TAMPEREEN
AMMATTIKORKEAKOULU

Virtuaalisen palvelinympäristön varmuuskopiointi

Samu Neulaniemi

Opinnäytetyö
Syyskuu 2017
Tietojenkäsittely
Tietoverkot

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tietojenkäsittely
Tietoverkot

NEULANIEMI, SAMU:
Virtuaalisen palvelinympäristön varmuuskopiointi

Opinnäytetyö 30 sivua
Syyskuu 2017

Opinnäytetyön tavoitteena oli kehittää varmuuskopiointitoteutus Cadmandata Oy:n sisäverkkoon. Tähän sisältyy virtuaalikoneiden varmuuskopiointi. Opinnäytetyön tarkoitus oli löytää mahdollisimman järkevä toteutus kyseiseen ympäristöön sekä toteuttaa se. Tähän kuuluvia toimenpiteitä oli ympäristön tarpeiden selvittäminen, eri varmuuskopiointiohjelmien vertailu, ja varmuuskopioinnin toteutus sopivimmalla ohjelmalla. Koska ympäristö on melko pieni, ratkaisu toteutettiin ilmaisilla varmuuskopiointiohjelmilla. Opinnäytetyön toteutuksen taustamateriaalina käytettiin teoria-aineistoa, jota sovellettiin tarpeen mukaan itse toteutukseen. Teoriaosassa kerrotaan varmuuskopioimisesta melko yleisellä tasolla, ja esitellään muun muassa yleisiä varmuuskopiointimenetelmiä ja parhaita käytäntöjä. Työssä käytettiin kvalitatiivisia menetelmiä, kun selvitettiin ympäristön varmuuskopiointitarpeita ja vertailtiin eri varmuuskopiointiohjelmia

Toteutus oli loppujen lopuksi varsin yksinkertainen ympäristön koon takia ja se tehtiin ohjelmilla Urbackup ja Cobian. Cobian on ollut yhtiön käytössä aikaisemminkin, mutta Urbackup on uusi ohjelma, joka soveltuu tähän toteutukseen monestakin systä; se on muun muassa helppokäyttöinen ja maksuton. Ominaisuuksiltaan siinä on jossain kohtaa parantamisen varaa, mutta sillä ei ollut tässä ympäristössä merkitystä. Ratkaisu sopi tähän verkkoon hyvin, vaikka se olikin erittäin yksinkertainen.

Asiasanat: varmuuskopiointi, palvelin, sisäverkko

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
Degree Programme in Business Administration Systems
Networking

NEULANIEMI SAMU:
Making a Back-Up of a Virtual Server Environment

Bachelor's thesis 30 pages
September 2017

The objective of this thesis was to find a backup solution for a small company's network that includes virtual machines. The company is called Cadmandata Oy. The purpose was to find the most practical solution for securing the data in the network and implementing it. This was done by comparing different backup programs and by finding out about the backup needs of the network. The theory section consists of different backup methods and information about backup at a general level, and this information will be applied to the solution to some extent. Qualitative research methods were used when comparing different programs and figuring out what the network needs and which programs to use.

A program called Urbackup was selected ultimately as it was found to be the best for implementing the backup. The reasons for this include it being freeware, it being really easy to use, and how easy it was to backup between virtual machines using the program. The solution serves this particular network well, and although the programs that were used lacked some features, that did not matter in this case, as the ease of use and them being freeware was far more important. There is still room for improvement in the solution, but it regardless proved to be practical and good.

Key words: backup, server, network

SISÄLLYS

JOHDANTO 7
1 VARMUUSKOPIOINTI 8
1.1 Varmuuskopioinnista tarkemmin 8
1.2 Erilaiset onnettomuudet 9
1.2.1 Laitteiston pettäminen 9
1.2.2 Inhimillinen erehdys 10
1.2.3 Tapahtuman pettäminen 10
1.2.4 Katastrofit 10
1.3 Disaster Recovery 11
2 ERILAISIA VARMUUSKOPIOINTIMENETELMIÄ 12
2.1 HSM 13
2.2 RAID 13
2.3 Bare metal restore 15
2.4 Synteettinen varmuuskopio 15
2.5 Enkryptaus 16
3 PARHAAT KÄYTÄNNÖT VARMUUSKOPIOINNISSA 17
3.1 Järkevä intervalli varmuuskopioinnissa 17
3.2 Varmuuskopioiden lokaatio 17
3.3 varmuuskopioinnin testaus 17
3.4 Tärkeimipien tietojen hahmottaminen 18
3.5 Täysien ja inkrementaalisten varmuuskopioiden balanssi 18
4 OMA TOTEUTUKSENI 19
4.1 Ympäristön infrastruktuuri 19
4.2 Käyttämäni ohjelmat ja kriteerit 20
4.2.1 UrBackup 20
4.2.2 Cobian 23
4.3 Muita varmuuskopiointiohjelmia 23
4.3.1 System Restore 24
4.3.2 Bacula 24
4.3.3 Amanda 25
4.3.4 Personal Backup 25
4.4 Yleistä varmuuskopiointiohjelmista 25
4.4.1 Yhteensopivuus 26
4.4.2 Helppokäyttöisyys 26
4.4.3 Ominaisuudet 26
4.5 Toteutukseni 27

5 POHDINTA 29
LÄHTEET 30

LYHENTEET JA TERMIT

BIA	Business Impact Analysis
Incremental Backup	Inkrementaalinen varmuuskopiointi
Full Backup	Täysi varmuuskopiointi
UPS	Uninterruptible Power Supply
RAID	Redundant Array of Independent Disks
HSM	Hierarchical Storage Migration
Striping	Lomitus
Mirroring	Peilaus

JOHDANTO

Opinnäytetyön aihe on virtuaalisen serveriympäristön varmuuskopiointi. Toimeksiantajana toimi Cadmandata Oy, joka on Tampereella toimiva IT-alan yritys. Idea syntyi työharjoittelun aikana, kun mietimme harjoittelupaikkani järjestelmäasiantuntijan kanssa sopivaa opinnäytetyötä. Työ on erittäin hyvä, koska sain tämäntapaisesta työstä kokemusta jo ollessani työharjoittelussa, kun toteutin asiakkaalle varmuuskopioinnin. Yrityksellä on pienehkö sisäinen verkko, joka toimii myös asiakkaiden varmuuskopiointi lokaationa (eli käytännössä pilvenä heille). Tämän lisäksi yrityksen omat virtuaalikoneet myös sisältyvät tähän varmuuskopiointiin. Tavoiteena oli keksiä mahdollisimman järkevä ja tehokas varmuuskopiointitoteutus, joka sopii yrityksen tarpeisiin. Tarkoituksena oli analysoida ympäristön tarpeet, ja vertailla eri varmuuskopiointi ohjelmia, ja tehdä toteutus valitulla ohjelmalla. Maksullista ohjelmaa ei työssä käytetty ja tämä työ kattaa kohtalaisen pienen ja yksinkertaisen varmuuskopiointitoteutuksen, sillä yhtiöllä ei ollut tarvetta sen suurempaan. Työhön kuuluu myös raportoinnin ohella lista parhaista käytännöistä varmuuskopioinnissa ja katsaus varmuuskopiointiin yleisesti. Työssä käytettiin kvalitatiivisia menetelmiä, kun selvitettiin ympäristön varmuuskopiointitarpeita ja vertailtiin eri varmuuskopiointiohjelmia. Tämä tapahtui lukemalla varmuuskopioinnista ja erilaisista käytännöistä, ja näiden tietojen perusteella sekä ympäristön tarpeet huomioon ottaen valittiin varmuuskopiointiohjelma ja itse toteutustapa.

Ennen toteutuksen tekemistä selvitettiin mikä ohjelma soveltuisi parhaiten varmuuskopioinnin toteuttamiseen vertailemalla eri ohjelmia, ja aikaisemminkin firman käytössä ollut Urbackup oli monestakin syystä hyvin soveltuva tähän; se on ilmainen, erittäin helppokäyttöinen ja sen avulla onnistuu varmuuskopiointi virtuaalikoneiden välillä helposti. Tämän lisäksi yrityksella oli jo ohjelman palvelinohjelmisto käytössä, joka asennettiin sinne työharjoitteluni aikana. Nämä asiat tekivät siitä loistavan vaihtoehdon. Tämän lisäksi käytettiin myös ohjelmaa nimeltä Cobian, joka oli yrityksen käytössä jo valmiiksi.

