Juha Riikonen

TIETOJÄRJESTELMÄN VARMUUSKOPIOINNIN SUUNNITTELU, TESTAUS JA TOTEUTUS
CASE: KP-SERVICEPARTNER OY

Tietojenkäsittelyn koulutusohjelma
Järjestelmäpalvelujen suuntautumisvaihtoehto

2009

samk
Satakunnan ammattikorkeakoulu

TIETOJÄRJESTELMÄN VARMUUSKOPIOINNIN SUUNNITTELU, TESTAUS JA TOTEUTUS CASE: KP-SERVICEPARTNER OY

Riikonen, Juha
Satakunnan ammattikorkeakoulu
Tietojenkäsittelyn koulutusohjelma
Maaliskuu 2009
Grönholm, Jukka
UDK: 004.056.3
Sivumäärä: 69

Asiasanat: käyttöönotto, tietojärjestelmät, suunnittelu, testaus, varmuuskopiointi

---

Tämän opinnäytetyön aiheena oli suunnitella, testata ja toteuttaa kohdeyrityksen tietojärjestelmän varmuuskopiointi. Kohdeyrityksenä oli KP-ServicePartner Oy, joka on teollisuuden kunnossapitopalveluja tarjoava yritys. Tietojärjestelmän varmuuskopioinnin kehittäminen oli osa yrityksen toimialuepalveluiden kehittämisprojektia. Työ toteutettiin pääosin tuotantokäytössä olevilla laitteilla.

Työn teoreettisessa osuudessa käsiteltiin yrityksen tietoverkon rakennetta ja aikaisempia varmuuskopiointiratkaisuja ja niihin liittyviä tekniikoita. Teoreettisessa osuudessa käsiteltiin myös varmuuskopioinnin perusteita, varmistusstrategioita ja erilaisia varmuuskopiointiratkaisuja. Lisäksi osuudessa käsiteltiin mitä yleensä kannattaa varmuuskopioida, millaisia ongelmia varmuuskopioimisessa on ja millaisia haasteita yrityksen verkko asettaa työlle.

Empiirisessä osiossa tehtiin järjestelmän määrittely, minkä pohjalta järjestelmä suunniteltiin. Suunnitelmassa vertailtiin kolmea varmuuskopiointiratkaisua, joista yksi valittiin käyttöönotettavaksi järjestelmäksi. Ratkaisuja vertailtiin vaatimusten, ominaisuuksien, rajoitusten ja tietoturvan kannalta. Lopullisen valinnan jälkeen työssä suunniteltiin mitä tietoja yrityksen järjestelmästä varmuuskopioidaan sekä milloin ja miten varmuuskopioinnit suoritetaan.

Suunnittelun jälkeen järjestelmän toimintaa testattiin palvelimella ja työasemilla. Testaamisen jälkeen järjestelmä otettiin käyttöön asteittain. Järjestelmä asennettiin ensiksi palvelimiin ja sen jälkeen työasemiin. Etäpisteissä sijaitsevat työasemat asennettiin viimeisinä. Käyttöönoton yhteydessä käsiteltiin myös ilmi tulleita ongelmia ja niihin löydettyjä ratkaisuja. Osiossa perehdyttiin myös järjestelmän ylläpitoon ja sen hienosäätöön.

Lopullinen järjestelmä toteutettiin BackupPC-ohjelmalla ja se saatiin toimimaan määrittelyssä tehtyjen vaatimusten mukaisesti. Yrityksen verkossa ilmeni järjestelmän käyttöönoton aikana joitakin puutteita, jotka rajoittivat järjestelmän toimintaa. Suurimpana yksittäisenä rajoittavana tekijänä oli yrityksen hitaat verkkoyhteydet. Työssä analysoitiin järjestelmän vaikutusta työasemiin, palvelimiin sekä verkon kuormitukseen. Myös varmuuskopiointijärjestelmän tulevaisuuden tarpeita pohdittiin työssä.

TO DESIGN, TEST AND IMPLEMENT A BACKUP SYSTEM FOR COMPANY'S INFORMATION SYSTEM. CASE: KP-SERVICEPARTNER OY

Riikonen, Juha
Satakunnan ammattikorkeakoulu, Satakunta University of Applied Sciences
Degree Programme in Business Information Systems
March 2009
Grönholm, Jukka
UDK: 004.056.3
Number of pages: 69

Key words: implementation, information systems, design, testing, backup

---

The purpose of this thesis was to design, test and implement a backup system for company's information system. The work was done for company called KP-ServicePartner, Inc. which provides maintenance services for industry. Development of the backup system was part of the company's development project for domain services. The work was done mainly with devices used in production.

The topics discussed in the theoretical part of the thesis include the company's network structure, previous backup solutions and the technology involved. The theoretical part also deals with basics of backup, backup strategies and different solutions to backup systems. Also what usually is useful to backup, what problems may occur when backing up and what challenges company's network structure sets for the work were dealt with.

In the empirical part of the thesis, the system was defined and therefore system was designed based on that definition. Three backup solutions were compared in the design stage and finally one was chosen for the implemented system. The selection was based on the requirements, features, limitations and data security of the solution. Also what information from the company's system will be backed up and also how and when the backups were meant to be done were planned.

After designing the system, it was tested with the server and workstations. After the testing period the system was gradually implemented. The system was first installed to the servers and afterwards to the workstations. The workstations located at the distant offices were installed last. Also the problems occurred and their solutions in the implementation stage were dealt with. Also maintenance and adjustment of the backup system were taken look at.

The final system was done with BackupPC program and it worked well with the requirements made in the definition. Some limitations occurred in the company's network during the implementation of the system which limits its operation. One major factor which limits the operation was the company's slow network connections. Systems influence to the workstations, servers and network traffic were also analyzed in the thesis. Also the future needs of the backup system were considered.

SISÄLLYS

SYMBOLI- JA TERMILUETTELO

Apache	Unix-varianteissa usein käytetty www-palvelin.
avoin lähdekoodi	Ohjelma, jonka lisenssi täyttää Open Source Initiativen määrittelemät vaatimukset.
CGI	Web-tekniikka, jonka avulla selain välittää dataa palvelimella suoritettavalle ohjelmalle.
CPU	Tietokoneen suoritin eli prosessori.
daemon	Taustalla jatkuvasti pyörivä palvelinohjelmisto Unix- ja Linux-järjestelmissä.
DHCP	Verkkoprotokolla, joka jakaa IP-osoitteita uusille lähiverkkoon kytketyille laitteille.
DMZ	Fyysinen tai looginen aliverkko, joka yhdistää organisaation oman järjestelmän turvattomampaan alueeseen.
G.SHDSL	Kansainvälinen standardi symmetriselle DSL-yhteydelle.
GPL	Vapaa ohjelmistolisenssi.
Intranet	Lähiverkko, joka on eristetty tietyn ryhmän käyttöön.
IP-osoite	Yksilöi jokaisen Internet-verkkoon kytketyn laitteen.
I/O	Tietojenkäsittelylaitteeseen tuleva ja siitä lähetetty tieto.
kompressointi	Tietyn informaation ilmaisuun tarvittavan datan määrän pienentämistä alkuperäisestä.

kova linkki	Tiedostojärjestelmässä sijaitseva viittaus fyysisellä tallennusvälineellä sijaitsevaan tiedostoon.
laiteajuri	Käyttöjärjestelmään lisätty koodi, jonka avulla tapahtuu tietokoneen ja laitteen välinen tiedonsiirto.
NFS	Menetelmä tiedostojärjestelmien jakamiseen Unix-järjestelmien välillä.
palvelin	Palvelinohjelmistoa suorittava tietokone.
RSH	Ohjelma, jolla voidaan suorittaa komento etäkoneella ilman kirjautumista siihen.
Service Pack	Tietokoneohjelmiston täydennysosa, ns. huoltopäivitys, jolla korjataan ohjelmistossa olevia virheitä ja mahdollisesti lisätään uusia ominaisuuksia.
skripti	Ohjelmointikielellä kirjoitettu komentosarja.
SSH	Turvalliseen tiedonsiirtoon tarkoitettu järjestelmä.
symbolinen linkki	Unix-tyylisen järjestelmän tiedostopuussa sijaitseva viittaus toisaalle.
virtualisointi	Tekniikka, jolla fyysisen resurssin tekniset piirteet piilotetaan muilta järjestelmiltä, sovelluksilta tai loppukäyttäjiltä.
VPN	Tapa, jolla yrityksen verkkoja voidaan yhdistää julkisen verkon yli muodostaen näennäisesti yksityisen verkon.
ZIP	Tiedonpakkaukseen käytettävä menetelmä.

1 JOHDANTO

Yritysmaailmassa tietojen säilyvyyttä pidetään yrityksen toiminnalle erityisen tärkeänä asiana, mutta samalla se kuitenkin on yrityksen työntekijöille lähes näkymätön osa yrityksen toimintaa. Varmuuskopioinnin tarpeellisuus huomataan usein vasta tilanteessa, jossa tärkeä työ on tuhoutunut pysyvästi eikä siitä ole olemassa varmuuskopiota. Tarjolla olevia ratkaisuja tietojärjestelmien varmuuskopioimiseen pidetään usein kalliina ja vaikeasti toteutettavina.

Opinnäytetyössäni suunnittelin, testasin ja otin käyttöön varmuuskopiointijärjestelmän yritykselle, jonka aiempi varmuuskopiointiratkaisu oli päivittämisen tarpeessa. Työssä tutustun erilaisiin vaihtoehtoihin rakentaa itsenäisesti toimiva, luotettava ja kustannustehokas varmuuskopiointijärjestelmä, joka on myös helposti ylläpidettävissä. Työssäni tutustuin varmuuskopioimiseen erityisesti yrityksen näkökulmasta ja pohdin järjestelmän käyttöönoton eri vaiheissa tekemiäni havaintoja. Opinnäytetyöni avulla on mahdollista toteuttaa vastaava ratkaisu myös toisenlaisessa ympäristössä.

2 PROJEKTIN TAVOITE

Opinnäytetyöni tavoitteena oli suunnitella, testata ja lopuksi toteuttaa KP-Servicepartner Oy:n tietojärjestelmän varmuuskopiointi. Tietojärjestelmän varmuuskopioinnin kehittäminen oli osa yrityksen toimialuepalveluiden kehittämisprojektia. Työ toteutettiin tuotantokäytössä olevilla laitteilla eli järjestelmän toteutus ei saanut aiheuttaa minkäänlaisia ongelmia tuotantoon. Tarkoituksena oli toteuttaa järjestelmä, joka korvaisi käytössä olevan järjestelmän.

Käytössä olevan järjestelmän suurimpana heikkoutena oli varmuuskopioiden hajanaisuus. Osa varmuuskopioista oli synkronoitu palvelimelle ja varmuuskopioitu sieltä, kun

taas osa kopioista oli erillisillä medioilla työasemien luona. Ratkaisut ovat epävarmoja ja erityisesti moninkertainen synkronointi vie huomattavasti levytilaa. Erillisten järjestelmien ajastaminen niin, että ne eivät käytä kaikkea verkkokaistaa kerralla, on hankalaa. Lisäksi ratkaisut ovat vaatineet toimenpiteitä käyttäjiltä, jotka ovat itse hoitaneet työasemiensa varmuuskopioinnin.

Uuden järjestelmän avulla varmistettiin yritykselle tärkeiden tietojen säilyvyys. Järjestelmä piti suunnitella myös mahdollisimman dynaamiseksi ja kustannustehokkaaksi olemassa olevilla työkaluilla.

3 KP-SERVICEPARTNER OY

KP-Servicepartner Oy on teollisuuden kunnossapitopalveluja tarjoava yritys. Yritys kuuluu ServicePartner yritysverkostoon ja toteuttaa ABB Oy:n ServicePartner kunnossapitokonseptia ja siihen liittyvää toiminnanohjausjärjestelmää sekä tukipalveluita. Yrityksellä on toimipisteitä yhdeksällä eri paikkakunnalla ympäri Suomea ja niissä työskentelee noin 100 työntekijää. Yrityksen tarjoamia palveluita ovat tehdaslaitosten kokonaisvastuullinen kunnossapito, kunnossapidon yksittäispalvelut, koneistukset, pinnoitukset ja tuotantolinjojen modernisoinnit. (KP-ServicePartner Oy kotisivut. 2008)

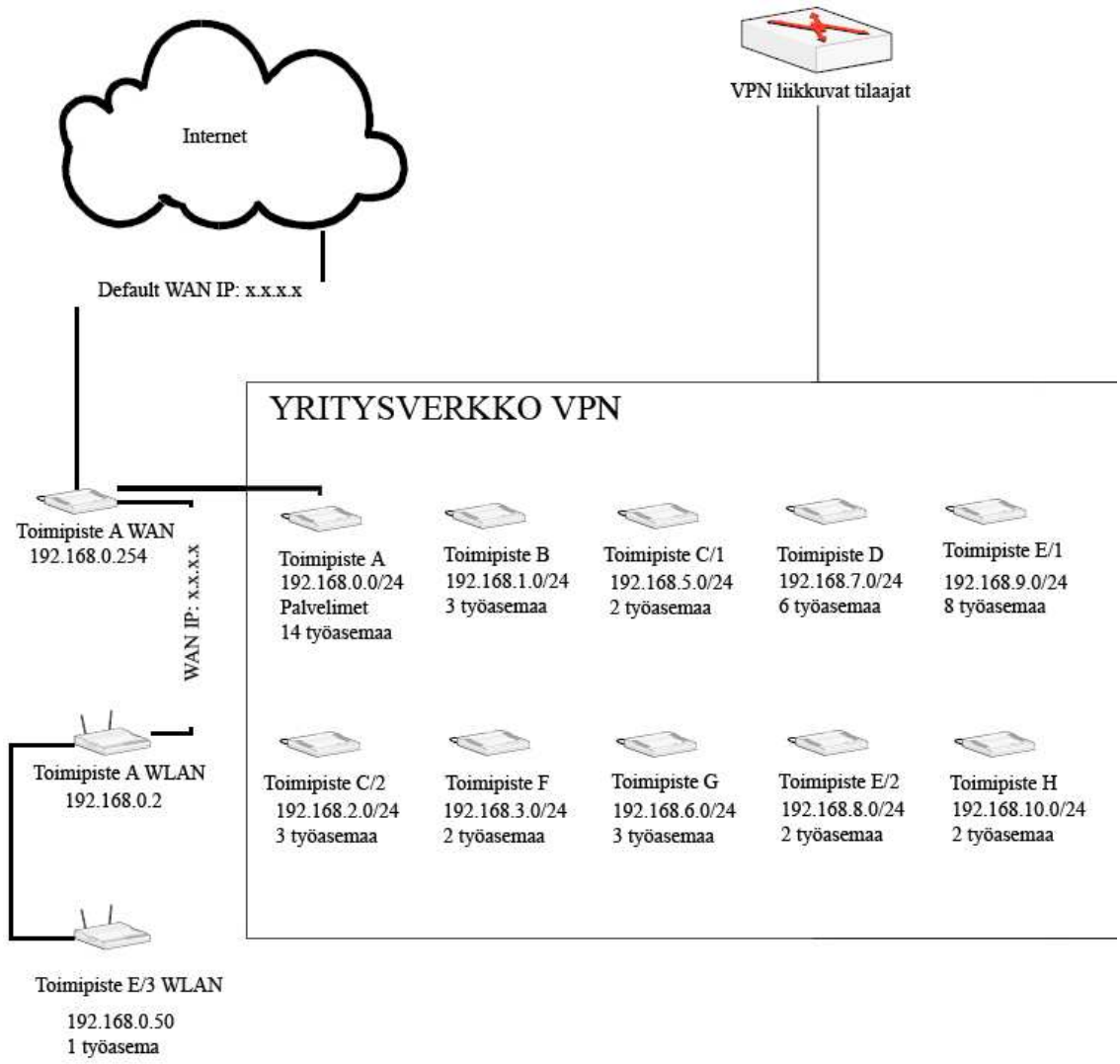
3.1 Yrityksen tietoverkon rakenne

Yrityksen verkon palvelut tuottaa kolme fyysistä palvelinta, jotka sijaitsevat samassa toimipisteessä. Palvelimissa on lisäksi myös palvelimia virtualisoituna. Työasemia yrityksen verkossa on noin 50 kappaletta. Työasemia on yrityksen johdon, työnjohtajien sekä työntekijöiden käytössä. Koneiden käyttöympäristöt vaihtelevat normaaleista toimistoympäristöistä vaativampiin pölyisiin teollisuusympäristöihin.

Palvelimet ovat Linux-palvelimia, ja työasemista suurin osa käyttää Windows XP -käyttöjärjestelmää, joihin on asennettuna vähintään Service Pack 2. Muutamissa työasemissa on käytössä Linux- tai Windows Vista -käyttöjärjestelmä. Työasemiin on lisäksi asennettuna oletuksena .NET Framework -ohjelmistokomponenttikirjasto sekä UltraVNC-ohjelmisto etähallintaa varten. Työasemat on liitetty toimialueeseen ja profiilit muutettu paikallisiksi.

Yrityksen verkko koostuu yhdeksästä maantieteellisesti toisistaan erillään olevasta lähiverkosta, jotka on yhdistetty salatusti yhdeksi suljetuksi yritysverkoksi G.SHDSL-yhteyden avulla mahdollistaen verkkopalvelujen käytön kaikissa toimipisteissä. Palveluun on liitetty myös pääsy julkiseen internetiin ja lisäksi etätyöntekijöillä on mahdollisuus liittyä yritysverkkoon. Työssä on tässä käytetty yrityksen verkon IP-osoitteina esimerkkinä yksityisosoiteryhmää 192.168.0.0/255.255.255.0 (Kuva 1). Toimipisteet ovat kaikki omissa C-luokan aliverkoissa.

Yrityksen palvelimet sijaitsevat kaikki toimipisteessä A (Kuva 1). Yrityksellä on käytössä langaton lähiverkko eli WLAN (Wireless Local Area Network) kaikissa toimipisteissä. Lisäksi toimipisteissä A ja E olevat WLAN-tukiasemat on sillattu toisiinsa VPN-tekniikalla (Virtual Private Network). Toimipisteessä A verkon nopeus on 2 Mbit/s symmetrisesti internetiin ja 2 Mbit/s symmetrisesti muihin toimipisteisiin. Muissa toimipisteissä on käytössä nopeudella 512 kbit/s sekä 2 Mbit/s toimivia yhteyksiä.



Kuva 1. KP-ServicePartner Oy:n verkon kuvaus.

3.2 Aiempi varmuuskopiointiratkaisu

Yrityksen tietojärjestelmän varmuuskopiointi on aiemmin hoidettu verkkokeskeisellä varmuuskopiointijärjestelmällä. Työasemat synkronoidaan useita kertoja päivässä palvelimelle. Kaikki palvelimet synkronoidaan öisin keskitetylle varmuuskopiointipalvelimelle. Varmuuskopiointipalvelimella on levyjärjestelmä, joka on varmistettu RAID1 (Redundant Array Of Inexpensive Disks) -tekniikalla ja se on dynaamisesti laajennettavissa LVM (Logical Volume Management) -tekniikan avulla.

Työasemien varmuuskopiointiin käytetään Syncback-ohjelmaa. Syncback-ohjelma kopioi aina työasemista muuttuneet tiedot palvelimen verkkolevylle. Varmuuskopioitavat

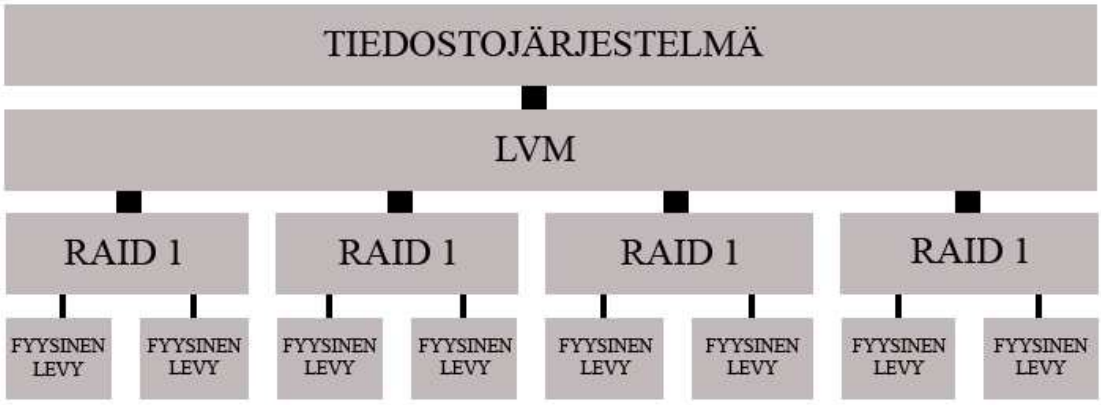
hakemistot ovat käyttäjäkohtaisia ja synkronointi on käytössä pääsääntöisesti vain työnjohtajien työasemissa. Muilla verkon käyttäjillä on käytössä varmuuskopioinnin kannalta ainoastaan tunnuskohtainen verkkojako palvelimella. Osa verkon käyttäjistä on myös suorittanut omatoimista varmuuskopiointia ulkoiselle medialle.

Palvelimien varmuuskopiointi tapahtuu rsync-kirjastoa käyttävällä rdiff-backup -ohjelmalla. Sen avulla on mahdollista kopioida paikallisesti sekä SSH:n (Secure Shell) yli suojattuna tietoa palvelimilta ja työasemilta. Ohjelma kopioi ainoastaan muuttuneet tiedostot erilliseen tietovarastoon ja pitää otoskohtaista kirjanpitoa jokaisen otoksen tiedostoista. Tämä mahdollistaa tarvittaessa palauttamisen pitkänkin ajan takaiseen tilanteeseen. Ohjelma on komentorivipohjainen, joten se on erittäin skaalautuva ja kevyt. (Escoto, B. 2008)

Suurimpana ongelmana käytettävässä järjestelmässä oli se, että osa yrityksen työntekijöistä ei ole käyttänyt kotihakemistoa tietojensa tallentamiseen, jolloin tärkeitä tietoja on saattanut jäädä varmuuskopioimatta. Lisäksi jatkuva nauhojen vaihtaminen on hankalaa ja Syncback-ohjelman käyttäminen vie kaksinkertaisesti levytilaa palvelimella, koska tiedot ovat palvelimella käyttäjän kotihakemistossa sekä varmuuskopioituna tietovarastossa.

3.3 Yrityksen levyjärjestelmä

Yrityksen palvelimissa käytetään ohjelmistopohjaista RAID 1-tekniikkaa, jossa keskusprosessori hoitaa datan ohjaamisen oikeille levyille. RAID-osioiden päälle on luotu LVM-tekniikkaa käyttäen loogiset osiot (Kuva 2), joita voidaan muokata niin sanotusti ”lennossa”. Tämän avulla levyjen lisääminen tai siirtäminen muuhun käyttöön on erittäin helppoa. Yrityksen käytössä oleva ratkaisu on periaatteessa RAID1+0, jossa taso 0 on toteutettu LVM:n avulla.



Kuva 2. Yrityksen levyjärjestelmä.

3.3.1 RAID-järjestelmä

RAID-järjestelmä perustuu siihen, että kaksi tai useampi levy yhdistetään yhdeksi levyjärjestelmäksi. Perusideana on muodostaa useita kiintolevyjä yhdistämällä vikasietoinen ja suorituskykyinen sekä kapasiteetiltaan suuri levypakka, joka näkyy tietokoneelle yhtenä kiintolevynä. Tällaista levypakkaa kutsutaan myös levyaltaaksi (disk pool). Tiedon tallennus levylle määräytyy RAID-tasojen mukaan. Yleisimmin käytettyjä tasoja ovat 0, 1 ja 5 sekä tasojen 0 ja 1 yhdistelmä. RAID 1 -tasolla kaikki data tallennetaan kahteen kertaan eri levyille eli ns. peilataan. Jos toinen levy jostain syystä rikkoutuu, jatkaa ehjä levy toimintaansa suorituskyvyn pysyessä lähes samana. Lukunopeus on 1-tasolla parhaimmillaan kaksinkertainen, mutta tilahävikki on tiedon kahdentamisen vuoksi puolet levyjärjestelmän kapasiteetista. (Sundell 2000, 34-37)

On kuitenkin tärkeää huomioida, että vaikka tiedon menetys levyjärjestelmän vikatilanteissa vähenee niin tiedot voidaan menettää esimerkiksi käyttäjän tuhotessa tiedoston tai kirjoittamalla tiedoston päälle. Myös erilaiset virukset voivat saada tiedon katoamaan pysyvästi etenkin Windows-ympäristössä. Jos tiedosto on tuhottu tai sen päälle on kirjoitettu, niin levyjärjestelmä ei voi sitä palauttaa. Tämän vuoksi RAID-levyjärjestelmä ei ole ratkaisu varmuuskopiointiin. (Leaver 2007, 2)

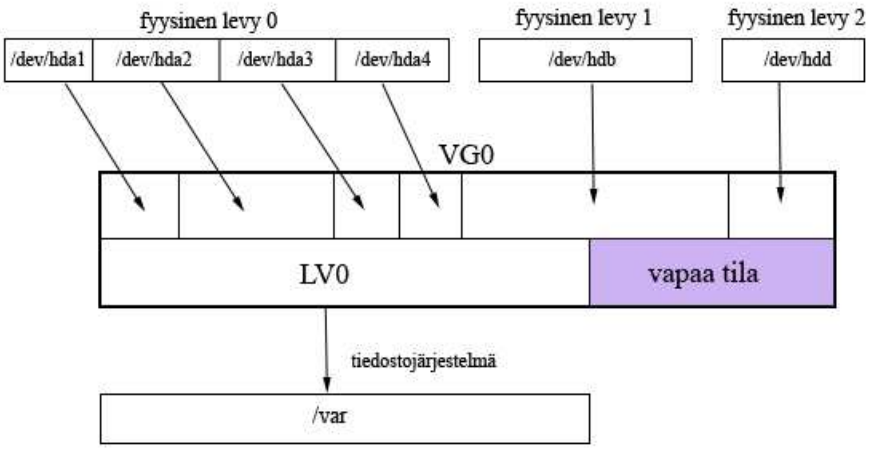
3.3.2 Logical Volume Management

Logical Volume Management on järjestelmien tapa järjestää fyysisten levyjen hallinta korkeammalle tasolle ja usein yksinkertaisempaan muotoon. Sen avulla kaikki fyysiset levyt ja osiot, niiden hajanaisuudesta ja koosta riippumatta, voidaan nähdä yhtenä varastolähteenä. Kun osiot ja kokonaiset levyt kerätään yhdeksi virtuaaliseksi levyksi, voidaan pienet varastointitilat summata suuremmaksi yhdistetyksi varastoksi. Tällaista varastoa kutsutaan nimellä Volume Group. (Kiwi, K. 2007)

Lisäksi LVM:n avulla on mahdollista

- lisätä levyjä/osioita levyaltaaseen ja laajentaa tiedostojärjestelmiä.
- esimerkiksi vaihtaa kaksi 80GB levyä yhteen 160GB levyyn ilman, että järjestelmä pitää kytkeä pois päältä tai käsin siirtää tiedostoja levyjen välillä.
- kutistaa tiedostojärjestelmiä ja tarvittaessa poistaa levyjä altaasta.
- suorittaa yhdenmukaisia varmuuskopioita ottamalla levykuvia. (Kiwi, K. 2007)

Linuxin LVM koostuu kolmesta osasta (Kuva 3), jotka ovat fyysiset volyymit (Physical Volumes), volyymiryhmät (Volume Groups) ja loogiset volyymit (Logical Volumes). Fyysiset volyymit ovat fyysisiä levyjä tai fyysisten levyjen osia (esim. /dev/hda1 tai /dev/hdb1). Volyymiryhmä on fyysisten volyymien kooste ja se voidaan osioida loogisiksi volyymeiksi. Kuvassa 3 fyysisen levyn 0 kaikki neljä osiota ja fyysiset levyt 1 ja 2 on lisätty fyysisinä volyymeina volyymiryhmään VG0. Nyt voidaan kyseisen volyymiryhmän pohjalta luoda halutun kokoinen looginen volyymi. Kuvassa on luotu looginen volyymi LV0 ja jätetty vielä vapaata tilaa muille loogisille volyymeille tai kyseisen volyymin mahdolliseen kasvattamiseen. Loogiset volyymit ovat käytännössä samanlaisia kuin fyysisen levyn osiot. Loogista volyymia voidaan käyttää halutussa tiedostojärjestelmässä sen luomisen jälkeen. (Kiwi, K. 2007)



Kuva 3. Fyysiset levyt muodostavat loogisen volyymin LVM:ssa.

