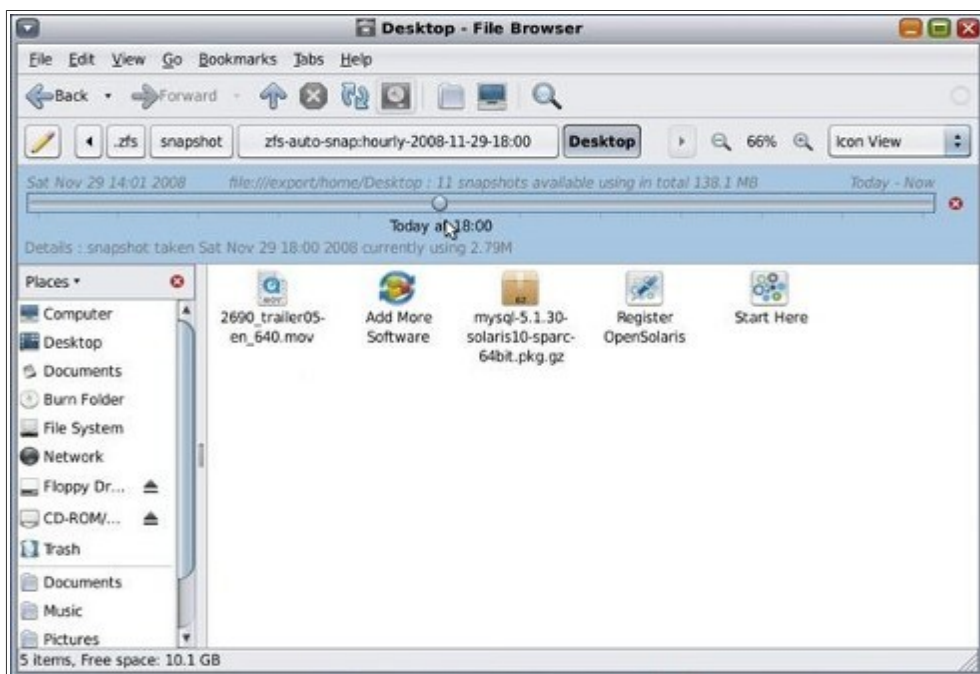
Kuva 1: Inkrementaalinen varmuuskopiointi.



Kuva 2: Differentiaalinen varmuuskopiointi.



On myös olemassa moderneja Copy-on-Write-tiedostojärjestelmiä, kuten Oraclen ZFS, GNU/Linuxin Btrfs tai Microsoftin Windows 8:n julkistuksen myötä tuleva ReFS [5.], joista voidaan sanoa, että ne osaavat tehdä inkrementaalista varmuuskopiointia tiedostojärjestelmätasolla. Microsoftin NTFS:ään tämä on toteutettu sovellustasolla Volume Shadow Copy -menetelmällä. Tämä tarkoittaa sitä, että tiedostoista, hakemistoista tai kokonaisista levyosioista voidaan ottaa tilannekuvia, joista voidaan palauttaa tiettyjä tiedostoja tai peruuttaa tehtyjä muutoksia (rollback). Käyttöjärjestelmässä voi esimerkiksi pyöriä jonkinlainen palvelu, joka ottaa aina tietyin väliajoin tilannekuvan ennalta määritellyistä hakemistoista. Tiedostohallintaan tarkoitettulla työkalulla voi kätevästi selata ja palauttaa edellisiä versioita tiedostoista (kuten Solariksen Time Slider ominaisuus, kuva 3). On hyvä kuitenkin muistaa, että jos tiedostojärjestelmä rakentuu vain yhden levyn varaan, niin nämä tilannekuvat eivät pelasta fyysiseltä levyrikolta. ZFS ja Btrfs kuitenkin tukevat levyjen liittämistä tiedostojärjestelmään integroituu, ohjelmistopohjaiseen RAID-pakkaan, jolloin yksittäiset levyrikot eivät vielä aiheuta tiedostokatoa. ZFS tukee myös näiden tilannekuvien kopioimista tai ns. lähettämistä (send) toiselle levyille tai verkon yli kokonaan toiselle tietokoneelle.



Kuva 3: Oracle Solariksen Time Slider -ominaisuus tiedostoselaimessa.

## 2.2 Laitteisto

### 2.2.1 Perinteiset ulkoiset & sisäiset tallennusmediat

Tänä päivänä hinta-tallennuskapasiteetti-suhteeltaan hyvät vaihtoehdot varmuuskopiointiin kotikäytössä ja PK-yrityksissä ovat perinteiset ulkoiset ja sisäiset tallennusmediat, kuten USB-muistitikut ja -kiintolevyt, CD/DVD-levyt, NAS-laitteet [6]. CD:ssä tai DVD:ssä on kuitenkin rajoitettu kapasiteetti ja hidas tallennusnopeus. Myös ylikirjoittaminen on yleensä hidasta ja hankalaa [7]. Nykyisin USB-muistitikut ovatkin korvanneet optiset mediat varmuuskopiointimediana. USB-muistitikuissakin kapasiteetti on myös rajallinen kiintolevyihin verrattuna, joten ainakin täydelliseen tai inkrementaaliseen / differentiaaliseen varmuuskopioimiseen paras ratkaisu kotikäyttöön ja PK-yrityksen työasemien varmuuskopioimiseen on USB-kiintolevy tai NAS.

PK-yrityksessä yksi vaihtoehto voi olla myös erillinen varmuuskopiointipalvelin, josta kerrotaan tarkemmin kappaleessa 2.1.2.3. Pienissä, alle kolmenkymmenen työaseman työympäristöissä kuitenkin riittävällä kapasiteetilla varustettu NAS riittää työasemien varmuuskopioimiseen.

### 2.2.2 Magneettinauhat

Magneettinauhat ovat vanha ja suhteellisen luotettava varmuuskopiointimedia [8, s. 37]. Niitä käytetään pääasiassa yrityksissä palvelimien varmuuskopioimiseen, ja ne ovat kapasiteetiltaan sen verran suuria, että nauhoille voidaan ottaa täydellisiä varmuuskopioita.

Tyypillisesti magneettinauhavarmuuskopiointi toimii siten, että varmuuskopioitavaan palvelimeen liitetään nauha-asema (kuva 4). Se ottaa palvelimesta täydellisen varmuuskopion joka yö. Jos nauha-asemasta löytyy automaattinen kasetinvaihto-ominaisuus, voidaan varmuuskopioita säilyttää esimerkiksi viikon ajan, kunnes sykli alkaa taas alusta ja vanhin nauha ylikirjoitetaan.



Kuva 4: Sunin nauha-asemarobotti.

Magneettinauhat ovat kuitenkin viime vuosina hieman harvinaistuneet, mutta eivät kokonaan hävinneet. Nauha-asemien kallis hinta, kiintolevyjen halpeneminen ja varmuuskopioiden hankala palauttaminen ovat verottaneet magneettinauhujen suosiota varmuuskopiointimediana. Nykyisin magneettinauhuja käytetään usein varmuuskopion varmuuskopiointiin. Tätä kutsutaan ”levy-levy-nauha”-menetelmäksi. [1, s. 28; 9.]

### 2.2.3 Dedikoitu laitteisto

Varmuuskopiointiin dedikoidulla laitteistolla tarkoitetaan palvelinta tai jotakin muuta laajempaa järjestelmää, jonka pääasiallinen tarkoitus on varmuuskopioiden ottaminen sekä niiden säilyttäminen ja hallitseminen. Yksinkertaisimmillaan varmuuskopiointipalvelin voi olla tiedostopalvelin, joka tarjoaa yrityksen lähiverkkoon levykapasiteettia, johon palvelimet ja työasemat voivat tallentaa varmuuskopionsa. Monimutkaisempi varmuuskopiointipalvelin ottaa automaattisesti varmuuskopioita kohdejärjestelmistä, säilyttää niitä tietyn aikaa ja poistaa automaattisesti vanhimpia kopioita. Lisäksi palvelin voi automaattisesti ylläpitää jonkinlaista tilannekuvajärjestelmää (snapshot

controlling) yrityksen tiedostopalvelimesta, jolloin yksittäisten tiedostojen palautus on käyttäjälle helpompaa.

Varmuuskopiointiin dedikoitujen palvelimien varmuuskopiointiohjelmisto voi koostua laajasta kirjosta ohjelmia, joista rakennetaan toimiva kokonaisuus automatisoimalla skriptejä, jotka ajavat näitä ohjelmia. Vaihtoehtoisesti voidaan käyttää varmuuskopiointien keskitettyyn hallintaan tarkoitettuja ohjelmistoja, kuten Amandaa, Baculaa tai BackupPC:tä.

PK-yrityksessä voi yksi dedikoitu varmuuskopiointipalvelin riittää palvelemaan kaikkia yrityksen varmuuskopiointitarpeita edellyttäen, että levykapasiteettia on riittävästi. Suuremmissa yrityksissä voidaan tarvita useita varmuuskopiointipalvelimia: jokainen yhtiä segmenttiä varten.

### 2.3 Online- ja offline-varmuuskopio

Varmuuskopioiden säilyttämisestä voidaan käyttää termejä online- ja offline-varmuuskopio. Online-varmuuskopioiksi voidaan kutsua medioita, jotka ovat aina saatavilla ja kytkettyinä järjestelmään. Pilveen tai internetiin tapahtuvaa varmuuskopiointia kutsutaan myös online-varmuuskopioinniksi, koska palvelu ja varmuuskopiot ovat aina saatavilla. Offline-varmuuskopioista voidaan puhua silloin, kun varmuuskopiomedia viedään varmuuskopioinnin jälkeen esimerkiksi paloturvalliseen kassakaappiin, jolloin se ei ole kytkettyinä mihinkään järjestelmään.

Käytännössä, online- ja offline-varmuuskopioita käytetään usein rinnan siten, että varmuuskopiointiin dedikoitu palvelin kopioi varmuuskopiot kohdejärjestelmistä omille levyille. Tämän jälkeen esimerkiksi vuorokauden tai viikon välein varmuuskopiointipalvelimesta otetaan varmuuskopio magneettinauhoille, jotka viedään tai vaihdetaan paloturvallisessa tai fyysisesti eri rakennuksessa olevien edellisten offline-varmuuskopioiden kanssa. Tällä varmistetaan se, että esimerkiksi yrityksen palvelinhuoneen ja sen laitteiston tuhoutuessa tulipalossa voidaan palata korkeintaan viikon takaiseen tilanteeseen, kun offline-varmuuskopiot paloturvallisesta säilöstä palautetaan.

### 3 Järjestelmän suunnittelu

Varmuuskopiointijärjestelmän ja infrastruktuurin suunnittelu TAG Systems Finland Oy:lle tapahtui annettujen vaatimusten ja laitteistokapasiteetin puitteissa. Vanhaa varmuuskopiointi-infrastruktuuria ei tarvinnut huomioida suunniteltaessa uutta, vaan kokonaisuutta lähdettiin suunnittelemaan niin sanotusti ”puhtaalta pöydältä”, koska toimistupuolen henkilöstön kaikki työasemat ja palvelimet olivat juuri päivityksen alla. Suunnitelmasta ei tehty mitään erityistä dokumenttia, vaan muistiinpanoja sekä yhteenvetoja itseämme varten.