1 VARMUUSKOPIOINTI

Varmuuskopiointi on tietojen kopiointia ja varastointia sen varalta, että alkuperäinen tieto menetään syystä tai toisesta. On sanomattakin selvää, että varmuuskopiointi on erittäin tärkeää, sillä koko yhtiön toiminta voi potentiaalisesti kaatua tietojen menetykseen.Varmuuskopiointi on ollut äärimmäisen tärkeää tietotekniikan yleistymisestä asti, mutta vasta lähiaikoina sitä ollaan alettu kunnolla kunnioittamaan ja sen suunniteleminen on paljon helpomaa kuin aiemmin, johtuen lähinnä teknologian kehityksestä, mikä näkyy levyjen halpoina hintoina ja siirtonopeuksien kasvuna. (Little, Farmer, El-Hilali 2007, 13.) Varmuuskopioinnin toteutus on monien asioiden summa, ja hyvä varmuuskopiointi ei ole aina niin yksinkertaista toteuttaa.

Hyvän varmuuskopioinnin pitäisi pystyä mahdollistamaan järjestelmän toiminnan palautumisen virheen tai keskeytyksen jälkeen mahdollisimman nopeasti ja toimittamaan dataa paikkaan jossa sitä tarvitaan, kun sitä tarvitaan. Hyvälle varmuuskopiointiratkaisulle on tärkeää pystyä kopioimaan kaikki data, riippumatta sen alkuperästä. Kopioituun dataan pitää myös päästä käsiksi, ja sitä pitää pystyä kopioimaan eteenpäin. Myös skaalautuvuus on tärkeää yrityksen kasvaessa. Varmuuskopioinnin suunnitelu voi vaikuttaa helpolta ja yksinkertaiselta, mutta hyvän varmuuskopioinnin suunnitelussa yksityiskohtiin pitää kiinnittää kunnolla huomiota. Tärkeimpiä kysymyksiä varmuuskopioinnin suunnitelussa on tärkeän datan määritteleminen, sen kopioimisen ajankohta ja millä se kopioidaan. Näiden asioiden määrittelemistä kutsutaan BIA:ksi (Business impact analysis). On kovin yleistä, että varmuuskopiointikäytännön heikkoudet huomataan vasta, kun jotain pahaa tapahtuu, BIA:lla tätä yritetään välttää. (Little ym. 2007, kappale 1, sivu 3.)

1.1 Varmuuskopioinnista tarkemmin

Varmuuskopiointisuunnitelma voidaan jakaa tasoihin, niinkuin W. Curtis Preston kirjassaan Backup & Recovery tekee: “minimum coverage, unexpected disasters, get me driving now, major disasters ja maximum protection”. Minimum coverage tarkoittaa yksinkertaisesti kopioiden ottamista päivittäin, unexpected disasters kohdassa käytetään hyväkseen Uninterruptible power supplyja (UPS) ja journaling file systemiä. Get me driving now kohta käyttää disk mirroringia ja hot swap levyjä. major disasters ja

maximum protection kohdissa tieto lähetään turvaan myös muualle kuin itse työpaikalle. (Preston 2009, kappale 1.)

Tämä ei toki ole mikään virallinen luokittelu, mutta mielestäni se antaa hyvän kuvan eri tasoisista varmuuskopiointisuunnitelmista ja siitä näkee hyvin sen, että varmuuskopiointi voi olla muutakin, kuin kopioiden ottamista päivittäin muistitikulle.

Varmuuskopioinnissa on tärkeää kartoittaa yrityksen tarpeet ja suunnitella varmuuskopiointi sen mukaan. Hyviä kysymyksiä ovat esim. Mikä tieto on kaikista tärkeintä varmuuskopioida? Kuinka usein kannattaa varmuuskopioida? Varmuuskopiointilokaatio? Inkrementaalisten ja täysien varmuuskopioiden intervallit? Puhuin aiemmin BIA:sta eli Business impact analysiksestä, joka kattaa nämä kysymykset. BIA on tärkeä, kun määritellään minkälaisia ratkaisuja mikäkin yritys tarvitsee. (Little ym. 2007, kappale 1, sivu 3, 6-7.)

Pienelle yritykselle saattaa hyvin kelvata pelkkä päivittäinen varmuuskopioiden otto, mutta iso firma jolla on huipputärkeää tietoa luultavasti haluaa hieman edistyneemmän ja kehittyneemmän toteutuksen. Esimerkiksi tässä työssä pävittäinen kopiointi toiselle palvelimelle riittää ihan hyvin, mutta tämä tuskin riittää, kun puhutaan miljoonaluokan yritysten varmuuskopiointisuunnitelmista.

1.2 Erilaiset onnettomuudet

Asiat voivat mennä vikaan ja järjestelmä voi lakata toimimasta monesta eri syystä. Esittelen tässä muutamia yleisimpiä syitä sille, miksi onnettomuuksia tapahtuu ja miksi varmuuskopiointia tarvitaan

1.2.1 Laitteiston pettäminen

Laitteisto voi vikaantua monesta eri kohtaa. Esimerkiksi kovalevyn vikaantuminen voi jo aiheuttaa huonosti varmuuskopioiduissa järjestelmissä suurta vahinkoa. Tämän lisäksi eri tietokoneen osat voivat vikaantua, mikä yleensä ei ole niin harmillista, sillä tällöin itse data ei välttämättä vahingoitu. Tätä voidaan välttää pitämällä laitteisto

ajantasaisessa kunnossa, mutta vika voi tulla yllättäen täysin toimivaankin laitteistoon. (IBM Redbooks 2005, 5.) Tämän varalle on olemassa montakin teknologiaa, joita käsittellään myöhemmissä kappaleissa.

1.2.2 Inhimillinen erehdys

Yksi yleisimmistä onnettomuuden syistä on ihmisen tekemä virhe, esimerkiksi tärkeän datan poistaminen vahingossa. Tätä on aina tapahtunut, ja tulee aina tapahtumaan. Helpoin tapa välttää tälläistä, on erilaisien keinojen soveltaminen, joilla vältetään kokonaan sellaisten tilanteiden synty, jossa tälläistä pääsisi tapahtumaan. Koko mahdollisuus tälläiseen erehdykseen eliminoidaan, esimerkiksi rajoittamalla pääsy tälläiseen dataan. Dataan käsiksi pääsy on aina suositeltavaa rajoittaa vain niille henkilöille, jotka sitä oikeasti tarvitsevat. Mitä vähemmän luodaan tilanteita, joissa virheitä voi ylipäätään sattua, sen parempi. (IBM Redbooks 2005, 4.)

1.2.3 Tapahtuman pettäminen

Laitteiston lisäksi myös itse käynnissä oleva tapahtuma voi pettää ja yllättäen keskeytyä. Esimerkiksi varmuuskopiointi toiselle palvelimelle voi yllättäen keskeytyä vaikkapa lyhyen nettikatkoksen takia, jolloin oikein huonon onnen sattuessa data voi vahingoittua. Tälläinen on kohtalaisen harvinaista ja yleensä näistä palautuminen on helpompaa, kuin muunlaisista onnettomuuksista. (IBM Redbooks 2005, 6.)

1.2.4 Katastrofit

Katastrofeilla tarkoitetaan erilaisten luonnonvoimien aiheuttamaa tuhoa. Suomessa tälläinen on harvinaista, sillä täällä ei nähdä maanjäristyksiä tai hurrikaaneja, mutta esimerkiksi tulipalo on aivan huomioonotettava riski. On sanomattakin selvää, että koko paikan tuhoutuessa syystä tai toisesta, palautuminen on mahdotonta ilman varmuuskopioita, jotka sijaitsevat muualla kuin tuhoutuneessa paikassa. Etävarmuuskopiointi onkin oikeastaan ainut tapa varautua useimpien katastrofien varalta. (IBM Redbooks 2005, 6.)

1.3 Disaster Recovery

DR eli Disaster recovery tarkoittaa onnettomuuden sattuessa kykyä palauttaa data. Varsinkin menneisyydessä tätä ei juurikaan testailtu tai suunniteltu sen tarkemmin, vaan dataa pidettiin vain säilössä. Nykyään disaster recoveryyn panostetaan paljon enemmän ja erilaisten suunnitelmien suunnitelu ja testaus on normaalia. DR ja aikaisemmin mainittu BIA yhdistyvät siinä, että BIA:n avulla määritellään mikä data on tärkeintä, sillä pelkän raa'an datan säilöminen ei välttämättä ole ratkaisu mikä toimii; pitää ottaa myös huomioon datan sidoinnaisuus toiseen dataan. Hyvä disaster recovery-suunnitelma ottaa huomioon monenlaiset onnettomuudet ja pitää sisällään suunnitelmat niiden varalle. (Little ym. 2007, kappale 1, sivu 6-7.)