4 VARMUUSKOPIOINTI

Hyvä varmuuskopiointi- ja palautusjärjestelmä on elintärkeä kaiken kokoisille yrityksille. Valitettavasti järjestelmälle ei aina varata sen tarvitsemaa osaa yrityksen budjetista. Vaikka yrityksellä olisi pieni budjetti, ei se tarkoita sitä, että pitäisi tulla toimeen ilman varmuuskopiointijärjestelmää. Iso osa järjestelmistä voidaan toteuttaa myös pienissä ja kustannustehokkaissa ympäristöissä. (Preston 2007, 3)

Esimerkiksi KP-ServicePartner Oy:n varmuuskopiointiratkaisu on tähän mennessä maksanut alle 500 euroa. Maksetusta levytilastakin on ylimääräinen levytila hyötykäytössä, sillä se peilaa Linux Debianin pakettikirjastoa öisin, joten kaistaa ei tarvitse käyttää siihen päivisin työajalla.

Prestonin (2007, 8-10) mukaan yritys voi menettää myös paljon muutakin kuin tiedostoja, jos tietoja ei ole varmuuskopioitu. Kaikista menetyksistä konkreettisin ja pahin on yrityksen mahdollisesti menettämät asiakkaat. Jos esimerkiksi yrityksen asiakastietokanta katoaa kokonaan, kadotetaan mahdollisesti osa asiakaskontakteista lopullisesti. Asiakas voi myös olla riippuvainen jostain yrityksen tarjoamasta tiedosta ja sen menettäminen saattaa olla kohtalokasta. Lisäksi yritys voi menettää tilauksia, kun kadotetaan tietokanta, jossa tilauksien tiedot ovat. Tietojen menettäminen voi vaikuttaa negatiivi-

sesti myös yrityksen imagoon ja yrityksen työntekijöiden moraaliin. Asiakkaiden luottamus yritykseen saattaa olla lopullisesti menetetty, ja myös yrityksen sisällä voi luottamus omaan järjestelmäylläpitoon heikentyä, kun huomataan laiminlyönnit varmuuskopioinnin suhteen.

4.1 Täysi, inkrementaalinen ja differentiaalinen varmistus

Varmuuskopiointityyppejä on kolme, joihin suurin osa varmistusstrategioista perustuu. Ne eroavat toisistaan vain siinä, mitä milloinkin varmistetaan. Täysi varmistus (full backup) varmistaa koko tietojärjestelmän eli jokaisen tietojärjestelmän käyttäjän kaikki tiedostot varmuuskopioidaan. Inkrementaalinen varmistus (incremental backup) varmuuskopioi ainoastaan muuttuneet ja lisätyt uudet tiedostot. Yleensä inkrementaalinen varmuuskopio otetaan kerran tai useammin täysien varmistusten välissä. Differentiaalinen varmistus (differential backup) varmuuskopioi kaikki muuttuneet ja lisätyt tiedostot edellisen täyden varmistuksen jälkeen. Se ei siis ota huomioon aiempia differentiaalisia varmistuksia lainkaan vaan vertailee tiedostoja aina täyteen varmistukseen. Differentiaalisia varmistuksia suoritetaan yleensä yksi tai useampia täysien varmuuskopioiden välissä. (Durham 2002, 332)

Täysi varmistus on järjestelmän ylläpidon perustoiminto. Se käyttää yleensä paljon aikaa ja tallennusresursseja, joten se kannattaa suorittaa silloin, kun järjestelmän kuormitus on pienimmillään. Usein tällainen ajankohta on öisin, kun järjestelmän käyttäjät ovat muualla. Inkrementaalinen varmistus varmuuskopioi ainoastaan muuttuneet ja uudet tiedostot, jotka on luotu viimeisimmän varmistuksen jälkeen. Jos järjestelmä jostain syystä romahtaa, joutuu ylläpito palauttamaan edellisen täyden varmistuksen lisäksi jokaisen sen jälkeen tehdyn inkrementaalisen varmistuksen. Differentiaalinen varmistuksen kanssa ei tällaisessa tilanteessa tarvitse palauttaa kuin viimeisin differentiaalinen varmistus täyden varmistuksen lisäksi. Differentiaalinen varmistus kuitenkin käyttää reilusti enemmän tallennusresursseja kuin inkrementaalinen varmistus. Varmuuskopioinnissa kuitenkin ensimmäisenä vaiheena on aina ottaa täysi varmuuskopiointi. (Durham 2002, 332-333)

4.2 Varmistusstrategiat

Yrityksen kannattaa varmuusstrategiaa luodessaan huomioida omat tarpeensa. Palautuksen tekemisen helppouteen voi vaikuttaa valitsemalla inkrementaalisen tai differentiaalisen varmistuksen täyden varmistuksen lisäksi. Varmistusstrategioista yleisempinä pidetään sellaista, jossa täysi varmistus tapahtuu kerran viikossa ja inkrementaalinen varmistus jokaisena päivänä. Täysi varmistus suoritetaan usein viikonloppuisin, koska silloin järjestelmän käyttöaste on yleensä pienin. Tärkeänä asiana kannattaa muistaa se, että varmistusmediaan ei koskaan pidä täysin luottaa. Vikatilanteita voi aina tapahtua ja esimerkiksi varmistusnauhat voivat korruptoitua tai kulua, jolloin kaikki työ tiedon varmistamiseksi menee hukkaan. Parhaimpia tapoja tietojen arkistoimiseen on sijoittaa yksi varmistus yhdelle tallennusvälineelle. (Durham 2002, 333)

Varmistusstrategioiden toteuttaminen vaatii yritykseltä aikaa, vaivaa ja rahaa. Tehokkainta olisikin varmistaa tiedot heti, kun ne on luotu. Peilauksen avulla voidaan näin tehdä, jolloin tiedot tallennetaan reaaliaikaisesti kahteen paikkaan yhden sijasta. Tietokoneessa oleva toinen kovalevy on yleensä tämä toinen paikka. Ratkaisu on myös vikasietoinen, koska tiedot ovat kahdella eri kiintolevyllä. Toisen kiintolevyn hajotessa tiedot löytyvät kuitenkin vielä toiselta kiintolevyltä. Tämä on kuitenkin ratkaisu vain yksittäisen koneen varmuuskopiointiin. Tehokkaampaa on käyttää tietojen varmistamiseen vikasietoisen järjestelmän ja ulkoista tietovälinettä käyttävän varmistusvälineen yhdistelmää. (Durham 2002, 333-334)

4.3 Varmuuskopiointiratkaisut

Varmuuskopioiden tekemiseen on olemassa useita erilaisia vaihtoehtoja. Esimerkiksi Windows XP:n mukana tulee käyttöjärjestelmän oma varmuuskopiointiohjelma ja markkinoilta löytyy myös laaja valikoima erilaisia varmuuskopiointiin suunniteltuja ohjelmistoja. Internetissä toimii erilaisia palveluja, jotka tarjoavat maksullista varmuuskopiointia suojatuilla yhteyksillä. Normaalille kotikäyttäjälle usein riittää varmuuskopioiminen esimerkiksi DVD- tai CD-levyille, mutta erilaisia kuvagalleriasivustojakin voidaan käyttää esimerkiksi valokuvien varmuuskopioimiseen. Kokeneempi kotikäyttäjä yleensä hankkii ulkoisen kovalevyn tietojensa varmistamiseen. Tietojen tallennukseen

löytyy myös lukuisia yrityksiä, jotka tarjoavat tilaa palvelimiltaan kuukausimaksua vastaan. Kopioiminen palvelimelle tapahtuu yleensä valmistajan tarjoaman verkkopalvelun avulla. (Karhulahti, M. 2007)

Usein järjestelmien ylläpitäjät eivät hanki kaupallista varmuuskopiointiohjelmaa, vaan päätyvät toteuttamaan oman ratkaisunsa. Esimerkiksi Linux-käyttöjärjestelmän vakiotyökaluilla voidaan toteuttaa varmistus. Varmistus tapahtuu komennoilla, jotka voidaan myös automatisoida. Linuxiin on myös saatavana varmuuskopiointiohjelmia, joita kannattaa harkita, kun tarvitaan integroitua varmistusjärjestelmää. Ilmainen varmuuskopiointiohjelma Amanda käyttää tar- ja awk-komentoja, jotka yleensä sisältyvät Linux-jakeluun. Kun käytössä on varmuuskopiointipalvelin, jossa on nauhan vaihtajalla varustettu nauha-asema, voidaan sen avulla varmistaa verkon kaikkien käyttäjien työasemat. (Durham 2002, 334-337)

4.4 Mitä kannattaa varmuuskopioida?

Varmuuskopioinnissa on otettava tarkkaan huomioon se, mitä kaikkea halutaan varmistaa. Ohjelmia, joita ajetaan, ei kannata varmistaa, koska se on epäkäytännöllistä ja jopa vaarallista. Ajettavat ohjelmat käyttävät usein suuren määrän erilaisia kirjastoja, joten varmuuskopiot pitäisi ottaa myös kaikista ohjelman käyttämistä kirjastoista. Lisäksi ajettavien ohjelmien kanssa on olemassa riski siitä, että jos koneelle murtaudutaan ja järjestelmän binäärejä korvataan sopivasti muokatuilla, päätyvät muokatut tiedostot myös varmistusmedialle. Palautustilanteessa tästä aiheutuisi täydellinen katastrofi. Varmistukset onkin järkevintä ottaa ainoastaan varsinaisista työtiedostoista. Sovellusohjelmia ei kannata lähteä varmistamaan, koska kaikki tarvittavat ohjelmat voi helposti aina asentaa uudelleen. (Boström 2003, 102-103)

4.5 Yrityksen verkon asettamat haasteet

Lähtökohtaisesti haastavimpana asiana järjestelmän toteuttamiselle pidin yrityksen verkon hitaita nettiyhteyksiä ja toimipisteiden sijoittumista ympäri Suomea. Varmuuskopioinnit aiheuttavat kopioinnin aikana kuitenkin suuren määrän liikennettä verkkoon, jol-

loin hitaat yhteydet saattavat aiheuttaa erilaisia ongelmatilanteita. Mielenkiintoisen haasteen järjestelmälle antoi myös yrityksen määrittelemät vaatimukset varmuuskopiointiohjelmasta ja se, että järjestelmä toteutettiin tuotantokäytössä oleviin laitteisiin. Ohjelman oli hyvä myös olla GPL (General Public License) -lisenssillä tai vastaavalla, koska yrityksessä on pyritty turvautumaan mahdollisimman paljon avoimen lähdekoodin ratkaisuihin. Yrityksen henkilökuntaan kuuluu osaavia ohjelmoinnin ammattilaisia, jolloin ohjelmistojen muokkaamisen mahdollisuus omiin tarkoituksiin on tärkeää.

Myös verkon käyttäjät antoivat lisähaasteita projektille. Käyttäjiä on yrityksen verkossa monenlaisia ja -ikäisiä, joten kaikkien tietotekniset taidot eivät välttämättä ole samalla tasolla. Käyttäjien ohjeistaminen olikin siis erityisen tärkeässä asemassa.

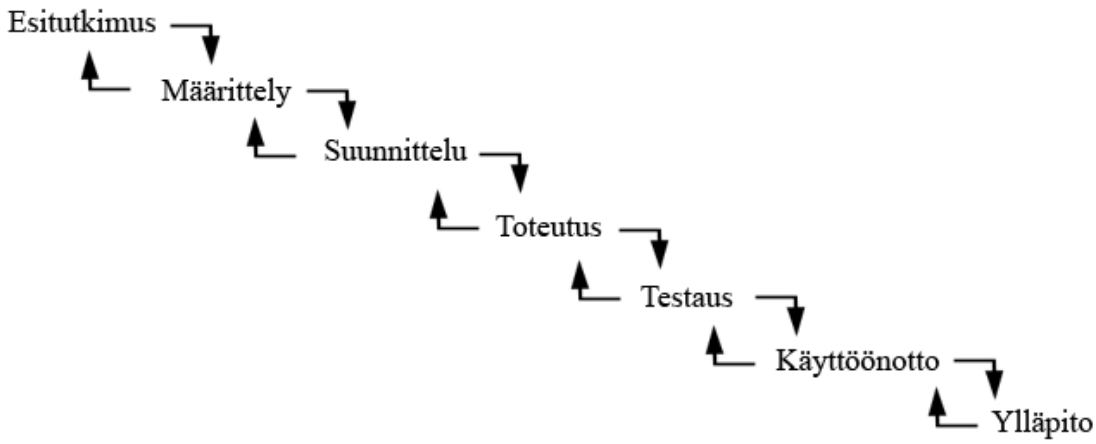
4.6 Ongelmat varmuuskopioimisessa

Tietoturvan kannalta varmuuskopioinnissa on omat ongelmansa. Tietovarkauksien suhteen varmuuskopioinnit luovat keskitetyn tietovaraston, josta löytyy mahdollisesti kaikki tuoreimmat tiedot yrityksen työasemista. Ongelmia saattaa aiheuttaa myös varmuuskopioiden säilyttäminen. Kopioiden on oltava nopeasti saatavilla laiterikon sattuessa ja usein tämä tarkoittaakin sitä, että varmuuskopiot ovat samassa tilassa kuin koneet ja levypalvelin. Jos yrityksen tiedot ovat niin arvokkaita, että niiden vuoksi harkitaan hyökkäystä yrityksen verkkoon, voidaan hyökkäys mahdollisesti tehdä myös fyysisesti. Fyysisen varkauden sattuessa onkin siis erityisen tärkeää, että yrityksen palvelimet sijaitsevat murtautumiselta suojatuissa tiloissa. (Boström 2003, 100-102)

Lisäksi, kun varmuuskopioita otetaan useita lisää jokainen uusi varmuuskopiointi luottamuksellisten tietojen paljastumisriskiä. Palvelimet, joilla varmuuskopioita säilytetään, pitää suojata siis erityisen hyvin. On tärkeää myös muistaa, että jos yritys haluaa tuhota tiedostoja lopullisesti, tulee hävittää myös tuhottujen tiedostojen varmuuskopiot. (Järvinen 2002, 99-103)

5 JÄRJESTELMÄN SUUNNITTELU

Järjestelmän suunnittelussa päädyin käyttämään perinteistä elinkaarimallia eli vesiputousmallia (Kuva 4). Vesiputousmalli kehitettiin jo 1960-luvun lopussa perinteisten fyysisten prosessimallien pohjalta. Mallissa tietojärjestelmien kehittäminen mielletään eteenpäin vievänä prosessina, jossa taaksepäin meneminen on hankalaa. Mallissa tietojärjestelmän kehittämisen vaiheet seuraavat toisiaan alkaen esitutkimuksesta ja lopulta päättyen järjestelmän käyttöönoton jälkeen sen ylläpitoon. Asiat voisivat hoitua näin yksinkertaisesti ideaalissa tapauksessa, mutta usein kehityshankkeissa vaiheet ovat toisistaan riippuvaisia. Monesti tietyn vaiheen suorittaminen paljastaa virheitä edeltävissä vaiheissa, jolloin prosessissa on mentävä taaksepäin korjaamaan virhe. (Pohjonen 2002, 40)



Kuva 4. Vesiputousmalli.

Vaikka tiedostin vesiputousmalliin liittyvät erilaiset ongelmat, katsoin sen kuitenkin selkeimmäksi malliksi projektille. Koska yrityksellä oli jo ennestään varmuuskopiointijärjestelmä käytössä, päättelin yrityksellä olevan sen käytöstä johtuen kokemusta määritellä tarpeensa riittävän hyvin uudelle järjestelmälle. Joten selkeän määrittelyn ja hyvän suunnittelun avulla uskoin vesiputousmallin soveltuvan työhöni hyvin. Toinen mahdollisuus olisi ollut käyttää esimerkiksi prototyyppilähestymistapaa, jossa järjestelmästä olisi tehty prototyyppi asiakkaalle ennen lopullista järjestelmää. Kyseinen ratkaisu ei kuitenkaan olisi kovinkaan kustannustehokas. Toisaalta sovelsin hieman myös tätä lähestymistapaa omassani, koska projektin aikana olin paljon tekemisissä yrityksen järjes-

telmävastaavan kanssa ja sain suoraa palautetta työn eri vaiheissa.

5.1 Järjestelmän määrittely

Järjestelmän määrittely toteutui keskustelemalla yrityksen järjestelmäylläpitäjän kanssa yrityksen tarpeista ja vaatimuksista tulevan järjestelmän suhteen. Järjestelmä oli suunniteltava mahdollisimman dynaamiseksi ja kustannustehokkaaksi mikä tarkoitti sitä, että järjestelmä oli oltava helposti muokattavissa ja sen toteuttaminen ei aiheuttaisi lisäkustannuksia yritykselle. Yritykselle tärkeiden tietojen säilyvyys piti myös varmistaa järjestelmän avulla esimerkiksi tietojen kahdentamisella erilliselle medialle.

Järjestelmää suunniteltaessa tuli ottaa huomioon seuraavat seikat:

- Varmuuskopioiminen saa vaatia hyvin vähän toimenpiteitä käyttäjiltä.
- Etäpisteiden varmuuskopiointi ei saa haitata verkkopalvelujen käyttöä.
- Tieto ei saa muuttua, kun varmuuskopioidaan etäpisteistä.
- Palauttamisen mahdollisuus on oltava ylläpidolle ja edistyneimmille käyttäjille.
- Palauttaminen on oltava mahdollista suoraan koneelle tai erilliselle medialle.
- Järjestelmän on oltava yksinkertainen ylläpitää ja tarkkailla.
- Järjestelmän on oltava tietoturvallinen.
- Järjestelmän vaiheiden testaus tulee suorittaa useilla työasemilla.

Varmuuskopiointijärjestelmän on toimittava automaattisesti ja itsenäisesti. Ylläpitoa varten järjestelmässä on hyvä olla monipuolinen käyttöliittymä, josta saa myös tarkkailtua järjestelmän toimivuutta ja mahdollisia virhetilanteita. Lisäksi järjestelmässä olisi hyvä olla mahdollisuus raportointiin, esimerkiksi sähköpostiin. Suunniteltaessa oli otettava myös huomioon järjestelmän migraatio tulevaisuudessa.

5.2 Varmuuskopiointiratkaisujen vertailu

Varmuuskopiointiratkaisuja on saatavilla runsaasti erilaisia, joten valitsin vertailuun näistä kolme vaihtoehtoa ennen lopullista päätöksen tekoa. Valintakriteerien pohjana käytin järjestelmän määrittelyä ja omaa osaamistani, koska järjestelmän asentamisen ja

käyttöönoton suorittaisin itse. Määrittelyn perusteella ratkaisun piti olla kustannustehokas ja helposti muokattavissa mikä tarkoitti, että varmuuskopiointiohjelman täytyi perustua avoimeen lähdekoodiin. Ratkaisun tuli myös olla suunnattu yrityskäyttöön ja suuriin verkkoihin, joten tavalliseen kotikäyttöön tarkoitetut ratkaisut eivät tulleet kysymykseen. Itselläni ei ollut aiempaa kokemusta vastaavien järjestelmien tekemisestä, joten tärkeänä kriteerinä pidin sitä, että ohjelmistolle oli löydyttävä kattavat ja selkeät ohjedokumentit. Lisäksi otin valintaa tehdessäni huomioon, sen että ohjelmasta oli saatavilla riittävän uusi versio ja sen sivustoa oli päivitetty lähiaikoina. Tämä sen vuoksi, että ei olisi järkevää valita ohjelmaa jota ei enää kehitetä.

Kriteerien pohjalta ohjelmia löytyi kuitenkin useita, joten päätin tutustua muiden käyttökokemuksiin erilaisten foorumien ja nettisivujen kautta. Käyttökokemusten ja suositusten pohjalta löysinkin lopulta kolme sopivaa ohjelmaa, joita ryhdyin tarkemmin vertailemaan. Vertailuun valitsin Amanda-, BackupPC- ja Bacula-ohjelmat. Näiden lisäksi on saatavilla monia muitakin ratkaisuja kuten esimerkiksi Cobian Backup.

5.3 Amanda

Amanda (The Advanced Maryland Automatic Network Disk Archiver) on yksi tunnetuimmista avoimen lähdekoodin varmuuskopiointiohjelmistoista. Amanda kehitettiin alunperin Marylandin yliopistossa vuonna 1991 tarkoituksena turvata tiedostoja suuresta määrästä asiakaskoneita yhden varmuuskopiointipalvelimen avulla. Amanda on yksi tunnetuimmista varmuuskopiointiratkaisuista ja se sisältyykin kaikkiin suuriin Linux-jakeluihin. Amandan avulla voidaan pystyttää yksi varmuuskopiointipalvelin varmistamaan useita Linux-, Unix-, Mac OS X- ja Windows-työasemia monille erilaisille tallennusmedioille. (Preston 2007, 125-126)

5.3.1 Ominaisuudet

Preston (2007, 127-128) pitää Amandan suosion avaintekijänä sitä, että se helpottaa järjestelmäylläpidon työntekoa, koska sen avulla voidaan helposti varmuuskopioida useita verkossa olevia koneita yhden palvelimen avulla nauhalle, levylle tai optiselle medialle.

Amanda on optimoitu varmuuskopioimaan levylle ja nauhalle. Sen avulla on mahdollista myös varmuuskopioida kummallekin medialle yhtäaikaisesti. Varmistetut tiedot on lisäksi mahdollista palauttaa levyltä nopeasti verkon kautta.