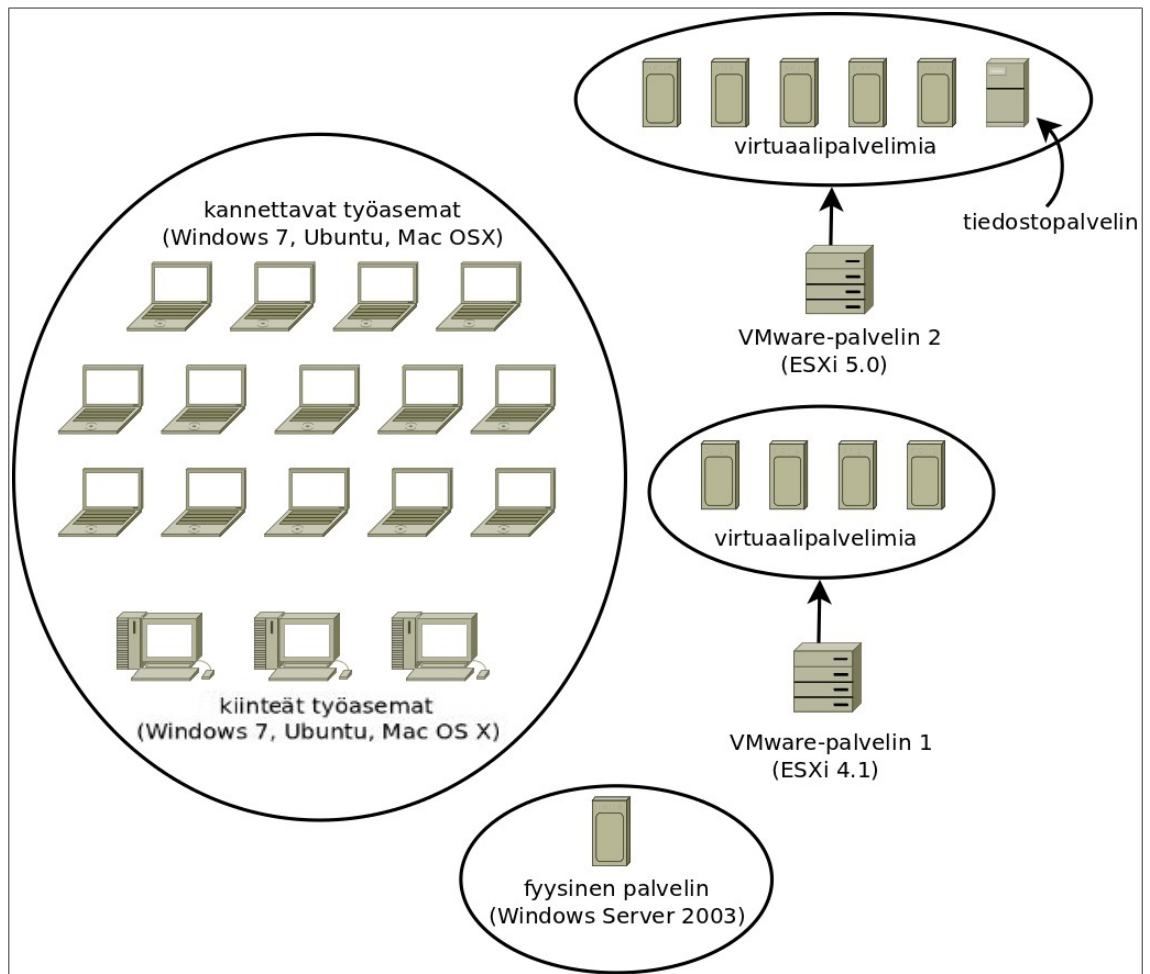
#### 3.1 Vaatimukset

Järjestelmän tuli kattaa sekä toimistohenkilöstön työasemat että myös kaikki fyysiset ja virtuaaliset palvelimet (kuva 5). Työasemista tuli ottaa täydellisiä varmuuskopioita siten, että koko työaseman tai sen järjestelmälevyn vaihtuessa pystyttiin vanha käyttöjärjestelmä kokonaisuudessaan ja kaikki tiedostot palauttamaan siihen pisteeseen, jossa se oli ollut ennen varmuuskopion ottamista. Lisäksi työasemista tuli ottaa inkrementaalisia tai differentiaalisia varmuuskopioita siten, että käyttäjä pystyi palauttamaan yksittäisiä tiedostoja tai hakemistoja. Työasemien varmuuskopioita tuli säilyttää niin pitkään kuin se on mahdollista käytettävissä olevalla tai hankittavilla laitteistolla. Varmuuskopiointin tuli tapahtua myös mahdollisimman huomaamattomasti ja mielellään yöaikaan. Lisäksi varmuuskopiointin yhteyteen oli hyvä tehdä jonkinlainen ilmoitusjärjestelmä lähettämään sähköpostia henkilölle silloin, kun hänen työasemastaan ei syystä tai toisesta ollut otettu riittävän pitkään aikaan varmuuskopiota.

Fyysisistä palvelimista tuli ottaa tapauskohtaisesti joko täydellisiä varmuuskopioita joka yö tai sitten ainoastaan tietyistä tiedostoista ja hakemistoista inkrementaalista varmuuskopiota. Virtuaalisista palvelimista tuli ottaa täydellisiä levykuvia metatietoineen arkiöisin ja säilyttää niitä mahdollisimman pitkään. Toimistupuolen tiedostopalvelimen tiedostojaoista tuli myöskin ottaa erilliset inkrementaaliset tai differentiaaliset varmuuskopiot, joihin IT-

henkilöstö pääsee tarvittaessa käsiksi mahdollisimman helposti. Näitä varmuuskopioita tuli säilyttää myös niin pitkään kuin mahdollista.

Järjestelmän suunnittelun ja rakentamisen jälkeen sitä tuli testata niin, että kaikki sen osat toimivat niin kuin ne oli suunniteltu. Tämä voitiin toteuttaa virtuaalisesti.



Kuva 5: Ympäristön looginen kartta (varmuuskopioitavat laitteet ympyröitynä).

## 3.2 Varmuuskopiointiratkaisut

### 3.2.1 Työasemat

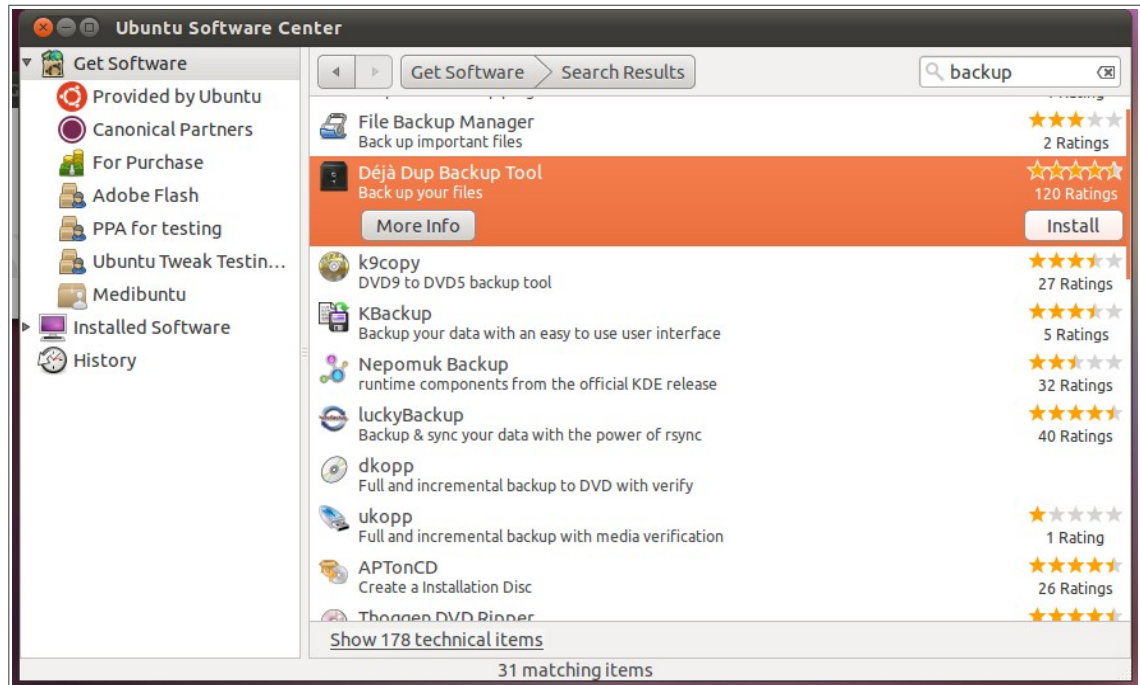
Aiemmin työasemien käyttöjärjestelmänä oli Microsoft Windows XP, ja varmuuskopiointiin oli käytetty Symantecin valmistamaa Norton Ghost -ohjelmistoa. Nyt uusittujen työasemien käyttöjärjestelmä oli pääasiassa Microsoft Windows 7:aa, mutta muutamia Mac OS X 10.6:lla ja Ubuntu 10.04:lla varustettuja työasemiakin löytyi. Näihin jokaiseen tuli suunnitella oma käyttöjärjestelmäkohtainen ratkaisu. Tavoitteena oli, että kaikista työasemista saataisiin varmuuskopiot toimistoverkossa oleville NAS-laitteille tai erilliselle varmuuskopiointipalvelimelle.

Windows 7:ssa oli uusittu Windowsin omaa, käyttöjärjestelmään integroitua varmuuskopiointiratkaisua merkittävästi [10, s. 7]. Tämän vuoksi Windows-työasemien varmuuskopiointi suunniteltiin siten, että se rakennettaisiin Windows 7:n oman varmuuskopiointityökalun varaan. Windows 7:n varmuuskopiointiohjelmisto tuki vaadittuja ominaisuuksia: inkrementaalista varmuuskopiointia ja varmuuskopioinnin pystyi konfiguroimaan tapahtumaan automaattisesti joka yö niin, että käyttäjä tuskin tiedosti varmuuskopioinnin edes tapahtuvan. Lisäksi siitä löytyi täydellisen palautuksen mahdollistava toiminto ja varmuuskopiot oli mahdollista tallentaa verkkolevylle [11].

Mac OS X:llä varustettuja työasemia oli yhteensä kolme kappaletta, joista yksi oli hieman vanhempi. Siinä varmuuskopiointi hoidettiin jo OS X:n omalla Time Machine -varmuuskopiointiohjelmistolla ulkoiselle USB-kiintolevylle. Time Machine suoritti varmuuskopioinnin lähes huomaamattomasti, ja tiedostojen palautus oli helppoa graafisen käyttöliittymän kautta. Kahden uuden Mac-työaseman varmuuskopiointi suunniteltiin siten, että se rakennettiin OS X:n Time Machinen varaan.

Ubuntu-työasemien kanssa oli aluksi hieman hankalaa päättää, mitä lukuisista ohjelmistokatalogista löytyvistä, täysin ilmaisista varmuuskopiointiohjelmistoista tultaisiin käyttämään (kuva 6). Suunnitelmassa päädyttiin kuitenkin käyttämään Déjà Dup -nimistä ohjelmistoa, koska se täytti kaikki vaa-

timuksemme. Lisäksi siitä oli tulossa Ubuntu'n oletusvarmuuskopiointiohjelmisto seuraavasta Ubuntu-versiosta lähtien [12].



Kuva 6: Ubuntu'n ohjelmistokatalogin hakutulokset sanalle "backup".

### 3.2.2 Palvelimet

Fyysisiä, varmuuskopioitavia palvelimia oli vain yksi, sillä VMware ESXi -virtualisointialustoja ei suunnitelman mukaan aiottu erikseen varmuuskopioida, koska niissä pyörivien virtuaalikoneiden varmuuskopiointi oli riittävä. Tämä jäljelle jäänyt fyysinen palvelin oli Windows 2003 Server -käyttöjärjestelmällä varustettu tuotannon testipalvelin, joka oli vähäisellä käytöllä. Tämän palvelimen varmuuskopiointissa suunniteltiin hyödynnettävän Windows 2003 Serverin omaa varmuuskopiointiohjelmistoa. Riittävää oli, että testipalvelimesta kaikista tiedostoista otettaisiin varmuuskopio kerran viikossa ja niitä säilytettäisiin mahdollisimman pitkään.

Varmuuskopioitavia virtuaalipalvelimia oli yhteensä kuusi kappaletta, ja ne pyörivät kahdella eri virtualisointipalvelimella. Molemmissa niissä pyöri VMware ESXi -käyttöjärjestelmä, mutta toisessa ESXi:n versio oli 4.1 ja toi-



sessä 5.0. VMware ESXi:n virtuaalikoneiden varmuuskopioimiseen oli olemassa kaupallisia ratkaisuja, kuten VMwaren oma Consolidated Backup, PHD:n valmistama esXpress ja Vizioncoren vRanger Pro. Näiden lisenssimaksut olivat kuitenkin TAG Systemsin IT-ympäristön kokoon nähden liian korkeita, joten virtuaalipalvelimien varmuuskopiointi suunniteltiin siten, että siinä käytettäisiin ilmaista vaihtoehtoa nimeltään GhettoVCB. GhettoVCB oli VMware-käyttäjyhteisön kehittämä ilmainen, avoimeen lähdekoodiin perustuva Bash-skripti, jolla pystyi varmuuskopioimaan VMware-ympäristössä pyöriä virtuaalikoneita VMwareen liitetulle NFS-tiedostojaolle tai paikalliselle levyille. Virtuaalipalvelimien varmuuskopiointi suunniteltiin siten, että täydelliset varmuuskopiot otettaisiin joka yö ja niitä säilytettäisiin mahdollisimman pitkään.