2 ERILAISIA VARMUUSKOPIOINTIMENETELMIÄ

Varmuuskopiointimenetelmät voidaan jakaa kahteen suurempaan ryhmään: offline varmuuskopiointiin, ja online varmuuskopiointiin. Offline varmuuskopiointi tarkoittaa varmuuskopiointia, joka suoritetaan järjestelmän ollessa tilassa, jolloin sitä ei voi käyttää mihinkään muuhun tarkoitukseen, kuin varmuuskopiointiin. Online varmuuskopiointi taas viittaa varmuuskopiointiin, joka tehdään järjestelmän ollessa käynnissä ja suorittaessa muita operaatioita. Järjestelmä on siis täysin normaalissa käytössä tämän aikana. (IBM Redbooks 2005, 8.)

Varmuuskopiointi voidaan jakaa myös täysiin ja inkrementaalisiin varmuuskopioihin. Täysi varmuuskopio, niin kuin nimestä voi päätellä, tarkoittaa, että kaikki varmuuskopioitava data varmuuskopioidaan, eikä mitään jätetä pois. Inkrementaalisten varmuuskopioiden ottaminen on tämän jälkeen mahdollista ja se tarkoittaa vain muuttuneen datan varmuuskopiointia. Yleinen käytäntö on, että täysiä varmuuskopioita otetaan harvemmin (esimerkiksi kerran viikossa), ja näitä täydennetään inkrementaalisilla varmuuskopioilla. Näin säästetään aikaa ja resursseja, sillä inkrementaalisten varmuuskopioiden ottaminen on luonnollisesti nopeampaa ja helpompaa datan määrän ollessa pienempi. On olemassa myös differential varmuuskopiointia, joka on muuten hyvin samankaltainen inkrementaalisen varmuuskopioinnin kanssa, mutta ensimmäisen varmuuskopiointikerran (täysi varmuuskopiointi) jälkeen se käyttää täyttä varmuuskopiota vertauksenaan, josta se katsoo mikä data on muuttunut, kun taas inkrementaalinen käyttää myös aikaisempia inkrementaalisia kertoja. Näin ollen voidaan sanoa differential varmuuskopioinnin olevan ns. välimalli näiden kahden välillä ja tila sekä resurssit joita se vaatii, ovat myös näiden kahden välimaastossa. (IBM Redbooks 2005, 8.)

Kuten jo aikaisemmin mainittiin, erilaisia teknologioita ja menetelmiä, joita hyödynneetään varmuuskopioinnissa on paljon. Helpoin ja yksinkertaisin on yksinkertaisesti ottaa kopiot tiedostoista päivän päätteeksi vaikkapa muistitikulle, mutta seuraavaksi esittellään muutamia hieman edistyneempiä teknologioita.

2.1 HSM

HSM tulee sanoista Hierarchical Storage Migration. HSM liikuttaa dataa automaattisesti hitaamman ja nopeamman tallennusmedian välillä, HSM siis säilöö dataa hitaammissa medioissa ja kun dataa tarvitaan siirtää sen nopeammalle medialle (esim. SSD). Tämä voi toimia monellakin tapaa, esimerkiksi varmuuskopioitu data, jota ei ole pitkään aikaan käytetty voidaan automaattisesti siirtää säilöön hitaammalle ja halvemmalle medialle. Jos varmuuskopioidaan paljon dataa jota ei juurikaan käytetä, on tämä metodi erittäin tehokas ja säästää aikaa ja rahaa. Tästäkin huolimatta HSM ei juurikaan käytetä, lähinnä sen monimutkaisuuden takia. Tähän myös vaikuttaa se, että HSM integroituu suoraan käyttöjärjestelmään, joka vaikeuttaa tälläisen ratkaisun toteuttamista. (Little yms. 2007, 5-6.)

2.2 RAID

RAID eli redundant array of independent disks on tekniikka, jossa käyttämällä useita levyjä saadaan vikasietoisuutta ja datan saatavuutta nostettua huomattavasti. RAIDin käyttäminen on nykyään erittäin yleistä ja voidaankin olettaa, että sitä käytetään lähes kaikissa yrityksien data centereissä. (Little yms. 2007, 17-18.)

Tätä tekniikkaa voidaan soveltaa erilaisilla tavoilla, ja näitä tapoja on olemassa monia. Näitä kutsutaan RAID-tasoiksi. Tässä kappaleessa esitellään yleisimmät, ja mainitaan myös vähemmän käytetyt:

RAID 0 – Striping eli lomitus
Lomituksessa monta levyä yhdistetään yhdeksi loogiseksi levyksi. Tällöin luku- ja kirjoitusnopeus moninkertaistuu riippuen siitä, kuinka monta levyä on käytössä. Tämä RAID-taso ei tarjoa minkäänlaista vikasietoisuutta, sillä yhden levyn hajotessa kaikki tieto menetetään. RAID 0-tasoa käytetäänkin suoritukyvyn nostamiseen, mutta dataa sillä ei voida turvata. (Little yms. 2007, 24.)

RAID 1 – Mirroring eli peilaus
Peilauksessa kahdelle tai useammalle erilliselle levylle kirjoitetaan sama tieto, jolloin yhden levyn rikkoutuessa tieto säilytetään. RAID 1-taso nostaa datan saatavuutta

huomattavasti lisätallennustilan kustannuksella. Yleensä tämä myös nopeuttaa lukunopeutta. (Little yms. 2007, 19.)

RAID 4

RAID 4-taso toimii käytännössä lähes samalla tavalla, kuin RAID 0, mutta siinä käytetään useampia levyjä, joista yksi on ”parity” levy. RAID 4 lisää lukunopeutta huomattavasti, mutta kirjoitusnopeus kärsii. RAID 4 ei ole yleisessä käytössä. (Little yms. 2007, 19.)

RAID 5

RAID 5-tasossa ”parity” data on jaettu kaikille levyille tasapuolisesti, joka toisin kuin RAID 4-tasossa lisää vikasietoisuutta. Jos yksi levy menetetään, tieto säilytetään. Enemmän kuin yhden levyn menetyksessä menetetään kaikki data. (Little yms. 2007, 19.)

RAID 2

RAID 2-taso ei ole enää käytössä, sillä sen tuoma hyöty on nykyään kovalevyjen perusominaisuus. Tämän ominaisuuden luominen vaatisi siis vain ylimääräistä työtä. RAID 2-taso ei ole relevantti enää. (Vadala 2009, 6.)

RAID 3

Myös RAID 3-tasoa nähdään erittäin harvoin käytössä, sillä se vaatii levyjen synkronoitua pyörimistä, eikä tarjoa mitään merkittävää hyötyä muihin tasoihin verrattuna. (Vadala 2009, 6.)

RAID 10

RAID 10-tasossa käytetään RAID 1 ja RAID 0 tekniikoita yhdessä. RAID 10 voi olla joko RAID 0 + 1, jossa levyt aluksi lomitetaan ja sen jälkeen peilataan, tai RAID 1 + 0, jossa levyt aluksi peilataan ja sen jälkeen lomitetaan eri laitteille. (Little yms. 2007, 20.)

RAID 50

RAID 50-taso käyttää RAID 5 ja RAID 0 tekniikoita. Tämä tapahtuu niin, että RAID 5 ryhmät lomitetaan samalla tavalla kuin levyt RAID 0 tekniikalla. (Little yms. 2007, 20-21.)

Kuten sanottu, kaikki muut paitsi RAID 0-taso lisäävät vikasietoisuutta ja datan saatavuutta huomattavasti. RAID 0-taso taas puolestaan lisää luku- ja kirjoitusnopeutta. (Little yms. 2007, 21.)

