Virtualisoidun palvelinympäristön varmuuskopiointiratkaisun modernisointi

Anders Eronen

Opinnäytetyö

Informaatiotekniikka

2015

EXAMENSARBETE	
Yrkeshögskolan Arcada	
Utbildningsprogram:	Informations- och medieteknik
Identifikationsnummer:	4818
Författare:	Anders Eronen
Arbetets namn:	Modernisering av en säkerhetskopieringslösning i en virtualiserad servermiljö
Handledare (Arcada):	Göran Pulkkis
Uppdragsgivare:	Kiinko

Sammandrag:

Detta examensarbete baserar sig på moderniseringen av säkerhetskopieringssystemet för Kiinkos (sammansatt namn för Kiinteistöalan Koulutuskeskus Oy och Kiinteistöalan Koulutussäätiö) virtualiserade servermiljö. Arbetets teoretiska del behandlar säkerhetskopieringens teknik. Den teknik som beskrivs fungerar som grund för de val och beslut som görs i själva moderniseringsprojektet. Moderniseringsprojektet påbörjades genom att kartlägga uppdragsgivarens nuvarande säkerhetskopieringssystem. De styrkor och brister som identifierades kunde sedan utnyttjas i valet av komponenterna för det nya systemet. Moderniseringen gällde inte bara de tekniska komponenterna av systemet utan även processer, praxis och säkerhetskopieringsstrategin. Fastän projektets huvudsakliga mål var att skapa säkerhetskopior som ligger utanför fastigheten resulterade det i att så gott som alla komponenter förnyades. Uppdragsgivarens tidigare säkerhetskopieringsprogramvara ersattes med en annan, säkerhetskopieringsstrategin förenklades, lagringssystemen ersattes med nyare apparatur och lagringsmedia samt ett molnbaserat system för transportering och lagring av säkerhetskopior utanför fastigheten togs i bruk. Det nya systemets programvara installerades och konfigurerades tillsammans med leverantörens konsult. Systemet vidareutvecklades sedan med finjustering av konfigurationen samt med förnyande av hårdvara. Systemets uppbyggnad kunde ytterligare utvecklas genom att virtualisera även servern för säkerhetskopieringsprogramvaran vilket skulle möjliggöra en mer flexibel återhämtningsprocess.

Nyckelord:	Kiinko, Virtualisering, Säkerhetskopiering, Veeam, Hyper-V, Backup Exec
Sidantal:	50
Språk:	Finska
Datum för godkännande:	1.4.2015

DEGREE THESIS	
Arcada University of Applied Sciences	
Degree Programme:	Information and Media Technology
Identification number:	4818
Author:	Anders Eronen
Title:	Modernization of a Backup System Solution in a Virtualized Server Environment
Supervisor (Arcada):	Göran Pulkkis
Commissioned by:	Kiinko

Abstract:
This thesis is based on the modernization of the data backup system for Kiinkos (common name for Kiinteistöalan Koulutuskeskus Oy and Kiinteistöalan Koulutussäätiö) virtualized server environment. The theoretical part of the thesis describes the technology of data backup systems. The topics examined therein act as a foundation for the choices and decisions made in the actual modernization project. The modernization project began by examining the current data backup system. Its shortcomings and strengths were then used to define the requirements for choosing the components for the new system. The modernization project covered all parts of the system, including the backup process and practices, the backup strategy and the technical components. Even though the main goal of the project was to create offsite backup copies, all components were replaced. The main backup software was replaced, a simplified backup strategy was introduced, existing storage solutions were replaced with more modern devices and storage medias, and a cloud based offsite backup was implemented. The installation and initial configuration of the software was done in cooperation with a consultant from the service provider. The system was then further developed with minor configuration tweaks and with replacement of hardware components. The system could be developed even further by virtualizing the server hosting the backup software. This would result in a more flexible disaster recovery process.