Tiedostopalvelimen kohdalla lisävaatimuksena oli, että tiedostoista ja hakemistoista, joita palvelin jakoi, tuli ottaa erilliset inkrementaaliset tai differentiaaliset varmuuskopiot joka arkiyö. Tiedostopalvelin itsessään oli yksi varmuuskopioitavista virtuaalikoneista, mutta tiedostotason inkrementaalinen varmuuskopiointi suunniteltiin toimivan siten, että siinä hyödynnettäisiin erillistä varmuuskopiointipalvelinta. Siihen asennettaisiin Ubuntu GNU/Linux ja yksi palvelimen levyistä tai levyosioista alustettaisiin Btrfs:ksi. Kuten luvussa 2.1.3 kerrottiin, Btrfs mahdollisti tilannekuvien ottamisen tiedostojärjestelmästä, joten sillä voitiin toteuttaa edellä mainittu tiedostotason versioiva varmuuskopiointi tiedostopalvelimesta.

### 3.2.3 Laitteisto

Varmuuskopiointijärjestelmään varattu laitteisto koostui yhdestä palvelimesta. Se oli aikaisemmin toiminut tiedosto- ja domain-palvelimena ja nyt tehtiin varmuuskopiointipalvelin. Käyttäjärjestelmäksi siihen suunniteltiin Ubuntu GNU/Linuxia. Lisäksi suunniteltiin, että palvelimeen lisätään levytilaa. Palvelimen lisäksi työasemien varmuuskopiointien säilyttämistä varten suunniteltiin hankittavan tarpeeksi suurella kapasiteetilla varustettu NAS. Magneettinauhoja, nauha-asemia tai erillisiä offline-varmuuskopioita ei suunniteltu käytettäväksi.

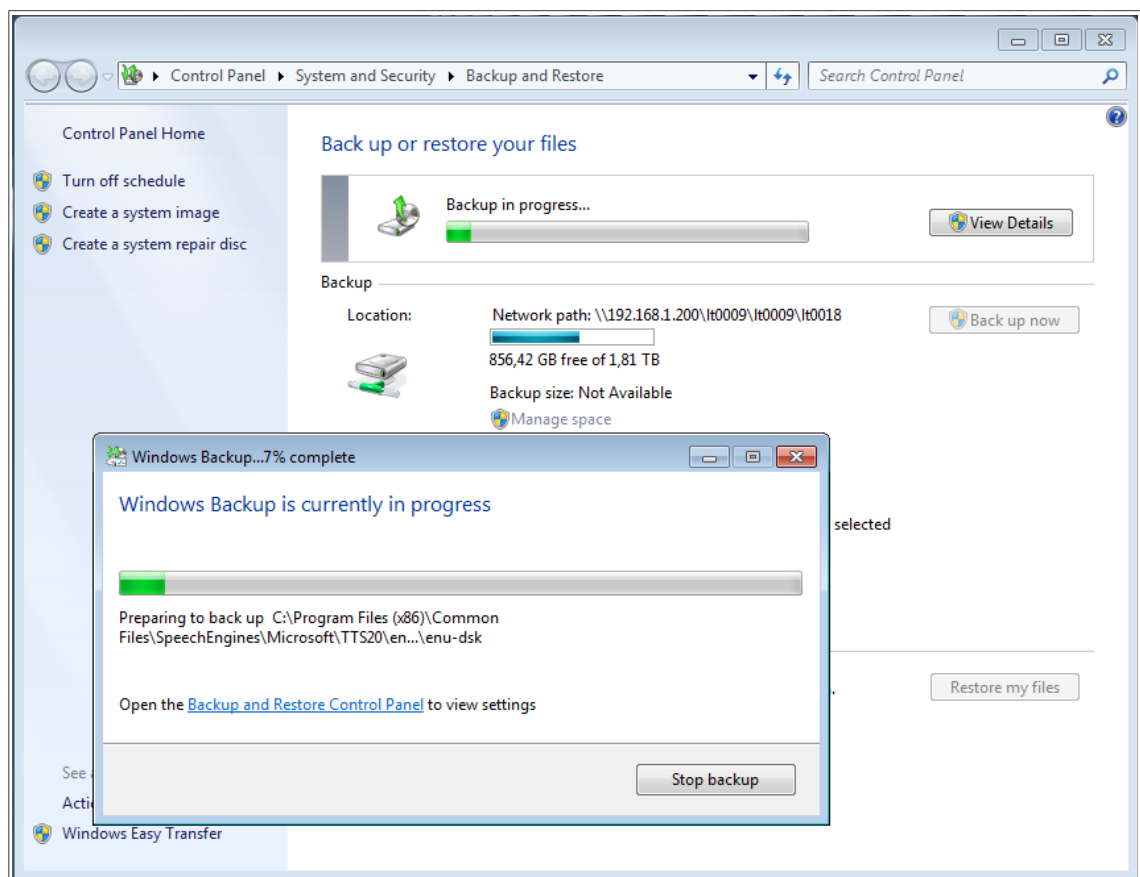
## 4 Järjestelmän toteutus

Varmuuskopiointijärjestelmä toteutettiin edellisen kappaleen suunnitelman mukaisesti. Järjestelmän rakentaminen aloitettiin työasemista, jonka jälkeen se tehtiin palvelimille. Kappaleen lopussa on toteutuneen ympäristön looginen kartta, jossa varmuuskopiointijärjestelmä on myös mukana (kuva 9).

### 4.1 Työasemat

Työasemien varmuuskopiointia varten TAG Systemsin palvelintilaan hankittiin ja asennettiin kahden teratavun tallennustilalla varustettu Western Digitalin NAS. NAS:n hankinnassa oli vaatimuksena SMB/CIFS- ja SFTP-protokollien tukeminen. Lisäksi Western Digitalin NAS mahdollisti selainpohjaisen hallintatyökalun lisäksi ottaa etäterminaaliyhteyden SSH:n kautta, jonka kautta pääsi muokkaamaan joitakin asetuksia, mitä selaimen hallintatyökalulla ei päässyt. Western Digitalin NAS:n piti tukea myös käyttäjätunnusten autentikointia Windows Active Directory domain -palvelinta vasten, mutta tätä ominaisuutta ei saatu toimimaan. Tämä johtui siitä, että NAS ei tukenut Domain functionality level 2008r2:sta [13], jolle domain oli konfiguroitu, joten jouduimme tekemään jokaiselle työasemalle omat tunnukset ja hakemistot varmuuskopiointia varten. Tämä ei kuitenkaan ollut suuri ongelma, sillä kyse oli pienestä määrästä työasemia. Mikäli työasemia tulisi lisää myöhemmin, voitiin konekohtainen tunnus luoda aina alustavan työasemakonfiguroinnin yhteydessä.

Windows-työasemien varmuuskopiointi toteutettiin Windows 7:n omalla varmuuskopiointityökalulla, joka konfiguroitiin ottamaan varmuuskopion työasemasta joka yö verkkolevylle, jonka edellisessä luvussa kuvailtu NAS työasemille jakoi. Työkalun kautta pystyi myös luomaan järjestelmän palautuslevyn (system repair disc), jonka avulla työasemalle pystyi palauttamaan täydellisen varmuuskopion tarvittaessa. Kun konfigurointi oli suoritettu loppuun, Windows alkoi heti ottaa ensimmäistä varmuuskopiota (kuva 7), eikä asetuksiin sen koommin tarvinnut enää koskea. Edelliset toimenpiteet toistettiin kaikille lopuille Windows-työasemille.



Kuva 7: Windows 7:n varmuuskopiointi käynnissä.

Windowsin varmuuskopiointi perustui tietyn väliajoin otettaviin täydellisiin varmuuskopioihin, joiden lisäksi otettiin lohkotason inkrementaalisia varmuuskopioita. Windows kuitenkin piilotti käyttäjältä tiedot siitä oliko esimerkiksi viimeksi otettu varmuuskopio täydellinen vai inkrementaalinen. NAS:lta näki kuitenkin varmuuskopioiden rakenteen, sillä Windows tallensi aina tietyn väliajoin uudet täydelliset varmuuskopiot ja siihen liittyvät inkrementaaliset varmuuskopiot erillisiin hakemistoihin.

Myöhemmin Windows-työasemien varmuuskopiointin kanssa tuli ongelmia NAS:n levyn täyttymisen vuoksi. Windows ei automaattisesti poistanutkaan vanhimpia varmuuskopioita, vaan säilytti ne kaikki alusta asti. Windows ei antanut konfiguroida, kuinka pitkään varmuuskopioita säilytetään verkkolevyllä. Paikalliselle tai USB-kiintolevyllä tämä raja pystyttiin asettamaan, mutta ei verkkolevyllä. Tästä syystä NAS:lle tehtiin Bash-skripti (liite 1), joka ajastettiin ajautumaan joka yö. Tämä skripti kävi läpi kaikki työasemien var-

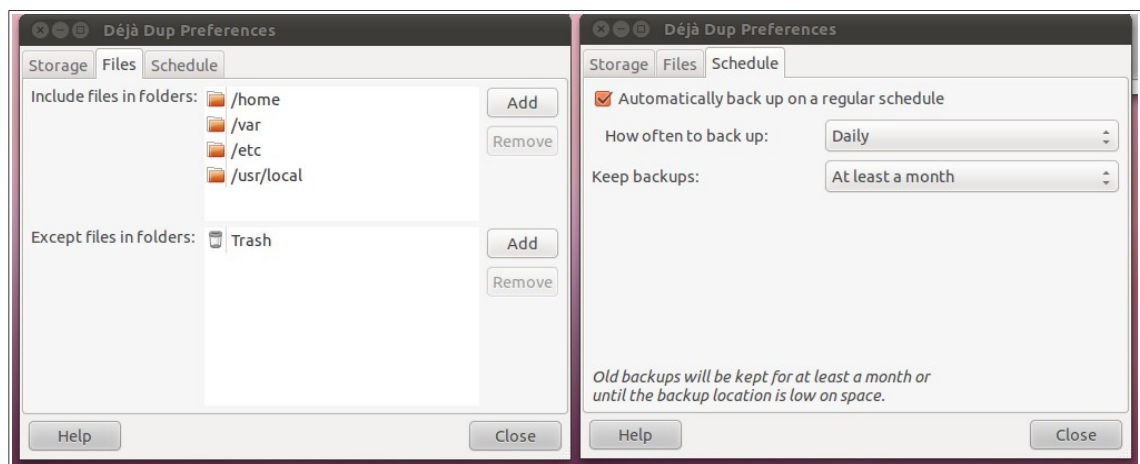
muuskopiointihakemistot ja poisti niistä yli kuukauden vanhat tiedostot. Koodiesimerkistä 1 nähdään konkreettinen komento vanhojen varmuuskopioiden poistamiseen. Skriptin ajamisen ja ajastamisen Cronilla mahdollisti Western Digitalin NAS:ssa pyörivä, lähes täysiverinen GNU/Linux -ympäristö.

```
1. find /mnt/backupnas/** \( ! -name "Download" ! -name "*.bin" ! -name
  "BASE*" ! -name "WINDOWS*" ! -name "ALL*" ! -name "*.DAT" ! -name "*.TXT" !
  -name "*.ini" ! -name "MediaId" ! -name "GlobalCatalog.wbcat" ! -name
  "virtdisk.dll.vd.log" \) -type f -mtime +30 -exec rm -rf {} \;
```

Koodiesimerkki 1: Yli 30 päivää vanhojen Windows-varmuuskopioiden poisto find-komentoa hyödyntäen Linuxissa.