Amanda ei käytä mitään valmistajakohtaisia laiteajureita, joten kaikki laitteet joita käyttöjärjestelmä tukee toimivat hyvin. Amanda käyttää yleisiä työkaluja kuten dump ja GNU tar, joten tiedot voidaan palauttaa näillä työkaluilla jopa ilman Amandaa. Amanda on hyvin skaalautuva ohjelma ja sitä voidaankin käyttää vain yhdessä asiakaskoneessa tai jopa tuhansissa. Amanda on kirjoitettu C-ohjelmointikielellä, jossa on joitain Perl-kielellä kirjoitettuja skriptejä mukana ja se on siirrettävissä Linux-, Unix- ja Mac OS X -järjestelmiin. Windows-asiakaskoneet voidaan varmistaa käyttämällä Sambaa tai Cygwin-asiakasohjelmaa, joka on Linuxin kaltainen ympäristö Windowsille. (Preston 2007, 127-129)

Koska Amanda käyttää yleisiä työkaluja, tarjoaa se mahdollisuuden varmistaa myös sparse-tiedostot ja kovat linkit (hard links). Tiedostojen aikaleimat eivät myöskään muutu varmuuskopioinnin aikana. Lisäksi tiedostoja ja kansioita voidaan määrittää pois varmuuskopioinnista. Amandaan on mahdollista myös liittää mikä tahansa nauha-asema mitä pystytään normaalistikin käyttämään valitulla käyttöjärjestelmällä, koska Amanda ei käytä valmistajakohtaisia ajureita. Tämän vuoksi Amandan voi myös turvallisesti päivittää uudempaan versioon. (Preston 2007, 130)

Amanda on suunniteltu perinteiseksi asiakasohjelma/palvelin -arkkitehtuuriksi. Amandan palvelin on yhdistettynä suoraan tai tallennusverkon yli nauha-asemaan tai nauhavaihturiin. Jokaisen asiakaskoneen varmistusohjelma on ohjeistettu kirjoittamaan standardia ulostuloa, jonka Amanda kerää ja lähettää nauhapalvelimelle. Arkkitehtuurin vuoksi Amanda skaalautuu yhden asiakaskoneen ja CD-ROM:n ympäristöstä aina satoja asiakaskoneita ja suuria nauhakirjastoja käsittäviin ympäristöihin. Sen vuoksi myös kaikki kokoonpanoasetukset voidaan tehdä Amanda-palvelimelle, ja kun ne on ensimmäisen kerran tehty, voidaan uusia asiakaskoneita lisätä vaivatta järjestelmään. Arkkitehtuurin vuoksi varmuuskopioidut tiedostot voidaan myös kompressoida ja salata asiakaskoneella ennen niiden lähettämistä palvelimelle. (Preston 2007, 130-131)

Amanda käyttää ns. väliaikaista levyä (holding disk), joka on yksi tai useampi hakemisto jossain tiedostojärjestelmässä, mihin on pääsy palvelimelta. Se voi olla esimerkiksi 10GB suuruinen kansio palvelimen levyllä tai jopa 10TB kokoinen kuituyhteyksinen RAID-levyjärjestelmä. Väliaikaista levyä käytetään välimuistina asiakaskoneiden varmuuskopiointitiedostoille, josta myöhemmin itsenäinen prosessi siirtää varsinaiset varmuuskopioinnit nauha-asemalle parhaalla mahdollisella suoritusteholla. Ratkaisu lisää tietoturvaa tilanteessa, jossa nauha menee rikki tai asemassa on vääränlainen nauha. Amandaa voidaan myös käyttää ilman väliaikaista levyä, jolloin varmuuskopiointien suorituskyky heikkenee selkeästi. (Preston 2007, 133-134)

Palautus Amandassa tapahtuu amrecover- ja amrestore-ohjelmilla. Amrecover palauttaa tiedostot käyttöliittymän avulla, joka mahdollistaa varmuuskopion tiedostojen tarkastelun tietyltä päivämäärältä ja palautettavien tiedostojen valinnan. Amrestore palauttaa ko-ko tiedostojärjestelmän suoraan nauhalta. Amrecover voidaan suorittaa jokaiselta asia-kaskoneelta ja palvelimelta, kun taas amrestore voidaan suorittaa vain Amanda-palvelimelta. Amrecoverin käyttäminen vaatii, että varmuuskopioinnit on indeksoituina järjestelmässä. Amanda tarjoaa kattavan käyttäjien tekemän Wiki-tietosanakirjan ja lisäksi myös kaupallista tukea on tarjolla Zmanda-yhtiön kautta. (Preston 2007, 145-146)

5.3.2 Tietoturva

Amandan asiakaskoneet kommunikoivat palvelimen kanssa sen omien verkkoprotokollien avulla TCP- ja UDP-protokollien päällä. Käytettäessä Amandaa on pidettävä huolta siitä, että vain oma Amanda-palvelin voi kommunikoida asiakaskoneiden kanssa. Amandassa on tähän tarkoitettu oma tiedosto (.amandahosts). Vahvempaan tiedonsiirron suojaamiseen Amanda voi käyttää OpenSSH:ta, jonka avulla voidaan siirrettävä tieto suojata vahvalla autentikoinnilla ja oikeuttamisella. Amanda tarjoaa myös mahdollisuuden varmistusmedialla olevan tiedon suojaamiseen salaamalla tiedot symmetrisillä tai epäsymmetrisillä algoritmeilla. Salaus voidaan tehdä asiakaskoneella tai palvelimella, mutta etenkin etäpisteistä varmistettaessa on suositeltavaa tehdä salaus jo asiakaskoneella, jolloin tieto on valmiiksi salattua sen liikkuessa verkossa. (Preston 2007, 131-132)

5.3.3 Rajoitukset

Amandasta löytyy muutamia rajoituksia. Varmuuskopioitaessa Windows-työasemista käyttäen NFS:ää pitää tiedostojen oikeudet miettiä tarkkaan. Amandan palvelin tarvitsee luku- ja kirjoitusoikeudet. Lukuoikeuksia tarvitaan varmuuskopiointivaiheessa ja kirjoitusoikeuksia palautusvaiheessa. Sambaa käytettäessä mitään auki olevia tiedostoja ja tiedostojen laajennettuja ominaisuuksia ei voida varmuuskopioida. Amanda ei myöskään itse hallitse lainkaan salausavaimia, joten järjestelmäylläpitäjän pitää itse huolehtia avaimista ja niiden saatavuudesta palautuksen aikana. (Preston 2007, 132-143)

5.4 BackupPC

BackupPC on korkean suorituskyvyn omaava Linux- ja Windows-koneiden varmuuskopiointiin tarkoitettu järjestelmä, joka on tarkoitettu lähinnä yrityskäyttöön. BackupPC on laajasti säädettävissä ja helposti asennettava sekä ylläpidettävä. BackupPC on kirjoitettu Perl-ohjelmointikielellä ja se kerää varmuuskopioitavat tiedostot käyttäen SMB:tä (Server Message Block), tar (tape archiver) -komentoriviohjelmaa tai rsync-ohjelmaa. BackupPC on luotettava ja hyvin dokumentoitu avoimen lähdekoodin ohjelma, joka toimii GPL-lisenssin alla. BackupPC tarjoaa myös kattavat tukipalvelut käyttäjille dokumenttien ja sähköpostilistojen muodossa sekä käyttäjien ylläpitämän BackupPC-Wikipedia -palvelun. (Barratt, C. 2007)

5.4.1 Ominaisuudet

BackupPC:n tarjoaa runsaasti eri ominaisuuksia. Älykkään tietovarastoinnin ansiosta BackupPC vähentää levytilan käyttöä ja liikennettä levyjärjestelmässä. Kaikkien varmuuskopioiden kesken identtiset tiedostot samasta tai eri tietokoneesta tallennetaan järjestelmään vain kertaalleen. Esimerkiksi jos varmuuskopioidaan 95 työasemaa, joiden kokonaiset varmuuskopiot (full backup) ovat keskiarvoltaan 3.6GB työasemaa kohden ja jokainen osittainen varmuuskopio (incremental backup) keskiarvoltaan 0.3GB. Tallennettaessa kolme kokonaista varmuuskopiota ja kuusi osittaista varmuuskopiota, tulee

talletettavaa tietoa noin 1200GB, mutta tietovarastoinnin ja kompressoinnin avulla levytilaa tarvitaan ainoastaan 150GB. (Barratt, C. 2007)

BackupPC käyttää kompressointiin deflate- ja inflate-metodeja Compress::Zlib -moduulissa, joka perustuu zlib-kompressointikirjastoon. BackupPC toteuttaa kompressoinnin pienimmällä mahdollisella CPU-kuormituksella. Sen sijaan että kompressoidaan jokainen tuleva varmistustiedosto ja verrattaisiin sitä tietovarastoon, BackupPC laskee MD5-tiivistyksen perustuen kompressoimattomaan tiedostoon. Tätä taas verrataan tietovarastossa olevien kompressoimattomien tiedostojen ja tulevien varmuuskopioitavien tiedostojen kesken. (Barratt, C. 2007)

BackupPC:n hallinnointi tapahtuu nettiselaimessa ohjelman omalla käyttöliittymällä. Sen avulla voidaan säätää asetukset, tarkastella varmuuskopioita sekä käynnistää ja peruuttaa varmuuskopioinnit. Lisäksi myös kokonaisten työasemien tai yksittäisten tiedostojen palauttaminen onnistuu sen kautta. Käyttöliittymä kertoo myös järjestelmän tilan. BackupPC:n käyttäminen ei tarvitse erikseen asennettavaa ohjelmaa asiakaskoneille. Tiedot haetaan asiakaskoneista palvelimelle SMB-protokollaa käyttäen (Windows-koneet), tar-komentoriviohjelmalla yli ssh/rsh/nfs:n (Linux-koneet) ja BackupPC:n versiosta 2.0.0 alkaen myös rsync-ohjelman avulla niistä koneista, joissa on rsync-ohjelma tai rysncd-daemon. Työasemien palautus on mahdollista suoralla palautuksella tai lataamalla ZIP- tai TAR-paketti. (Barratt, C. 2007)

BackupPC:n asetuksista pääsee valitsemaan myös mitä jakoja ja kansioita halutaan tai ei haluta varmuuskopioida. Varmuuskopioiden ajankohtaa voidaan säätää kuten myös käyttäjien sähköpostimuistutusten ajankohtaa. Asetusten parametrit voidaan määrittää koko järjestelmälle tai konekohtaisesti. Järjestelmä voidaan siis asettaa lähettämään käyttäjille sähköpostia, jos heidän työasemiaan ei ole hetkeen varmuuskopioitu. BackupPC on testattu Linux-, Freenix- ja Solaris-palvelimilla sekä Linux- ja Windows 95/98/2000/XP -asiakaskoneilla. (Barratt, C. 2007)

5.4.2 Vaatimukset

BackupPC:n käyttäminen vaatii Linux-, Solaris- tai Unix-pohjaisen palvelimen, jossa on runsaasti vapaata levytilaa. Palvelimen prosessorin ja levyjärjestelmän teho määrittää kuinka monta yhtäaikaista varmuuskopiointia palvelin kykenee käsittelemään. Kohtuullisella palvelimella pystyy käsittelemään yhtäaikaisesti neljästä kahdeksaan varmuuskopiointia. BackupPC suosittelee myös käyttämään LVM- tai RAID-tekniikkaa, jolloin tarvittaessa tiedostojärjestelmää voidaan laajentaa. (Barratt, C. 2007)

Lisäksi palvelimessa on oltava asennettu Perl-ohjelmointikielen versio 5.8.0 tai uudempi. SMB:tä käytettäessä pitää asennettuna olla Samban smbclient- ja nmblookup-ohjelmat. Nmblookup-ohjelmaa tarvitaan myös jos ollaan varmistamassa Linux- tai Unix-pohjaisia DCHP-koneita. Jos käytetään tar-komentoriviohjelmaa pitää siitä olla vähintään versio 1.13.7 tai uudempi. Rsync-ohjelmaa käytettäessä pitää kaikissa Linux- ja Unix-asiakaskoneissa olla asennettuna siitä vähintään versio 2.6.3 tai uudempi. Lisäksi pitää asentaa Perl File::RsyncP -moduulista versio 0.68 tai uudempi. Palvelimeen pitää asentaa myös Apache-verkkopalvelin. (Barratt, C. 2007)

Sambaa tarvitaan, koska yrityksen verkon palvelimissa on Linux-käyttöjärjestelmä, joka käyttää tietoja verkkoon lähettäessä NFS:ää (Network File System). Kun taas verkon työasemissa on pääosin Microsoft Windows-käyttöjärjestelmä, joka käyttää tietojen lähettämiseen SMB:tä. Samban avulla saadaan nämä kaksi yhteensopimatonta tapaa toimimaan yhdessä. (Durham 2002, 30)

BackupPC käyttää kovia linkkejä (hard link) varmuuskopioiden yleisien tiedostojen varastoimiseen, joten sen tietovaraston on osoitettava yhteen tiettyyn tiedostojärjestelmään. RAID- ja LVM-tekniikan avulla onkin ainoa mahdollisuus laajentaa tiedostojärjestelmää ilman, että se pitää kopioida. Tiedostojärjestelmän pitää siis tukea kovia linkkejä, joita esimerkiksi kaikki standardit Linux- ja Unix-tiedostojärjestelmät tukevat. Windows-pohjaiset FAT- ja NTFS-tiedostojärjestelmät eivät tue kovia linkkejä. (Barratt, C. 2007)

5.4.3 Tietoturva

Oletusasetuksena BackupPC toimii itsenäisenä käyttäjänä palvelimella ja se käyttää ennalta jaettua SSH-avainta ilman salasanaa ottaessaan yhteyden asiakaskoneeseen root-käyttäjänä. Windows-asiakaskoneiden kanssa se käyttää salasanalla suojattua SMB:tä. Lisäksi asiakaskoneeseen on mahdollista asentaa rsync-palvelin, joka käyttää tallennettuja salasanoja. Kaikki BackupPC:n prosessit toimivat yhden käyttäjätunnuksen alla. Tällä käyttäjätunnuksella pitää olla rajoitetut oikeudet järjestelmään ja ne voidaan asettaa ohjelman asennusvaiheessa. (Preston 2007, 152)

5.4.4 Rajoitukset

BackupPC:ssä on joitakin rajoituksia. Esimerkiksi smbclient ei kykene lukemaan Windows-koneiden lukittuja tiedostoja, jolloin kyseiset tiedostot eivät tule varmuuskopioiduiksi. Tällaisia tiedostoja ovat esimerkiksi Windowsin rekisteritiedostot. Tämä on ongelmallista etenkin Microsoft Outlook -ohjelman kanssa, koska ohjelma tallentaa kaikki tiedot yhteen suureen tiedostoon ja pitää sen lukittuna, kun ohjelma on käytössä. Ongelmaan on kuitenkin saatavilla ohjelma, jolla kopiointi saadaan onnistumaan. Ongelma koskee myös muitakin samalla tavalla toimivia Windows-palveluita kuten SQL-tietokantoja. (Barratt, C. 2007)

Smbclient-ohjelma ei myöskään poimi Windowsin ACL (Access Control List) -ominaisuuksia, joten ainoastaan tiedostojen samanarvoiset ominaisuudet kopioidaan. BackupPC pystyy hallitsemaan suuria tiedostoja, mutta sen tietovarastot on oltava tiedostojärjestelmässä joka tukee suuria tiedostoja. Lisäksi Perl-ohjelmointikieli on käännettävä niin, että siinä on suurien tiedostojen käyttö määriteltynä. Muuten tiedoston suurin sallittu koko on 2GB. (Barratt, C. 2007)

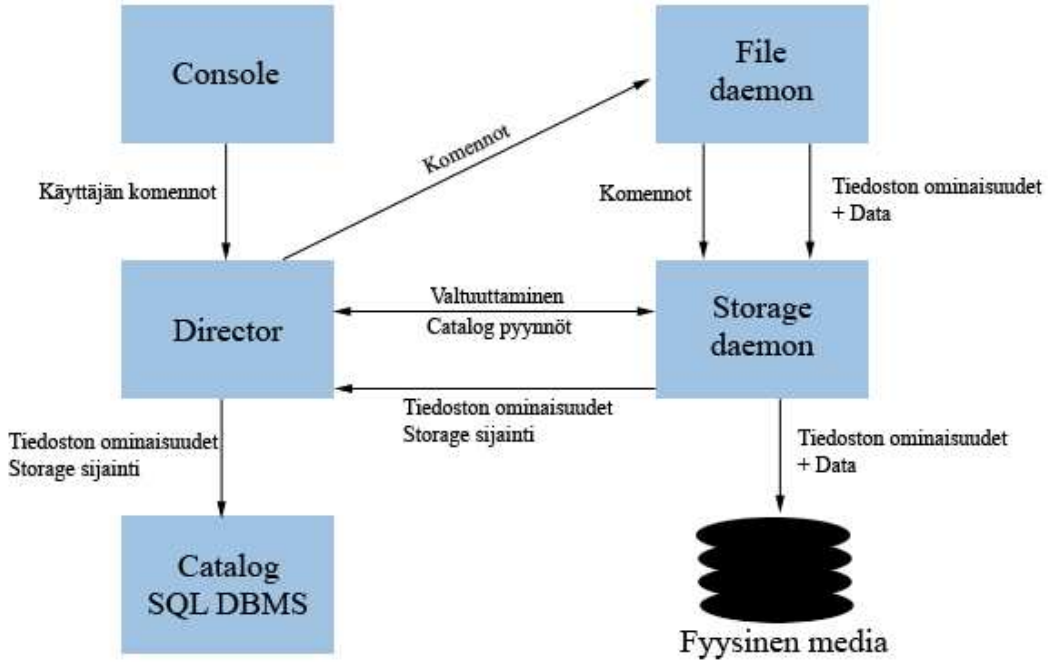
5.5 Bacula

Bacula on joukko avoimen lähdekoodin ohjelmia, jotka antavat mahdollisuuden järjestelmän ylläpidolle hallita varmuuskopiointia, palautuksia ja tiedon liikkumista verkon

erilaisten tietokoneiden välillä. Baculaa voidaan käyttää yhdeltä koneelta ja sen avulla voidaan varmuuskopioida erilaisille medioille kuten esimerkiksi levyjärjestelmille ja nauhoille. Bacula on siis palvelimiin ja asiakaskoneisiin perustuva varmuuskopiointiohjelma. Ohjelmaa on suhteellisen helppoa ja tehokasta käyttää ja se tarjoaa monia kehittyneitä varastoinnin hallintaominaisuuksia joiden avulla on helppoa löytää ja palauttaa tiedostoja. Bacula on suunniteltu niin, että sitä voidaan käyttää niin pienissä verkoissa kuin myös suurissa, jopa satoja koneita sisältävissä verkoissa. Suurin osa ohjelman lähdekoodista on julkaistu GPL-lisenssin alla. (Sibbald, K. 2008)

5.5.1 Ominaisuudet

Bacula-ohjelma koostuu viidestä isosta komponentista tai palvelusta (Kuva 5), joita ovat Director-, Console-, File-, Storage- ja Monitor-palvelut. Director-palvelu on ohjelma, joka valvoo kaikkia varmuuskopiointi-, palautus-, varmennus- ja arkistointioperaatioita. Järjestelmän ylläpito käyttää palvelua varmuuskopioinnin ajastamiseen ja tiedostojen palauttamiseen. Console-palvelu tarjoaa käyttäjälle mahdollisuuden kommunikoida Director-palvelun kanssa. Console-palvelusta on kolme versiota eli tekstipohjainen käyttöliittymä, GNOME-pohjainen käyttöliittymä sekä graafinen käyttöliittymä wxWidgets. (Sibbald, K. 2008)



Kuva 5. Bacula-ohjelman palveluiden vuorovaikutus.

File-palvelu on ohjelma, joka asennetaan varmuuskopioitaviin asiakaskoneisiin. Se välittää tiedostojen ominaisuudet ja datan Director-palvelun pyynnöstä. File-palvelu on myös vastuussa tiedostojärjestelmästä riippuvasta osasta, kun tiedostojen ominaisuuksia tai dataa ollaan palauttamassa. Ohjelma toimii daemon-taustaohjelmana asiakaskoneessa. Unix- ja Linux-järjestelmän daemon-ohjelman lisäksi on saatavilla myös vastaava Windows-järjestelmiin. Se toimii Windowsin NT-, 2000-, XP-, 2003- ja mahdollisesti myös Me- ja 98-versioissa. (Sibbald, K. 2008)

Storage-palvelu käsittää ohjelmat, jotka suorittavat tiedostojen ominaisuuksien ja datan varastoinnin fyysisille medioille sekä niiden palauttamisen niistä. Toisin sanoen se kirjoittaa ja lukee fyysisiltä medioilta. Monitor-palvelun avulla käyttäjä voi katsoa varmuuskopiointijärjestelmän tilan. Lisäksi Baculassa on Catalog-palvelu mikä muodostuu ohjelmista, jotka ylläpitävät luetteloita tiedostoista ja tietokannoista, joihin kaikki tiedot varmuuskopioidaan. Palvelun avulla käyttäjä voi nopeasti etsiä ja palauttaa haluamansa tiedoston. (Sibbald, K. 2008)

Ohjelmassa on sisäinen järjestelijä, minkä avulla voidaan automatisoida tehtäviä. Tehtäviä on mahdollista ajastaa suoritettavaksi myös useita samanaikaisesti. Tehtäville voi-

daan ohjelmassa asettaa tärkeysjärjestys. Ohjelman avulla voidaan palauttaa yksi tai useampia tiedostoja uusimmasta tai aiemmasta varmuuskopiosta. Bacula luo kattavan SQL-standardin tietokannan kaikista varmistetuista tiedostoista, jolloin niitä voidaan tarkastella verkosta. Vanhat tiedostot kuitenkin poistetaan tietokannasta automaattisesti. (Sibbald, K. 2008)

5.5.2 Vaatimukset

Bacula-ohjelmaa ajetaan Linux-, FreeBSD- ja Solaris-järjestelmillä. Sen kääntäminen vaatii GNU C++ -kääntäjästä version 2.95 tai uudemman. Baculan käyttäminen voi myös vaatia joitakin kolmannen osapuolen paketteja. Tietokannoista Bacula tukee MySQL:n versiota 4.1, PostgreSQL:n versiota 7.4 sekä SQLite:n versiota 2.8.16. Tietysti se tukee myös näiden tietokantojen uudempiakin versioita. Linux-jakeluista Bacula tukee ainakin Gentoo-, Red Hat-, Fedora-, Mandriva-, Debian-, OpenSuSE-, Ubuntu- ja Kubuntu-jakeluita. Bacula tukee asiakaskoneissa Windowsin versioita Win98/Me, WinNT/2K/XP ja Vista. Lisäksi se tukee Mac OS X/Darwin -koneita sekä OpenBSD- ja Irix-koneita. Bacula tukee myös nauha-asemia, mutta ei ole suoraan yhteydessä niihin. Nauha-aseman pitäisi kuitenkin toimia Baculassa, jos siihen vain pääsee käsiksi käyttöjärjestelmästä. (Sibbald, K. 2008)

5.5.3 Tietoturva

Lähetettäessä tietoja verkoissa, joihin ei luoteta voidaan Baculassa liikenne tunneloida stunnel- tai ssh port-forwarding -ohjelmalla. Tällöin pitää vain ohjata daemonit oikeisiin portteihin ja ohjelmat hoitavat autentikoinnin. Baculan nykyisissä versioissa on mukana TLS (Transport Layer Security) -tuki. Sen avulla voidaan varmistaa, että Baculan palveluiden välinen liikenne ei siirry selkeänä tekstinä. Baculan versiot versiosta 1.39 eteenpäin tukevat varmuuskopioitujen tietojen salausta estämään luvattomien käyttäjien pääsy tietoihin. Suuret yritykset vaativat nykyisin, että tieto on salattua tietoa siirrettäessä ja tallennettaessa. Se on tietysti hyödyllistä myös yksittäiselle käyttäjälle. Käyttäjä voi näin esimerkiksi estää varkaan lukemasta yksityisiä tiedostojaan, joita käyttäjä on varmistanut esimerkiksi DVD-levylle. Salauskoodi käyttää TLS-sertifikaatteja hallitse-

maan salausavaimia. (Preston 2007, 173-174)

5.5.4 Rajoitukset

Ohjelmassa on joitakin rajoituksia ja ongelmia. Täyden varmistuksen jälkeen tuhotut tiedostot esimerkiksi sisältyvät palautukseen, mikä on usein tyypillistä tämän tyylisille ratkaisuille. Baculan differentiaaliset ja inkrementaaliset varmuuskopiot perustuvat aikaleimoihin. Tästä johtuen esimerkiksi siirrettäessä tiedostoja olemassa olevaan kansioon täyden varmistuksen jälkeen, eivät nämä tiedostot tule varmistetuksi seuraavassa inkrementaalisessa varmistuksessa. Syynä tähän on se, että tiedostojen aikaleimoissa on edelleen vanha aika ja se pitäisi päivittää käsin. Bacula ei voi myöskään palauttaa kahta eri työtä samassa palautuksessa, koska töiden tietolohkot ovat voineet mennä sekaisin, jos töitä on tehty samanaikaisesti. (Sibbald, K. 2008)

Bacula voi yleensä palauttaa minkä tahansa varmuuskopion asiakaskoneesta toiseen asiakaskoneeseen. Jos verkon arkkitehtuuri on selkeästi poikkeava voi joitain rajoituksia ilmetä, esimerkiksi palautettaessa 32-bittisestä arkkitehtuurista 64-bittiseen tai Windows-koneesta Unix-koneeseen. Bacula tukee varmuuskopioiden ja palautusten tekoa useille eri laitteille ja medioille. Kuitenkin jos työ on varmuuskopioitu useaan varastolaitteeseen, voi Bacula tehdä palautuksen ainoastaan yhdestä. (Sibbald, K. 2008)

5.6 Ratkaisujen vertailu ja valinta

Varmuuskopiointiratkaisujen vertailussa kiinnitin huomiota järjestelmän määrittelyyn ja siinä ilmi tulleisiin vaatimuksiin. Vertailin ohjelmia keräämällä yhteen ohjelmien hyvät ja huonot puolet (Taulukko 1).

Taulukko 1. Varmuuskopiointiratkaisujen hyvät (+) ja huonot (-) puolet.

Amanda	BackupPC	Bacula
+ Varmistus useille medioille + Skaalautuva + Tietoturvallisin ratkaisu - Suunniteltu nauhajärjestelmille - Palautus kahdella ohjelmalla - Asentaminen vaikeaa - Vaikea hallita - Dokumentointi	+ Varmistus useille medioille + Skaalautuva + Dokumentointi + Älykäs tietovarastointi + Käyttöliittymä + Helppo asentaa + Helppo hallita + Raportointi - Tietoturva - Lukitut tiedostot	+ Varmistus useille medioille + Skaalautuva + Monipuolinen tehtävien automatisointi + Dokumentointi - Vaikea hallita - Vaatii ohjelman asiakaskoneisiin - Tietoturva

Kaikissa ratkaisuissa tuettiin varmistamista useille medioille ja kaikki olivat skaalautuvia eli niillä on mahdollista varmuuskopioida pieniä sekä suuria lukuisia koneita käsittäviä verkkoja. Amanda oli ohjelmista selkeästi tietoturvallisin vaikka tietoturvaa ei muissakaan oltu unohdettu. Baculan tietoturvallisuuden katsoin huonoksi puoleksi, koska siinä käyttäjä voi joutua itse määrittelemään porttiasetuksia. BackupPC ja Bacula ovat molemmat erinomaisen hyvin dokumentoitu ja pidin sitä tärkeänä asiana, koska se auttaa järjestelmän käyttöönotossa, ja siitä on mahdollisesti apua erilaisissa ongelmatilanteissa. Kiinnitin myös huomiota asennuksen, hallinnan ja palauttamisen helppouteen. Amandan asentaminen ja hallinta on selvästi vaikeinta. Lisäksi palauttamiseen on käytettävä kahta eri ohjelmaa, kun taas esimerkiksi BackupPC:llä palauttaminen ja järjestelmän hallinta tapahtuu kaikki samassa käyttöliittymässä.