2.3 Bare metal restore

Bare metal restorella tarkoitetaan systeemin varmuuskopiointia järjestelmälle, jossa ei ole käyttöjärjestelmää vielä laisinkaan. Bare metal restoren avulla voidaan siis kopioida koko käyttöjärjestelmä itsessään uudelle laitteelle, jos vanhalle tapahtuu jotain. Tämä ei yleensä onnistu normaalin varmuuskopioinnin avulla, jossa tavoitteena on säilyttää tietty data, ei koko käyttöjärjestelmää. BMR on siis erittäin tärkeä teknologia, jos pelkän yksittäisen datan varmuuskopiointi ei riitä. Bare metal restoressakin toki on omat ongelmansa; laitteiston, johon järjestelmä halutaan palauttaa, pitäisi olla täysin sama kuin järjestelmän, joka halutaan palauttaa. Jos tämä ei toteudu palauttaminen saattaa olla hankalaa eikä suju ilman virheitä. (Little yms. 2007, 41-43.)

2.4 Synteettinen varmuuskopio

Synteettisellä varmuuskopiolla tarkoitetaan varmuuskopiota, joka muistuttaa täyttä varmuuskopiointia, mutta se on tehty yhdistämällä inkrementaalisia varmuuskopioita. Tämän teknologian avulla ei periaatteessa tarvitse tehdä täyttä varmuuskopiointia koskaan ensimmäisen kerran jälkeen; sen sijasta voidaan tehdä syntettinen varmuuskopio kaikista inkrementaaleista varmuuskopioista. Täysi varmuuskopiointi vie niin aikaa kuin kaistaakin ja synteettinen varmuuskopiointi on erittäin hyvä tapa vähentää resursseja, joita täyteen varmuuskopiointiin vaaditaan. Myös onnettomuuden sattuessa voidaan järjestelmä palauttaa yhdestä täydestä, synteettisestä varmuuskopiosta. Normaalisti palauttamisprosessiin kuuluisi täyden varmuuskopion palauttaminen, ja sen jälkeen inkrementaalisten varmuuskopioiden palauttaminen. Synteettisen varmuuskopion luominen tapahtuu täysin varmuuskopioitavan järjestelmän ulkopuolella, jolloin sen luominen onnistuu, vaikka varmuskopioitava järjestelmä ei olisikaan saatavilla. (Little yms. 2007, 104-107.)

2.5 Enkryptaus

Enkryptaus on tiedon salaamista, eli sen lukemisen vaikeuttamista erilaisin keinoin. Tämä liittyy varmuuskopiointiin siinä mielessä, että esimerkiksi off site- sijainnissa oleva tieto saatetaan haluta kryptata, jos sen katsotaan olevan tarpeeksi tärkeää. Nykypäivänä enkryptaus on melko yleistä. Enkryptaus voi tapahtua joko asiakkaan puolella, jolloin tieto kryptataan ennen lähettämistä, tai sitten se voi tapahtua itse säilömismedialla lähetyksen jälkeen. (Little yms. 2007, 90-94.)

Enkryptaukseen tarvitaan kaksi asiaa: algoritmi ja siihen tarvittava avain. Enkryptaus tapahtuu altistamalla alkuperäinen tieto algoritmille, joka enkryptaa sen jollain avaimella. Tällä avaimella tieto saadaan alkuperäiseen kuntoonsa suorittamalla tiedolle tehty operaatio päinvastoin. Kirjassa Digital Data Integrity on tästä hyvä esimerkki: Otetaan sana ”Hello” ja otetaan jokaisen kirjaimen ASCII arvo: 72, 101, 108, 108 ja 111. Sitten lisätään näihin arvoihin luku 7, nyt sana muuttui sanaksi ”Olssv”. Tässä tapauksessa avain on siis luku 7. Poistamalla tämä luku uusista ASCII arvoista (79, 108, 115, 115 ja 118) saadaan alkuperäinen ”Hello”. (Little yms. 2007, 90-94.) Tämä on erittäin hyvä ja yksinkertainen esimerkki enkryptauksesta. Oikea enkryptaus ei tietenkään ole näin yksinkertaista ja siihen liittyy paljon ylimääräisiä prosesseja, mutta periaate on siinä täysin sama.

Enkryptaus ei ole tietenkään täysin ongelmantonta. Suurin ongelma enkryptauksessa liittyy juurikin edellä mainittuihin avaimiin; ne ovat elintärkeitä, jos tieto halutaan saada takaisin luettavaan kuntooon. Niiden oikeanlainen hallinta on siis erittäin tärkeää. Kun enkryptaus kasvaa monimutkaisemmaksi, saatetaan alkaa käyttämään esimerkiksi monesta osasta koostuvaa avainta, tämän avaimen komponentit eivät välttämättä sijaitse samassa paikassa, joka mahdollistaa sen, että yksi henkilö ei pysty lukemaan enkrytattua tietoa, vaan siihen vaaditaan kaikkien komponentti. Tämänkaltainen käytäntö toki tietenkin lisää riskiä, että yhtä komponenteista ei syystä tai toisesta saada toimintaan ja tietoa ei voida kääntää laisinkaan. (Little yms. 2007, 90-94.)

3 PARHAAT KÄYTÄNNÖT VARMUUSKOPIOINNISSA

Tässä osiossa kootaan yhteen mielestäni tärkeimpiä asioita varmuuskopioinnin suunnittelussa ja toteutuksessa. Nämä tiivistetäänn 5 asiaan.

3.1 Järkevä intervalli varmuuskopioinnissa

Tämä tarkoittaa sitä, kuinka usein tiedostot varmuuskopioidaan. Voisi luulla, että tähän pätisi mitä useammin sen parempi, mutta asia ei ole ihan näin yksinkertainen, sillä turha varmuuskopiointi on vain turhaa liikennettä, joka syö siirtokaistaa. Intervalliin vaikuttaa montakin asiaa, esimerkiksi kuinka usein data itsessään muuttuu ja miten tärkeätä se on. Esimerkiksi dataa joka säilyy kohtuullisen muuttumattomana pitkiäkin aikoja ei ole järkevää varmuuskopioida 12 tunnin välein. Kun taas tärkeälle datalle joka muuttuu useasti päivän aikana tämä saattaa olla varsin hyvä ratkaisu.

3.2 Varmuuskopioiden lokaatio

Tämä saattaa kuulostaa itsestäänselvyydeltä, mutta omasta kokemuksestanikin voin sanoa, että kaikille se ei sitä ole. Hyvinä varoittavina esimerkkeinä tästä on vaikkapa työntekijän henkilökohtaiselle muistitikulle varmuuskopiointi päivän päätteeksi. Tälläinen menettely pahimmassa tapauksessa tekee koko prosessin täysin turhaksi, jos data katoaa syystä tai toisesta. Yksinkertaisemmillaan tämä tarkoittaa että varmuuskopiointi lokaation pitäisi olla turvallinen paikka, josta tiedot eivät helposti häviäisi. Tämä paikka ei myöskään luonnollisesti saisi olla fyysisesti sama josta tiedot varmuuskopioidaan (esimerkiksi varmuuskopiointi virtuaalikoneelta pohjakoneelle).

3.3 varmuuskopioinnin testaus

Sait juuri viimeiseen koneeseen asennettua varmuuskopiointiohjelman ja yhteys näyttää toimivan, tämä oli siis tässä? Väärin, varmuuskopiointi kannattaa aina testata mahdollisimman tarkasti. Jos olosuhteet sen sallivat, kannattaa vaikka tehdä

varmuuskopiointi pienehköllä tiedostomäärällä selvittääksesi toimiiko yhteys oikeasti. Tämäkin saattaa kuulostaa itsestäänselvyydeltä, mutta on se silti mainitsemisen arvoista.

3.4 Tärkeimipien tietojen hahmottaminen

Ota selville, mitkä tiedostot ovat tärkeimpiä varmuuskopiointia varten. Vaikka tarkoitus olisikin varmuuskopioida koko järjestelmä, osa tiedostoista todennäköisesti ovat tärkeämpiä, kuin toiset. Täten voidaan säätää varmuuskopiointi järkevämmäksi, esimerkiksi varmuuskopioimalla nämä tärkeät tiedostot useimmin kuin toiset tiedostot, sen sijaan että varmuuskopioisit kaikki kerralla. Tämä kaikki tietenkin on täysin tapauskohtaista, ja voikin olla, että on järkevää varmuuskopioida kaikki tiedot kerrallaan.