Mac-työasemien varmuuskopiointi toteutettiin suunnitelman mukaisesti OS X:ään integroidun Time Machinen avulla. Ongelmia Time Machinen kanssa ilmeni kun kävi ilmi, ettei se tue varmuuskopioiden tallentamista verkkolevyille [14]. Tämä olisi ollut mahdollista, jos NAS olisi tukenut AFP-protokollaa ja sen tiettyjä ominaisuuksia. Monet NAS-laitteet mainostivat tukevansa AFP-protokollaa, mutta niistä ei silti välttämättä löytynyt kaikkia tarvittavia ominaisuuksia, joita Time Machinen käyttäminen vaati. Internetin keskustelufoorumit olivat pullollaan valituksia, kun valmistajan "X" NAS ei toiminut Time Machinen kanssa, vaikka AFP-protokollalle löytyikin tuki. Internetistä löytyi kuitenkin lista Time Machinen kanssa toimivista NAS-laitteista. Toinen vaihtoehto olisi ollut muuttaa OS X:n asetustiedostoja manuaalisesti ja pakottaa Time Machine näyttämään CIFS / SMB-verkkolevyt kohdeasemana varmuuskopioinneille. Tähän ei kuitenkaan ryhdytty, koska virallinen tuki toiminnolle ei ollut taattu. Oli siis joko hankittava toinen NAS-laite, josta löytyi tuki AFP-protokollalle ja Time Machinelle tai vaihtoehtoisesti jokaista Mac-työasemaa kohden USB-kiintolevy. Mac-työasemia oli vain kolme, joista yksi varmuuskopioitiin jo USB-kiintolevyille. Jäljelle jääneille Mac-työasemille hankittiin myös USB-kiintolevyt varmuuskopiointia varten. Hankintojen jälkeen Time Machinen konfigurointi oli yksinkertaista ja varmuuskopiointi tapahtui lähes huomaamattomasti. Sen sai myös tapahtumaan automaattisesti joka yö. Time Machine osasi myös huolehti siitä, että vanhimpia varmuuskopioita tuhotaan automaattisesti, jotta USB-kiintolevy ei täyty. Tarkkaa määrittelyä varmuuskopioiden säilymisajalle ei kuitenkaan pystytty asettamaan.

Ubuntu GNU/Linuxin varmuuskopiointiin käytettiin Déjà Dupia, kuten oli suunniteltu. Ohjelman sai haettua Ubuntun ohjelmarepositoreista suoraan, ja sen konfigurointi oli helppoa ohjelman graafisesta käyttöliittymän avulla (kuva 8). Sieltä valittiin varmuuskopioitavat tiedostot ja hakemistot, jonne ne tallennettiin sekä määriteltiin niiden säilytysaika. Ubuntu-työasemat laitetettiin tallentamaan varmuuskopiot SFTP-protokollan yli samalle NAS:lle, jota Windows-työasematkin käyttivät. Ensimmäinen varmuuskopiointi kesti hetken, jonka jälkeen se ajastettiin siten, että se tapahtui päivittäin ja täysin käyttäjän huomaamatta. Déjà Dup tarjosi mahdollisuutta myös kryptata varmuuskopiot, mutta tähän ei ollut tarvetta. Déjà Dupin varmuuskopiointi perustui tietyn ajoin tapahtuvaan täydelliseen varmuuskopioon, jonka päälle otettiin inkrementaalisia varmuuskopioita aina siihen asti, kunnes sykli alkoi alusta. Sykleistä syntyneitä edellisiä ”kokonaisuuksia” säilytettiin niin kauan kuin asetuksiin oli määritetty. Käyttäjälle ei suoraan näytetty, milloin tämä sykli oli aina alkanut ja loppunut tai mikä varmuuskopioista oli täydellinen ja mikä inkrementaalinen.



Kuva 8: Déjà Dupin asetuksia.

Pian kuitenkin huomattiin, että Déjà Dup ei tue käyttöjärjestelmän täydellistä varmuuskopiointia sillä tasolla, että sen voisi palauttaa suoraan tyhjälle levyllä käynnistyssektoria myöten. Tämä päätettiin korjata sillä, että varmuuskopioitaviksi hakemistoiksi valittiin /home (käyttäjien kotihakemistot), /etc (ohjelmien konfiguraatiodokumentit), /var (mahdollista sekalaista tärkeää dataa) ja /usr/local (paikallisesti asennetut kolmansien osapuolien ohjelmat). Lisäksi ajastimme Croniin komennon (koodiesimerkki

2), joka luetteloit työasemaan asennetut ohjelmapaketit `/etc/installed_software`-tiedostoon joka yö. Tämä helpotti järjestelmän palauttamista siten, että jos Ubuntu jouduttaisiin asentamaan kokonaan uusiksi, niin heti käyttöjärjestelmän uudelleenasetuksen jälkeen Déjà Dupilla palautettaisiin tarvittavat tiedostot työasemalle. Toimenpiteen jälkeen asennetut ohjelmat palautettaisiin asentamalla `/etc/installed_software`-tiedostoon oli listatut ohjelmat. Näin työaseman tilanne tulisi olemaan sama kuin varmuuskopiota otettaessa.

```
1. /usr/bin/dpkg -l > /etc/installed_software
```

Koodiesimerkki 2: Ubuntuun asennettujen ohjelmien luettelointi tiedostoon.

Lopuksi NAS:lle laitettiin ajautumaan kaksi kertaa viikossa Bash-skripti (liite 2), joka kävi ennalta määritetyt hakemistot läpi ja tarkasti, onko työaseman varmuuskopiointihakemiston sisältöä muokattu viimeisen kymmenen päivän aikana. Jos sisältöä ei ollut muokattu, niin se lähetti käyttäjälle sähköpostitse ilmoituksen, ettei hänen työasemastaan ole yli kymmeneen päivään otettu varmuuskopiota.

## 4.2 Palvelimet

### 4.2.1 Fyysiset palvelimet

Varmuuskopioitavia fyysisiä palvelimia oli suunnitelman mukaan vain yksi. Tästä palvelimesta tuli ottaa ainoastaan tiedostotason varmuuskopioita. Palvelimen varmuuskopiointiin käytettiin suunnitelman mukaan Windows 2003 Serverin omaa varmuuskopiointityökalua. Jotta varmuuskopiointi voitiin täysin automatisoida, tehtiin BAT-skripti (liite 3). Se luo viikoittain uuden varmuuskopion, johon kopioidaan kaikki tietokoneen tiedostot. Muina päivinä lisätään vain muuttuneet tiedostot hyödyntäen inkrementaalista varmuuskopiointia. Kun viikko vaihtuu, alkaa sykli taas alusta. Varmuuskopiotiedostot nimettiin varmuuskopio-viikkoX.bkf-tyylillä, jossa X-kirjain on aina meneillään olevan viikon numero. Skripti poisti myös automaattisesti yli 60 päivää vanhat varmuuskopiot. Tämä BAT-skripti laitettiin Windowsin ajastettujen tehtävien kautta ajautumaan joka yö.

#### 4.2.2 Virtuaaliset palvelimet

Virtuaalisten palvelinten varmuuskopiointiin hyödynnettiin VMware-yhteisön kehittämää ilmaista ja avointa lähdekoodia olevaa GhettoVCB Bash -skriptiä [15]. GhettoVCB:n toimintaperiaate oli se, että se ajettiin suoraan VMware-ympäristössä ja se otti varmuuskopioitavasta virtuaalikoneesta reaaliaikaisen tilannekuvan (snapshotin), jonka jälkeen virtuaalikone ja sen metatiedostot kopioitiin konfiguraatitiedostossa määriteltyyn paikkaan. Reaaliaikainen tilannekuva mahdollisti sen, ettei virtuaalikone tiedostanut varmuuskopioinnin olevan käynnissä, eikä sen toimintaan tullut minkäänlaista katkoa sen aikana. Varmuuskopioinnin jälkeen virtuaalikoneen tilannekuva poistettiin.

Virtuaalipalvelimien varmuuskopiointi rakennettiin varmuuskopiointipalvelimelle. Palvelin jakoi NFS:n kautta levyn VMware-ympäristöön, jonne varmuuskopiot otettiin. Tämä NFS-jako tuli konfiguroida VMware-ympäristöön VMwaren vSphere Client -hallintatyökalulla. Toimenpide käynnistettiin aina varmuuskopiointipalvelimelta käsin niin, että Croniin oli ajastettu erillinen Bash-skripti ajautumaan arkiöisin. Se kopioi ensin GhettoVCB:n ja sen konfiguraatitiedoston VMware-ympäristöön. Tämän jälkeen se käynnisti itse varmuuskopioinnin VMware-ympäristössä SSH:n yli etänä. Lisäksi tämä erillinen Bash-skripti (liite 4) poisti vanhat varmuuskopiot ennen GhettoVCB:n käynnistämistä. Toimenpiteen päätteeksi varmuuskopiointipalvelin lähetti yhteenvedon ja lokitiedoston IT-ylläpidolle sähköpostitse.

Virtuaalipalvelimien täydelliset varmuuskopiot veivät hyvin paljon tilaa ja niitä pystyttiin säilyttämään vain viikon ajan, jonka jälkeen vanhimmat kopiot poistettiin uusien tieltä.

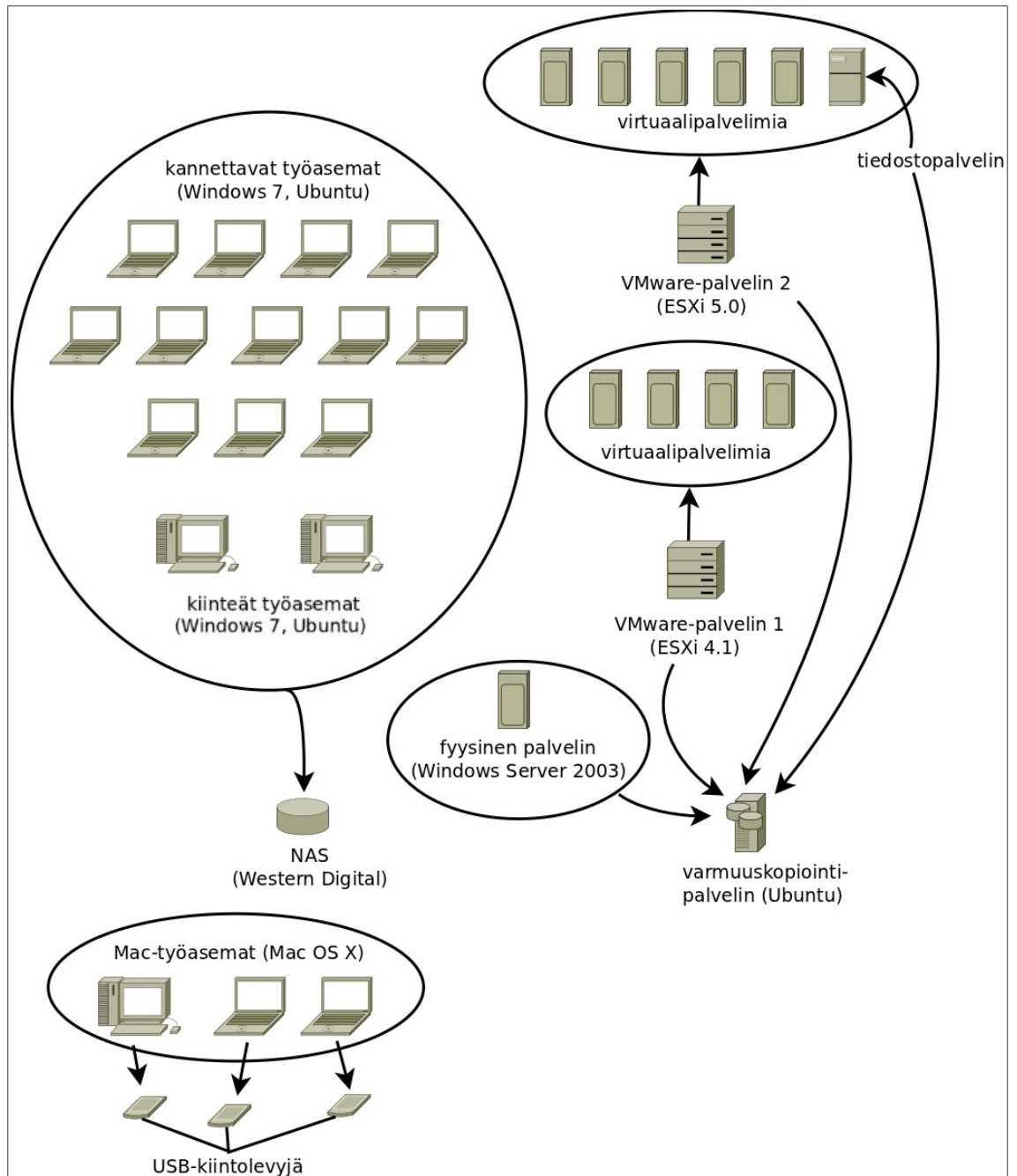
#### 4.2.3 Tiedostopalvelimen tiedostojaot

Tiedostopalvelimen varmuuskopiointi poikkesi hieman muista, sillä vaikka se oli jo yksi varmuuskopioitavista virtuaalipalvelimista, tuli sen tiedostojaoista ottaa erikseen varmuuskopioita. Tämän tuli tapahtua niin, että menneeltä

ajalta olisi helppoa palauttaa yksittäisiä tiedostoja tai hakemistoja. Kuten suunnitelmassa mainittiin, tämä toteutettiin alustamalla yksi varmuuskopio-palvelimen levyosioista Btrfs:ksi, joka mahdollisti tilannekuvien (snapshot-tien) oton tiedostojärjestelmästä.