Baculan huonoin puoli oli se, että asiakaskoneisiin pitää asentaa oma ohjelma. Tämän vuoksi Bacula erosikin selkeästi muista ratkaisuista ja lopullisen valinnan suoritinkin Amandan ja BackupPC:n välillä. Vertailu kääntyi lopulta BackupPC:n hyväksi. Tärkeimpinä kriteereinä pidin sen erinomaista käyttöliittymää, hyvää dokumentointia ja älykästä tietovarastointia, jossa tiedot tallennetaan palvelimelle vain kertaalleen. BackupPC vaikutti selvästi sopivammalta ratkaisulta yrityksen verkon rakenteeseen, kun taas Amanda soveltuu selkeästi enemmän verkkoihin, joissa on suuria nauhakirjastoja.

Valittu ratkaisu myös vastasi järjestelmän määrittelyä. BackupPC:n käyttäminen on helppoa ja ohjelma tarjoaa monipuoliset mahdollisuudet palauttamiselle. Varmuuskopiointien onnistumista on helppo monitoroida ja ohjelman käyttöliittymässä on monipuoliset mahdollisuudet säätää järjestelmän toimintoja. BackupPC tarjoaa myös riittävän ta-

son tietoturvassa vaikka se ei olekaan ratkaisuista tietoturvallisin vaihtoehto. BackupPC on kokonaisuutena selvästi paras vaihtoehto yritykselle.

5.7 Järjestelmän suunnitteleminen

Pohjosen (2002, 32) mukaan suunnittelun tarkoituksena on muuntaa järjestelmän toiminnallinen määrittely järjestelmän tekniseksi määrittelyksi, joka kuvaa järjestelmän toteutuksen. Hänen mukaan suunnittelulle asetettavia tavoitteita ovat selkeys, ymmärrettävyys, tehokkuus, luotettavuus, ylläpidettävyys sekä siirrettävyys. Prestonin (2007, 18-27) mielestä järjestelmää suunniteltaessa on tärkeää miettiä miksi ylipäänsä ollaan varmistamassa. Hänen mielestään on tärkeää myös valita mitä varmuuskopioidaan, miten varmuuskopioidaan ja milloin varmuuskopioidaan.

Suunniteltaessa on hyvä ottaa huomioon järjestelmän mahdollinen kasvaminen. On hyvä suunnitella mitä tällaisessa tilanteessa tulee tehdä. Muutenkin suunnittelussa on hyvä pyrkiä katsomaan eteenpäin ja varautumaan tulevaisuuden haasteisiin. Varmuuskopiointijärjestelmä kannattaa tehdä hyvin heti ensimmäisellä kerralla. (Preston 2007, 39)

5.7.1 Varmuuskopioitavat tiedostot

Prestonin (2007, 19) mukaan kokemus on osoittanut, että yleisempiä syitä tietojen menetykseen on se, että kyseistä tietoa ei oltu koskaan määritetty varmistettavaksi. Hänen mielestään päätös siitä, mitä varmistetaan, onkin erityisen tärkeä. Preston (2007, 21) pitää erityisen tärkeänä sitäkin, että varmuuskopiointipalvelin on myös varmistettu.

Järjestelmää suunnitellessa otin huomioon yrityksen verkon nopeudet sekä työasemien käyttötarkoitukset, joiden vuoksi katsoin järkeväksi varmuuskopioida ainoastaan kriittiset tiedostot työasemista sekä palvelimet, jotka tuottavat yrityksen toiminnan kannalta olennaiset palvelut. Kokonaisia työasemia ei ollut mahdollista lähteä varmuuskopioimaan rajallisen verkon suorituskyvyn vuoksi. Tärkeämpää olikin rajata selkeästi varmuuskopioiminen käsittämään kaikki yrityksen toiminnalle tärkeät tiedostot. Mitään ohjelmiakaan ei kannattanut lähteä varmistamaan, koska niiden uudelleen asentaminen

ei aiheuta suurta vaivaa. Toimipisteessä A asennus hoituu nopeasti, koska ylläpito löytyy samasta toimipisteestä. Muut toimipisteet voidaan hoitaa etäyhteyden avulla ja isommat asennukset kuten käyttöjärjestelmän uudelleenasennukset voidaan hoitaa lähtemällä paikan päälle tai postittamalla työasema toimipisteeseen A, jos ilman työasemaa tullaan muutama päivä toimeen.

Päädyin ratkaisuun, jossa työasemista varmuuskopioidaan Documents And Settings -kansio kokonaisuudessaan. Kansio sisältää käyttäjien henkilökohtaiset profiilit, dokumentit ja kansiot, Käynnistä-valikon tiedot, työpöydän pikakuvakkeet ja tiedostot, Internet-selaimen suosikit sekä sähköpostit. Käytännössä siis kaikki käyttäjälle tärkeät tiedot. Yrityksen verkon työasemia tutkittuani kyseinen kansio oli yleensä kooltaan yhdestä kolmeen gigatavuun, mikä olisi sopivissa rajoissa yrityksen verkon kapasiteetille tekemäni laskelman perusteella (Taulukko 2). Lisäksi käyttäjille on oltava myös mahdollisuus lisätä muitakin kansioita varmuuskopioitavaksi, koska kaikki tärkeät työtiedostot eivät välttämättä ole tallennettuna Documents And Settings -kansioon. Yrityksen työntekijöiden käytössä kuitenkin on erilaisten teknisten laitteiden ohjaamiseen tarkoitettuja ohjelmistoja ja suunnittelusovelluksia, joiden työtiedostot yleensä tallentuvat omiin kansioihin. Windows Vista -käyttöjärjestelmässä Documents And Settings -kansiota vastaa Users-kansio. Ratkaisun vuoksi on myös tärkeää ohjeistaa käyttäjiä tallentamaan työnsä kyseiseen kansioon tai työpöydälle, jolloin ne tulevat varmasti varmuuskopioiduksi. Lisäksi heitä pitää ohjeistaa pitämään kyseinen kansio sopivan kokoisena verkon kapasiteetin vuoksi.

Taulukko 2. Yrityksen verkon siirtonopeudet ja esimerkkinä 3GB:n siirron kesto minuuteissa.

	Nopeus (MB(s)	3GB siirron kesto (min)
Palvelimet	15,79 - 33,29	1,54 - 3,24
Työasemat (Toimipiste A)	1,21 - 8,66	5,91 - 42,31
Työasemat (Muut)	0,05 - 1,63	31,41 - 1024

Tiedostoja varmuuskopioitaessa on vältettävä tilannetta, jossa varmuuskopiota ei tiettynä hetkenä ole olemassa ollenkaan. Jossain ratkaisuissa esimerkiksi täyttä varmuuskopiointia otettaessa vanhan täyden varmuuskopion päälle ei varmuuskopiota ole kirjoittamisen aikana olemassa. Jos tällaisessa tilanteessa tapahtuu jokin kriittinen virhe, voi varmuuskopio ja alkuperäinen tieto kummatkin tuhoutua. BackupPC:ssä tällaista tilannetta ei kuitenkaan pääse syntymään, koska ohjelma säilyttää useita kokonaisia var-

muuskopioita eikä koskaan kirjoita uusia tiedostoja vanhojen kokonaisten varmuuskopioiden päälle. BackupPC käyttää kovia linkkejä viitatessaan tiedostoihin varmuuskopioiden välillä.

5.7.2 Varmuuskopioitavat työasemat ja palvelimet

Yrityksen työasemista suurin osa on henkilökohtaisessa käytössä hallinnon työntekijöillä ja insinööreillä. Muut työasemat ovat tehtaiden tuotantotyöntekijöiden yleisessä käytössä. Näitä työasemia käytetään pääasiassa merkitsemään tehdyt työt Maximo-kunnossapitojärjestelmään ja satunnaiseen nettiselailuun. Maximo-järjestelmä sijaitsee yhteistyökumppani ABB Oy:n omilla palvelimilla, joten kyseisissä työasemissa ei juuri ole kriittisiä tiedostoja, joita pitäisi varmistaa. Tärkeintä onkin varmuuskopioida kaikki ne työasemat, jotka ovat henkilökohtaisessa käytössä ja millä tehdään töitä päivittäin.

Yrityksen kolmesta fyysisestä palvelimesta kahdella on yrityksen toiminnan kannalta tärkeitä palveluita. Palvelin A tuottaa palveluina toimialueen tunnistuksen, toimialueen levyjaot sekä henkilökohtaiset levyjaot ja Intranetin. Palvelin B sisältää virtuaalikonepalvelun, Linux Debianin peilipalvelun, tietokannan ja työssä asennettavan varmuuskopiointijärjestelmän. Lisäksi sen virtuaalikoneissa pyörii Pandan virustorjuntapalvelin ja DMZ-kone. Kolmas palvelin on testikäytössä eikä sisällä yrityksen toiminnalle tärkeitä tietoja. Palvelimista pitää varmuuskopioida kummatkin palveluita tuottavat palvelimet. Testipalvelinta ei tarvitse varmuuskopioida, mutta se voidaan tarvittaessa liittää helposti myöhemmin varmistettavaksi.

5.7.3 Milloin varmuuskopioidaan?

Prestonin (2007, 27) mukaan jokainen järjestelmä eroaa toisistaan tavoissa kuinka usein täysi varmuuskopiointi tehdään, kuinka usein inkrementaalinen varmistus tehdään ja millaisilla asetuksilla nämä otetaan. Hänen mielestään kuitenkin yhden asian pitäisi yhdistää kaikkia järjestelmiä – jokaisena yönä pitäisi ottaa ainakin jonkin asteen varmuuskopiointeja.

Yrityksessä työskennellään pääsääntöisesti päivävuorossa, mutta myös iltaisin. Öisin ja viikonloppuisin työskennellään harvemmin ja työt eivät yleensä aiheita liikennettä verkkoon. Verkon kuormituksen vuoksi on järkevintä ajoittaa varmuuskopiointi sellaiseen ajankohtaan, jolloin yrityksen verkon käyttöaste on pienimmillään. Tällainen ajankohta on siis öisin ja viikonloppuisin. Varmuuskopioinnin ajankohtaa voidaan myöhemmin hienosäätää käyttökokemuksien perusteella tarkemmaksi. Alkuun on kuitenkin hyvä lähteä siitä, että varmistukset tapahtuvat arkipäivinä öisin ja viikonloppuina mahdollisesti koko vuorokauden aikana.

Täysi varmistus on hyvä ottaa ainakin kerran viikossa ja inkrementaaliset varmistukset päivittäin. Täysi varmistus aiheuttaa verkkoon huomattavasti enemmän kuormitusta, joten se on paras suorittaa viikonloppuisin, jolloin vältytään varmistuksen venymisestä seuraavan työpäivän aamulle. Inkrementaaliset varmistukset on hyvä ottaa päivittäin etenkin arkisin, jolloin syntyy uusia työtiedostoja ja vanhat tiedostot muuttuvat työnteon aikana.

5.8 Varmuuskopioiden varmistus

Prestonin (2007, 21) mukaan on erittäin tärkeää varmuuskopioida myös varmuuskopiot, kun ne on tallennettu keskitetysti yhdelle palvelimelle. Koska kaikki tiedot sijaitsevat varmuuskopioituina yhdessä paikassa on tämä selvästi järjestelmän kriittisin piste. Yrityksen palvelimet on varmistettu lisäksi nauhalle, joten varmuuskopioinnit sijaitsevat järjestelmässä kolmeen kertaan. Yksi varmuuskopiointijärjestelmässä, toinen peilatulla levyllä ja kolmas arkistoituna nauhalle. Tietysti alkuperäiset tiedot löytyvät myös työasemalta, josta ne on varmuuskopioitu. Tällaisenaan järjestelmä on mielestäni riittävän hyvin varmistettu.

Yrityksessä käytetään nauha-asemaa, joka tukee maksimissaan 72 gigatavun nauhoja. Nauhojen kierrätys on neljällä päivänauhalla, yhdellä viikkonauhalla sekä aina uusittavilla kuukausinauhoilla. Palvelimet varmistetaan päivänauhoille maanantaisin, tiistaisin, keskiviikkoisin sekä torstaisin. Perjantaisin otetaan viikon varmuuskopio. Päivä- ja viikkonauhat ovat kiertävässä käytössä. Kuukauden viimeisenä perjantaina otetaan kuukausikopio aina uudelle nauhalle, joka arkistoidaan lukittuun tilaan. Koska nauhapalvelin

on eri palvelimella kuin varmuuskopioinnit, pitää ne ensiksi siirtää samalle palvelimelle ja sitten kopioida tar-ohjelmalla nauhalle.

5.9 Suunnitelman dokumentointi

Varmuuskopioiminen on järjestelmäylläpidon osa-alue, jossa huono dokumentointi tarkoittaa ongelmia tulevaisuudessa. Jos esimerkiksi varmuuskopioinnista vastaava henkilö organisaatiossa jostain syystä vaihtuu tai on vaikka lomalla, on jonkun muun vaikea päästä selville järjestelmästä ilman hyvää dokumentaatiota. Tämän vuoksi järjestelmästä pitäisikin olla olemassa tarvittavat dokumentit, joiden avulla voidaan järjestelmää käyttää ilman järjestelmän asiantuntijan läsnäoloa. (Preston 2007, 51)

Yrityksen toiveesta tein järjestelmän suunnitelmasta erillisen dokumentin, jonka yritys säilyttää arkistossaan (Liite 1). Dokumentti sisältää järjestelmän suunnitelman yksityiskohtineen.

6 TESTAUS

Preston (2007, 47) pitää varmuuskopioiden testaamista erityisen tärkeänä ja kertoo, että testaaminen jätetään usein vallan tekemättä ja viat huomataan vasta palautuksen yhteydessä, jolloin se on jo liian myöhäistä. Hänen mielestään tätä seikkaa ei voida painottaa tarpeeksi, ja jos varmuuskopioita ei testata, tullaan takuulla kokemaan ikäviä yllätyksiä jossain vaiheessa.

Varmuuskopioinnin kannalta on tärkeää testata kaiken tyyppiset palautukset. Tietojärjestelmän varmuuskopiointeja testatessa kannattaa testausvaiheessa palauttaa ja vertailla useita yksittäisiä tiedostoja, tiedostojen vanhempia versioita ja kokonaisia levyjä tai tiedostojärjestelmiä. Lisäksi voidaan kuvitella erilaisia järjestelmän vikatilanteita ja koettaa palautua niistä. Tietokantojen palautusta voidaan testata palauttamalla osan

tietokannasta tai palauttamalla koko tietokanta toiselle palvelimelle, jolloin voidaan saada selville mitkä tiedostot eivät palaudu. Tietokanta voidaan palauttaa myös aiempaan hetkeen, joka olisi tarpeellista esimerkiksi tilanteessa, jossa tietokannan edellisen yön varmuuskopiointi olisi epäonnistunut. (Preston 2007, 47-48)

Testaaminen kannattaa ottaa yleiseksi tavaksi, sillä se, mikä toimii nyt, ei välttämättä toimi enää kuukauden kuluttua. Yksi vaihtoehto on tehdä esimerkiksi lista palautustoimenpiteistä ja testata näitä sattumanvaraisesti kuukausittain. Hallinta, laitteisto ja tietoverkot sekä käyttöjärjestelmien ja tietokantojen versiot muuttuvat, jolloin järjestelmän toiminta voi myös muuttua niiden asentamisen jälkeen. (Preston 2007, 48)

Järjestelmään ei kannata tehdä muutoksia ja sen jälkeen vyöryttää niitä kerralla kaikkiin järjestelmän laitteisiin. Muutosta kannattaa testata aluksi kehitysympäristössä tai järjestelmässä, jota et normaalisti varmista. Vanhaa toimivaa versiota järjestelmästä ei kannata poistaa ennen kuin ollaan sataprosenttisen varmoja, että uusi versio toimii täydellisesti. Kun muutoksia ryhdytään siirtämään verkon laitteisiin, kannattaa se tehdä portaittain yksi laite kerrallaan ja katsoa miten se vaikuttaa järjestelmän toimintaan. (Preston 2007, 50)

6.1 Testaaminen palvelimella

Asensin BackupPC-ohjelmiston aluksi testipalvelimelle, joka minulla oli käytössä. Tarkoitukseni oli testata järjestelmän asennuksen onnistumista ja sen toimintaa. Sain ohjelman asennettua helposti ohjeiden avulla eikä minkäänlaisia ongelmia ilmennyt asennuksen aikana. Tässä vaiheessa testasin ohjelman selainpohjaisen käyttöliittymän toimintaa tekemällä asetuksiin muutoksia ja tarkkailemalla niiden onnistumista. Muuta testaamista pystyin suorittamaan vasta sitten, kun olin liittänyt työaseman varmuuskopioitavaksi järjestelmään.

6.2 Testaaminen työasemilla

Testikäyttöön otin omassa henkilökohtaisessa käytössäni olevan työaseman, jonka asensin varmuuskopioitavaksi. Liitin työaseman varmuuskopioitavaksi BackupPC-ohjelmassa ja koneestani laitoin Documents And Settings -kansion jaettavaksi ja ohjelmalle oikeudet lukea kyseistä kansiota. Tämän jälkeen laitoin varmuuskopioinnin siirtymään palvelimelle. Kansion varmuuskopiointi onnistui ja kansion tiedostoja pääsi tarkastelemaan BackupPC-ohjelmasta. Ohjelmasta kuitenkin ilmeni, että siirrossa tapahtui joitakin siirtovirheitä (Xfer errors). Virheitä pääsi helposti tarkastelemaan ja ilmeni, että ohjelma ei siirtänyt ns. lukittuja tiedostoja, koska olin kirjautuneena työasemaani (Kuva 6). Varmuuskopiointi kuitenkin onnistuu vaikka tällaisia virheitä tuleekin. Koska kopioinnit tehdään työajan ulkopuolella pitää käyttäjiä ohjeistaa kirjautumaan ulos työasemistaan töistä lähtiessään, jolloin siirtovirheitä tulisi mahdollisimman vähän.

```
NT_STATUS_SHARING_VIOLATION opening remote file \NetworkService\NTUSER.DAT (\NetworkService\)
NT_STATUS_SHARING_VIOLATION opening remote file \NetworkService\ntuser.dat.LOG (\NetworkService\)
[ skipped 17 lines ]
```

Kuva 6. BackupPC:n virheilmoitus varmuuskopioinnin siirrossa. Lukitut tiedostot eivät siirry.

Testasin varmuuskopiointia vielä toisella kansiolla, jonka jälkeen kokeilin tiedostojen palauttamista mikä onnistui myös hyvin. Yrityksen muut työasemat ovat tuotantokäytössä, joten en päässyt niitä varsinaisesti tässä vaiheessa vielä testaamaan. Minun oli luotettava siihen, että voin testata työasemia etenkin muilta paikkakunnilta niiden järjestelmään asentamisen yhteydessä. Tämän vuoksi olikin tärkeää liittää järjestelmään yksi työasema kerrallaan ja tarkkailla järjestelmän toimintaa muutamia päiviä aina liittämisen jälkeen. Näiden testausten jälkeen ryhdyin asentamaan järjestelmää tuotantokäyttöön.

7 KÄYTTÖÖNOTTO

Testauksen jälkeen järjestelmä voidaan ottaa käyttöön. Käyttöönottoon liittyy aina tekijöitä joita tulee ottaa huomioon. Tällaisia tekijöitä ovat mahdollisten tietojen, tiedostojen ja tietokantojen siirtäminen uuteen järjestelmään. Olemassa olevat aikaisemmat ja rinnakkaiset järjestelmät tulee myös huomioida. Tärkeää on myös käyttäjien ja ylläpitohenkilökunnan kouluttaminen uuden järjestelmän käyttöön. Käyttäjille pitää vähintään tehdä asianmukainen käyttöohjeistus. (Pohjonen 2002, 37)

7.1 Asennus palvelimiin

Palvelimessa johon BackupPC-ohjelman asensin on käyttöjärjestelmänä Linux Ubuntu -distribuutio. Ennen varsinaisen ohjelman asentamista tarkistin löytyykö palvelimelta kaikki tarvittavat ohjelmat, joita BackupPC vaatii ja asensin puuttuvat. Palvelimesta piti siis löytyä Perl-ohjelmointikieli, Apache-verkkopalvelin, smbclient ja nmblookup SMB:tä varten, tar- ja rsync-ohjelmat sekä Perl File::RsyncP -moduuli. Lisäksi asensin Compress::Zlip -moduulin varmuuskopioiden kompressointia varten, Archive::Zip -moduulin tukemaan palauttamista Zip-tiedostoilla ja XML::RSS -moduulin mahdollista RSS-ominaisuutta varten. BackupPC:n asennuspaketti asentaa nämä kaikki myös automaattisesti.

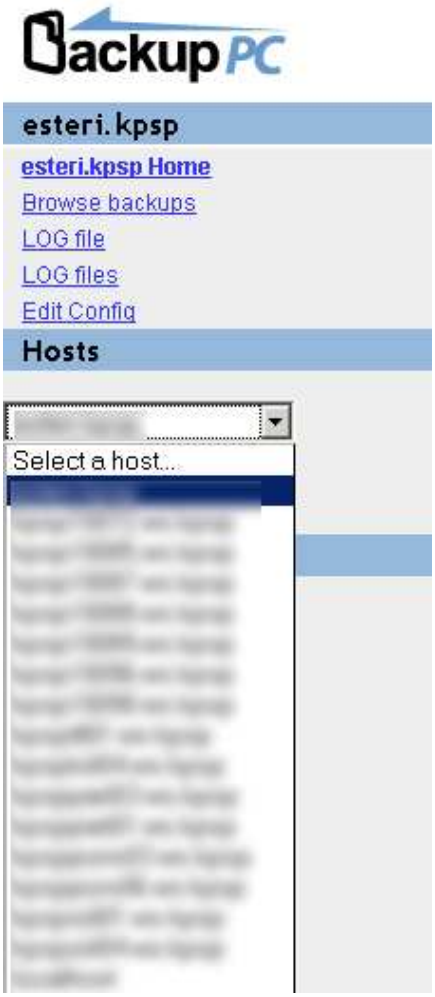
Varsinaisen ohjelman asentaminen on varsin yksinkertaista. Latasin BackupPC:n asennuspaketin (uusimman version 3.1.0) ohjelman kotisivujen kautta ja purin sen palvelimelle ja käynnistin asennustiedoston. Ohjelman asennus kysyy asennuksen aikana käyttäjänimeä ohjelmalle, konenimeä (hostname) ja kohdekansioita varmuuskopioinneille, asennustiedostoille sekä CGI:lle (Common Gateway Interface). Käyttäjänimeksi määritin BackupPC, jolle annettiin kaikki oikeudet käyttää ohjelmaa palvelimella ja kohdekansiot sekä konenimen jätin oletusarvoiksi. CGI-tiedot menevät automaattisesti Apachen kansioon. Asennuksen jälkeen tarkistin ohjelman toiminnan menemällä selaimessa ohjelman hallintasivulle (http://palvelimenosoite/backuppc), josta pääsee tarkkailemaan BackupPC:n toimintaa ja muuttamaan asetuksia. Yrityksen ylläpidon pyynnöstä

BackupPC:n varmuuskopiointitiedostojen oletuskansio linkitettiin vielä symbolisella linkillä palvelimessa olevalla toiselle levylle, jolloin itse ohjelma ja varmuuskopioidut tiedostot ovat eri levyillä.

Onnistuneen asennuksen jälkeen oli asetukset varmuuskopioimisen suhteen ohjelmassa asetettava kuntoon. Ohjelman hallinta tapahtuu pääosin nettiselaimen avulla, joten asetusten asettaminen on varsin helppoa ja käytännöllistä. Lisäksi ohjelman kaikki asetukset on linkitetty suoraan BackupPC:n ohjekirjaan, jolloin ohjeet ovat helposti saatavilla. Ohjetta ei tarvitse erikseen etsiä vaan linkki vie aina suoraan oikeaan kohtaan ohjekirjassa. Asetukset tehdään käyttöliittymän Edit Config -linkistä aukeavalla yleisten asetusten hallintaikkunassa (Main Configuration Editor) (Liite 2). Asetukset ovat ohjelmassa oletusarvoiltaan valmiiksi sellaiset, että niiden avulla pystyy hyvin aloittamaan varmuuskopioimisen. Tässä vaiheessa muutin ainoastaan WakeupSchedule-arvoa ja muut arvot jätin oletusarvoiksi. WakeupSchedule määrittelee ajat, milloin varmuuskopiointipalvelin herää ja tarkistaa onko verkossa varmuuskopioitavia koneita ja ryhtyy suorittamaan kopiointeja. Oletuksena ohjelma herää tunnin välein klo 00.00 - 06.00 yöllä. Koska yrityksessä työskennellään pääosin klo 06.00 – 16.00 ja verkon siirtonopeudet (Taulukko 1) eivät riitä oletusarvon mukaisesti suorittamaan kaikkia varmuuskopiointeja, piti arvoa muuttaa sopivammaksi. Muutin arvon niin, että palvelin herää ensimmäisen kerran klo 19.00 ja tästä eteenpäin aina puolen tunnin välein klo 05.30 asti. Yhtäaikaisia varmuuskopiointeja ei kannata verkon hitauden vuoksi ottaa enempää kuin kaksi kerrallaan, joten palvelimen on hyvä herätä useammin kuin tunnin välein. Etenkin inkrementaaliset varmuuskopioinnit saattavat siirtyä paljon nopeammin, joten on järkevää aloittaa uusi varmuuskopiointi heti edellisen jälkeen, jolloin varmuuskopioinnit varmasti onnistuvat yön aikana.