Keywords:	Kiinko, Virtualization, Backup, Veeam, Hyper-V, Backup Exec
Number of pages:	50
Language:	Finnish
Date of acceptance:	1.4.2015

OPINNÄYTETYÖ	
Ammattikorkeakoulu Arcada	
Koulutusohjelma:	Informaatio- ja mediatekniikka
Tunnistenumero:	4818
Tekijä:	Anders Eronen
Työn nimi:	Virtualisoidun palvelinympäristön varmuuskopiointiratkaisun modernisointi
Työn ohjaaja (Arcada):	Göran Pulkkis
Toimeksiantaja:	Kiinko

Tiivistelmä:
Tämä opinnäytetyö perustuu Kiinkon (yhteisnimi Kiinteistöalan Koulutuskeskus Oy:lle ja Kiinteistöalan Koulutussäätiölle) virtualisoidun palvelinympäristön varmuuskopiointijärjestelmän modernisoimiseen. Työn kirjallisiin lähteisiin perustuva teoriaosa käsittelee varmuuskopioinnin tekniikkaa ja siinä käsiteltävät asiat toimivat perustana valinta- ja käyttöönottoprojektissa tehdyissä päätöksissä. Varsinainen uudistamisprojekti aloitettiin kartoittamalla toimeksiantajan nykyinen varmuuskopiointiratkaisu. Kartoituksessa esiintyneitä epäkohtia ja vahvuuksia hyödynnettiin sitten uuden järjestelmän komponentteja valittaessa. Työ ei koskenut vain järjestelmän teknisiä komponentteja vaan myös varmuuskopiointiin liittyviä käytäntöjä ja prosesseja sekä varmuuskopiointistrategiaa. Vaikka uudistustyön ensisijaiseksi tavoitteeksi muodostui toimeksiantajan kiinteistön ulkopuolella sijaitsevien varmuuskopioiden luominen, päädyttiin projektissa lähes kaikkien komponenttien uudistamiseen. Toimeksiantajan olemassa ollut varmuuskopiointiohjelmisto korvattiin toisella ohjelmistolla, varmuuskopiointistrategiaa yksinkertaistettiin, tallennusratkaisut korvattiin uudemmilla mutta vastaavilla laitteilla ja tallennusmedioilla sekä käyttöön otettiin pilvipalveluun perustuva järjestelmä varmuuskopioiden siirtämiseen ja taltioimiseen kiinteistön ulkopuolelle. Uuden järjestelmän perusohjelmistojen asennus ja käyttöönotto suoritettiin yhteistyössä palveluntarjoajan konsultin kanssa. Varsinaisen käyttöönottoprojektin jälkeen järjestelmää kehitettiin edelleen laiteuusintojen sekä asetusten hienosäätöjen muodossa. Järjestelmän rakennetta on mahdollista kehittää edelleen virtualisoimalla myös varmuuskopiointiohjelmiston palvelin joustavamman palautusprosessin mahdollistamiseksi.

Avainsanat:	Kiinko, Virtualisointi, Varmuuskopiointi, Veeam, Hyper-V, Backup Exec
Sivumäärä:	50
Kieli:	Suomi
Hyväksymispäivämäärä:	1.4.2015

INNEHÅLL / CONTENTS

Kuvat

LYHENTEET

CRM Customer Relationship Management

DC Domain Controller

iSCSI Internet Small Computer System Interface

LTO Linear Tape Open

NAS Network Attached Storage

RAID Redundant Array of Inexpensive/Independent Disks

SAN Storage Area Network

SFTP SSH File Transfer Protocol

SSD Solid State Drive

SSH Secure Shell

USB Universal Serial Bus

VPN Virtual Private Network

1 JOHDANTO

Tallennustilan halventuessa myös säilytettävän tiedon määrä on kasvanut yrityksissä räjähdysmäisesti. Tämä on tuonut uusia haasteita niin infrastruktuurille kuin itse tietohallinnollekin. Suuren tietomäärän säilyttäminen merkitsee myös suuren tietomäärän menettämisen mahdollisuutta, varmuuskopioinnilla pyritään minimoimaan tämä riski.