3.5 Täysien ja inkrementaalisten varmuuskopioiden balanssi

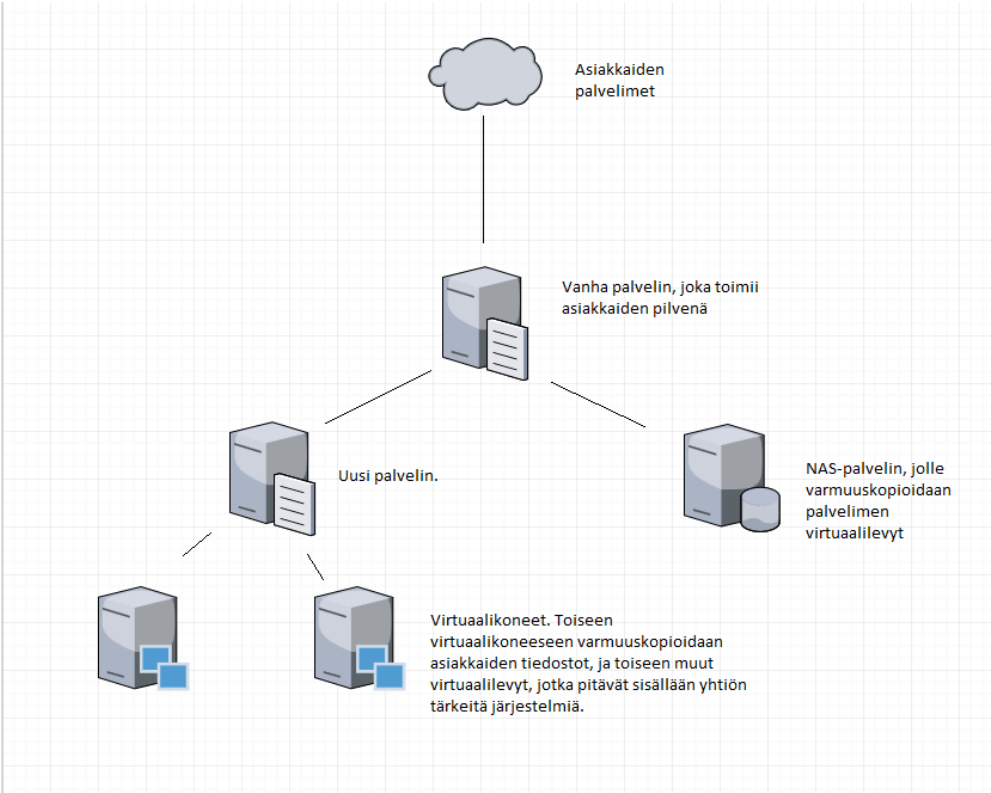
Hahmota, kuinka usein on järkevää ottaa täysiä varmuuskopioita, ja kuinka usein inkrementaalisia. Täydet varmuuskopiot vaativat enemmän aikaa ja resursseja, kuin inkrementaaliset, tästä syystä täysiä varmuuskopioita usein otetaan harvemmin ja inkrementaalisen varmuuskopioiden otto onkin jokapäiväistä. Tämänkin määrittää ympäristö ja monet muuttujat. Inkrementaalisten ja täysien varmuuskopioiden lisäksi voidaan myös ottaa jo aikaisemmin mainitsemiani differentaalisia varmuuskopioits. Näidenkin ottoa kannattaa harkita ja miettiä, sopivatko ne suunnitelmaasi.

4 OMA TOTEUTUKSENI

4.1 Ympäristön infrastruktuuri

Yhtiön infrastruktuuri ei ole suuri tai monimutkainen. Mitä varmuuskopiointiin tulee, yhtiöllä on yksi palvelin, jossa on virtuaalikoneet johon asiakkaiden varmuuskopiot tulevat. Näiltä samoilta virtuaalikoneilta löytyy myös kaikki yhtiön tärkeät tiedot ja systeemit. Kutsutaan tätä palvelinta vanhaksi palvelimeksi. Työn aikana käyttöön saatiin myös toinen palvelin, jota käytetään nimenomaan vain ja ainoastaan varmuuskopioiden tallennustilana. Kutsutaan tätä uudeksi palvelimeksi. Ongelmaksi tässä muodostui se, että uudella palvelimella on vähän tilaa, joten asikkaiden varmuuskopioita sinne ei työn tekohetkellä saatu, mutta vanhan palvelimen virtuaalilevyt sinne saatiin varmuuskopioitua.

Yhtiön infrastrukturiin kuuluu siis 2 palvelinta ja yksi NAS-palvelin. Kuvassa 1 on yksinkertaistettu kuva ympäristöstä. Alunperin vanhaan palvelimeen menivät asikkaiden varmuuskopiot suoraan pohjakoneelle, mutta tämä muodostui ongelmalliseksi, sillä yhtiöllä ilmeni tarvetta uudelleenkäynnistää kyseistä palvelinta,



KUVA 1. Yksinkertaistettu kuva työn kannalta keskeisistä palvelimista

jossa asiakkaiden tiedot olivat, jolloin tietenkin kaikki palvelimella sijaitsevat virtuaalikoneetkin uudelleenkäynnistyisivät. Varmuuskopiointi siirrettiin siis vanhalla palvelimella sijaitsevalle virtuaalikoneelle, jolloin pelkästään tämä virtuaalikone voidaan uudelleenkäynnistää pohjakoneen sijaan, jos tarvetta tälle ilmenee. Muut koneella olevat virtuaalikoneet pitävät sisällään tärkeitä yhtiön järjestelmiä.

Ympäristöön kuuluu myös NAS-palvelin, johon vanhan palvelimen virtuaalilevyt varmuuskopioidaan Cobian ohjelmalla. Tämä käytäntö oli käytössä jo ennen työn aloittamista.

4.2 Käyttämäni ohjelmat ja kriteerit

Tärkeimpinä kriteereinä ohjelman valinnassa oli ohjelman maksuttomuus, helppokäyttöisyys, mahdollisuus varmuuskopioida verkon yli (eli palvelimelta palvelimelle) sekä ohjelmiston nopea ja yksinkertainen asennus. Urbackup sopii tähän erittäin hyvin, ja yhtiön palvelimelle oltiin asennettu ohjelman palvelinohjelmisto jo aikaisemmin. Tulevassa kappaleessa esittellään myös muita varmuuskopiointiohjelmia, ja perustellaan, miksi ne eivät soveltuneet työhön.

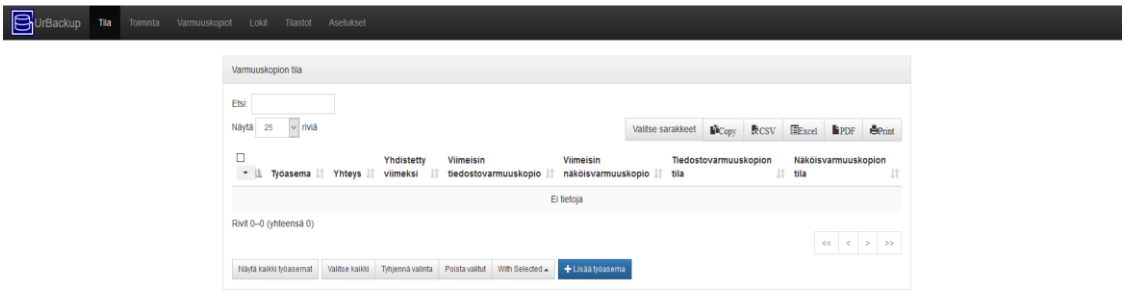
4.2.1 UrBackup

Urbackup on ilmainen open source varmuuskopiointiohjelma. Ohjelmasta on palvelin- ja asiakasohjelma. Tämä ohjelma valittiin sen maksuttomuuden ja helppokäyttöisyyden vuoksi, lisäksi olin saanut kokemusta ohjelman käytöstä jo aikaisemmin, kun käytin sitä toteuttaessani varmuuskopioinnin asiakkaalle ollessani työharjoittelussa. Myös virtuaalikoneelta virtuaalikoneelle varmuuskopiointi on erittäin helppoa ja nopeaa ohjelman toimintavasta johtuen. Ohjelman palvelinohjelma asennetaan palvelimelle, johon tiedostot halutaan varmuuskopioida, ja asiakasohjelmat asennetaan koneille, joiden tiedostot halutaan varmuuskopioida. Palvelinohjelman käyttöliittymään pääsee käsiksi selaimen kautta, käyttämällä ohjelman oletusporttia 55414 kirjoittamalla osoiteriville localhost:55414. Kuvassa 2 näkyy palvelinohjelman käyttöliittymä. Asiakasohjelma käyttää normaalia käyttöliittymää, johon selainta ei tarvita. Kuvassa 3 näkyy asiakasohjelman käyttöliittymä. Yksi suuri syy myös tämän ohjelman valintaan