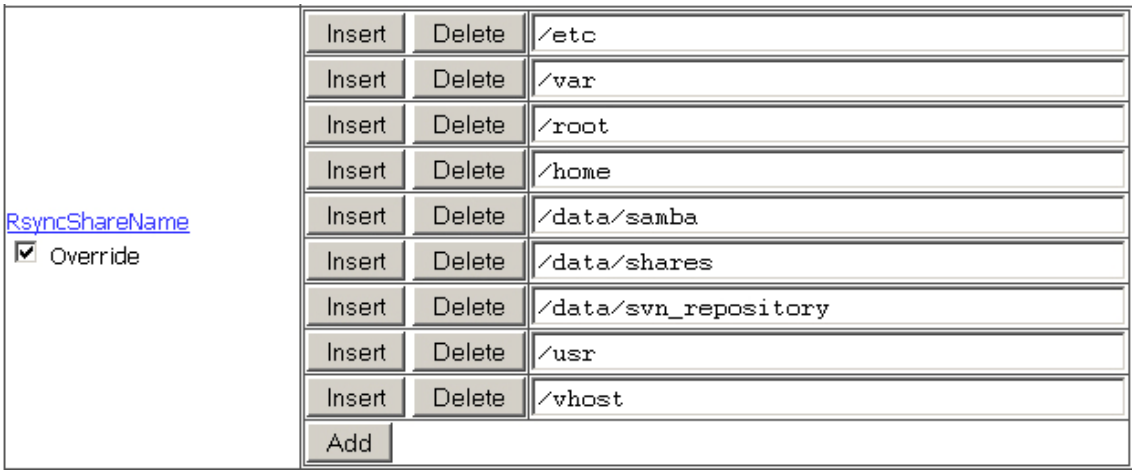
Seuraavaksi liitin yrityksen palvelimet varmuuskopioitavaksi. Koska tuotantokäytössä olevia palvelimia ei ollut mahdollista testata ennakkoon, piti varmuuskopioitavaksi asentaa alkuun vain toinen palvelin ja tarkkailla sen toimintaa varmuuskopioinnin suhteen. Palvelinten ja työasemien lisääminen varmuuskopioitavaksi tapahtuu käyttöliittymässä yleisten asetusten hallintaikkunan Hosts-välilehdellä. Lisääminen tapahtuu valitsemalla lisää (Add) ja kirjoittamalla palvelimen tai työaseman konenimi (host) sekä käyttäjänimi (user). Lopuksi asetukset tallennetaan, jolloin lisätyt koneet ilmestyvät ohjelman Hosts-valikkoon. Kyseisestä valikosta pääsee tarkastelemaan yksittäisten palve-

limien ja työasemien varmuuskopioita ja muuttamaan asetuksia (Kuva 7).



Kuva 7. BackupPc:n Hosts-valikko mahdollistaa yksittäisten koneiden tarkastelun.

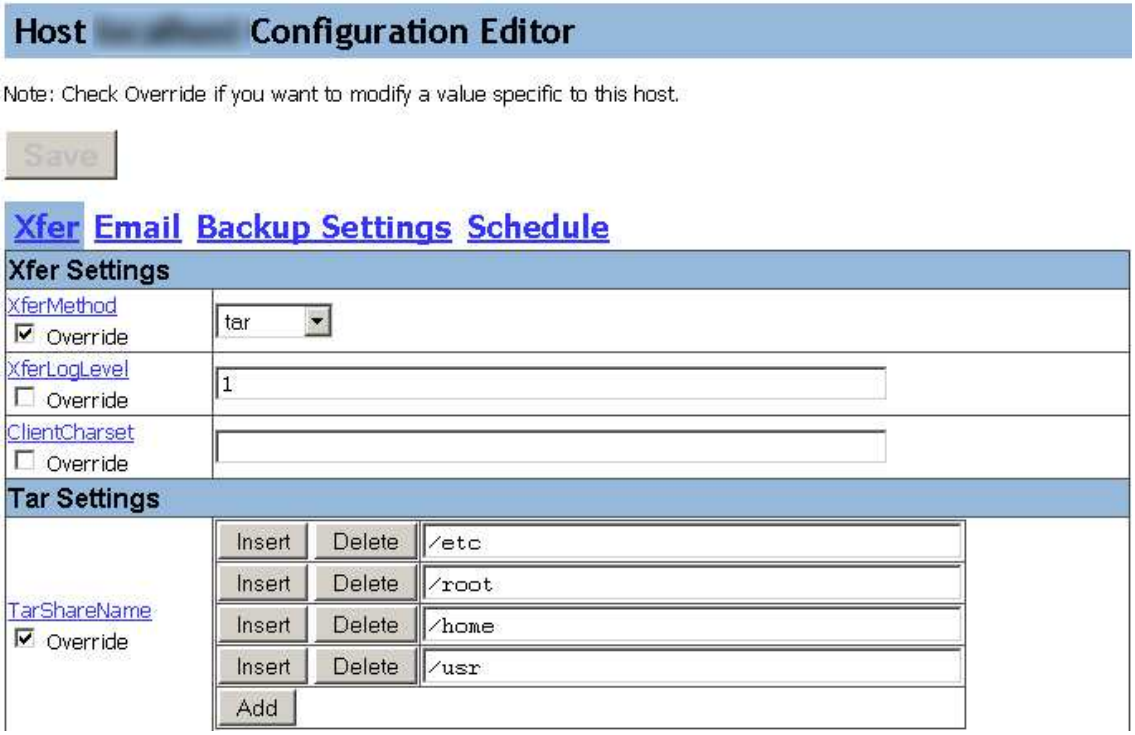
Ensimmäisenä varmuuskopioitavaksi palvelimeksi valitsin palvelimen A, joka tuottaa yrityksen verkon toiminnan kannalta tärkeimmät palvelut. Lisäämisen jälkeen palvelimen asetukset piti asettaa sen omassa asetusten hallintaikkunassa (Liite 3). Kyseisellä sivulla voidaan asettaa yleisten varmuuskopiointiasetusten lisäksi yleisasetuksista poikkeavia varmuuskopiointiaikoja (Schedule), sähköpostimuistutuksia (Email) sekä siirtoasetuksia (Xfer). Palvelimen siirtoasetuksiin tein muutamia muutoksia. Siirtotavaksi (Xfer Method) valitsin rsync, joka käyttää tietojen salaamiseen SSH:ta, jolloin varmuuskopioitavat tiedostot siirtyvät palvelimelta toiselle salattuna. Lisäksi määritin palvelimelta kaikki tärkeät kansiot varmuuskopioitavaksi (Kuva 8).



Kuva 8. Palvelimelta A määritetyt kansiot, jotka varmuuskopioidaan.

Lisäksi käyttäjälle BackupPC piti määrittää palvelimelle SSH-avain ilman salasanaa ja antaa käyttäjälle täydet oikeudet rsync-siirtoihin palvelimella. Myös palvelimelta varmuuskopioitavien kansioiden oikeuksiin piti lisätä oikeudet kyseiselle käyttäjälle. Palvelin oli nyt valmis varmuuskopioitavaksi, joten ensimmäisen varmuuskopioinnin otin pakottamalla varmuuskopioinnin päälle ohjelmasta. BackupPC-ohjelmassa käyttäjä voi halutessaan käynnistää manuaalisesti kokonaisia ja inkrementaalisia varmistuksia sekä keskeyttää käynnissä olevia varmistuksia. Manuaalisesta käynnistyksestä ei ollut haittaa verkon yleiselle käytölle, koska palvelimet ovat samassa verkossa ja tiedonsiirto niiden välillä on nopeaa. Varmuuskopioinnit onnistuivat hyvin ja myös järjestelmä toimi hienosti muutamia päiviä kestäneen testaamisen aikana.

Seuraavana varmuuskopioitavaksi liitin palvelimen B, jossa myös varmuuskopiointijärjestelmä sijaitsee. Palvelimen lisääminen varmistettavaksi tapahtui samalla tavalla kuin ensimmäisen palvelimen eli lisäsin sen varmuuskopioitavien koneiden listaan ja laitoin sen omat asetukset kuntoon. Siirtotavaksi valitsin kuitenkin palvelimelle tässä tapauksessa tar-siirtomuodon (Kuva 9), koska palvelin varmuuskopioi itseään ja tiedot siirtyvät vain palvelimen sisällä. Tämän vuoksi siirrettävää tietoa ei tarvitse erikseen salata. Asetuksiin lisäsin vielä varmuuskopioitavat kansiot (Kuva 9), joille ei enää erikseen tarvinnut määrittää oikeuksia, koska ohjelmalla ne jo alun perin on.



Kuva 9. Palvelimen siirtomuodoksi valittu tar ja varmuuskopioitaviksi määritetyt kansiot.

Asetusten jälkeen laitoin ohjelman ottamaan varmuuskopion palvelimesta onnistuneesti. Palvelimen varmuuskopioinnit onnistuivat hyvin myös automaattisessa kopioinnissa, joten pääsin seuraavaksi lisäämään työasemia järjestelmään. Testikäytössä olevaa palvelinta ei tässä vaiheessa ollut aiheellista liittää varmuuskopioitavaksi, mutta se voidaan tarvittaessa helposti liittää järjestelmään samoin kuin edellä liitetyt palvelimet.

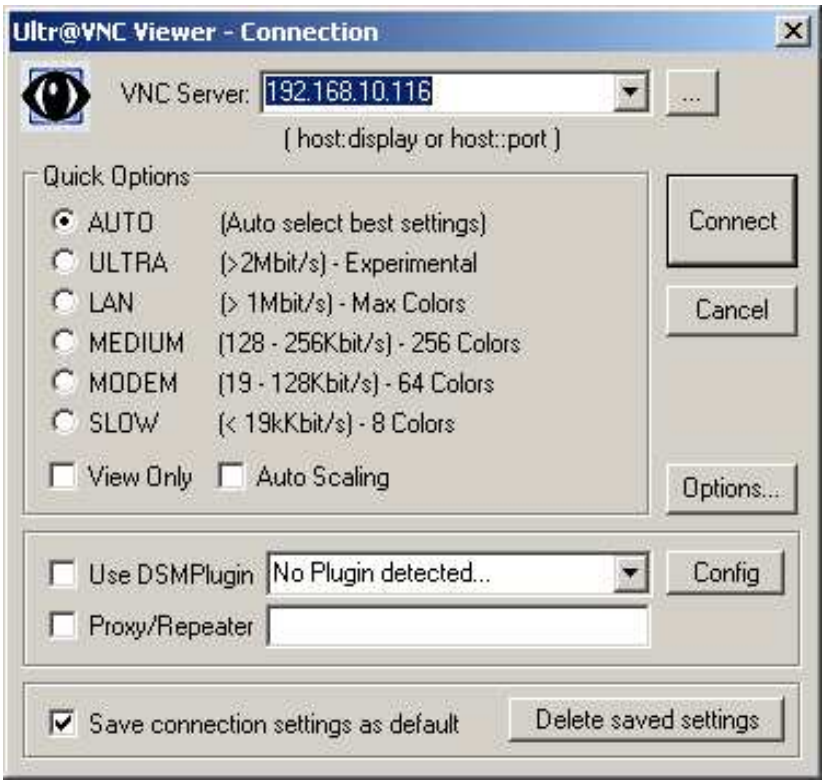
7.2 Asennus työasemiin

Työasemien varmuuskopioinnin aloitin kartoittamalla kaikki yrityksen verkon koneet, jotka ovat sellaisessa käytössä, että ne pitää varmuuskopioida. Tämä tarkoitti siis työasemia, jotka ovat pääosin henkilökohtaisessa käytössä insinööreillä ja hallinnon työntekijöillä. Kartoituksessa käytin apuna yrityksen verkon laitehallintaa, johon on selvästi kirjattuna ylös kaikki työasemat ja niiden käyttäjät. Lisäksi apuna kartoituksessa oli yrityksen järjestelmävastaavan tietämys verkon laitteiden käyttötarkoituksista. Varmuuskopioitavia koneita löytyi yhteensä 20 kappaletta, joista kuusi sijaitsi toimipisteessä A ja loput muissa toimipisteissä. Myöhemmin projektin aikana tuli mukaan vielä yksi kone erään insinöörin erikoiskäyttöön hankitun uuden työaseman muodossa.

Työasemien varmuuskopioinnin suoritin asteittain yksi työasema kerrallaan, jolloin pystyin seuraamaan tarkasti kopioinnin vaikutuksia järjestelmään. Tämä oli järkevää, koska työasemasta pitää aina ensimmäisenä ottaa kokonainen varmuuskopiointi, mikä kuormittaa verkkoa paljon. Asteittain työasemia järjestelmään liitettäessä saadaan samalla kokonaisten varmuuskopiointien ajankohdat porrastettua niin, että järjestelmä ottaa ne eri päivinä. Verkon hitauden vuoksi tämä takaa paremmin kokonaisten varmuuskopiointien onnistumisen työajan ulkopuolella. Aloitin työasemien lisäämisen järjestelmään toimipisteestä A, jossa pystyin hoitamaan asennuksen paikan päällä. Toimipisteen verkko on lisäksi selvästi muita toimipaikkoja suorituskykyisempi.

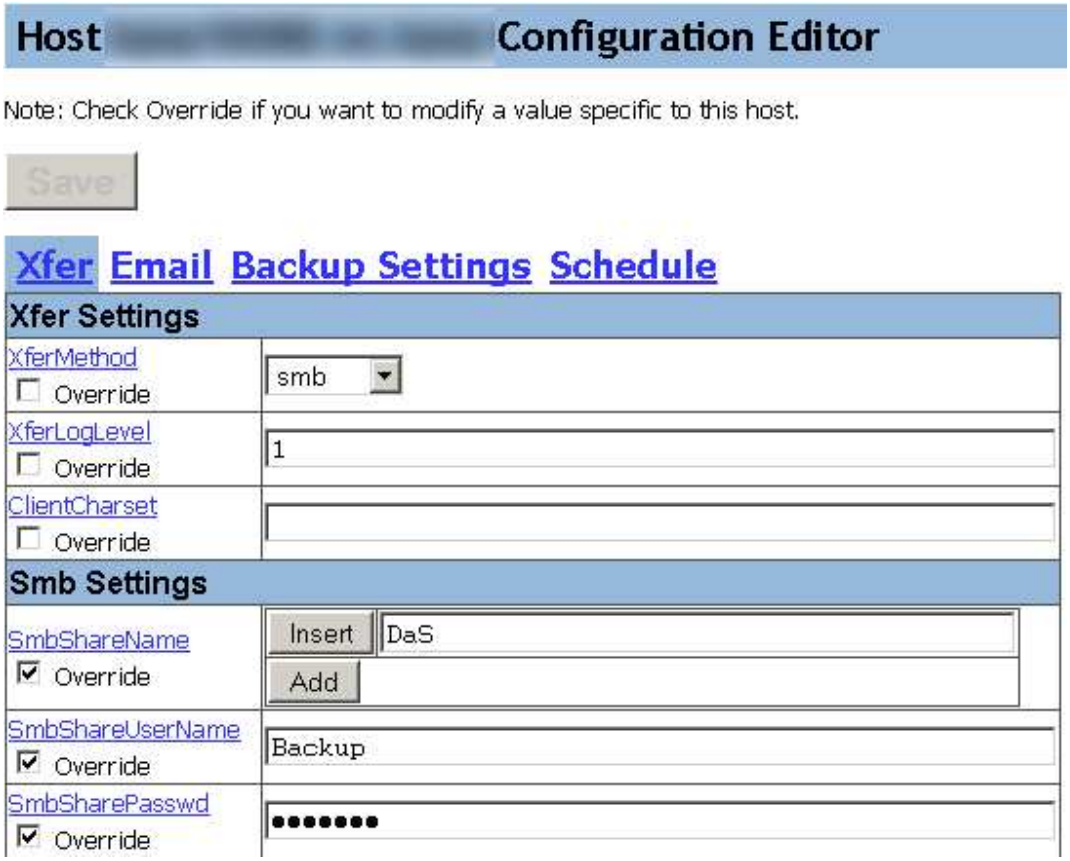
Helpointa oli aloittaa lisäämällä omassa käytössäni ollut kone järjestelmään ja sen jälkeen muut yksi kerrallaan. Toimipisteessä A suoritin koneiden järjestelmään lisäämisen kysymällä työasemien käyttäjiltä henkilökohtaisesti sopivan ajankohdan, jolloin en häiritsisi heidän työntekoaan. Hyvä hetki tehdä tarvittavat toimenpiteet työasemalle on esimerkiksi, kun työaseman käyttäjä on ruokatunnilla. Muissa toimipisteissä sijaitsevien työasemien varmuuskopioimisesta olin yhteydessä käyttäjiin puhelimen sekä sähköpostin välityksellä. Tiedustelin aina käyttäjälle sopivaa ajankohtaa, milloin voisin olla etäyhteydessä heidän koneeseensa häiritsemättä työntekoa. Samalla selvitin heille järjestelmän toimintaa ja pyrin jo tässä vaiheessa ohjeistamaan heidät toimimaan niin, että varmuuskopioinnit onnistuisivat myös tulevaisuudessa. Lisäksi näissä keskusteluissa kävi yleensä ilmi, jos käyttäjällä oli tärkeitä tiedostoja myös muualla kuin Documents And Settings -kansiossa. Tällöin pystyin lisäämään myös kyseiset kansiot varmuuskopioitaviksi. Esimerkiksi eräällä käyttäjällä oli tärkeän suunnitteluohjelman tallennustiedostoja ohjelman omassa kansiossa, jonka lisäsin varmuuskopioitavaksi.

Varmuuskopioitavat työasemat lisätään järjestelmään BackupPC:n käyttöliittymässä ja lisäksi työasemista on laitettava varmuuskopioitavat kansiot jaettaviksi. Toimipisteessä A tämän pystyi tekemään paikallisesti, mutta muiden toimipisteiden työasemiin otin etäyhteyden UltraVNC-etähallintaohjelman avulla (Kuva 10). Ohjelmalla muodostetaan yhteys toiseen koneeseen, jolloin koneen työpöytä näkyy omalla näytöllä ja sitä voidaan hallita omalla hiirellä sekä näppäimistöllä. Koneeseen johon yhteys muodostetaan pitää olla UltraVNC Server asennettuna ja päällä, jolloin yhteyden muodostaminen siihen onnistuu. Yrityksen kaikissa koneissa kyseinen ohjelma on valmiiksi asennettuna.



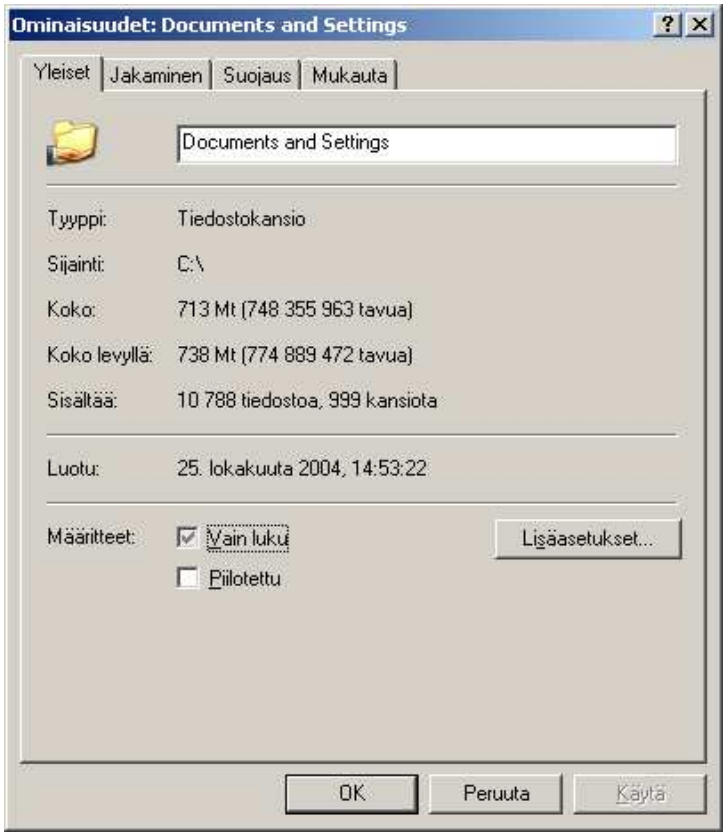
Kuva 10. UltraVNC-etähallintaohjelmalla otetaan yhteys työasemiin etäpisteissä.

Työasema liitetään varmuuskopioitavaksi BackupPC:n käyttöliittymässä samoin kuin palvelimetkin eli yleisten asetusten hallintaikkunan Hosts-välilehdellä lisätään työaseman konenimi listalle. Varmuuskopioitavan työaseman asetukset muutetaan sen omassa hallintaikkunassa (Kuva 11). Työaseman siirtoasetuksista muutin siirtotavaksi SMB:n, jota käytetään Windows-asemien tiedonsiirrossa. Lisäksi määritin työasemista varmuuskopioitavat kansiot (SmbShareName) sekä käyttäjätunnuksen (SmbShareUserName) ja salasanan (SmbSharePasswd), jolla on oikeus kyseisiin kansioihin. Oletuksena kaikkiin työasemiin määritin Documents And Settings -kansion varmuuskopioitavaksi ja annoin kansiolle jakonimeksi DaS. Muita kansioita lisäsin käyttäjien toiveiden mukaan tapauskohtaisesti.

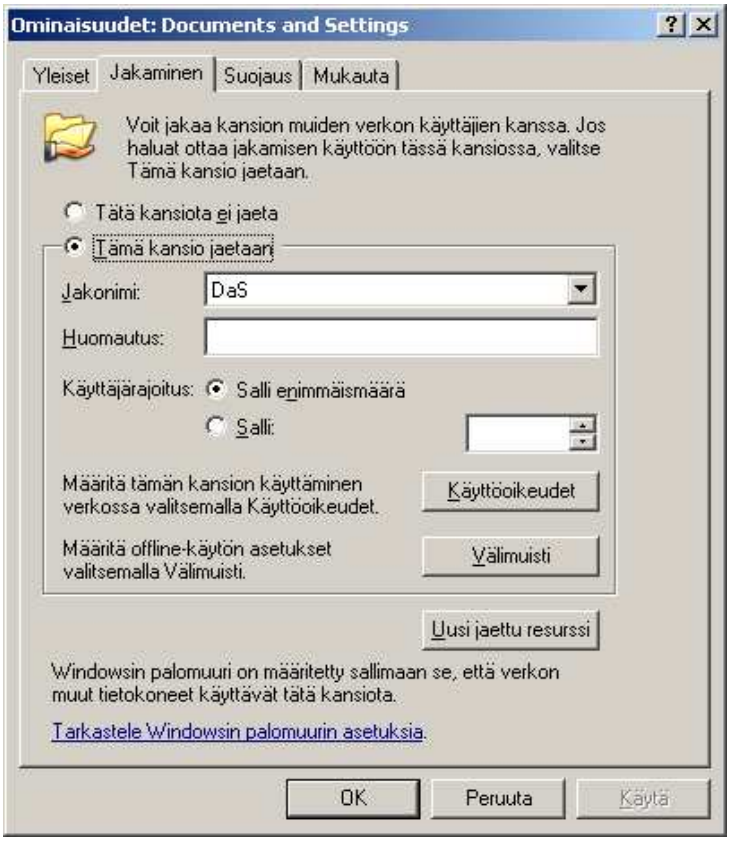


Kuva 11. Työaseman siirtoasetukset.

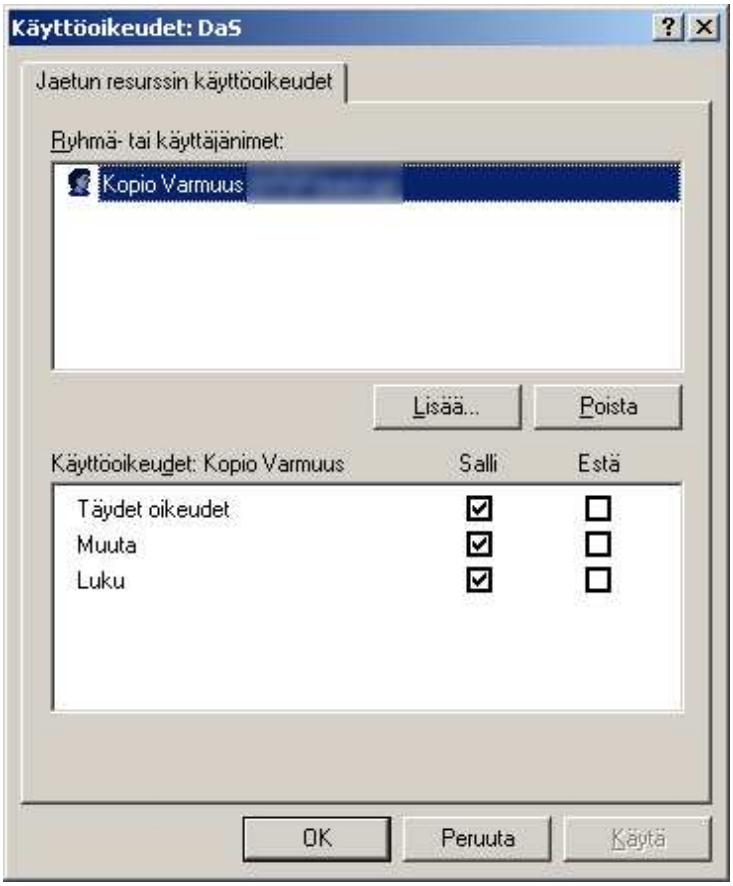
Asetusten jälkeen tein tarvittavat asetukset varmuuskopioitavaan työasemaan. Työasemasta valitaan kansio Documents And Settings, joka löytyy C-aseman juuresta. Windows Vista -käyttöjärjestelmässä kyseistä kansiota vastaa Users-kansio. Kansion ominaisuuksista tarkistin aluksi kansion koon (Kuva 12), koska liian suurten kansioiden varmuuskopioiminen venyisi työajalle. Tämän jälkeen kansion ominaisuuksista valitsin kansion jaettavaksi ja sille jakonimeksi DaS (Kuva 13). Jaettavalla kansiolle piti vielä määrittää käyttöoikeudet, jolloin lisäsin kansion käyttäjien listalle käyttäjän Backup ja annoin sille täydet oikeudet (Kuva 14). Pelkät lukuoikeudet eivät riitä, koska mahdollisessa palautustilanteessa tarvitaan myös kirjoitusoikeuksia.



Kuva 12. Varmuuskopioitavan Documents and Settings -kansion koon tarkistaminen.



Kuva 13. Documents and Settings -kansion jakaminen.



Kuva 14. Jaettavan kansion käyttöoikeuksien määrittäminen.