Tämä opinnäytetyö keskittyy toimeksiantajan varmuuskopiointijärjestelmän päivittämiseen vastaamaan nykyajan tarpeita ja vaatimuksia.

1.1 Tavoite

Tavoitteena on modernisoida toimeksiantajan nykyinen varmuuskopiointiratkaisu. Varmuuskopiointiratkaisu käsittää käytössä olevan ohjelmiston, tallennusratkaisut sekä itse varmuuskopiointistrategian ja siihen liittyvät käytännöt ja menettelytavat.

Ratkaisun kaikkia osia ei välttämättä korvata, vaan käytössä olevia komponentteja pyritään hyödyntämään mikäli mahdollista. Käytössä olevien komponenttien kunto, suorituskyky, luotettavuus sekä yhteensopivuus uusien komponenttien kanssa tulee kuitenkin huomioida.

Tarkoituksena on vertailla eri toimittajien tarjoamia tuotteita ja ratkaisuja sekä huolehtia valitun ratkaisun onnistuneesta käyttöönotosta ja konfiguroinnista toimeksiantajan tarpeiden mukaiseksi.

1.2 Menetelmät

Työn teoreettinen osa perustuu kirjallisuuteen ja muista, pääosin elektronisista, lähteistä hankittuun tietoon. Tuotteiden ja palveluiden ominaisuudet ja kuvaukset saadaan suoraan valmistajien ja palveluntarjoajien tarjoamasta materiaalista.

Osittain työ perustuu myös kommunikaatioon palveluntarjoajien ja tuotteiden toimittajien ja heidän konsulttien kanssa. Useimmat yritykset tarjoavat räätälöityjä ratkaisuja joten kommunikaatio on tärkeä osa hankintaprosessia.

1.3 Toimeksiantajan esittely

Toimeksiantajana on Kiinko, joka on yhteisnimi Kiinteistöalan Koulutuskeskus Oy:lle ja Kiinteistöalan Koulutussäätiölle. Kiinteistöalan koulutussäätiö on virallinen valtakunnallinen erityisoppilaitos. Kiinko tarjoaa lisä- ja täydennyskoulutusta, ammattitutkintoja kiinteistöalan ammateissa toimiville ja alalle hakeutuville henkilöille, sekä osaamisen kehittämiseen liittyviä konsultointipalveluja, tilavuokraus ja henkilöstönvalintapalveluja. Kiinteistöalan Koulutuskeskus Oy on perustettu 1978 ja Kiinteistöalan Koulutussäätiö on perustettu 1989.

1.3.1 Palvelin- ja verkkoympäristön kuvaus

Toimeksiantajalla on kaksi toimipistettä, joista ensimmäinen sijaitsee Helsingin Malmissa ja toinen Helsingin ydinkeskustassa Annankadulla. Toimipisteet on yhdistetty toisiinsa VPN-sillalla. Palvelinhuone sijaitsee Malmin toimipisteen tiloissa, jossa myös valtaosa työasemista sijaitsee.

Toimeksiantajan palvelinympäristö on virtualisoitu kolmelle Microsoft Windows Server 2008R2 Hyper-V alustapalvelimelle joitakin poikkeuksia lukuun ottamatta. Kaikki virtualisoidut palvelimet ovat myös ”Windows Server 2008R2”–pohjaisia.

Käytännössä kaikki toimeksiantajan tuotantokäytössä olevat palvelimet ovat virtualisoituja. Toimeksiantajalla on näiden lisäksi tuotantokäytöstä poistettuja palvelimia sisäiseen käyttöön. Näillä palvelimilla ei sijaitse tuotantokriittistä dataa ja niiden varmuuskopiointi ei sisälly toteutettavaan ratkaisuun. Toimeksiantajalla on lisäksi kaksi ulkoistettua virtuaalipalvelinta joiden varmistuksesta palveluntarjoaja vastaa.