Tiedostojen varmuuskopiointia varten tehtiin Bash-skripti (liite 5), joka ajettiin Cronin avulla joka arkiyö. Tämä Bash-skripti toimi niin, että se otti ensin edellisestä levytilanteesta tilannekuvan, jonka jälkeen se Rsync-ohjelmalla synkronoi kaikki tiedostopalvelimen tiedostojaot ajan tasalle varmuuskopiointipalvelimelle. Edellisiä tilannekuvia säilytettiin 60 päivän ajan. Päiviä vähennettiin automaattisesti levytilan käydessä vähiin ja tästä tilanteesta lähetettiin myös sähköpostitse ilmoitus. Nyt varmuuskopiointipalvelinta käyttävien henkilöiden oli helppo päästä käsiksi vanhoihin tiedostoihin ka-laamalla vain päivämäärän mukaan hakemistoja, joita edellä mainittu Bash-skripti oli luonut.





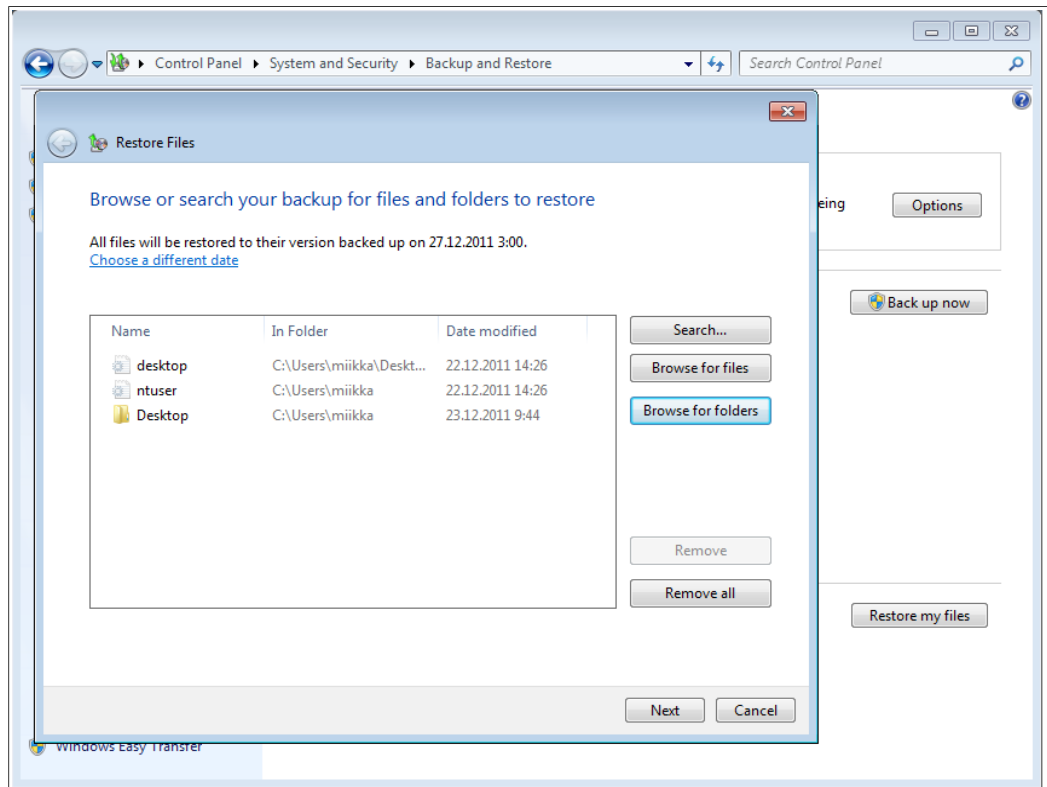
Kuva 9: Lopullinen, toteutunut ympäristön looginen kartta, missä on varmuuskopiointijärjestelmä mukana.

## 5 Järjestelmän testaus

Valmista järjestelmää tuli testata, jotta voitiin todentaa kokonaisuuden toimivan, kuten se oli suunniteltu. Testaus tapahtui yksinkertaisesti palauttamalla varmuuskopioita eri tilanteissa. Työmäärää vähensi se, että osa testauksesta voitiin suorittaa virtuaalisesti VMware-ympäristössä.

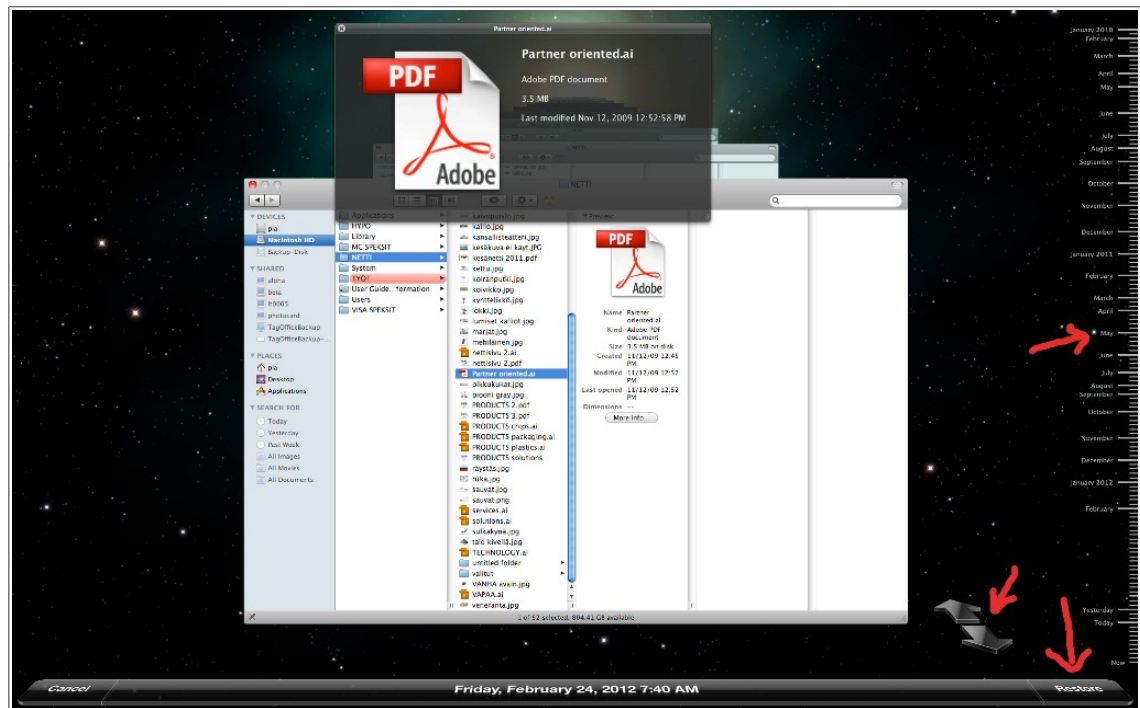
### 5.1 Yksittäiset tiedostot

Windows-työasemissa yksittäisiin tiedostoihin pääsi käsiksi samalla työkalulla, kuin millä varmuuskopiointikin oli suoritettu. Ensin valittiin päivämäärä, jolta varmuuskopioituja tiedostoja ja hakemistoja haluttiin palauttaa (kuva 10). Seuraavaksi valittiin joko yksitellen palautettavia tiedostoja tai hakemistoja. Tämän jälkeen tehtiin vielä valinta alkuperäisten tiedostojen palauttamisesta paikoilleen (mahdollisesti ylikirjoittaen nykyiset versiot tiedostoista) tai niiden sijoittamisesta jonnekin muualle (kuva 11). Sitten tiedostot kopioituivat takaisin NAS:lta työasemalle, jonka jälkeen ne olivat käytettävissä. Kaikki näytti toimivan niin kuin oli suunniteltu. Toimenpide oli melko suoraviivainen, joten se oli helppo opastaa myös työasemaa käyttäville henkilöille.



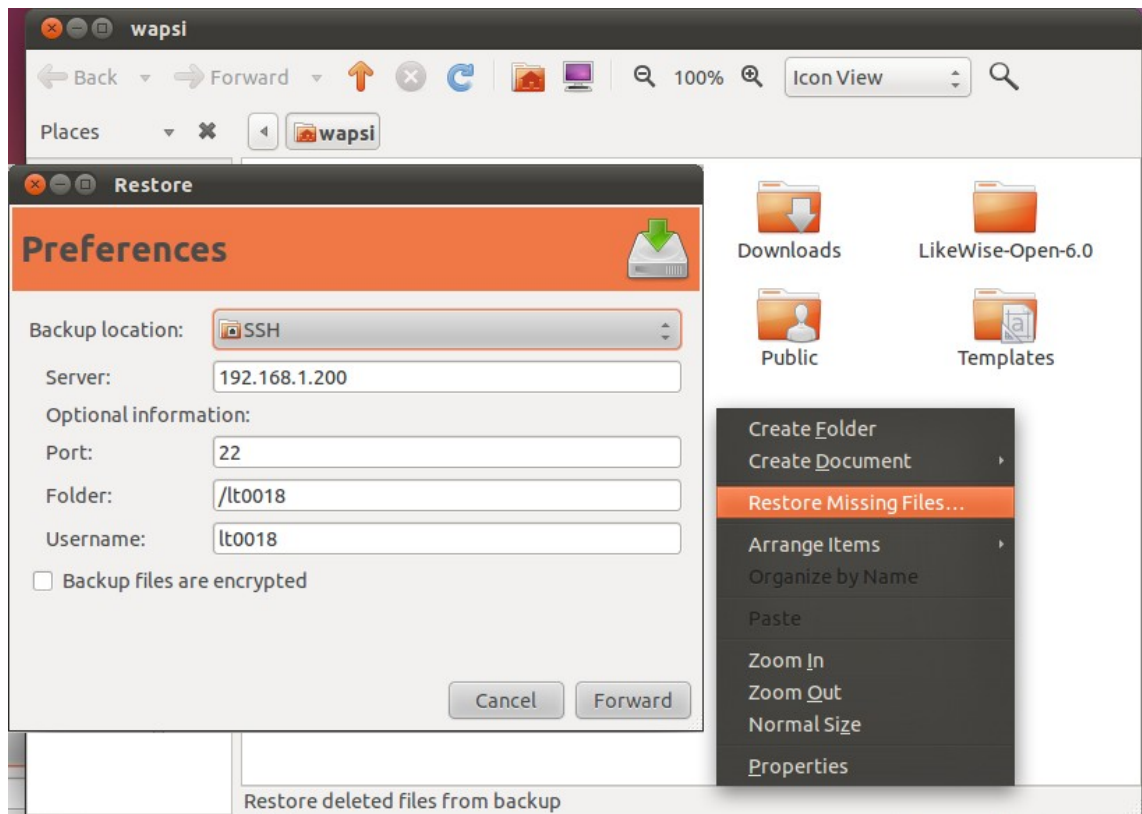
Kuva 11: Yksittäisten tiedostojen palautus Windowsissa. Kun päivämäärä on valittu, voidaan valita palautettavat tiedostot ja hakemistot.

Mac OS X:ssä Time Machinella tiedostojen palautus oli tehty käyttäjälle helposti ja visuaalisesti näyttäväksi (kuva 12). Time Machine otti Solariksen Time Slider -ominaisuuden tapaan tilannekuvia työaseman tiedostoista, joita oli helppo selata ensin tunti ja sitten päivä kerrallaan taaksepäin. Käyttöliittymä on sama kuin OS X:n Finder-tiedostoselain. Kun palautettavat tiedostot ja hakemistot oli valittu, ne voitiin palauttaa haluttuun paikkaan. Time Machinen avulla Mac-työasemien varmuuskopiointi sujui suunnitelman mukaisesti.



Kuva 12: Time Machinen tiedostopalautusnäky. Nuolet osoittavat ajan selaustoimintoja sekä palautuspainikkeen.