Työasema on näiden asetusten jälkeen valmis varmuuskopioitavaksi. Sopiessani käyttäjien kanssa asennuksista, pyysin heidät jättämään koneensa päälle töistä lähtiessään, jolloin asetin ensimmäisen täyden varmuuskopioinnin siirtymään manuaalisesti. Muiden toimipisteiden työasemiin oli paras ajankohta tehdä asetukset perjantaisin, jolloin sai ensimmäiset täydet varmuuskopioinnit siirtymään viikonlopun ajaksi. Näin varmistin sen, että kopioinnit siirtyivät ennen seuraavaa työpäivää. Ohjelma ilmoittaa varmuuskopioinnin onnistuneesta käynnistymisestä ja varmuuskopioitavien laitteiden yhteenvetosivulla (Host Summary) (Liite 4) näkyy laitteiden tilavärit. Käynnissä olevan varmuuskopioinnin tunnistaa vihreästä tilaväristä (Kuva 15). Yhteenvetosivulla näkee myös kokonaisten ja inkrementaalisten varmuuskopiointien lukumäärän, koon, siirtonopeuden sekä viimeisten varmuuskopiointien iän päivinä.

Kuva 15. Vihreä tilaväri kertoo varmuuskopioinnin olevan käynnissä (backup in progress).

Varmuuskopioinnin onnistumista voidaan seurata myös tarkkailemalla verkon eri rajapintoja. Työaseman varmuuskopioinnin onnistumista voidaan tarkkailla esimerkiksi seuraamalla työaseman sijaintipaikan reitittimeltä lähtevää liikennettä ja varmuuskopiointipalvelimen Ethernet-portin liikennettä. Kopioinnin aikana siirtyvän datan määrän pitäisi kasvaa selvästi.

7.3 Asetusten hienosäätöä ja vikatilanteita

Järjestelmän asetukset ovat asennuksen jälkeen valmiiksi asetettu sellaisiksi, että varmuuskopioinnit onnistuvat. Kuitenkin joitakin asetuksia minun oli muutettava järjestelmästä, jotta se vastaisi paremmin yrityksen tarpeita. Myös erilaisia vikatilanteita ilmeni työn eri vaiheissa joiden vuoksi ohjelmaa oli hienosäädettävä.

Aiemmin kerroin kappaleessa 7.1 tekemistäni muutoksista ohjelman WakeupSchedule-asetuksiin. Muutokset periytyvät automaattisesti ohjelman BlackoutPeriods-arvoihin (Kuva 16), jotka määrittelevät milloin ohjelmaa ei käytetä. Arvoja ei tarvinnut lähteä enää muuttamaan, koska niiden mukaan ohjelma ei ole arkisin työaikoina päällä. Muutoksia tein ohjelmassa arvoihin FullPeriod ja IncrPeriod, jotka määrittelevät kuinka usein kokonainen ja inkrementaalinen varmuuskopiointi tehdään. Oletusarvoina kokonainen varmuuskopiointi tapahtuu 7 päivän välein ja inkrementaalinen varmuuskopiointi vuorokauden välein (Kuva 17). Oletusarvot sopivat hyvin toimipisteeseen A, mutta muiden toimipisteiden aikavälejä piti muuttaa. Koska varmuuskopioitavia koneita on enemmän muissa toimipisteissä ja siirtoyhteydet ovat selvästi hitaammat, voivat varmuuskopiointiajat venyä liian pitkiksi. Muutin arvot lopulta sellaisiksi, että toimipisteessä A otetaan kokonainen varmuuskopiointi kerran viikossa ja inkrementaalinen varmuuskopiointi joka päivä. Muissa toimipisteissä kokonainen varmuuskopiointi otetaan 28 päivän välein ja inkrementaalinen varmuuskopiointi joka toinen päivä.

Kuva 16. Varmuuskopiointiohjelma ei ole käytössä arkisin klo. 07.00 – 18.30.

Full Backups	
FullPeriod	6.97
FullKeepCnt	5, 0, 6, 2, 2
FullKeepCntMin	1
FullAgeMax	90
Incremental Backups	
IncrPeriod	0.97
IncrKeepCnt	30
IncrKeepCntMin	1
IncrAgeMax	30
IncrLevels	1
IncrFill	☐

Kuva 17. Kokonaisen ja inkrementaalisen varmuuskopioinnin aikavälien asetukset.

Lisäksi tein muutoksen kokonaisten varmuuskopiointien säilytysaikaan (FullKeepCnt). Oletuksena kokonaisia varmuuskopioita säilytetään liian useita, jolloin levytilan käyttöaste on turhan suuri. Säilytettävien varmuuskopiointien ajat määritetään niin, että ensimmäinen arvo määrittää viikon välein säilytettävät, toinen kahden viikon välein, kolmas neljän viikon välein ja niin edelleen aikaa taaksepäin katsottaessa. Taulukosta 3 näkee miten varmuuskopioinnit säilytetään asettamillani arvoilla, jotka sovimme yhdessä yrityksen järjestelmävastaavan kanssa.

Taulukko 3. Varmuuskopioiden säilyttämisen aikavälit.

FullKeepCnt	5, 0, 6, 2, 2

FullkeepCnt	Arvo	Ikä
	1	nykyinen
	1	1 vko
5	1	2 vko
	1	3 vko
	1	4 vko
0	2	-
	4	8 vko
	4	12 vko
6	4	16 vko
	4	20 vko
	4	24 vko
	4	28 vko
2	8	36 vko
	8	44 vko
2	16	60 vko
	16	76 vko

Järjestelmässä ilmeni myös erilaisia vikatilanteita, jotka aiheuttivat muutoksia ohjelman asetuksiin. Muutamat muiden toimipisteiden varmuuskopioinnit antoivat varmuuskopiointia ensimmäistä kertaa ottaessa seuraavan vikailmoituksen: Last error is ”Ping too slow: 30.37msec (threshold is 30msec)”. Tämä siis tarkoittaa, että yhteys työasemaan ei ole riittävän nopea. Ratkaisu ongelmaan oli muuttaa järjestelmän asetuksista varmistettavan työaseman kohdalta arvoa PingMaxMsec, joka oletuksena on 30 millisekuntia. Kun arvon muutti 40:een millisekuntiin niin varmuuskopiointi onnistui.

Palvelinta A varmuuskopioitaessa tuli kerran virheilmoitus: Last error is ”Backup failed (unable to read 4 bytes)”. Tämä johtui siitä, että SSH-avain oli tietoturvallisuus syistä uusittu palvelimella, ja palvelimella B, jossa varmuuskopiointijärjestelmä sijaitsee, oli vielä vanha avain. Vika korjaantui, kun avainpari uusittiin vastaamaan toisiaan. Varmuuskopioitavista työasemista vain yhdessä oli käyttöjärjestelmänä Windows Vista ja kyseisen työaseman kanssa ilmenikin varmistuksessa pieniä ongelmia. Varmuuskopioinnit eivät suostuneet käynnistymään alkuun ollenkaan kunnes viaksi selvisi, että Windowsin oma palomuuri oli jäänyt työasemasta päälle. Palomuurin kytkeminen pois päältä näytti aluksi ratkaisevan ongelman, mutta varmuuskopioinnit keskeytyivät aina jonkin ajan kuluttua käynnistymisestä. Lopulta ongelma ratkesi, kun työasemaan asennettiin Windows Vista Service Pack 1, jota jostain syystä ei työasemaan vielä oltu asennettu.

On myös mahdollista, että verkkoyhteyksissä ilmenee ongelmia varmuuskopioinnin aikana. Esimerkiksi palveluntarjoajan yhteyksiin tulee vika, minkä vuoksi varmuuskopiointi katkeaa. Tällaisissa tilanteissa BackupPC muodostaa osittaisen varmuuskopion (partial dump) tiedostoista, jotka on ennen yhteyden katkeamista kopioitu. Osittaista varmuuskopiointia jatketaan seuraavalla kertaa, kun yhteyden muodostaminen kohteeseen jälleen onnistuu. Osittaisen varmuuskopioinnin huomaa helposti lokitiedostosta (Kuva 18).

```
2009-01-18 19:00:22 full backup started for share DaS
2009-01-18 20:46:01 Got fatal error during xfer (Total bytes written: 481929728)
2009-01-18 20:46:06 Backup aborted (lost network connection during backup)
2009-01-18 20:46:06 Saved partial dump 4
2009-01-18 21:01:02 no ping response
```

Kuva 18. BackupPC muodostaa osittaisen varmuuskopion jos verkkoyhteys katkeaa.

8 KÄYTTÄJIEN OHJEISTAMINEN

Tarkoitukseni oli opastaa työasemien käyttäjiä henkilökohtaisesti varmuuskopiointijärjestelmän käytön suhteen järjestelmän käyttöönoton aikana. Kerroin käyttäjille järjestelmän toimintaperiaatteista ja millaisia toimenpiteitä varmuuskopiointi heiltä vaatii. Lisäksi tein erillisen ohjedokumentin (Liite 5), jonka työn loppuvaiheessa lähetin sähköpostina kaikille niille käyttäjille joiden työasemista varmuuskopiot otetaan. Lisäsin ohjeen myös yrityksen intranetiin, jolloin ohje on helposti saatavilla myös mahdollisille uusille varmuuskopiointijärjestelmän käyttäjille.

Tein ohjeesta mahdollisimman lyhyen ja helposti ymmärrettävän, koska halusin kaikkien käyttäjien varmasti lukevan ohjeen kokonaan ja myös sisäistävän lukemansa. Yritin kuitenkin välttää jättämästä mitään järjestelmän käytön kannalta oleellista pois ohjeesta. Ohjeen tarkoitus oli myös helpottaa järjestelmän ylläpitoa. Varmuuskopioinnit onnistuvat paremmin, kun käyttäjät osaavat toimia oikein järjestelmän toiminnan kannalta.

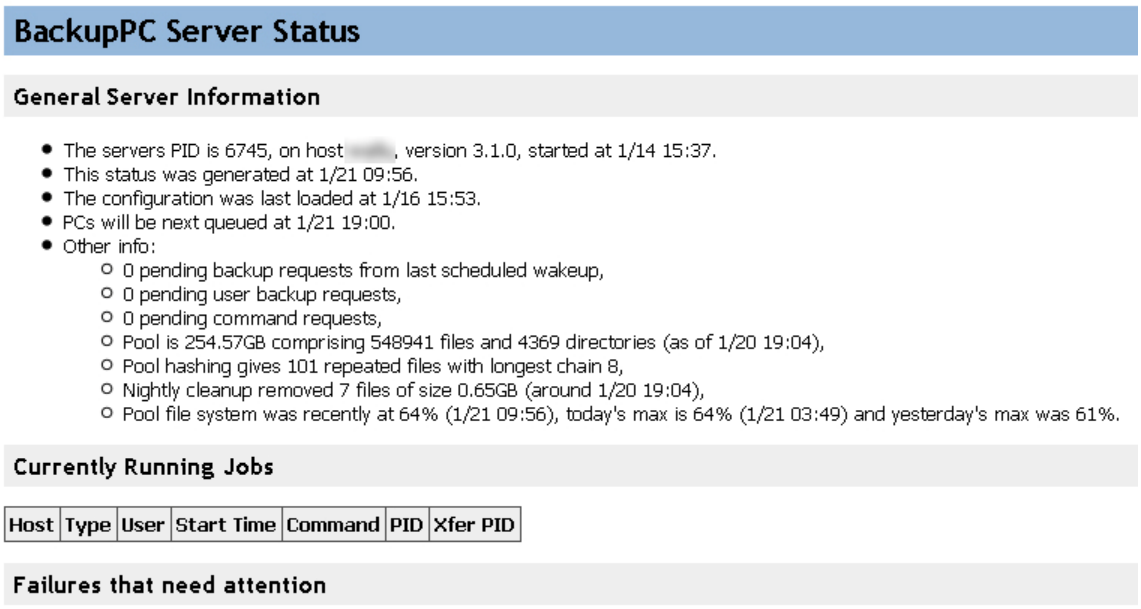
9 JÄRJESTELMÄN YLLÄPITO

Käyttöönotto ei ole järjestelmän elinkaaren päätepiste vaan sen jälkeen seuraa vielä elinkaaren pisin vaihe eli järjestelmän ylläpito. Ylläpitovaiheessa keskitytään korjaamaan tuotantokäytössä olevan järjestelmän virheitä, suorittamaan erilaisia muutostoimenpiteitä sekä jatkokehittämään järjestelmää. Järjestelmän ylläpitäminen kestää käytännössä järjestelmän elinkaaren loppuun saakka. Ylläpidon kannalta yleisin vaikeuttava tekijä kehityksen kannalta on järjestelmän puutteellinen dokumentaatio. Puutteellisen dokumentaation vuoksi järjestelmän kehittämisprosessia on vaikea jäljittää ja taustalla vaikuttavia ratkaisuja ymmärtää. Ylläpidon kannalta dokumentoinnin pitää olla kattavaa ja dokumentointia pitää tehdä koko järjestelmän elinkaaren ajan. (Pohjonen 2002, 37-38)

9.1 Monitorointi

Jos varmuuskopiointien onnistumisia ei valvota mitenkään on lähes varmaa, että ne eivät tee sitä mitä niiden pitäisi tehdä. Kaikille varmuuskopioinnille tulisi olla lokitiedosto, jota tarkkaillaan päivittäin. Järjestelmä voidaan myös automatisoida lähettämään esimerkiksi sähköpostia ylläpidolle, kun lokitiedostossa ilmenee jotain hälyttävää. (Preston 2007, 48-49)

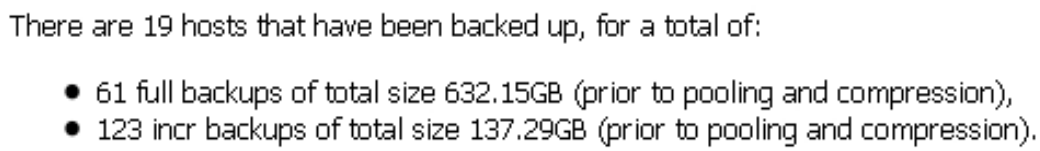
BackupPC:n käyttöliittymän Status-sivulta (Kuva 19) on helppo tarkkailla järjestelmän tilaa. Status-sivulta näkee monipuolisesti tietoja järjestelmän toiminnasta. Sivulta näkee käynnissä olevat varmuuskopioinnit (Currently Running Jobs) sekä huomiota tarvitsevat vikatilanteet (Failures that need attention). Tällaisia tilanteita ovat kaikki vikatilanteet lukuun ottamatta tilannetta, jossa koneeseen ei saada yhteyttä. Tältä sivulta ylläpidon onkin helpointa tarkistaa, jos järjestelmässä ilmenee ongelmia. Sivulta näkee myös kuinka paljon varmuuskopioinnit käyttävät todellisuudessa tilaa levyjärjestelmässä ja kuinka paljon ohjelma on poistanut käyttämättömiä tiedostoja öisin (Nightly cleanup).



Kuva 19. BackupPC:n Status-sivulta voi tarkkailla järjestelmän tilaa.

Host Summary -sivulta voi tarkastella tarkemmin varmuuskopioitavia koneita ja niiden tietoja (Liite 4). Sivulta näkee myös kuinka paljon kokonaiset ja inkrementaaliset varmuuskopioinnit ovat kooltaan yhteensä ennen kompressointia ja vastaavien tiedostojen

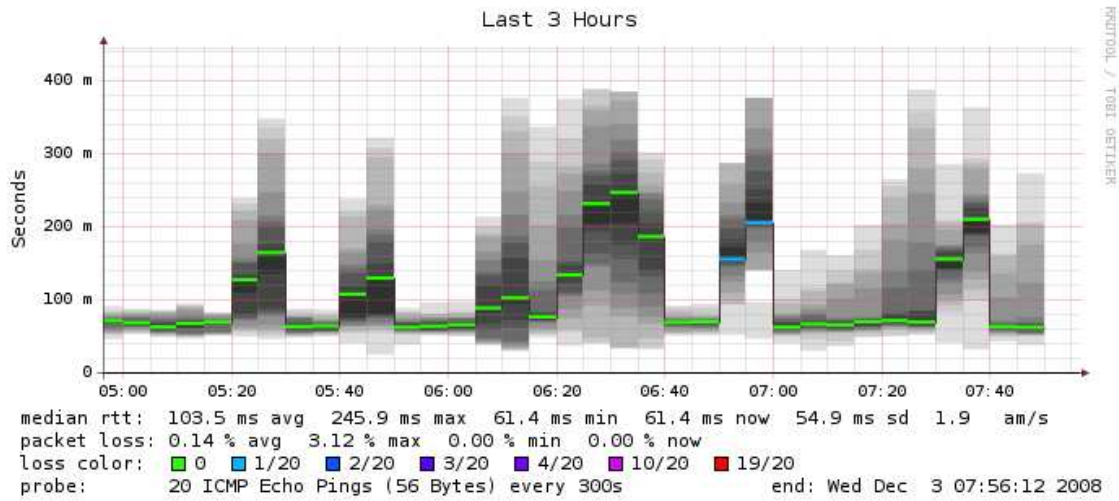
yhdistämistä (Kuva 20). Sivulta on helppo katsoa, koska koneet on viimeksi varmuuskopioitu ja minkä kokoisia varmuuskopioinnit ovat. Sivulta on myös helppo siirtyä tarkastelemaan yksittäistä työasemaa klikkaamalla sen nimeä. Käyttäjän nimeä klikkaamalla voidaan helposti lähettää sähköpostia käyttäjälle esimerkiksi tilanteessa, jossa työasemasta ei ole saatu varmuuskopiota useaan päivään.



Kuva 20. Kokonaisten ja inkrementaalisten varmuuskopioiden koko yhteensä ennen yhdistämistä ja kompressointia.

Yksittäisen työaseman omalta hallintasivulta voi lisäksi tarkastella yhteenvetoja työasemasta otetuista varmuuskopioinneista (Backup Summary), palautuksista (Restore Summary), siirtovirheistä (Xfer Error Summary), tiedostoista (File Size/Count Reuse Summary) sekä kompressoinneista (Compression Summary). Sivulta voidaan myös tarkastella ja palauttaa varmuuskopioita sekä tutkia lokitiedostoja. Näiden ominaisuuksien avulla varmuuskopiointien monitorointi onnistuu helposti.

Järjestelmän toimintaa voidaan myös monitoroida erilaisilla apuohjelmilla, jotka tarkkailevat liikennettä verkon eri pisteissä. Esimerkiksi SmokePing-ohjelmalla voidaan tarkkailla verkon latenssia eli aikaa mikä paketilta kuluu matkaan lähettäjältä vastaanottajalle (Kuva 21). Varmuuskopiointi lisää verkon liikennettä runsaasti ja tällöin myös latenssi kasvaa. Liikennettä voidaan tarkkailla myös palvelimelta, jolloin nähdään lisääntyykö tulevan liikenteen määrä varmuuskopioitaessa.



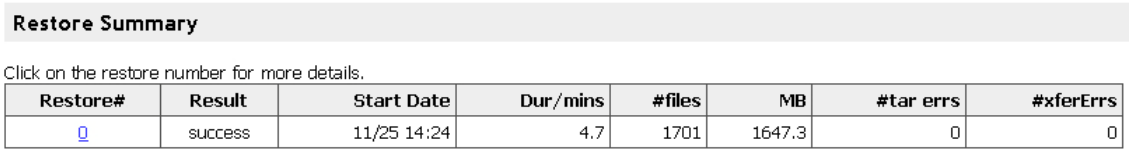
Kuva 21. SmokePing-ohjelmalla voidaan tarkkailla verkon latenssia.

9.2 Palautus

Varmuuskopioiden palauttaminen voi tulla kyseeseen kun käyttäjä esimerkiksi tuhoaa tiedoston vahingossa, tiedosto korruptoituu tai lakkaa muuten toimimasta. Myös laiteviat ovat aina mahdollisia ja palauttamisen pitää olla mahdollista, jos vaikka kiintolevy sattuu menemään rikki. Tiedostojen palauttaminen on BackupPC:ssä helppoa. Ohjelmasta valitaan työasema tai palvelin, jonka tiedostoja halutaan palauttaa, ja sen asetuksista valitaan näytettäväksi siitä otetut varmuuskopioinnit (Browse backups). Näkymästä voi valita, minkä päivän varmuuskopiointia haluaa tarkastella ja ohjelma näyttää kyseisen varmuuskopioinnin sisällön kansiopuuna (Liite 6). Kansiopuusta valitaan kansiot ja tiedostot, jotka halutaan palauttaa ja käsketään ohjelma palauttamaan ne (Restore selected files). Sivulta on mahdollista katsoa myös varmuuskopioitujen kansioiden historiaa (Liite 7).

Ohjelma antaa seuraavaksi kolme eri mahdollisuutta palautukselle (Liite 8). Suoralla palautuksella voidaan tiedostot palauttaa mihin tahansa järjestelmässä olevaan laitteeseen ja siinä oleviin jaettuihin kansioihin. Lisäksi palautettavat tiedostot voidaan ladata Zip- tai Tar-paketteina, jolloin palautus voidaan tehdä vaikka järjestelmän ulkopuoliseen työasemaan. Lopuksi järjestelmä varmistaa käyttäjältä vielä, että käyttäjä varmasti haluaa suorittaa palautuksen. Palautuksen jälkeen kyseinen palautus ilmestyy palautusten yhteenvetosarakkeen (Restore Summary) alle (Kuva 22). Yhteenvedosta voidaan nähdä

palautuksen onnistuminen, palautuksen kesto, tiedostojen lukumäärä ja koko sekä mahdolliset siirtovirheet. Palautusta voidaan tarkastella vielä hieman tarkemmin valitsemalla palautuksen numero (Liite 9).



Restore Summary

Click on the restore number for more details.

Restore#	Result	Start Date	Dur/mins	#files	MB	#tar errs	#xferErrs
0	success	11/25 14:24	4.7	1701	1647.3	0	0

Kuva 22. Palautusten yhteenvedosta näkee tietoja palautuksesta.

Koska varmuuskopioitava Documents and Settings -kansio sisältää käyttäjien sähköposteja sekä mahdollisesti myös muita henkilökohtaisia tiedostoja, on lainsäädäntö otettava tarkasti huomioon. Laki yksityisyyden suojasta työelämässä (L 13.8.2004/759) määrittää, että työnantajalla on tietyissä poikkeusolosuhteissa oikeus lukea työntekijänsä sähköposteista ainoastaan sellaisia, jotka kuuluvat työnantajalle. Tällaisia viestejä ovat esimerkiksi jonkin sopimuksen loppuun saattamiseen liittyvät sähköpostit, joita työntekijä on saanut esimerkiksi ollessaan poissa töistä. Työntekijöiden yksityisiä sähköposteja työnantajalla ei ole oikeutta lukea.

Tämä tekee palautuksesta hieman monimutkaisempaa, koska henkilökohtaisia tietoja voi palautusta tehdessä nähdä vaikka vahingossa. Koska palautuspyynnöt tulevat suoraan käyttäjältä, voidaan käyttäjälle kertoa mahdollisesta tietojen näkymisestä ja sopia menettelytavoista. Käyttäjiä pitää myös ohjeistaa tallentamaan henkilökohtaiset tiedot muualle ja pyrkiä pitämään vain työhön liittyviä tiedostoja kopioitavissa kansioissa. Moni kuitenkin käyttää yrityksen sähköpostiosoitetta henkilökohtaisten asioiden hoitoon, joten jatkossa voisi olla syytä miettiä erilaista ratkaisua sähköpostien tallennukselle.

10 JÄRJESTELMÄN ANALYSOINTI

Analysoin järjestelmän toimintaa muutenkin kuin pelkästään varmuuskopiointien ottamisen ja palauttamisen perusteella. Tarkkailin järjestelmän käytön vaikutuksia palvelimeen, työasemiin sekä verkkoliikenteeseen. Näitä tarkkailemalla pystyin hyvin muodostamaan käsityksen siitä, millaisia vaikutuksia varmuuskopiointijärjestelmä aiheuttaa yrityksen verkkoon kokonaisuudessaan. Tulosten pohjalta voidaan määritellä millaisia investointeja järjestelmä saattaa vaatia tulevaisuudessa.

10.1 Vaikutus palvelimeen

BackupPC on erittäin kevyt ohjelma ja se ei juurikaan kuormita tehokkaan palvelimen prosessoria tai muistia. Järjestelmän toiminta kuormittaa lähinnä levyjärjestelmää varmuuskopiointien ja palautusten aikana. Koska verkkoyhteydet etäpisteisiin ovat hitaat, levyjärjestelmä ei kuormitu kopioinnin aikana kovinkaan paljoa. Suurin vaikutus järjestelmällä on levyjärjestelmän käyttöasteeseen, sillä varmuuskopioinnit vaativat runsaasti tallennuskapasiteettia.

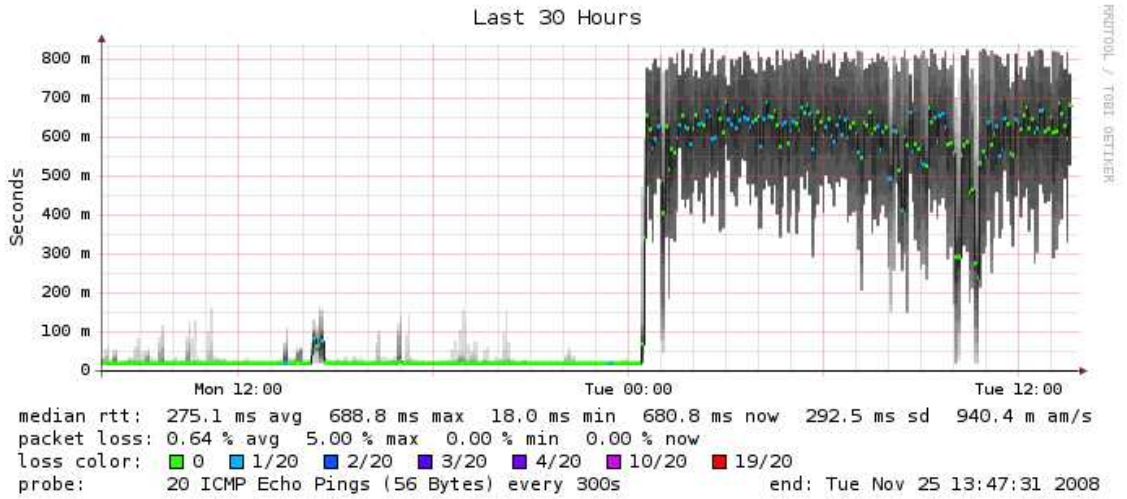
Kun järjestelmään oli asennettu varmuuskopioitavaksi 18 työasemaa ja 2 palvelinta, järjestelmän levykapasiteetista oli käytettynä 67 prosenttia. Varmuuskopiointijärjestelmällä on käytössä 587 gigatavua, josta 372 gigatavua on käytössä ja 186 gigatavua vapaana. Koska varmuuskopiointeja säilytetään pitkältä aikaväliltä, loppuu käytössä oleva tila nopeasti. Varmuuskopioissa ei kuitenkaan vielä ole käytössä kompressointia, koska se lisäisi selvästi prosessorin kuormitusta. Kompressoinnilla ja älykkäällä tietovarastoinnilla voidaan saavuttaa jopa kahdeksan kertaa pienempi levytilan käyttö, joten järjestelmällä on hyvin vielä varaa toimia kyseisellä levykapasiteetilla. Jossain vaiheessa levytilan kasvattaminen on kuitenkin väistämättä edessä.