2 VARMUUSKOPIOINNIN TEKNIIKKA

Varmuuskopiointi tarkoittaa tiedon kopioimista yhteen tai useampaan paikkaan. Varmuuskopiot tallennetaan tavallisesti eri tallennusmedialle kuin missä alkuperäistieto sijaitsee. Varmuuskopioinnilla halutaan saavuttaa tietty turvallisuustaso, esimerkiksi alkuperäisen tallennusmedian tuhoutuminen tai vaurioituminen ei saa aiheuttaa tietojen menetystä. Riittävän turvallisuustason saavuttamiseksi on tiedon aina oltava tallennettuna vähintään kahdessa eri paikassa. (Bosworth et. al. 2014 s. 1628)

Varmuuskopiot toimivat usein myös arkistona jolloin riittävän usein tehdyt varmuuskopiot toimivat eräänlaisena versionhallintana. Tämä tarkoittaa että esimerkiksi jossain vaiheessa vaurioituneen tiedoston aikaisempi sisältö on palautettavissa vaikka tiedoston päälle olisi myöhemmin tallennettu uutta tietoa, tai jos uusi samanniminen tiedosto on luotu alkuperäiseen tallennuspaikkaan. Tämä edellyttää tietenkin että varmuuskopiointijärjestelmä tukee tätä toiminnallisuutta.

Varmuuskopiointi ja vikasietoisuus (Backup, Redundancy) ovat termejä jotka joskus sekoitetaan keskenään. On kuitenkin erittäin tärkeää huomioida että nämä kaksi termiä eivät ole synonyymejä. Esimerkiksi RAID-tekniikka suojaa oikeinkonfiguroituna tietoja tehokkaasti levyrikoilta, mutta tiedostojen vahingossa poistamiselta tai ohjelmistovirheen aiheuttamalta tiedoston korruptoitumiselta se ei suojaa mitenkään. Varmuuskopiot tulee kuitenkin tallentaa mahdollisimman vikasietoisille tallennusmedioille, joten termit liittyvät etäisesti toisiinsa.

2.1 Varmuuskopioinnin tarkoitus

Varmuuskopioinnilla on siis kaksi tarkoitusta:

- Tiedon palauttaminen menetyksen jälkeen
- Tiedon palauttaminen aikaisemmasta ajankohdasta

Näistä ensimmäinen on varmuuskopioinnin pääasiallinen tarkoitus. (Skeppstedt 2015)

Tiedon totaalinen tai osittainen menetys voi johtua monesta eri asiasta. Tavallisia syitä ovat esimerkiksi laitteiden rikkoutumiset, ohjelmistovirheet ja inhimilliset tekijät (Smith 2003). Myös vakavammat tilanteet kuten tulipalot, vesivahingot sekä luonnonkatastrofit tulee ottaa huomioon. Tietomurroista johtuvista tiedonmenetyksistä palautuminen edellyttää yleensä että käytössä on toimiva, ja päätallennuspaikasta oikeatoimisesti eristetty arkisto. Jos tunkeutuja tai haittaohjelma tuhoaa tai vaurioittaa tiedostoja paikalliselta tallennusmedialta, ja media jolla varmuuskopiot sijaitsevat on suoraan kytketty samaan järjestelmään, on todennäköistä että hän tai se pystyy myös tuhoamaan varmuuskopiot.

Tilanne jossa halutaan palauttaa tiedosto aikaisemmasta ajankohdasta voi syntyä jos esimerkiksi työtiimi tallentaa tietoja samaan dokumenttiin joka sijaitsee verkkolevyllä. Lisätessään tekstiä dokumenttiin jokin henkilö aiheuttaa vahingossa sen että dokumentin aikaisempi sisältö tuhoutuu tai sen rakenne vaurioituu. Koska dokumenttiin lisätään tekstiä loppupäähän, ei hän välttämättä havaitse dokumentin alkupäässä tapahtuvaa muutosta. Täten voi syntyä tilanne jossa dokumentin virheet havaitaan vasta myöhemmin, jos käytössä ei ole minkäänlaista arkistoa varmuuskopioista on näitä tietoja mahdoton palauttaa.