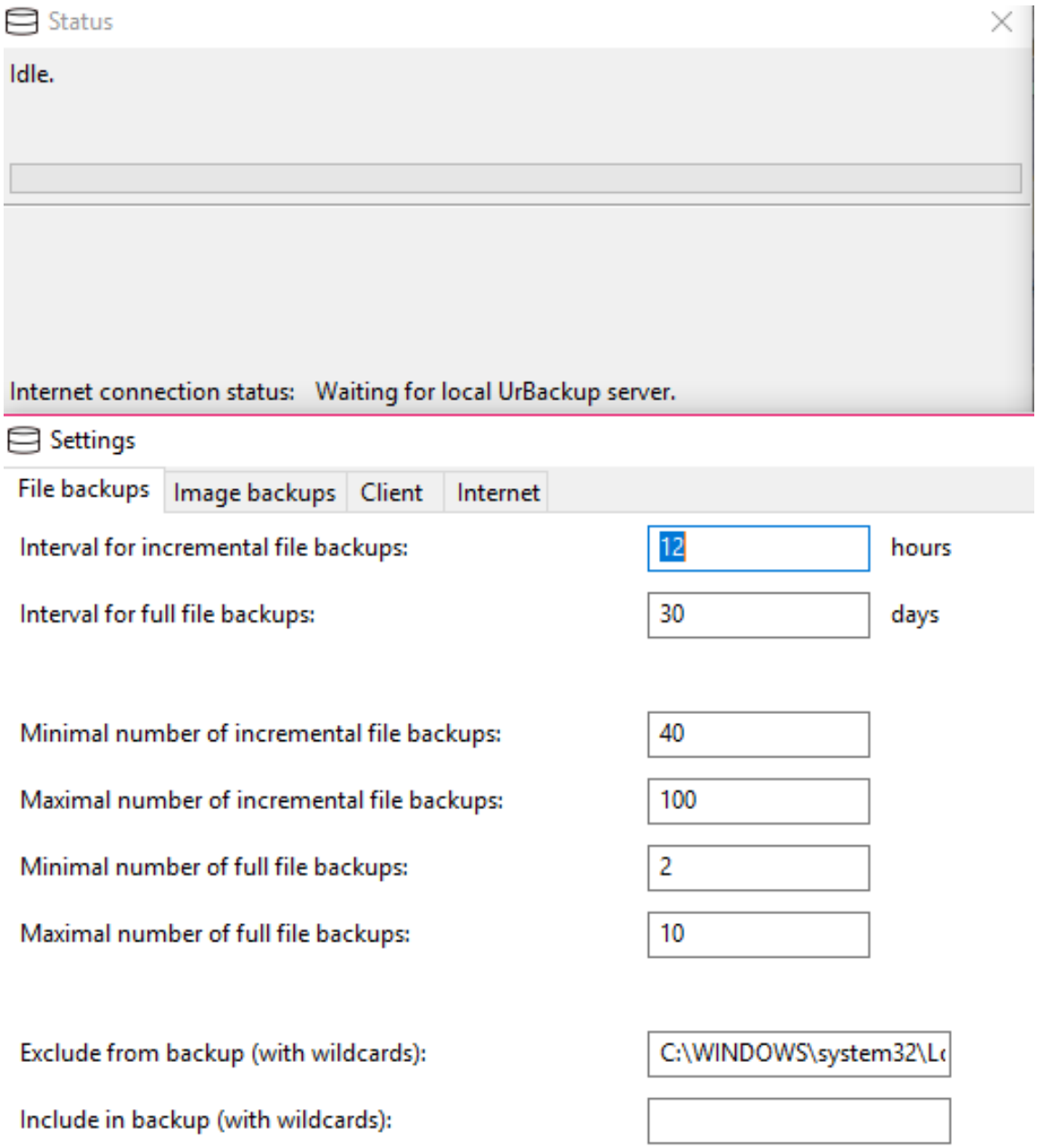
oli se, että sen avulla on erittäin helppo varmuuskopioida verkon yli toisesta lokaatiosta toiseen, joka auttoi kovasti virtuaalikoneelta virtuaalikoneelle varmuuskopiointia. Palvelinohjelman kautta voidaan valita salasanan, jota ohjelma käyttää, ja se tarvitsee ip-osoitteen lisäksi antaa asiakasohjelmistolle, jolloin se ottaa yhteyden verkon kautta palvelinohjelmaan. Erityisen helpoksi tämän tekee se, että palvelinohjelman avulla voidaan lisätä asiakkaita, ennenkuin niitä ollaan edes asennettu, ja ohjelma antaa valmiin asennustiedoston, jossa on kaikki asetukset automaattisesti kunnossa. Tätä asennustiedostoa käyttämällä asiakasohjelma ottaa automaattisen yhteyden palvelinohjelmaan ja aloittaa varmuuskopiointiprosessin. Salasanan saa myös kokonaan pois, jolloin tosin mikä tahansa asiakasohjelms voi ottaa yhteyden palvelimeen, kunhan vain tietää ip-osoitteen.

Ohjelmassa on huonojakin puolia. Hieman ärsyttävää on se, että varmuuskopioinnin tallennuslokaatiota ei voi määritellä erikseen jokaiselle varmuuskopioinnille, vaan palvelinohjelman avulla määritetään paikka, johon kaikki tiedostot varmuuskopioidaan. Ohjelma toki luo erilliset kansiot eri asiakkaille tänne lokaatioon. Tästä syystä tiedostojen kopiointi samalta koneelta eri kohteisiin on hankalaa. Tässä ympäristössä se ei tosin haitannut laisinkaan, vaan ohjelma soveltuukin juuri ympäristöön, jossa virtuaalikoneita on käytössä, sillä sen asennus erikseen eri virtuaalikoneille on yksinkertaista

Kaikki asetukset voidaan konfiguroida valmiiksi palvelinohjelman avulla, jonka jälkeen edellämainitsemani asennustiedosto voidaan ladata eikä se vaadi enää muuta konfigurointia, kuin varmuuskopioitavien tiedostojen määrittelemisen. Samassa sisäverkossa sijaitsevat ohjelmat tosin löytävät toisensa ilman mitään valmiiksi määritettyä asennustiedostoa, joten tämä prosessi on tarkoitettu lähinnä asiakasohjelmille, jotka eivät sijaitse samassa verkossa, jolloin ip-osoite ja salasana pitää määrittää.



KUVA 2. Urbackupin pavelinohjelman käyttöliittymä



KUVA 3. Urbackupin asiakasohjelman käyttöliittymä

4.2.2 Cobian

Cobian on Luis Cobianin kehittämä varmuuskopiointiohjelma. Ohjelma on osittain open source, sillä sen vanhemmat versiot julkaistiin mozilla public licensen alla, mutta uudemmat versiot eivät enää ole avoimia. Ohjelma on ollut yrityksen käytössä pitkään, ja tähän on syynä lähinnä sen maksuttomuus. Itse ohjelma on monimutkaisempi kuin Urbackup mutta sisältää myös paljon enemmän ominaisuuksia. Ohjelman avulla pystyy muun muassa määrittelemään kaikille eri varmuuskopioille erinnäiset tallennuspaikat, määrittelemään inkrementaalisten ja täysien varmuuskopioiden intervallit erikseen, ja määrittämään niiden ajankohdan tarkasti. Tämä eroaa valtavasti UrBacupista, joka vaihtaa tälläisen tarkan säätämisen erittäin yksinkertaiseen ja oikeastaan ylimääräistä konfigurointia vaatimattomaan käyttöön.

Cobian hoitaa virtuaalilevyjen varmuuskopioinnin NAS-palvelimelle. Tämä on vanha järjestely jota en muuttanut, koska ylimääräinen redundanssi ei ole pahasta. Cobiania en käyttänyt tämän enempää, sillä tämän yhtiön tarpeisiin sopii mielestäni paljon paremmin yksinkertaisempi UrBackup, sillä cobianin käyttö on hankalampaa, sekä sen avulla varmuuskopiointi virtuaalikoneelta virtuaalikoneelle ei onnistu niin helposti, johtuen siitä, että cobianilla onnistuu vain verkon sisäinen varmuuskopiointi, jolloin esimerkiksi toisessa verkossa olevalle virtuaalikoneelle varmuuskopionti ei olisi onnistunut.