Ubuntu GNU/Linuxin ja Déjà Dupin avulla yksittäisten tiedostojen ja hakemistojen palautus onnistui yhtä helposti kuin muillakin käyttöjärjestelmillä, tosin hieman eri tavalla. Yksittäisten tiedostojen ja hakemistojen palautus ei vain tapahtunut Déjà Dupin käyttöliittymän kautta, vaan Gnomen tiedostoselaimen (Nautilus) kautta. Hakemistonäkymässä hiiren oikeaa näppäintä painamalla sai auki valikon, josta valittiin poistettujen tai hävinneiden tiedostojen palautus (restore missing files) (kuva 13). Tällöin saatiin esiin luettelo tiedostoista, joita hakemistossa oli joskus ollut ja mikä versio tiedostosta haluttiin palauttaa. Painamalla hiiren oikeaa näppäintä olemassa olevan tiedosto- tai hakemistokuvakkeen päällä, saatiin esiin valikko, jossa näkyi optio sen palauttamisesta johonkin edelliseen versioon (restore to previous version). Déjà Dupin omankin käyttöliittymän kautta pääsi palauttamaan tiedostoja, mutta tätä kautta vain kokonaisten varmuuskopioiden palautus oli mahdollista. Palautuksen pystyi tekemään joko nykyisten tiedostojen päälle (revert) tai toisen hakemiston sisään, jolloin nykyisiä tiedostoja ei ylikirjoitettu.



Kuva 13: Yksittäisten tiedostojen tai hakemistojen palautus Déjà Dupissa on integroitu Gnomen tiedostoselaimeen, Nautilukseen.

Tiedostopalvelimen tiedostoja pystyi palauttamaan helposti ottamalla SSH-yhteys varmuuskopointipalvelimelle tai liittämällä sieltä SFTP-levy verkkolevyksi. Tämän jälkeen hakemistoja selattiin päivämäärän mukaan Btrfs-tilanekuvahakemistoista ja halutut tiedostot tai hakemistot voitiin palauttaa joko nykyisten versioiden päälle tai johonkin uuteen sijaintiin (kuva 14).

```

root@delta:/mnt/lacie/alpha# ls -l
drwx----- 1 root root    36 2011-06-13 07:37 alpha_001-newest
drwx----- 1 root root    36 2011-06-13 07:37 alpha_2011-11-02
drwx----- 1 root root    36 2011-06-13 07:37 alpha_2011-11-03
drwx----- 1 root root    36 2011-06-13 07:37 alpha_2011-11-04
...
drwx----- 1 root root    36 2011-06-13 07:37 alpha_2011-12-19
drwx----- 1 root root    36 2011-06-13 07:37 alpha_2011-12-20
drwx----- 1 root root    36 2011-06-13 07:37 alpha_2011-12-21
drwx----- 1 root root    36 2011-06-13 07:37 alpha_2011-12-22
drwx----- 1 root root    36 2011-06-13 07:37 alpha_2011-12-23
drwx----- 1 root root    36 2011-06-13 07:37 alpha_2011-12-26
drwx----- 1 root root    36 2011-06-13 07:37 alpha_2011-12-27
drwx----- 1 root root    36 2011-06-13 07:37 alpha_2011-12-28
drwx----- 1 root root    36 2011-06-13 07:37 alpha_2011-12-29
drwx----- 1 root root    36 2011-06-13 07:37 alpha_2011-12-30
drwx----- 1 root root    36 2011-06-13 07:37 alpha_2012-01-02
drwx----- 1 root root    36 2011-06-13 07:37 alpha_2012-01-03
-r-xr-xr-x 1 root root   688 2011-06-20 08:16 backup.sh
-r-xr-xr-x 1 root root  2361 2011-06-13 07:54 CheckFreeSpaceAndDel.sh
drwxr-xr-x 1 root root 10098 2012-02-29 23:50 logs
-r-xr-xr-x 1 root root   2758 2011-06-13 07:52 TakeSnapshot.sh

root@delta:/mnt/lacie/alpha# scp "/mnt/lacie/alpha/alpha_2012-01-03/data/tagsystems/Pictures/Kuvaus_15.8.07/PICT0032.JPG"
root@alpha: "/data/tagsystems/Pictures/Kuvaus\ 15.8.07/PICT0032_PALAUTETTU.JPG"
PICT0032.JPG

100% 392KB 391.9KB/s 00:00

root@delta:/mnt/lacie/alpha#

```

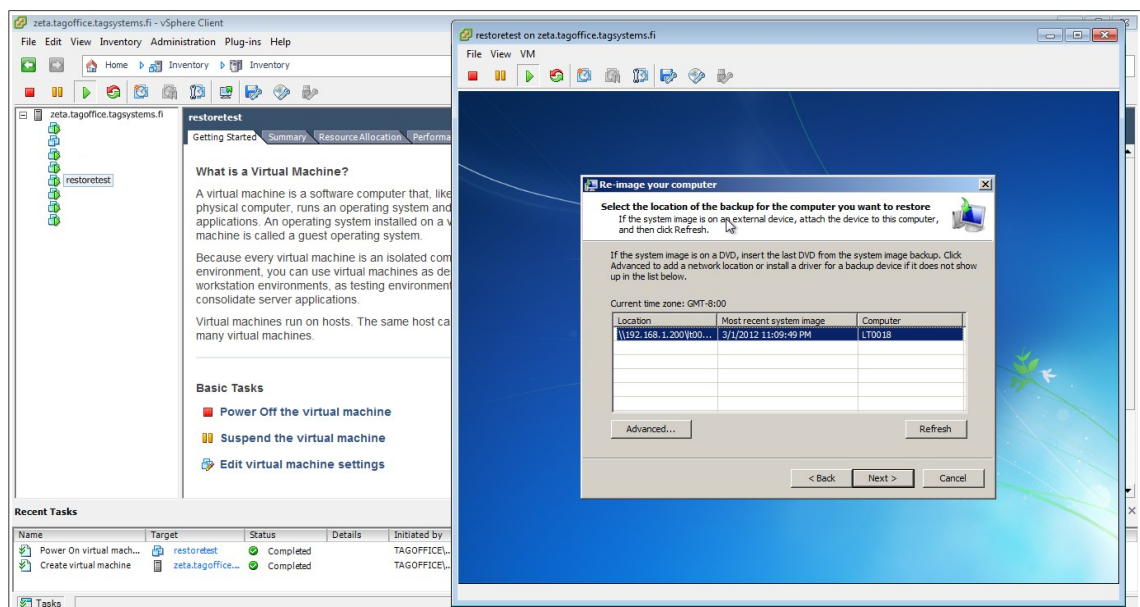
Kuva 14: Yksittäisen tiedoston palautus tiedostopalvelimelta alkuperäiselle sijainnille, toisella nimellä.

## 5.2 Täydellinen palautus

Työasemien ja palvelinten täydellistä palautusta testattiin virtuaalisesti Vmware-ympäristössä. Testaamisen yhteydessä kuviteltiin tilanne, jossa työasema tai palvelin tuhoutuisi, ja järjestelmää lähdetäisiin palauttamaan ”tyhjältä pöydältä”. Jokaista VMware-ympäristössä suoritettua täydellisen palautuksen testiä varten luotiin tilapäisesti uusi virtuaalikone. Näitä virtuaalikoneita ajettiin omassa virtuaalisessa verkossa VMware-ympäristön sisällä. Näin välttyttiin kaikilta mahdollisilta häiriöiltä, jotka olisivat vaikuttaneet toimistoverkossa pyöriiviin työasemiin ja palvelimiin (muun muassa IP-osoitteiden päällekkäisyyksiltä). Testausta varten luodut virtuaalikoneet tuhoettiin testien jälkeen.

### 5.2.1 Työasema

Windows-työaseman palautus onnistui käynnistämällä tyhjä virtuaalikone suoraan Windowsissa aiemmin luodulta palautuslevyltä (system repair disk). Levyltä käynnistyi Windowsin palautustyökalu. Saman työkalun sai käynnistettyä myös alkuperäiseltä Windows 7:n asennuslevyltäkin. Palautustyökälulle määriteltiin varmuuskopioiden sijainti (kuva 15), jonka jälkeen se lähti palauttamaan järjestelmää. Kun palautus oli valmis, poistettiin käynnistyslevy virtuaalisesti CD/DVD-asemasta ja järjestelmä käynnistettiin uudestaan. Nyt kone käynnistyi Windowsiin ja siihen tilaan, jossa se oli viimeistä varmuuskopiota otettaessa.



Kuva 15: Windows-työaseman täydellisen palautuksen testausta VMware-ympäristössä.

Mac OS X:n kanssa ei päästy kokeilemaan täydellistä palautusta, koska OS X:ää ei voi ajaa virtuaalisesti VMware-ympäristössä [16] ja yhtäkään kolmesta Mac-tietokoneesta ei tarkoituksellisesti haluttu tyhjentää. Internetistä löytyvien dokumenttien perusteella täydellinen palautus olisi kuitenkin tapahtunut niin, että Mac-työasema oltaisiin käynnistetty OS X:n asennuslevyltä ja varmuuskopiointiin käytetty USB-kiintolevy olisi ollut kiinnitettynä työasemaan. Heti asennuksen alkuvaiheessa olisi ylävalikosta valittu "Utilities", ja sen alta "Restore System from Backup". Tämän jälkeen työkalulle olisi osoitettu varmuuskopioiden sijaitsevan USB-kiintolevyllä, ja järjestel-

män palautus olisi käynnistynyt. Toimenpiteen jälkeen OS X:n asennus olisi käynnistänyt työaseman uudelleen, ja järjestelmän tilanne olisi ollut sama kuin varmuuskopiota otettaessa.

Ubuntu GNU/Linux -työasemien täydellistä palautusta testattiin niin, että tyhjä virtuaalikone käynnistettiin Ubuntun asennuslevyltä ja Ubuntu asennettiin normaalisti. Tämän jälkeen Ubuntuun asennettiin Déjà Dup ja sillä käynnistettiin varmuuskopion palautus verkkolevyltä. Déjà Dupissa valittiin varmuuskopion tiedostojen palautuvan entisille paikoilleen. Muun muassa /home-hakemisto palautettiin kokonaisuudessaan ja /etc:n ja /var:n alta joidakin tarvittavia konfiguraatioita. Esimerkiksi /etc/apt-, /etc/likewise-open- ja /var/lib/likewise-open-hakemistot palautettiin kokonaisuudessaan, jotta oikeat Ubuntun ohjelmakatalogit ja domain-autentikointi saatiin toimimaan. Kun tiedostot oli palautettu, /etc-hakemiston alta löytyi installed\_software-tiedosto, josta on kerrottu luvussa 4.1 tarkemmin. Tätä tiedostoa hyödyntämällä pystyttiin yhdellä komennolla asentamaan kaikki ohjelmat, jotka olivat asennettuna työasemaan alunperinkin (koodiesimerkki 3). Tiedostojen palautuksen, ohjelmien asennuksen ja työaseman uudelleenkäynnistyksen jälkeen pystyi työasemaan kirjautumaan sisään domain-käyttäjätunnuksella, ja kaikki käyttäjän tiedostot olivat paikoillaan sekä ohjelmat asennettuna. Kaikki näytti toimivan kuten pitikin.

```
1. sudo apt-get install `grep '^ii' /etc/installed_software|awk -F' ' '{ print $2 }'|xargs`
```

Koodiesimerkki 3: Ubuntun ohjelmien automaattinen asennus tiedostosta, johon ne on listattu.

### 5.2.2 Palvelin

Fyysisen palvelimen palautusta testattiin virtuaalisesti VMware-ympäristössä asentamalla tyhjälle virtuaalikoneelle Windows 2003 Server. Kun käyttöjärjestelmän asennus oli valmis, ajettiin Windowsista varmuuskopioiden palautustoiminto, josta valittiin viimeisin viikkovarmuuskopio. Tämän tiedoston sisältä valittiin palautettavaksi kaikki tiedostot viimeistä inkrementaalista varmuuskopiota myöten. Kun Windows 2003 Serverin palautustoiminto oli



suoritettu loppuun ja palvelin käynnistetty uudestaan, näyttivät kaikki tiedot ja ohjelmat olevan paikoillaan ja toimivan kuten ennenkin.