10.2 Vaikutus työasemiin

Työaseman käyttäjä ei huomaa varmuuskopiointijärjestelmän toimintaa juuri ollenkaan. Varmuuskopiointi vaikuttaa ainoastaan verkon liikenteeseen ja kopiointi tapahtuu pääosin sellaisena aikana milloin verkkoa ei käytetä. Jos varmuuskopiointi venyy työajalle, huomaa käyttäjä sen selvänä verkkoyhteyden hidastumisena. Varmuuskopioinnin palauttaminen kuormittaa työaseman kiintolevyn I/O:ta, jonka voi huomata toimipisteessä A palautuksen aikana. Työaseman käyttäminen palautuksen aikana voi olla hieman hitaampaa. Palautuksesta kannattaakin sopia erikseen käyttäjän kanssa ja pyytää pitämään vaikka kahvitauko palautuksen aikana. Muissa toimipisteissä verkkoyhteyksien hitauden vuoksi kiintolevyn I/O ei ole niin kovassa käytössä, joten palautusta tuskin edes huomaa. Palautus voi kuitenkin epäonnistua jos palautettavia tiedostoja käytetään palautuksen aikana, joten on parempi pyytää käyttäjää pois työaseman ääreltä palautuksen ajaksi.

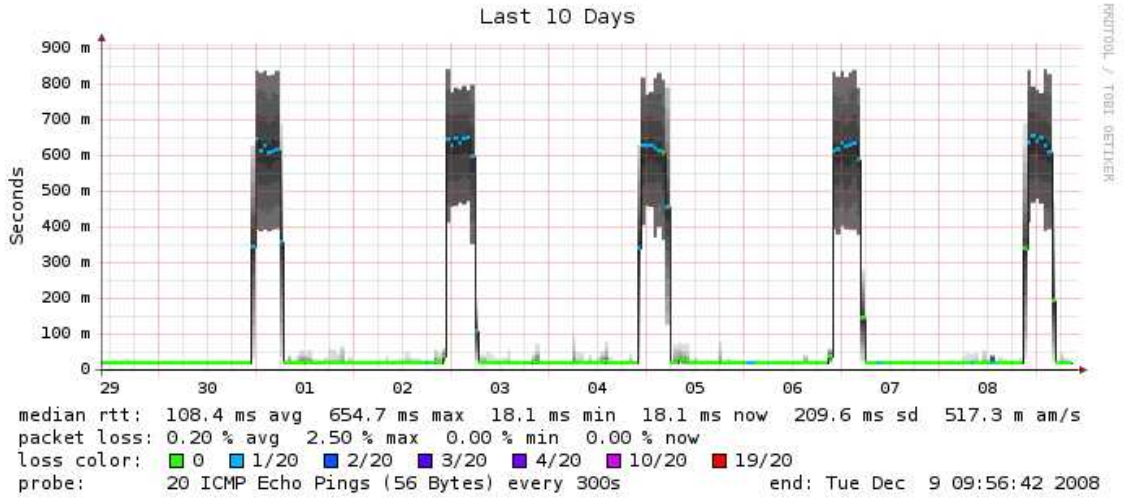
10.3 Verkon kuormitus

Järjestelmän toiminta näkyy selkeimmin verkon kuormituksessa. Etenkin etäpisteistä varmuuskopioitaessa verkkoyhteydet ovat käytännössä maksimikäytössä, jolloin verkon käyttäminen muuhun voi olla erittäin hidasta. Tämän vuoksi onkin tärkeää, että varmuuskopioinnit tulisi suoritetuiksi aikana, jolloin verkkoa ei muuten käytetä. Kuvasta 23 voidaan huomata selvä ero verkon latensseissa, kun varmuuskopiointia ryhdytään ottamaan. Pakettien menetykset lisääntyvät myös selvästi, jolloin varmuuskopioinnin suorittaminen kestää pidempään.

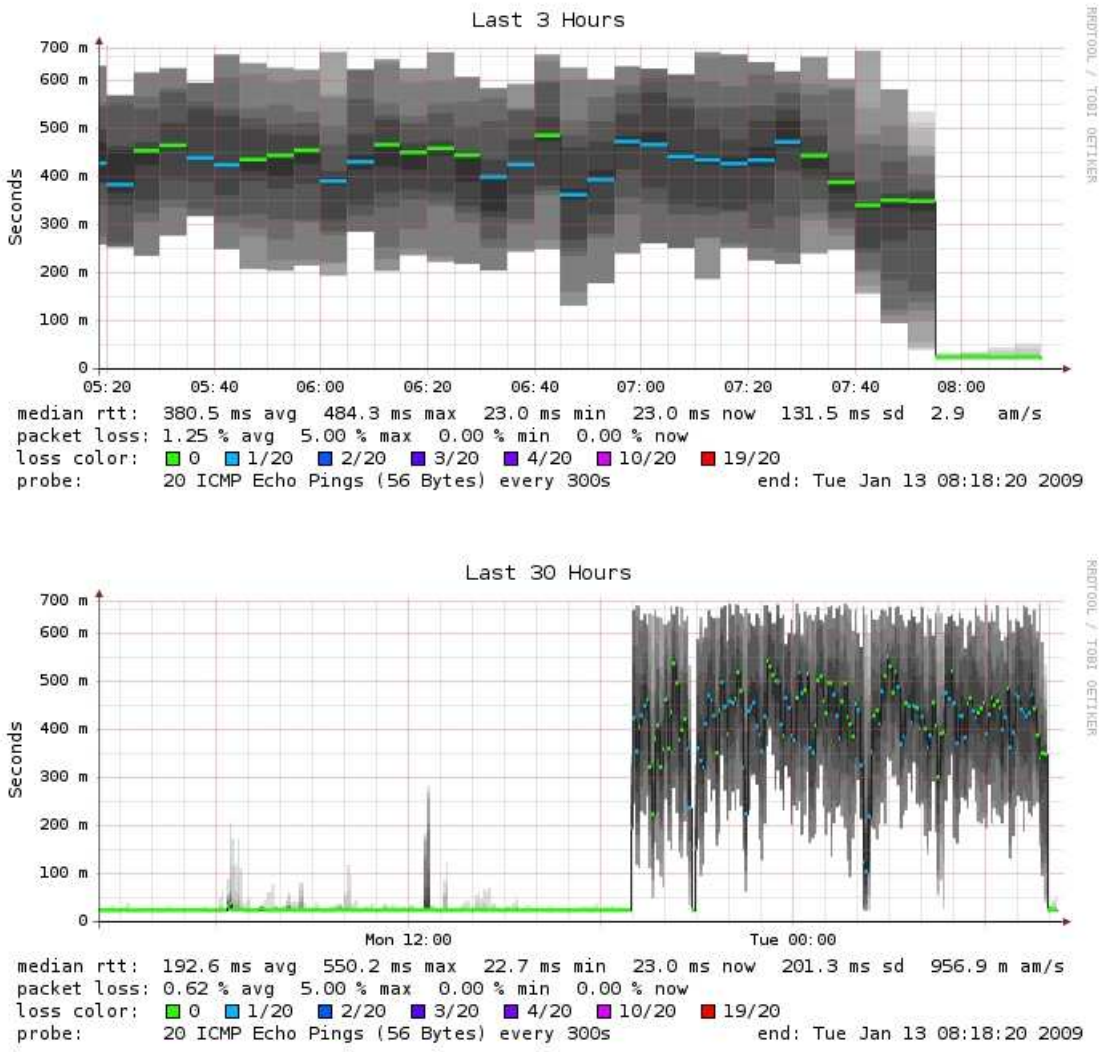


Kuva 23. Etäpisteessä verkon latenssi kasvaa ja pakettien menetykset lisääntyvät varmuuskopioinnin aikana.

Pitemmällä aikavälillä katsottuna varmuuskopiointien kestot pysyvät kuitenkin aika säännöllisinä (Kuva 24). Tämä helpottaa järjestelmän käyttämistä, kun tiedetään melko tarkkaan varmuuskopiointien vaatimat ajat. Näin voidaan luottaa varmemmin siihen, että varmuuskopioinnit onnistuvat määritettyinä aikoina jokaisella kerralla. Kuva 25 havainnollistaa vielä hieman tarkemmin yhden työaseman varmuuskopioinnin aiheuttamaa poikkeamaa verkon normaalissa käytössä.



Kuva 24. Etäpisteen viimeisen kymmenen päivän latensseista voi huomata selvät piikit varmuuskopiointien aikana. Kopiointien kestot pysyvät melko säännöllisinä.



Kuva 25. Etäpisteen työaseman varmuuskopiointi näkyy selvänä poikkeamana verkon normaalissa käytössä.

11 PROJEKTIN YHTEENVETO

Projekti onnistui kokonaisuudessaan mielestäni hyvin. Järjestelmä vastasi määrittelyä ja toimii luotettavasti sekä on selvästi parempi kuin yrityksen aiempi ratkaisu. Myös yritys oli tyytyväinen järjestelmään. Projektissa pysyin sovituissa aikatauluissa ja olin yhteydessä yrityksen järjestelmävastaavaan projektin kaikissa vaiheissa. Järjestelmän käyttöönotto oli mielestäni työn haastavin osuus ja se vaati myös aktiivista sosiaalista kanssakäymistä verkon käyttäjien kanssa. Projektin lopputuloksena yrityksellä on käytössään hyvin toimiva varmuuskopiointijärjestelmä, minkä elinkaarta voidaan tulevaisuu-

dessa helposti pidentää pienillä investoinneilla.

11.1 Määrittelyn onnistuminen

Järjestelmä määriteltiin mielestäni riittävän tarkasti ja sen pohjalta järjestelmän suunnitteleminen onnistui hyvin. Käyttöön otettu järjestelmä vastasi mielestäni myös hyvin määrittelyä. Järjestelmä on dynaaminen, helposti muokattavissa ja se toimii itsenäisesti. Järjestelmä ei vaadi työasemien käyttäjiltä juuri lainkaan toimenpiteitä vaan riittää, kun käyttäjät toimivat ohjeiden mukaisesti ja pitävät koneensa yrityksen verkossa myös työajan ulkopuolella. Järjestelmä ei myöskään häiritse verkkopalvelujen käyttöä etäpisteissä paitsi harvinaisesti tilanteessa jossa varmuuskopiointi venyy työajalle.

Määrittelyssä järjestelmältä haluttiin myös tietojen säilyvyyttä, palauttamisen mahdollisuutta ylläpidolle ja edistyneimmille käyttäjille sekä helppoa ylläpidettävyyttä. Järjestelmä takaa mielestäni tietojen säilyvyyden erinomaisesti niin varmuuskopioituna palvelimella kuin varmuuskopioitaessa palvelimelle. Järjestelmän käyttöönoton aikana en huomannut kertaakaan, että tallennetut tiedostot olisivat kadonneet tai muuttuneet kopioinnin aikana. Valmis järjestelmä tarjoaa hyvät mahdollisuudet ylläpidolle ja myös edistyneimmille käyttäjille tehdä palautuksia suoraan työasemille, palvelimelle ja ulkoisille medioille. Järjestelmää on myös erittäin helppoa ylläpitää ja tarkkailla. Määrittelyssä eräs tärkeimmistä seikoista oli järjestelmän kustannustehokkuus, joka onnistui mielestäni erittäin hyvin. Järjestelmän käyttöönotto ei aiheuttanut minkäänlaisia kuluja yritykselle. Tulevaisuudessa järjestelmän kehittäminen kuitenkin tulee vaatimaan joitakin investointeja yritykseltä.

11.2 Suunnittelun onnistuminen

Järjestelmän suunnittelu onnistui mielestäni kokonaisuutena hyvin. Yksityiskohtaisen määrittelyn avulla minun oli helppo rajata saatavilla olevista ratkaisuista selkeästi sopivimmat vertailtavaksi. Erilaisten ratkaisujen vertailu lisäsi myös selvästi tietoani kaikista erilaisista varmuuskopiointiin liittyvistä asioista, joita en välttämättä olisi huomannut tutustumalla pelkästään yhteen ratkaisuun. Lisäksi valitsemani ratkaisu soveltui

lopulta hyvin yrityksen tietojärjestelmän varmuuskopioimiseen.

Varmuuskopioitavien työasemien ja palvelimien rajaaminen vain kriittisimpiin laitteisiin oli oikea ratkaisu. Myös varmuuskopioinnin rajaaminen oletuksena pelkästään Documents and Settings -kansioon osoittautui sopivaksi ratkaisuksi. Järjestelmään työasemia lisätessä kävi kuitenkin ilmi, että monella käyttäjällä kyseisen kansion koko oli melkein kolme gigatavua ja muutamilla jopa enemmän. Tämä oli laskelmieni (Taulukko 2) mukaan lähellä maksimiarvoa, kun halutaan varmuuskopioinnin onnistuvan yön aikana. Tämän vuoksi ei juuri ole mahdollista varmuuskopioida muita kansioita, kun halutaan, että kopiointi ei vaikuttaisi normaaliin työskentelyyn. Työn aikana jouduin toki lisäämään joitain tärkeitä kansioita varmuuskopioitavaksi, mutta näiden koot olivat niin pieniä, että siitä ei ollut haittaa.

Suunnitelman onnistumisesta kertoi mielestäni myös se, että sen pohjalta järjestelmän käyttöönotto onnistui helposti ilman suurempia ongelmia. Kun olin ennalta tutustunut suunnitteluvaiheessa hyvin valitsemaani ratkaisuun, oli sen asennus helppoa ja vaivatonta. Lisäksi järjestelmän asetusten määrittämistä auttoi se, että olin etukäteen suunnitellut mitkä laitteet varmuuskopioidaan, mitkä tiedostot varmuuskopioidaan ja milloin varmuuskopioinnit otetaan.

11.3 Tulevaisuuden tarpeet

Järjestelmän suunnittelun, käyttöönoton ja käyttämisen aikana ilmeni erilaisia seikkoja, joihin yrityksen tulee tulevaisuudessa kiinnittää huomiota. Varmuuskopiointien tilan tarve levyjärjestelmässä kasvaa selvästi siihen asti kunnes järjestelmässä olevista kaikista laitteista on varmuuskopioituna 76 viikkoa vanhat kokonaiset varmuuskopioinnit. Tämän jälkeen uudet varmuuskopioinnit vievät tilaa vain uusien ja muuttuneiden tiedostojen osalta, kun järjestelmä poistaa aina vanhimman täyden varmuuskopioinnin. Käytännössä tilan tarvetta tulee tarkkailla jatkuvasti ja siihen on syytä varautua riittävän ajoissa. Levyjärjestelmän kasvattaminen on kuitenkin edullisin vaihtoehto pidentää varmuuskopiointijärjestelmän elinikää. Säilytettävien kokonaisten varmuuskopiointien määrää järjestelmässä voidaan myös vähentää, mutta tällöin tärkeiden tietojen säilyvyys heikkenee.

Tulevaisuuden tarpeena näen myös nauhavarmistuksen kehittämisen. Nykyisen nauhaaseman maksimi tallennuskapasiteetti on selvästi liian pieni, kun jo nyt varmuuskopiointijärjestelmän varmuuskopioimiseen joudutaan käyttämään useita nauhoja. Kierrätettäviä nauhoja tarvitaan suuri määrä ja tallentaminen on työlästä ja vie paljon aikaa. Monelta nauhalta palauttaminen on lisäksi hankalaa ja hidasta. Yksi ratkaisu on investoida tehokkaampaan nauhajärjestelmään. Toinen huomattavasti kustannustehokkaampi ratkaisu on vuokrata ulkoiselta palveluntarjoajalta varmistustilaa. Ratkaisu lisäisi myös selvästi tietoturvaa, koska varmuuskopioinnit ovat tällöin oman järjestelmän lisäksi ulkoisen palveluntarjoajan palvelimilla. Nämä palvelimet ovat yleensä erittäin hyvin varmistettuja, jolloin varmuuskopioinnit ovat varmistettuna moneen kertaan myös ulkoisen palveluntarjoajan järjestelmässä. Palvelut ovat myös luotettavia, koska palvelimet sijaitsevat yleensä lukituissa palvelinkeskuksissa, joissa on video- ja kulunvalvonta. Ennen päätöksen tekoa on kuitenkin syytä vierailla paikan päällä katsomassa, mihin yrityksen tietoja on siirtämässä ja miten palveluntarjoaja tietojen turvallisuuden ja säilyttämisen hoitaa.

Ulkoisen palveluntarjoajan palvelimille varmistettaessa siirrettävät tiedot salataan tehokkaasti jolloin tiedonsiirto on turvallista. Ratkaisun huonona puolena on kuitenkin se, että tiedonsiirto käyttää yrityksen verkon kaistaa ja siirrettävän datan määrä on suuri, kun varmuuskopioidaan koko järjestelmää. Omien verkkonopeuksien nostaminen onkin mielestäni tärkein asia, johon yrityksen kannattaa tulevaisuudessa kiinnittää huomiota. Verkon nopeuksia nostamalla saadaan varmuuskopiointijärjestelmä toimimaan huomattavasti tehokkaammin ja työasemista voidaan varmuuskopioida enemmän tietoa. Verkkonopeuksia nostamalla parannetaan myös yrityksen työasemien etähallintaa ja lisätään mahdollisuuksia ottaa käyttöön uusia verkkopalveluita.

Tulevaisuudessa yrityksellä on edessä myös siirtyminen käyttämään uudempia käyttöjärjestelmiä työasemissa nykyisen Windows XP:n sijaan. Microsoft julkaisee uuden version Windows-käyttöjärjestelmästä nimellä Windows 7, joka on Windows Vistan seuraaja. Jos yritys päättää pysyä Windows-käyttöjärjestelmissä niin uskoisin siirtymisen tapahtuvan suoraan Windows 7:ään Vistan sijasta. Toinen mahdollisuus on siirtyä käyttämään Linux-käyttöjärjestelmiä myös työasemapuolella. Tässä tosin on mahdollisia yhteensopivuusongelmia käytössä olevien ohjelmien kanssa. Oli ratkaisu sitten mikä tahansa, tulee yrityksen seurata BackupPC:n kehittämistä ja yhteensopivuutta uusien

käyttöjärjestelmien kanssa.

11.4 Näkökulmia

Työssäni ilmeni monia asioita, joita yrityksen kannattaa jatkossa pohtia. Yksi tällaisista asioista oli se, että miten voidaan varmuuskopioida käyttäjien sähköpostit niin, että ei vahingossakaan rikottaisi lakia. Sähköpostit on mahdollista myös tallentaa suoraan palvelimelle, mutta yhtä lailla palvelinta palautettaessa ylläpito voi vahingossa avata käyttäjien sähköposteja. Itse näkisin tässä tapauksessa yhdeksi vaihtoehdoksi kieltää työntekijöitä käyttämästä yrityksen sähköpostia henkilökohtaisten asioiden hoitoon.

Toinen vaihtoehto olisi antaa käyttäjille mahdollisuus tehdä palautukset, koska se on mahdollista BackupPC:ssä. Kun käyttäjille annetaan oikeudet kirjautua sisään ohjelmaan ja tehdä palautuksia itsenäisesti. Menetelmä kuitenkin vaatii sen, että käyttäjille pitäisi järjestää koulutusta ohjelman käytöstä. Koulutuksen järjestäminen taas tietäisi lisäkustannuksia yritykselle. Ratkaisusta voisi mahdollisesti seurata myös erilaisia virhetilanteita, kun järjestelmällä on useita käyttäjiä.

Työn aikana herätti runsaasti keskustelua medioissa eduskunnan käsittelyyn tuleva ns. Lex Nokia -lakiehdotus, joka antaisi yrityksille oikeuden tarkkailla työntekijöidensä sähköposteja entistä vapaammin. Tolvanen kirjoitti Satakunnan Kansassa (9.2.2009) Lex Nokiasta, että sen toteutuessa yrityksen tulisi tehdä asianmukaiset tietoturvallisuustoimenpiteet päästäkseen käsittelemään sähköisten viestien tunnistamistietoja. Yrityksen pitäisi siis estää työntekijöiden pääsy internetiin työasemilta tai vaihtoehtoisesti pääsy nettisähköposteihin, netin yhteisöpalveluihin ja pikaviestimiin. Tällaisia palveluita ovat esimerkiksi Gmail, Hotmail, Facebook, Messenger, Skype ja vastaavat palvelut. Lisäksi yrityksen pitäisi estää ulkoisten muistien käyttö ja seurata sitä. Tämä tarkoittaisi käytännössä sitä, että esimerkiksi USB-portit ja CD-ROM asemat pitäisi poistaa työasemista. Sähköisten viestien tunnistamistietojen seuraamisesta ei olisi suurta hyötyä yrityksille, kun samalla työntekijät voivat tallentaa yrityssalaisuuksia muistitikuille tai vuotaa niitä toisen sähköpostin kautta. Lakiesityksessä on mielestäni selvästi aukkoja, mutta tulevaisuudessa tällaisia lakiesityksiä pohditaan varmasti useammin ja yrityksen kannattaakin seurata näitä asioita myös varmuuskopiointijärjestelmän kehittämisen kan-

nalta.

Työn aikana huomasin myös sen, että varmuuskopioitavien työasemien käyttäjistä osa ottaa työasemansa kotiin työpäivän jälkeen. Tämän vuoksi työasema tulee varmuuskopioiduksi harvoin, koska järjestelmä ei varmuuskopioi työasemaa, joka ei ole yrityksen verkossa. Yrityksen tuleekin mielestäni kiinnittää huomiota tähän ja pyrkiä painottamaan työntekijöille varmuuskopioinnin tärkeyttä. Monissa lähteissä kerrottiin, että varmuuskopiointien tärkeys opitaan yrityksissä vasta tilanteessa, kun tarvittavaa varmuuskopiointia ei ole olemassa. Tällainen tilanne voidaan helposti välttää, kun käyttäjät saadaan pitämään koneensa yrityksen verkossa myös työajan ulkopuolella.

Kun jatkossa yrityksessä otetaan käyttöön uusia työasemia, on ne mielestäni hyvä asentaa varmuuskopioitavaksi jo asennusvaiheessa. Näin koneesta saadaan ensimmäinen kokonainen varmuuskopiointi helposti eikä asennuksia tarvitse suorittaa etäyhteydellä vaan kone on varmuuskopioituna valmiiksi, kun työntekijä saa koneen käyttöönsä. Jos taas työasema on elinkaarensa päässä, kannattaa vanha varmuuskopiointi jättää järjestelmään ja ottaa uudesta hankitusta työasemasta uusi kokonainen varmuuskopio. BackupPC tallentaa samat tiedot palvelimelle kuitenkin vain kertaalleen. Jos työntekijä jostain syystä poistuu yrityksen palveluksesta, ei mielestäni kyseisen työntekijän varmuuskopiointeja kannata poistaa erikseen järjestelmästä. Järjestelmä poistaa vanhentuneet varmuuskopiot automaattisesti ja järjestelmään jää lopulta vain yksi kokonainen varmuuskopio. Jos BackupPC-ohjelma jostain syystä menee epäkuntoon ei kannata sitä erikseen ruveta palauttamaan, koska sen uudelleen asentaminen on helppoa. Riittää, kun asentaa ohjelman uudelleen ja palauttaa ainoastaan konfiguraatiot tai asettaa ne uudelleen.

LÄHTEET

Barratt, C. 2007. BackupPC documentation [verkkodokumentti]. [Viitattu 1.12.2008] Saatavissa: http://backuppc.sourceforge.net/faq/BackupPC.html

Boström, M. 2003. Kotimikron tietoturva. Jyväskylä. Gummerus.

Durham, J. 2002. Linux+-sertifikaatti. Helsinki. Edita Publishing Oy.

Escoto, B. 2008. rdiff-backup user manual [verkkodokumentti]. [Viitattu 12.12.2008] Saatavissa: http://nongnu.org/rdiff-backup/rdiff-backup.1.html

Järvinen, P. 2002. Tietoturva & yksityisyys. Porvoo. Docendo Finland Oy.

Karhulahti, M. 2007. Vaihtoehtoja varmuuskopiointiin [verkkodokumentti]. [Viitattu 15.12.2008] Saatavissa: http://sinuhe.jypoly.fi/~karmi/tutoriaalit/Varmuuskopiointi.htm

Kiwi, K. 2007. Logical volume management [verkkodokumentti]. [Viitattu 9.12.2008] Saatavissa: http://www.ibm.com/developerworks/linux/library/l-lvm2/index.html

KP-ServicePartner Oy kotisivut. [Viitattu 17.11.2008]
http://www.kp-servicepartner.com/

L 13.8.2004/759. Laki yksityisyyden suojasta työelämässä.

Leaver, M. 2007. RAID is not a backup solution [verkkodokumentti]. [Viitattu 19.11.2008] Saatavissa: http://www.2brightsparks.com/resources/articles/

Pohjonen, R. 2002. Tietojärjestelmien kehittäminen. Jyväskylä. Docendo Finland Oy.

Preston, C. 2007. Backup and Recovery. Yhdysvallat. O'Reilly Media, Inc.

Sibbald, K. 2008. It comes in the night and sucks the essence from your computers –

Bacula manual [verkkodokumentti]. [Viitattu 4.12.2008] Saatavissa:
http://www.bacula.org/en/rel-bacula.pdf

Sundell, S. 2000. RAIDia koko kansalle. MikroPC 2000 (17). 34 – 40.