4.3 Muita varmuuskopiointiohjelmia

Tässä esittellään muita yleisesti hyväksi todettuja varmuuskopiointiohjelmia, joita ei työssä käytetty ja perustellaan, miksi niitä ei käytetty. Tässä ei käydä läpi kaikkia netistä saatavia varmuuskopiointiohjelmia joita vertailtiin, sillä syy sille, miksi jotain ohjelmaa ei valittu oli hyvin usein sama: ohjelma oli hyvin usein trial-versio, josta puuttui ominaisuuksia ja ohjelma jatkuvasti muistutti olevansa sellainen. Tämän lisäksi jotkin ohjelmat vaativat tekemään tilin, jotta ohjelman voi ladata. Tässä nimetään muutama ohjelma, joita ei käytetty näistä syistä:

-EaseUs Backup
-Paragon Backup & Recovery
-FBackup

-HDClone
-Genie Timeline

4.3.1 System Restore

System restore on Windowsin oma työkalu, jolla voidaan luoda snapshot Windows järjestelmästä, jolla järjestelmän palauttaminen onnettomuuden sattuessa on mahdollista. Tämä ei sinänsä ole varmuuskopiointityökalu; sillä ei voida varmuuskopioida mitään muita tietoja, kuin tärkeät windowsin järjestelmä tiedot, joista järjestelmä palautetaan. System restore on kuitenkin tärkeä mainita, sillä sen avulla Windowsin palauttaminen on helppoa ja sen ollessa osa Windowsia sitä käytetään melko usein. (Preston 2009, kappale 3.)

Suurin osa työn palvelimista käyttivät Windowsia, mutta System Restorella ei kuitenkaan voi korvata kunnollista varmuuskopiointoohjelmaa, sillä kyse on vain snapshotin ottamisesta, ja esimerkiksi onnettomuuden sattuessa, täytyy tiedostojen sijaita fyysisesti jossain muualla, jotta niiden palauttaminen on varmaa ja niihin päästään heti käsiksi.

4.3.2 Bacula

Bacula on avoimen lähdekoodin varmuuskopiointiohjelma. Bacula julkaistiin vuonna 2002, 2 vuotta sen ollessa kehityksessä Kern Sibbaldin ja John Walkerin toimesta, joista Walker kylläkin jätti projektin sen alkuvaiheiden jälkeen. Baculaan kuuluu monta komponenttia. Näihin komponentteihin kuuluu Director, joka on koko ohjelman ”ydin”, database server, joka pitää listaa varmuuskopiointilokaatioista, storage daemon, joka hoitaa median kanssa keskustelemisen, administrative console, joka on ohjelman käyttöliittymä, jolla ohjelmaa operoidaan, sekä file daemon, joka hoitaa itse datan siirtämisen varmuuskopiointikohteeseen. (Preston 2009, kappale 6.)

Kuten voidaan päätellä, Baculan käyttö on paljon monimutkaisempaa, kuin esimerkiksi työssä käytetyn UrBackupin. Jokaisella komponentilla (paitsi database serverillä) on oma asetustiedostonsa, joten tämän ohjelman käyttäjän pitää tarkalleen tietää mitä tekee.

Toki näin monikomponenttinen ohjelma myös takaa sen, että osaava henkilö voi kustomoida ohjelman käyttöä paljon enemmän kuin esimerkik UrBackupin tapauksessa ja tämä ohjelma sopiikin paremmin suurempiin ympäristöihin. Tämän ohjelman käyttö on tosin paljon hankalampaa ja asennus paljon työläämpää, kuin Urbackupin.

4.3.3 Amanda

Amanda eli Advanced Maryland Automated Network Disk Archiver on jo vuonna 1991 Marylandin yliopistossa kehitetty vapaan lähdekoodin varmuuskopiointi ohjelma. Amandaa on kehitetty ja testattu vuosien varrella erittäin paljon, jonka vuoksi sitä pidetään erittäin vakaana ja toimivana ohjelmana. Amanda käyttää yhtä varmuuskopiopalvelinta. Ohjelma toimii niin Linuxin, Unixin, Mac OS X:n ja Windowsin kanssa. Amanda on yleisessä käytössä suurissa ympäristöissä ympäri maailman juurikin äsken mainitun luotettavuuden takia. (Preston 2009, kappale 4.)

Amanda olisi voinut olla käypä ratkaisu tässä pienemmässäkin ympäristössä, tosin sen asennus olisi ollut hieman työläämpää kuin UrBackupin.

4.3.4 Personal Backup

Personal backup on Jürgen Rathlevin kehittämä varmuuskopiointiohjelma. Ohjelman käyttöliittymä on melkoisen sekavan näköinen, eikä se monista ominaisuuksistaan huolimatta sopinut tähän työhön. Ohjelman käyttö ei ollut aivan yksinkertaista ja ei ollutkaan mitään syytä käyttää sitä erittäin yksinkertaisen UrBackupin sijasta. Myöskään eri lokaatiossa sijatsevalle virtuaalikoneelle varmuuskopiointi ei olisi sujunut kovin vaivattomasti, sillä ohjelma soveltui paremmin saman palvelimen sisällä tapahtuvaan varmuuskopiointiin.

4.4 Yleistä varmuuskopiointiohjelmista

Tässä käsitellään asioita, jotka ovat mielestäni tärkeitä ja joita kannattaa harkita ja miettiä valitessaan varmuuskopiointiohjelmaa.

4.4.1 Yhteensopivuus

Yhteensopivuus on ohjelmaa valitessa lähtökohtana, sillä luonnollisesti ohjelman pitää toimia käytössä oleven järjestelmien kanssa, tai se on täysin turha. Ympäristössä voi olla esimerkiksi käytössä Linux ja Windows laitteistoa, jolloin ohjelman pitää olla yhteensopiva molempien käyttöjärjestelmien kanssa.

4.4.2 Helppokäyttöisyys

Tämä kohta ei ole niin yksiselitteinen, kuin yhteensopivuus. Vaikka helppokäyttöisyys on tietenkin hyvä asia, saattaa se joskus tarkoittaa sitä, että ohjelma ei ole kykenevä suorittamaan vaikeampia ja monimutkaisempia tehtäviä. Tässä kohdassa kannattaa miettiä, kumpi on ympäristössä tärkeämpää. Toki tämähän ei aina pidä paikkaansa, mutta oman, joskin tosin melko rajoitetun kokemukseni perusteella helppokäyttöisemmät ohjelmat ovat myös yksinkertaisempia, joka luonnollisesti tarkoittaa sitä, että niillä ei monimutkaisempia tehtäviä suoriteta. Urbackup on tästä hyvä esimerkki, vaikkakin työni tapauksessa se soveltui pieneen ympäristöön loistavasti, ja se kykeni kaikkeen mihin sitä tarvittiin. Saattaa tietenkin myös olla, että helppokäyttöisyydellä ei ole kaikille käyttäjille mitään väliä, mutta yleisesti ottaen asiat sujuvat helpommin, jos ohjelman kanssa ei tarvitse turhaan tapella.

4.4.3 Ominaisuudet

Eri varmuuskopiointiohjelmat eroavat ominaisuuksiltaan huomattavasti. Kannattaa miettiä, kuinka edistyneitä toimintoja oikeasti tarvitaan, sillä olen huomannut, että usein ominaisuuksiltaan edistyneemmät ohjelmat ovat maksullisia, kun taas yksinkertaisemmat ohjelmat saattavat olla ilmaisia. Palaan tässä taas omaan ratkaisuuni; UrBackup oli ilmainen ja yksinkertainen, mutta se sopi täydellisesti pienehköön ympäristöön. Yksi haittapuoli Urbackupissa oli muun muassa se, että sillä on melko

hankalaa yhdistää monta palvelinta yhteen asiakaskoneeseen, tarkoittaen siis sitä, että jos halutaan varmuuskopioida samalta koneelta enemmälle kuin yhdelle palvelimelle, se ei onnistu mitenkään. Palvelin luo valmiiksi konfiguroidun asiakasohjelmatiedoston, joka automaattisesti yhdistää palvelimeen, kun se on asennettu. Tähän palvelimeen lähtevät kaikki tiedostot, jotka valitaan varmuuskopioitavaksi, enkä löytänytkään pitkistä selvittelyistä huolimatta mitään keinoa varmuuskopioida joitain tiedostoja eri palvelimelle, kuin toisia. Tämä ei kuitenkaan ollut juuri tässä ympäristössä mikään miinus. Tämä on juuri se asia mitä varmuuskopiointiohjelmaa hankkiessaan mielestäni pitää miettiä: mitä ominaisuuksia oikeasti tarvitaan, ja jos niitä ei ole, kuinka suuri haitta siitä syntyy?