Virtuaalipalvelinten palautusta testattiin palauttamalla yksi virtuaalipalvelimen täydellisestä kopiosta ja sen metatiedoista takaisin VMware-ympäristöön. Kun yksi virtuaalipalvelimista oli kopioitu takaisin VMware ESXi:n levyille, se määriteltiin VMware-ympäristöön uudeksi virtuaalikoneeksi VMware vSphere Client -ohjelman avulla. Palautettu virtuaalipalvelin kuitenkin nimettiin eri tavalla kuin alkuperäinen, ja palvelimen virtuaalinen verkkokortti liitettiin kappaleessa 4.3.2 mainittuun, testausta varten luotuun virtuaaliseen verkkoon. Näin voitiin samaa aikaan ajaa varmuuskopiota virtuaalipalvelimesta, joka tosiasiallisesti pyöri kaiken aikaa VMware-ympäristössä. Tämän jälkeen se käynnistettiin ja tarkastettiin siten, että kaikki toimi suunnitelman mukaisesti. Ongelmia ei ilmennyt.

## 6 Yhteenveto

Työ alkoi varmuuskopiointijärjestelmän suunnittelulla ja eri varmuuskopiointitekniikoihin tutustumisella. Kokonaiskuva varmuuskopiointijärjestelmästä alkoi hahmottua samalla, kun työasemia ja palvelimia uusittiin. Suunnittelu- vaiheessa pyrittiin ottamaan erityisesti huomioon ympäristössä esiintyvät erilaiset alustat ja käyttöjärjestelmät. Tästä oli paljon apua toteutuksessa, sillä suunnitelmasta ei tarvinnut poiketa (muutamia asioita lukuun ottamatta). Toteutuksen aikana ilmeni kuitenkin jonkin verran muita odottamattomia ongelmia, kuten työmäärän lisääntyminen varmuuskopioiden automatisoinnin rakentamisessa. Tästä ei syntynyt kuitenkaan merkittävää haittaa, koska aikataululle ei ollut asetettu tiukkoja rajoja.

Testausvaihe sujui suunnitelmien mukaan lukuun ottamatta Mac-työasemien täydellistä palauttamista, jota ei päästy käytännön tasolla testaamaan. Testaus antoi hyvän kuvan järjestelmän lopullisesta toimivuudesta ja harjoitti mahdollisia tositilanteita varten.

Kokonaisuudessaan työ oli onnistunut ja sille asetetut tavoitteet saavutettiin. Varmuuskopioiden ottamista ja niiden säilytystä seurattiin muutamia kuukausia tarkasti, ja kaikki näytti toimivan odotetulla tavalla.

Tulevaisuudessa järjestelmää voidaan laajentaa sen mukaan, kun uusia työasemia tai palvelimia siihen liitetään. Fyysisten palvelinten osalta varmuuskopiointi tulee kuitenkin ratkaista tapauskohtaisesti, mutta työasemien ja virtuaalisten palvelimien varmuuskopiointin osalta voidaan toteuttaa vain samaa kaavaa, kuin mitä tässä työssä on esitetty. Erityisen yksinkertaista on uusien virtuaalipalvelimen liittäminen järjestelmään, sillä se onnistuu vain lisäämällä yksi rivi (virtuaalikoneen nimi) GhettoVCB-skriptin konfiguraatioihin. Mac-työasemien kanssa on hyvä siirtyä käyttämään verkkopohjaista varmuuskopiointiratkaisua, mikäli niiden määrä vielä kasvaa.

Varmuuskopiopalvelimesta ja NAS-laitteesta olisi myös hyvä ottaa varmuuskopiot esimerkiksi nauha-aseamalla, joka sijaitsee fyysisesti vielä eri tiloissa. Näin saataisiin lisäturvaa esimerkiksi palvelinhuoneen täydellistä tuhoutumista vastaan (kuten raju tulipalo).

## Lähteet

1. Preston W. Curtis. 2007. Backup & Recovery, Inexpensive Backup Solutions for Open Systems. O'Reilly Media, USA.
2. Imationin tutkimus. 2009. Verkkodokumentti. <<http://www.visionist.fi/2009/03/20/imation-vain-32-prosenttia-yri-tyksista-testaa-varmuuskopioinnin-toimivuuden/>>. Luettu 6.3.2012.
3. Douthitt David, RAID is not a backup! 2009. Verkkodokumentti. <<http://administratosphere.wordpress.com/2009/01/27/raid-is-not-a-backup/>>. Luettu 6.3.2012.
4. Webopedia, Backup Server. Verkkodokumentti. <[http://www.webopedia.com/TERM/B/backup\\_server.html](http://www.webopedia.com/TERM/B/backup_server.html)>. Luettu 6.3.2012.
5. Sinofsky Steven, Building the next generation file system for Windows: ReFS. 2012. Verkkodokumentti. <<http://blogs.msdn.com/b/b8/archive/2012/01/16/building-the-next-generation-file-system-for-windows-refs.aspx>>. Luettu 6.3.2012.
6. TopTenReviews, Removable Backup Media: Pros and Cons. 2012. Verkkodokumentti. <<http://data-backup-software-review.toptenreviews.com/removable-backup-media.html>>. Luettu 6.3.2012.
7. BackupChain, FastNeutron Inc. 2012. Verkkodokumentti. <<http://backupchain.com/why-you-shouldnt-use-optical-media-for-Backup.html>>. Luettu 6.3.2012
8. Nelson Steven B. 2011. Pro Data Backup and Recovery. Apress, USA.
9. TiVi, Pervilä Markku. 2011. Verkkodokumentti. <<http://www.tie-toviikko.fi/cio/nauha+hiipuu+vaan+ei+kuole/a584922>>. Luettu 6.3.2012.
10. Microsoft. 2009. Verkkodokumentti. <[http://download.microsoft.com/download/3/1/2/3128F2A9-6ED4-44D5-864B-D606E9F14CA1/0956\\_Windows7NewFeatures\\_WSG\\_external.docx](http://download.microsoft.com/download/3/1/2/3128F2A9-6ED4-44D5-864B-D606E9F14CA1/0956_Windows7NewFeatures_WSG_external.docx)>. Luettu 6.3.2012.
11. Supersite for Windows, Thurrott Paul. 2010. Verkkodokumentti. <<http://www.winsupersite.com/article/windows-7/windows-7-feature-focus-backup-and-restore>>. Luettu 6.3.2012.
12. OMG! Ubuntu!, Sneddon Joey. 2011. Verkkodokumentti. <<http://www.omgubuntu.co.uk/2011/05/deja-dup-backup-tool-proposed-for-default-in-ubuntu-11-10/>>. Luettu 6.3.2012.

13. Western Digital Community. 2010. Verkkodokumentti.  
<<http://community.wdc.com/t5/My-Book-World-Edition/Unable-to-join-worldbook-to-active-directory/td-p/19406>>. Luettu 6.3.2012.
14. Apple OS X and Time Machine Tips, Pond James. Verkkodokumentti.  
<<http://pondini.org/TM/2.html>>. Luettu 6.3.2012.
15. VMware Communities: GhettoVCB. 2008. Verkkodokumentti.  
<<http://communities.vmware.com/docs/DOC-8760>>. Luettu 6.3.2012.
16. Apple, Mac OS X 10.6 EULA. Verkkodokumentti.  
<<http://www.apple.com/legal/sla/docs/macosx106.pdf>>. Luettu 6.3.2012

## Skripti 1

Skripti poistaa kaikki yli 30 päivää vanhat Windows 7:n varmuuskopiot.

```
1. #!/bin/bash
2.
3. cd /root/removeOldBackups
4.
5. umount -f /mnt/backupnas 2> /dev/null
6. mkdir -p /mnt/backupnas
7. ./auto.expect
8. sleep 5
9.
10. if [ -d "/mnt/backupnas/Public" ]; then
11.     mkdir -p "/mnt/backupnas/Public/Shared Music"
12.     mkdir -p "/mnt/backupnas/Public/Shared Pictures"
13.     mkdir -p "/mnt/backupnas/Public/Shared Videos"
14.     rm -f "/mnt/backupnas/Public/Shared Music/dummy" 2> /dev/null
15.     rm -f "/mnt/backupnas/Public/Shared Pictures/dummy" 2> /dev/null
16.     rm -f "/mnt/backupnas/Public/Shared Videos/dummy" 2> /dev/null
17.     rm -f "/mnt/backupnas/Download/dummy" 2> /dev/null
18.     touch "/mnt/backupnas/Public/Shared Music/dummy"
19.     touch "/mnt/backupnas/Public/Shared Pictures/dummy"
20.     touch "/mnt/backupnas/Public/Shared Videos/dummy"
21.     touch "/mnt/backupnas/Download/dummy"
22.     # Poistetaan yli 30pv. vanhat tiedostot
23.     find /mnt/backupnas/*/ \(! -name "Download" ! -name "*.bin" ! -name
"BASE*" ! -name "WINDOWS*" ! -name "ALL*" ! -name "*.DAT" ! -name "*.TXT" !
-name "*.ini" ! -name "MediaId" ! -name "GlobalCatalog.wbcat" ! -name
"virtdisk.dll.vd.log" \) -type f -mtime +30 -exec rm -rf {} \;
24.     # Poistetaan tyhjät hakemistot
25.     find /mnt/backupnas/*/ -depth -type d -empty -exec rmdir {} \;
26. fi
27.
28. umount -f /mnt/backupnas
29. rmdir /mnt/backupnas
```

```
1. #!/usr/bin/expect
2. set timeout -1
3. spawn -ignore HUP /usr/bin/sshfs -p 22 root@192.168.1.200:/shares
/mnt/backupnas
4. #spawn /usr/bin/sshfs -p 22 root@192.168.1.200:/shares /mnt/backupnas
5. expect "*assword*"
6. send "PASSWORD"
7. expect "\n"
```

## Skripti 2

Skripti tarkastaa kuinka kauan viimeisimmästä varmuuskopioinnista on aikaa ja jos siitä on yli kymmenen päivää, lähetetään käyttäjälle siitä ilmoitus.

```
1. #!/bin/bash
2.
3. #
4. # Copyright TAG Systems Finland Oy 2011
5. #
6. # Tämä skripti tarkastaa onko hakemistoa muokattu
7. # tarpeeksi vähän aikaa sitten. Jos ei ole, niin
8. # lähetetään infoa siitä käyttäjälle meilitse.
9. #
10. # ver. 1.0 -MVe 12.11.2011
11. #
12.
13. # Montako päivää saa maksimissaan olla hakemiston
14. # viimesimmästä muokkauksesta?
15. maxtime=10
16.
17. # Data on muodossa: hakemistonimi,meiliosote
18. data=""
19. /data/backups/pc0001,miikka@tagsystems.fi
20. /data/backups/pc0002,testi@tagsystems.fi
21. "
22.
23. maxtime=$((maxtime * 60 * 60 * 24))
24. rajaaika=$((date +%s` - $maxtime))
25. for i in $data ; do
26.     hakemisto=`echo $i|awk -F',' '{ print $1 }'`
27.     if [ -d "$hakemisto" ] ; then
28.         aikaleima=`ls -ld --time-style="+%s" "$hakemisto"|awk -F' '
29.         '{ print $6 }'`
30.         if [ $aikaleima -lt $rajaaika ] ; then
31.             meili=`echo $i|awk -F',' '{ print $2 }'`
32.             # Lähetetään ilmoitus
33.             echo "Työasemastasi ei ole otettu varmuuskopiota
34.             viimeiseen kymmeneen päivään." | /bin/mail -s "Varmuuskopiovaroitutus"
35.             "$meili"
36.         fi
37.     else
38.         echo "Virhe: hakemistoa $hakemisto ei ole olemassa!"
39.     fi
40. done
```