Tolvanen, K. Nokiakaan ei voisi nyt soveltaa Lex Nokiaa ja seurata posteja. Satakunnan Kansa 9.2.2009, s. 3.

LIITELUETTELO

KP Service Partner

IT-yksikkö
Juha Riikonen

9.2.2009

VARMUUSKOPIOINTIJÄRJESTELMÄN SUUNNITELMA

Tämä dokumentti sisältää suunnitelman yrityksen tietojärjestelmän varmuuskopioimisesta.

JÄRJESTELMÄN MÄÄRITTELY

Järjestelmä on suunniteltava mahdollisimman dynaamiseksi ja kustannustehokkaaksi eli järjestelmän muokkaaminen on oltava helppoa eikä se saa aiheuttaa yritykselle lisäkustannuksia. Yritykselle tärkeiden tietojen säilyvyys on varmistettava järjestelmän avulla.

Järjestelmää suunniteltaessa tulee ottaa huomioon lisäksi seuraavat seikat:

- Varmuuskopioiminen saa vaatia hyvin vähän toimenpiteitä käyttäjiltä.
- Etäpisteiden varmuuskopiointi ei saa haitata verkkopalvelujen käyttöä.
- Tieto ei saa muuttua kun varmuuskopioidaan etäpisteistä.
- Palauttamisen mahdollisuus on oltava ylläpidolle ja edistyneimmille käyttäjille.
- Palauttaminen on oltava mahdollista suoraan koneelle tai erilliselle medialle.
- Järjestelmän on oltava yksinkertainen ylläpitää ja tarkkailla.
- Järjestelmän on oltava tietoturvallinen.
- Järjestelmän vaiheiden testaus tulee suorittaa useilla työasemilla.

Varmuuskopiointijärjestelmän on toimittava automaattisesti ja itsenäisesti. Lisäksi järjestelmässä olisi hyvä olla monipuolinen käyttöliittymä, jolla voi tarkkailla järjestelmän toimintaa ja vikatilanteita. Raportoinnin mahdollisuus on myös huomioitava sekä järjestelmän migraatio tulevaisuudessa.

MITÄ VARMUUSKOPIOIDAAN

Kaikki yrityksen toiminnalle tärkeät tiedostot tulee varmuuskopioida. Palvelimista tuleevarmuuskopioida kaikki verkon palveluita tuottavat palvelimet ja työasemista kaikki ne työasemat, joita käytetään henkilökohtaisessa työssä. Palvelimet varmuuskopioidaan kokonaisuudessaan ja työasemista varmuuskopioidaan Documents And Settings -kansio, joka sisältää käyttäjille tärkeät tiedostot (profiilit, dokumentit ja kansiot, työpöydän, kirjanmerkit, sähköpostit).

MILLOIN VARMUUSKOPIOIDAAN

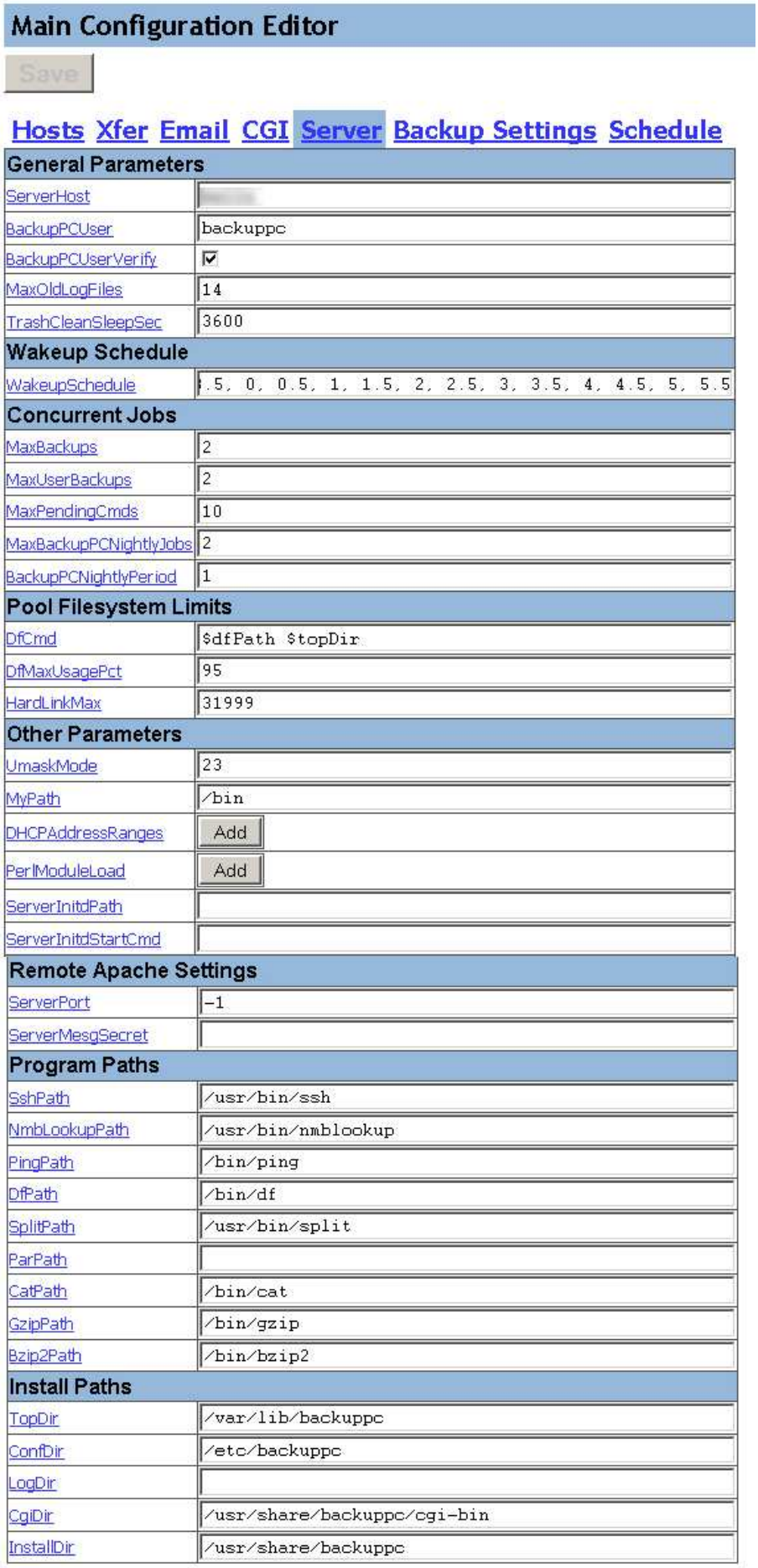
Varmuuskopioinnit tulee suorittaa sellaiseen aikaan, jolloin verkkoa käytetään mahdollisimman vähän. Tällainen ajankohta on öisin ja viikonloppuisin. Ajankohtaa voidaan myöhemmin säätää tehokkaammaksi kokemusten perusteella. Sopiva lähtökohta on, että varmuuskopiot otetaan arkisin öisin ja viikonloppuisin koko vuorokauden aikana. Täysi varmuuskopiointi olisi hyvä ottaa kerran viikossa ja inkrementaaliset varmuuskopiot kerran vuorokaudessa ainakin arkisin, jolloin töitä tehdään.

VARMUUSKOPIOIDEN VARMISTAMINEN

Varmuuskopiointijärjestelmä varmistetaan nauhajärjestelmällä vanhan varmuuskopiointijärjestelmän mukaisesti. Tulevaisuudessa tulee pohtia tehokkaampaan nauha-asemaan investoimista tai ulkopuolisen palveluntarjoajan palvelintilan vuokraamista varmuuskopioiden varmuuskopioimiseen.

KÄYTTÄJIEN OHJEISTUS

Työasemien käyttäjiä ohjeistetaan henkilökohtaisesti järjestelmän käyttöönoton aikana ja lisäksi käyttäjille tehdään erillinen ohjedokumentti koskien varmuuskopiointijärjestelmän käyttöä. Ohjedokumentti lähetetään jokaiselle käyttäjälle kenen työasemaa varmuuskopioidaan ja lisäksi dokumentti tallennetaan yrityksen Intranet-sivuille.

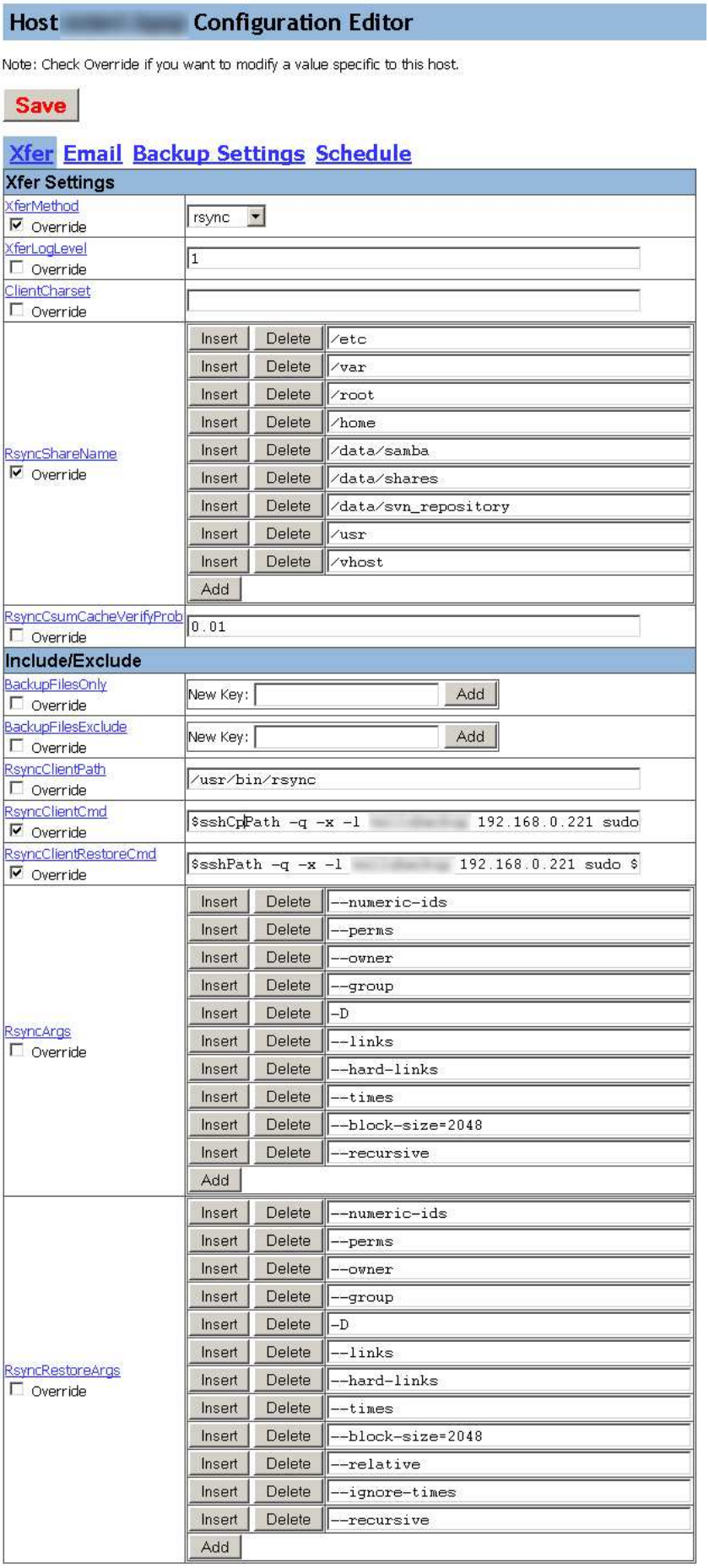


Main Configuration Editor

Save

Hosts Xfer Email CGI Server Backup Settings Schedule

General Parameters	
ServerHost	[redacted]
BackupPCUser	backuppc
BackupPCUserVerify	☑
MaxOldLogFiles	14
TrashCleanSleepSec	3600
Wakeup Schedule	
WakeupSchedule	.5, 0, 0.5, 1, 1.5, 2, 2.5, 3, 3.5, 4, 4.5, 5, 5.5
Concurrent Jobs	
MaxBackups	2
MaxUserBackups	2
MaxPendingCmds	10
MaxBackupPCNightlyJobs	2
BackupPCNightlyPeriod	1
Pool Filesystem Limits	
DfCmd	$dfPath $topDir
DfMaxUsagePct	95
HardLinkMax	31999
Other Parameters	
UmaskMode	23
MyPath	/bin
DHCPAddressRanges	Add
PerlModuleLoad	Add
ServerInitdPath	
ServerInitdStartCmd	
Remote Apache Settings	
ServerPort	-1
ServerMesgSecret	
Program Paths	
SshPath	/usr/bin/ssh
NmbLookupPath	/usr/bin/nmblookup
PingPath	/bin/ping
DfPath	/bin/df
SplitPath	/usr/bin/split
ParPath	
CatPath	/bin/cat
GzipPath	/bin/gzip
Bzip2Path	/bin/bzip2
Install Paths	
TopDir	/var/lib/backuppc
ConfDir	/etc/backuppc
LogDir	
CgiDir	/usr/share/backuppc/cgi-bin
InstallDir	/usr/share/backuppc



Host [redacted] Configuration Editor

Note: Check Override if you want to modify a value specific to this host.

Save

Xfer Email Backup Settings Schedule

Xfer Settings

XferMethod ☑ Override	rsync
XferLogLevel ☐ Override	1
ClientCharset ☐ Override	
RsyncShareName ☑ Override	Insert Delete /etc Insert Delete /var Insert Delete /root Insert Delete /home Insert Delete /data/samba Insert Delete /data/shares Insert Delete /data/svn_repository Insert Delete /usr Insert Delete /vhost Add
RsyncCsumCacheVerifyProb ☐ Override	0.01

Include/Exclude

BackupFilesOnly ☐ Override	New Key: Add
BackupFilesExclude ☐ Override	New Key: Add
RsyncClientPath ☐ Override	/usr/bin/rsync
RsyncClientCmd ☑ Override	$sshCmdPath -q -x -l [redacted] 192.168.0.221 sudo
RsyncClientRestoreCmd ☑ Override	$sshPath -q -x -l [redacted] 192.168.0.221 sudo $
RsyncArgs ☐ Override	Insert Delete --numeric-ids Insert Delete --perms Insert Delete --owner Insert Delete --group Insert Delete -D Insert Delete --links Insert Delete --hard-links Insert Delete --times Insert Delete --block-size=2048 Insert Delete --recursive Add
RsyncRestoreArgs ☐ Override	Insert Delete --numeric-ids Insert Delete --perms Insert Delete --owner Insert Delete --group Insert Delete -D Insert Delete --links Insert Delete --hard-links Insert Delete --times Insert Delete --block-size=2048 Insert Delete --relative Insert Delete --ignore-times Insert Delete --recursive Add

BackupPC: Host Summary

This status was generated at 1/22 15:33.

Hosts with good Backups

There are 20 hosts that have been backed up, for a total of:

- 63 full backups of total size 636.09GB (prior to pooling and compression),
- 129 incr backups of total size 149.86GB (prior to pooling and compression).

Host	User	#Full	Full Age (days)	Full Size (GB)	Speed (MB/s)	#Incr	Incr Age (days)	Last Backup (days)	State	Last attempt
[illegible]	[illegible]	7	4.9	39.96	16.19	16	0.5	0.5	idle	idle
[illegible]	[illegible]	1	1.0	3.34	0.05	0		1.0	idle	done
[illegible]	[illegible]	7	2.8	2.76	3.98	14	0.5	0.5	idle	idle
[illegible]	[illegible]	1	6.0	2.69	0.05	2	1.9	1.9	idle	idle
[illegible]	[illegible]	1	42.1	4.54	5.54	0		42.1	idle	no ping (no ping response)
[illegible]	[illegible]	1	15.0	4.35	0.05	2	1.9	1.9	idle	idle
[illegible]	[illegible]	7	0.5	0.61	1.34	12	1.5	0.5	idle	restore done
[illegible]	[illegible]	3	23.8	3.75	0.05	6	1.7	1.7	idle	idle
[illegible]	[illegible]	7	2.9	16.66	8.24	16	0.5	0.5	idle	idle
[illegible]	[illegible]	1	42.1	1.22	1.36	0		42.1	idle	no ping (no ping response)
[illegible]	[illegible]	1	6.0	0.62	7.41	1	3.9	3.9	idle	no ping (no ping response)
[illegible]	[illegible]	6	5.8	10.41	6.46	15	0.5	0.5	idle	idle
[illegible]	[illegible]	1	48.0	1.56	0.05	1	45.9	45.9	idle	no ping (no ping response)
[illegible]	[illegible]	1	51.0	2.51	0.04	0		51.0	idle	no ping (no ping response)
[illegible]	[illegible]	1	52.0	1.03	0.05	2	3.9	3.9	idle	no ping (no ping response)
[illegible]	[illegible]	6	2.8	3.64	3.95	14	0.5	0.5	idle	idle
[illegible]	[illegible]	7	2.8	3.63	2.97	17	0.5	0.5	idle	idle
[illegible]	[illegible]	0		0.00		1	0.8	0.8	backup in progress	
[illegible]	[illegible]	2	9.8	2.63	0.07	3	7.8	7.8	idle	no ping (no ping response)
[illegible]	[illegible]	2	1.5	69.57	27.85	7	0.5	0.5	idle	idle

KP Service Partner

IT-yksikkö
Juha Riikonen

7.2.2009

OHJEET TYÖASEMAN VARMUUSKOPIOIMISESTA

Tämä ohje on tarkoitettu niille käyttäjille, joiden työasema on liitetty yrityksen varmuuskopiointi-järjestelmään. Järjestelmään on liitetty työasemat, joissa on katsottu olevan yrityksen toiminnan kannalta tärkeitä säilytettäviä tietoja. Ota yhteyttä ylläpitoon, jos mielestäsi työasemasi tulisi liittää järjestelmään tai sinulle ilmenee muuta kysyttävää.

1. Työasemasta varmuuskopioidaan oletuksena Documents And Settings -kansio (Vistassa Users-kansio). Kansio sisältää käyttäjän profiilin, dokumentit ja kansiot, työpöydän, Internet-selaimen suosikit sekä sähköpostit.

2. Tallenna työtiedostot aina työpöydälle tai Documents And Settings -kansioon.

3. Varmuuskopioitavaksi voidaan tapauskohtaisesti lisätä myös muita kansioita. Ota yhteyttä ylläpitoon, jos mielestäsi tärkeitä tiedostoja on myös muualla kuin Documents And Settings -kansiossa.

4. Pidä varmuuskopioitava kansio alle 3 gigatavun kokoisena. Älä siis tallenna suuria tiedostoja (esim. videoita) kyseiseen kansioon.

5. Tallenna varmuuskopioitavaan kansioon vain työtiedostoja. Tallenna henkilökohtaiset tiedostot toiseen kansioon.

6. Työaseman varmuuskopiointi tapahtuu öisin ja viikonloppuisin, joten jätä työasema päälle töistä lähtiessäsi. Kirjaudu kuitenkin ulos koneelta.

7. Ota yhteyttä ylläpitoon jos vahingossa tuhoat tärkeän tiedoston, kirjoitat tiedoston päälle tai tiedosto ei enää jostain syystä toimi. Varmuuskopioidut tiedostot voidaan palauttaa järjestelmästä.

8. Järjestelmä ei varmuuskopioi työasemaa, jos se ei ole päällä. Muista jättää työasema päälle aina töistä lähtiessäsi.

9. Järjestelmä ei myöskään varmuuskopioi työasemaa, jos se ei ole yrityksen verkossa. Muista jättää työasema riittävän usein työpaikalle, jos käytät työasemaa myös kotona.

10. Noudattamalla ohjeita tiedostosi säilyvät ja samalla parannat yrityksen tietoturvaa.

Backup browse for [redacted]

- You are browsing backup #79, which started around 1/22 03:31 (0.3 days ago),
- Select the backup you wish to view: #79 - (1/22 03:31)
- Enter directory: /juha.riikonen Go
- Click on a directory below to navigate into that directory,
- Click on a file below to restore that file,
- You can view the backup history of the current directory.

Contents of DaS/juha.riikonen

- DaS
  - All Users
  - Default User
  - isoveli
  - juha.riikonen
    - .gimp-2.4
    - .thumbnails
    - .VirtualBox
    - Application Data
    - Contacts
    - Cookies
    - Käynnistä-valikko
    - Local Settings
    - Mallit
    - New Folder
    - Omat tiedostot
    - Recent
    - SendTo
    - Suosikit
    - Tulostinympäristö
    - Työpöytä
    - UserData
    - Verkkoympäristö
  - Järjestelmänvalvoja
  - LocalService
  - NetworkService

Name	Type	Mode	#	Size	Date modified
Select all			Restore selected files		
.gimp-2.4	dir	0755	79	0	2008-10-28 09:44:27
.recently-used.xbel	file	0644	79	9936	2008-09-23 07:47:18
.thumbnails	dir	0755	79	0	2008-09-22 08:19:40
.VirtualBox	dir	0755	79	0	2008-09-10 12:42:53
Application Data	dir	0755	79	0	2008-12-04 12:07:16
Contacts	dir	0755	79	0	2008-09-09 09:01:52
Cookies	dir	0755	79	0	2009-01-21 15:00:48
ErrorLog.txt	file	0644	79	6246	2008-10-13 08:08:21
Käynnistä-valikko	dir	0755	79	0	2006-02-09 12:59:23
Local Settings	dir	0755	79	0	2006-02-09 12:59:22
Mallit	dir	0755	79	0	2006-02-09 12:59:22
New Folder	dir	0755	79	0	2008-10-06 11:24:45
Nimetön.xcf	file	0644	79	1030935	2008-09-22 11:25:37
ntuser.ini	file	0644	79	188	2006-02-09 11:34:06
Omat tiedostot	dir	0755	79	0	2008-10-14 13:03:50
Recent	dir	0755	79	0	2009-01-21 15:15:28
SendTo	dir	0755	79	0	2006-02-09 12:59:22
Suosikit	dir	0755	79	0	2008-09-08 08:54:50
Thumbs.db	file	0644	79	3584	2008-09-22 10:56:56
Tulostinympäristö	dir	0755	79	0	2006-02-09 12:59:22
Työpöytä	dir	0755	79	0	2009-01-21 15:16:57
UserData	dir	0755	79	0	2008-09-09 09:02:10
Verkkoympäristö	dir	0755	79	0	2006-02-09 12:59:22
Select all			Restore selected files		

Directory backup history for [redacted]

This display shows each unique version of files across all the backups:

- Click on a backup number to return to the backup browser,
- Click on a directory link (dir) to navigate into that directory,
- Click on a file version link (v0, v1, ...) to download that file,
- Files with the same contents between different backups have the same version number,
- Files or directories not present in a particular backup have an empty box.
- Files shown with the same version might have different attributes. Select the backup number to see the file attributes.

History of DaS

Backup number	0	26	56	63	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
Backup time	10/9 13:29	11/11 00:40	12/10 19:02	12/17 19:00	1/7 19:00	1/8 19:00	1/9 19:00	1/10 19:00	1/11 19:00	1/12 19:26	1/13 19:01	1/14 19:16	1/15 19:20	1/16 19:31	1/17 19:36	1/18 19:20	1/19 19:58	1/21 03:49	1/22 03:31
All Users										dir									
Default User										dir									
isoveli										dir									
JRJEST~1.LOG										v0									
juha.riikonen										dir									
Järjestelmänvalvoja										dir									
LocalService										dir									
NetworkService										dir									

Restore Options for [redacted]

You have selected the following files/directories from share DaS, backup number #78:

- /juha.riikonen/Työpöytä/Opinnäytetyö kuvia/ultravnc.jpg

You have three choices for restoring these files/directories. Please select one of the following options.

Option 1: Direct Restore

You can start a restore that will restore these files directly onto [redacted].

Warning: any existing files that match the ones you have selected will be overwritten!

Restore the files to host [redacted]
Restore the files to share DaS
Restore the files below dir (relative to share) /juha.riikonen/Työpöytä/Opinnäytetyö kuvia

Start Restore

Option 2: Download Zip archive

You can download a Zip archive containing all the files/directories you have selected. You can then use a local application, such as WinZip, to view or extract any of the files.

Warning: depending upon which files/directories you have selected, this archive might be very very large. It might take many minutes to create and transfer the archive, and you will need enough local disk space to store it.

☑ Make archive relative to /juha.riikonen/Työpöytä/Opinnäytetyö kuvia (otherwise archive will contain full paths).
Compression (0=off, 1=fast,...,9=best) 5

Download Zip File

Option 3: Download Tar archive

You can download a Tar archive containing all the files/directories you have selected. You can then use a local application, such as tar or WinZip to view or extract any of the files.

Warning: depending upon which files/directories you have selected, this archive might be very very large. It might take many minutes to create and transfer the archive, and you will need enough local disk space to store it.

☑ Make archive relative to /juha.riikonen/Työpöytä/Opinnäytetyö kuvia (otherwise archive will contain full paths).

Download Tar File

Restore #0 Details for [redacted]

Number	0
Requested by	backuppc
Request time	11/25 14:24
Result	ok
Error Message	
Source host	[redacted]
Source backup num	39
Source share	DaS
Destination host	[redacted]
Destination share	DaS
Start time	11/25 14:24
Duration	4.7 min
Number of files	1701
Total size	1647.3 MB
Transfer rate	5.82 MB/sec
TarCreate errors	0
Xfer errors	0
Xfer log file	View, Errors

File/Directory list

Original file/dir	Restored to
[redacted]	[redacted]

LYHENTEET

CD-ROM	Compact Disc Read-Only Memory
CGI	Common Gateway Interface
CPU	Central Prosessing Unit
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DVD	Digital Versatile Disc
GB	Giga Byte
G.SHDSL	Symmetric High-Speed Digital Subscriber Line
GPL	General Public License
I/O	Input/Output
NFS	Network File System
RSH	Remote Shell
RSS	Really Simple Syndication
SSH	Secure Shell
TB	Tera Byte
USB	Universal Serial Bus
VPN	Virtual Private Network