4.5 Toteutukseni

Ratkaisu oli tehdä uudelle palvelimelle kaksi virtuaalikonetta, johon toiseen varmuuskopioitiin vanhalla palvelimella olevat virtuaalilevyt, ja toiseen asiakkaiden varmuuskopiot vanhan palvelimen virtuaalikoneelta. Näin asiakkaiden varmuuskopiot löytyvät kahdesta eri paikasta (uudelta palvelimelta ja vanhalta palvelimelta) siltä varalta, että jommalle kummalle palvelimelle tapahtuu jotain. Kummallakin uuden palvelimen virtuaalikoneella on Urbackupin palvelinohjelmisto, johon on valmiiksi määritelty varmuuskopiointilokaatio virtuaalikoneessa. Näiden avulla luotiin asiakasohjelmisto, joista toinen asennettiin vanhan palvelimen pohjakoneelle virtuaalilevyjen varmuuskopiointiin, ja toinen vanhan palvelimen virtuaalikoneelle, josta asiakkaisen tiedot varmuuskopioidaan. Korostettakoon vielä, että Urbackup sopi tähän juurikin loistavasti sen helpon asennuksen ja asiakasohjelmiston automaattisen luonnin takia, muilla ohjelmilla virtuaalikoneilta virtuaalikoneelle varmuuskopiointi olisi hankaloitunut huomattavasti, tai ainakin huomattavasti enemmän aikaa se olisi vienyt ohjelmien asennuksen ja konfiguraation takia.

Yhtiön omia tärkeitä tietoja sisältävien virtuaalikoneiden virtuaalilevyt varmuuskopioitiin myös kahteen paikkaan, sillä ne varmuuskopioitiin myös uudella palvelimella sijaitsevan virtuaalikoneen lisäksi NAS-palvelimelle cobianilla, tämä oli ennestään käytössä ollut käytöntä, jota ei ollut tarpeen muuttaa, sillä enempi redundanssi on aina parempi.

Kuten aikasemmin todettiin, uudella palvelimella ei ollut vielä tarpeeksi muistia, että sinne saataisiin varmuuskopioitua asikkaiden varmuuskopiot, mutta Urbackupin ohjelmisto asennettiin sillä tavalla, että kun tilaa saadaan lisää, niin kaikki asetukset ovat valmiina ja varmuuskopioitavat tiedostot vain lisätään ohjelman listalle. Urbackup asetettiin ottamaan täydet varmuuskopiot 10 päivän välein, ja inkrementaaliset päivittäin, tämä on yhtiön järjestelmäasiantuntijan mukaan yleinen käytäntö, jossa on hyvä tasapaino turvallisuuden ja kaistan käytön välillä, ja hän suositteli tätä siitä syystä.

Ratkaisu oli loppujen lopuksi kovin yksinkertainen, eikä käytä juurikaan mitään edistyneempiä ominaisuuksia. Tärkeintä työssä oli löytää yksinkertainen ja toimiva ratkaisu maksuttomilla ohjelmilla. Tämä ratkaisu tarjosi redundanssia melko paljon, ja oli erittäin riittävä, sillä vanhan palvelimen virtuaalilevyjen varmuuskopiot, ja asiakkaiden varmuuskopiot löytyvät molemmat kahdesta eri fyysisestä paikasta, joten on erittäin epätodennäköistä, että molemmille tapahtuisi jotain. Tämän lisäksi varmuuskopiointi tapahtui virtuaalikoneille, joka tarkoittaa sitä, että pohjakoneeseen ei tarvitse koskea laisinkaan, jos esimerkiksi palvelinohjelmisto tarvitsee sammuttaa jostain syystä. Ympäristö, joka sisältää virtuaalikoneita olisi ollut paljon hankalampaa varmuuskopioida muita ohjelmia kuin Urbackuppia käyttäen, joten valinta oli sopiva. Yhtiön Järjestelmäasiantuntija oli ratkaisuun tyytyväinen ja hyväksyi sen.

5 POHDINTA

Loppujen lopuksi työn toteutus oli melko helppoa, ympäristö oli sen verran yksinkertainen, eikä mitään vaativampaa ratkaisua tarvittu. Tämä oli sinänsä ihan hyvä, sillä ainoa kokemukseni tälläisestä oli työharjoitteluni aikana. Lukiessani materiaalia aiheesta ja tehdessäni työtä tunsin, että sain jonkinlaista kuvaa siitä, minkälaista varmuuskopiointi voi olla suuremmissa ympäristöissä. Tästä minulla ei aikaisemmin ollut juurikaan mitään tietoa, joten työ oli siltä osin aika mielenkiintoinen, että minulla oli erittäin vähän pohjatietoa aiheesta. Tästä huolimatta työ sujui hyvin, joka myös johtui siitä, että sain kohtalaisen vapaat kädet työn tekemisessä, eikä työssä ollut mitään suuria paineita saada ratkaisusta juuri tietynlainen. Vaativampaa oli kaiken teorian kirjoittaminen, sillä varmuuskopiointikirjoista suurin osa keskittyi johonkin tiettyyn ohjelmaan, joten oli haastavaa löytää kirjoja, jotka olisivat puhuneet varmuuskopioinnista yleisesti. Luin kirjoja, ja poimin eri kirjoista osioita, joissa puhuttiin mielestäni tärkeistä aiheista, ja kirjoitin niistä. Tällä tavalla sain mielestäni ihan kelpo paketin informaatiota varmuuskopioinnista yleisellä tasolla, menemättä sen syvemmälle asioihin, joita minäkään en olisi itse ymmärtänyt.

Itse totetutustahan voi aina parantaa, mutta nykyinen toimii moitteettomasti ja tarkoituksenmukaisesti. Itse koin, että työ oli lähinnä tilaisuus minulle kokeilla ja kehittyä, eikä se toki ole mikään lopullinen ratkaisu. Käteen tästä työstä jäi tietoa varmuuskopioinnista, jota minulla ei ollut ennen tämän työn aloittamista laisinkaan. Itse totetukseni varmasti tuntuu hieman yksinkertaiselta kaiken kirjoittamani jälkeen, mutta vaatimuksena oli, että ratkaisu pitää olla maksuton, eikä yhtiöllä ollut suunnittelmissa investoida rahaa tähän, joka olisi ollut mielestäni hölmöä muutenkin, kun varmuuskopioinnin pystyi hoitamaan ihan hyvin maksuttomastikin ja useissa tapauksissa asiakkaille itselleen oltiin myös asennettu lokaali palvelin, johon varmuuskopiot myös menivät itse paikan päällä. Asiakkaiden tietojen katoaminen olisi erittäin valitettavaa, mutta edellä mainituista syistä se on erittäin epätodennäköistä.

LÄHTEET

Preston, W. 2009. Backup and Recovery. Sebastopol: O'Reilly Media

IBM Redbooks. 2005. Content Manager OnDemand Backup/Recovery and High Availability. New York: I B M

Little, D., Farmer, S., El-Hilali, O. 2007. Digital Data Integrity. The Evolution From Passive Protection To Active Management. Chichester: Wiley

Vadala D. 2009. Managing RAID on Linux. Sebastopol: O'Reilly Media

TechTarget. What you need to know about bare metal recovery. Luettu 21.6.2017. http://searchdisasterrecovery.techtarget.com/podcast/What-you-need-to-know-about-bare-metal-restore-and-bare-metal-recovery

TechTarget. Full, incremental or differential: How to choose the correct backup type. Luettu 27.6.2017. http://searchdatabackup.techtarget.com/feature/Full-incremental-or-differential-How-to-choose-the-correct-backup-type

ISACA. 2012. Databse Backup and Recovery Best Practises. Luettu 19.6.2017. https://www.isaca.org/Journal/archives/2012/Volume-1/Pages/Database-Backup-and-Recovery-Best-Practices.aspx

TechTarget. Backup best practices: Easy fixes for your enterprise backup system. Luettu 12.6.2017. http://searchdatabackup.techtarget.com/feature/Backup-best-practices-Easy-fixes-for-your-enterprise-backup-system

TechTarget. RAID levels and benefits explained. Luettu 25.5.2017. http://searchstorage.techtarget.com/answer/RAID-types-and-benefits-explained

https://www.urbackup.org/documentation.html