## Skripti 3

Skripti suorittaa automaattisesti varmuuskopiointin Windows Server 2003:ssa (viikon sykli: ensimmäisenä täydellinen varmuuskopio, muut inkrementaalisia).

```
1. @echo off
2. REM Copyright: TAG Systems Finland Oy
3. REM
4. REM ver. 1.0 -MVe
5. REM This script creates a backup. It creates an incremental
6. REM backup if the destination file exists and a full backup
7. REM if there's no the destination file. It deletes old backups
8. REM also (*.bkf).
9. REM
10. REM This script is designed for backuping up Windows 2003
11. REM Server named Beta and it takes backup of all information
12. REM and files from the server.
13. REM
14.
15. REM We need to know the week number
16. SET getWeekScript=C:\backups-script\week.vbs
17.
18. FOR /F "tokens=" %%A IN ('CSCRIPT "%getWeekScript%" //NoLogo') DO SET %%A
19.
20. REM Set the destination filename
21. SET kohdehakemisto=Z:\
22. SET kohdetiedosto=Beta-varmuuskopio-viikko%WEEK%.bkf
23.
24. REM Set the file, which contains the list of files or drives to be
25. REM backed up (WITHOUT QUOTES!)
26. SET backuptiedostolistaus=C:\backups-script\beta-backup.bks
27.
28. REM Name of the backup set
29. SET backupnimi="beta-backup"
30.
31. REM Set the maximum age of backups (in days)
32. SET maksimisailytsaika=60
33.
34.
35. REM Map network drive
36. net use Z: \\delta\betabackups /USER:betabackup
37.
38.
39.
40. REM Deleting old backups
41. echo Deleting older backups than %maksimisailytsaika% days from %kohdehakemisto% (if
any)...
42. forfiles /p %kohdehakemisto% /m *.bkf /d -%maksimisailytsaika% /c "cmd /c echo @path" 2>
NUL
```



```
43.
44. REM Backing up
45. if exist "%kohdehakemisto%%kohdetiedosto%" (
46. REM The destination file exists, let's take an incremental backup
47. echo Processing an incremental backup...
48. C:\WINDOWS\system32\ntbackup.exe backup "@%backuptiedostolistaus%" /a /v:no /r:no /rs:no
    /hc:off /m incremental /j %backupnimi% /l:s /f "%kohdehakemisto%%kohdetiedosto%"
49. ) else (
50. echo Processing a full backup...
51. REM The destination file doesn't exist, let's take a full backup
52. C:\WINDOWS\system32\ntbackup.exe backup "@%backuptiedostolistaus%" /a /v:no /r:no /rs:no
    /hc:off /m normal /j %backupnimi% /l:s /f "%kohdehakemisto%%kohdetiedosto%"
53. )
```

## Skripti 4

Skripti suorittaa automaattisesti virtuaalipalvelimien varmuuskopiointia hyödyntäen GhettoVCB-skriptiä.

```
1. #!/bin/bash
2.
3. # Skripti varmuuskopioi ghettoVCB-skriptin avulla VMWare ESXi:stä
   virtuaalikoneita
4. # HUOM! ghettoVCB-skriptit/konffit tulee laittaa kuntoon, SSH-palvelin
   tulee olla päällä ESXi:ssä
5. # ja ilman salasanaa toimiva (authorized keys) -autentikointi päällä. NFS-
   liitos pitää myös olla kunnossa!!
6. # Tee NFS-liitos Vmware vSphere Clientilla! PS. asenna myös sendemail -
   paketti apt-getillä.
7. # -MVe 13.11.2011
8.
9. # Listaa kaikki virtuaalikoneet tiedostoon, jonka annat parametrina tälle
   skriptille
10. # Esimerkkitiedosto:
11. # epsilon
12. # ticket
13. # alpha
14.
15.
16. VMsToBackup=$1
17. SSHUserHost=$2
18. BackupMaxCount=$3
19. backupsarestored=/mnt/seagate/Backups/VMs
20. WorkingDir='/mnt/seagate/Backups'
21. LOGFILE=/tmp/vmware-backup.log
22.
23. ##### SKRIPTI ALKAA #####
24.
25.
26. if [ "$1" != "" ] && [ "$2" != "" ] && [ "$3" != "" ]; then
27.
28. cd $WorkingDir
29.
30. rm -f $LOGFILE 2> /dev/null
31.
32.
33. # Poistetaan vanhoja backuppeja
34. (
35. while read line
36. do
37.     while true; do
38.         count=`ls -p $backupsarestored/$line|grep /|grep -c $line`
39.         if [ $BackupMaxCount -gt $count ]; then
40.             break
41.         fi
```

```

42.     oldest=`ls -p $backupsarestored/$line/|grep /|grep -m 1 $line`
43.     echo "Poistetaan vanha varmuuskopio: $backupsarestored/$line/$oldest"
    >> $LOGFILE
44.     rm -rf $backupsarestored/$line/$oldest >> $LOGFILE 2>&1
45.     done
46.     done
47. ) < $VMsToBackup
48.
49. ssh $SSHUserHost "mkdir -p /ghettoVCB" 2>> $LOGFILE
50. scp ghettoVCB.sh $SSHUserHost:/ghettoVCB/ghettoVCB.sh > /dev/null 2>>
    $LOGFILE
51.
52. scp $VMsToBackup $SSHUserHost:/ghettoVCB/vms_to_backup > /dev/null 2>>
    $LOGFILE
53.
54. scp ghettoVCB.conf $SSHUserHost:/ghettoVCB/ghettoVCB.conf > /dev/null 2>>
    $LOGFILE
55.
56. ssh $SSHUserHost "/ghettoVCB/ghettoVCB.sh -g /ghettoVCB/ghettoVCB.conf -f
    /ghettoVCB/vms_to_backup" >> $LOGFILE 2>&1
57.
58. ssh $SSHUserHost "rm -rf /ghettoVCB" 2>> $LOGFILE
59.
60. # Yritetään kymmenen kertaa lähettää loki meilinä... (ei omistu läheskää
    joka kerta meinaa)
61. for i in {1..10}; do
62.     sendmail -s smtp.saunalahti.fi -u "Office ESXi: Backup logs" -m "Office
    VMware ESXi: virtual machine backup log attached" -a $LOGFILE -f office-
    VMware-Backup@tagsystems.fi -t alerts@tagsystems.fi
63.     if [ "$?" == "0" ]; then
64.         break
65.     fi
66. done
67.
68. else
69.     echo ""
70.     echo " VMsToBackup = tiedosto, missä on rivivaihdolla eroteltuna
    virtuaalikoneiden nimet, mitkä tulee varmuuskopioida"
71.     echo " user@ssh.host = SSH-käyttäjänimi ja hostname (ESXi-palvelimelle
    tulee olla SSH-pääsy ilman salasanaa)"
72.     echo " MaxBackupCount = varmuuskopioiden maksimimäärä (eli kuinka monta
    varmuuskopita säilytetään --> ylimenevät poistetaan vanhimmasta alkaen)"
73.     echo ""
74.     echo " Käyttö: ./vmware-backup.sh VMsToBackup user@ssh.host
    MaxBackupCount"
75.     echo ""
76.     echo " Esim: ./vmware-backup.sh vmstobackup.txt root@gamma 5"
77.     echo ""
78. fi

```

## Skripti 5

Skripti ottaa Btrfs-tilannekuvan tiedostopalvelimen varmuuskopioista, jonka jälkeen se synkronoi tiedostot tiedostopalvelimelta varmuuskopiointipalvelimelle.

```
1. #!/bin/bash
2.
3. LOGFILE=/mnt/lacie/alpha/logs/alpha-backup-`date +%Y-%m-%d`.log
4.
5. cd /mnt/lacie/alpha
6. /mnt/lacie/alpha/TakeSnapshot.sh 60 >> $LOGFILE
7. sleep 30
8. rsync --log-file=$LOGFILE -avz --fuzzy --delete -e ssh root@alpha:/data
  alpha_001-newest/ > /dev/null 2>&1
9. rsync --log-file=$LOGFILE -avz --fuzzy --delete -e ssh root@alpha:/home
  alpha_001-newest/ > /dev/null 2>&1
10. rsync --log-file=$LOGFILE -avz --fuzzy --delete -e ssh root@alpha:/etc
    alpha_001-newest/ > /dev/null 2>&1
11. rsync --log-file=$LOGFILE -avz --fuzzy --delete -e ssh root@alpha:/var
    alpha_001-newest/ > /dev/null 2>&1
12. rsync --log-file=$LOGFILE -avz --fuzzy --delete -e ssh root@alpha:/root
    alpha_001-newest/ > /dev/null 2>&1
```

## TakeSnapshot.sh:

```

1. #!/bin/bash
2. #
3. # Tämä skripti ottaa btrfs-snapshotin ja poistaa tarvittaessa vanhoja
   snapshotteja:
4. # * Skripti poistaa yli maksimimäärän menevät snapshotit uusien alta pois
5. # * Skripti poistaa myös vanhimmasta päästä snapshotteja, jos maksimi
   levykäyttö lähenee (varoitukseili)
6. # * Skripti lähettää varoitukseiliin, jos kaikki snapshotit on poistettu ja
   silti maksimi levykäyttö on ylitetty
7. #
8. #   ver. 1.0 10.11.2011 -MVe
9. #
10. #
11.
12.
13. # BTRFSBASE -muuttuja on btrfs "root"-mountin paikka
14. # TAKESNAPSHOTFROM on se btrfs subvolume, mistä snapshotti otetaan
15. # SNAPSHOTDIR on se, paikka mihin snapshotteja tallennetaan
16. # THRESHOLD on se %, minkä yli ei saa levykäyttö mennä
17.
18. if [ "$1" == "" ]; then
19.     echo "Käyttö: konffaa eka skriptin sisältä parametrin ja sitten:
   ./TakeSnapshot.sh MaxSnapshotMaara"
20.     echo " * Esim: ./TakeSnapshot.sh 30"
21.     exit
22. fi
23. CHECKFREESPACE=/mnt/lacie/alpha/CheckFreeSpaceAndDel.sh
24. BTRFSBASE=/mnt/lacie
25. TAKESNAPSHOTFROM=/mnt/lacie/alpha/alpha_001-newest
26. SNAPSHOTDIR=/mnt/lacie/alpha
27. MAXSNAPSHOTS=$1
28.
29. #BTRFSCTL=/sbin/btrfsctl
30. BTRFSCTL=/usr/local/bin/btrfsctl
31. BASHBIN=/bin/bash
32.
33. # Skripti alkaa
34.
35. function deloldsnap {
36.
37. for i in $( ls -p $SNAPSHOTDIR | grep / | grep -v "alpha_001-newest/" );
38. do
39.     OLDEST=`echo $i|sed 's/:::g'`
40.     echo "Poistetaan vanhin snapshotti ($SNAPSHOTDIR/$OLDEST)"
41.     00K00=`$BTRFSCTL -D $OLDEST $SNAPSHOTDIR | grep -c "operation complete"
2> /dev/null`
42.     if [ "$00K00" == "1" ]; then
43.         TULOS=1
44.         break
45.     else
46.         echo "Snapshotin poistaminen epäonnistui! Kokeillaan seuraavaa..."
47.         fi
48.         TULOS=0
49.     done

```

```
50. }
51.
52. function takesnapshot {
53.     while [ 1 ]
54.     do
55.         SNAPLKM=`ls -p $SNAPSHOTDIR|grep -c /`
56.         if [ "$SNAPLKM" -ge "$MAXSNAPSHOTS" ]; then
57.             deloldsnap
58.             if [ "$TULOS" == 0 ]; then
59.                 echo "Ei onnistu... Yhtään snapshottia ei pystytty ottamaan."
60.                 sendemail -s smtp.saunalahti.fi -u "WARNING: Problems with Alpha
rsync-backup or btrfs-snapshot" -m "WARNING: There were some problems with
Alpha rsync-backup or btrfs-snapshot. Check out logs from
/mnt/lacie/alpha/logs in Delta" -f alpha-Backup@tagsystems.fi -t
alerts@tagsystems.fi
61.                 exit
62.             fi
63.             else
64.                 TULOS=1
65.                 break
66.             fi
67.         done
68.         if [ "$TULOS" == 1 ]; then
69.             echo "Otetaan snapshotti... ($SNAPSHOTDIR/alpha_`date +%Y-%m-%d`)"
70.             $BTRFSCTL -s $SNAPSHOTDIR/alpha_`date +%Y-%m-%d` $TAKESNAPSHOTFROM >
/dev/null
71.             fi
72.         }
73.
74.         NIMI=`basename $0`
75.         RUNNING=`ps aux|grep $BASHBIN|grep -c $NIMI`
76.         if [ $RUNNING -gt 2 ]; then
77.             echo "$NIMI on jo käynnissä. Toista prosessia ei kannata käynnistää!"
78.             exit
79.         fi
80.
81.         RUNNING=`ps aux|grep $BASHBIN|grep -c $CHECKFREESPACE`
82.         if [ $RUNNING -gt 2 ]; then
83.             echo "$NIMI on jo käynnissä. Toista prosessia ei kannata käynnistää!"
84.             exit
85.         fi
86.
87.         $BASHBIN $CHECKFREESPACE
88.
89.     takesnapshot
```