Muita käyttötarkoituksia varmuuskopioinnilla ja arkistoinnilla voivat olla esimerkiksi:

- Lakisääteisten tiedonsäilytysvaatimusten täyttäminen
- Rikosten ratkominen ja epäiltyjen tunnistaminen rikostutkinnassa
- Tilastojen laatiminen
- Yrityksen omaisuuden turvaamiseen liittyvien sisäisten vaatimusten täyttäminen

(Bosworth et al. 2014 s. 1628–1629).

2.2 Varmuuskopiointiohjelmistot

Tyypillisesti varmuuskopiointiin käytettävä järjestelmä muodostuu monesta eri osasta. Yksinkertaisimmillaan se koostuu ohjelmasta tai komentojonosta joka suorittaa tiedos-

tojen kopioimisen sekä tallennusmediasta jolle se tallennetaan. Kopioinnin automatisointi on kuitenkin äärimmäisen tärkeää riittävän luotettavuuden saavuttamiseksi. Yksinkertaisilla palvelimilla tai esimerkiksi kotitietokoneilla voi hyvinkin riittää että yksinkertainen komentojono kopioi tiedostot ulkoiselle tallennusmedialle tai sftp-yhteyden yli toiselle palvelimelle ajastetusti. Useimmat käyttöjärjestelmät tarjoavatkin jonkinlaista varmuuskopiointitoiminnallisuutta ilman erikseen hankittavia ohjelmistoja (Microsoft 2014, Apple Inc. 2014, Red Hat Inc. 2014).

Kun käyttöjärjestelmän omat työkalut eivät enää täytä tavoiteltuja vaatimuksia on yleistä että käytetään erityistä ohjelmistoa joka hoitaa varmuuskopioinnin. Tämä ohjelmisto hoitaa yleensä kaikki varmuuskopiointiin liittyvät tehtävät. Tärkein näistä on tietenkin itse tiedostojen kopioiminen ja arkiston ylläpitäminen, ohjelmistot osaavat usein esimerkiksi hyödyntää magneettinauha-asemia ja ylläpitää magneettinauha-arkistoa. Ohjelmisto osaa ajoittaa varmuuskopioinnin niin että se ajetaan esimerkiksi joka yö, viikko tai kuukausi. Ohjelmisto huolehtii tiedostojen indeksoimisesta, tiedostoihin tehtyjen muutosten tarkkailusta, pakkauksesta sekä varmuuskopioiden salauksesta. Varmuuskopiointiohjelmisto osaa usein myös tarkkailla varmuuskopioinnin kulkua, varoittaa esimerkiksi sähköpostitse alhaisesta levytilasta, epäonnistuneista varmuuskopioinneista tai muista vikatilanteista. (Symantec Corporation 2011)

Ohjelmiston toinen tärkeä tehtävä itse varmuuskopioinnin lisäksi on huolehtia tietojen palauttamisesta. Ohjelmisto toimii siis käyttöliittymänä ja rajapintana varmuuskopioituihin tiedostoihin. Palautettavia tiedostoja voidaan selata ja palauttaa hakukäyttöliittymän avulla. Jotkut ohjelmistot osaavat esimerkiksi hakea yksittäisiä sähköpostiviestejä sähköpostipalvelimen tietokannan varmuuskopiosta (Veeam Software 2014a). Ohjelmistoa valittaessa on siis syytä kiinnittää vähintäänkin yhtä suuri huomio palautusominaisuuksiin kuin itse varmuuskopiointiominaisuuksiin.

Modernit varmuuskopiointiohjelmistot osaavat myös tarkkailla varmuuskopioiden luettavuutta jo kirjoitushetkellä ja tehdä palautustestejä automaattisesti, kunhan tätä toiminnallisuutta ei poisteta käytöstä nopeutta tavoitellessa (Bosworth el al. 2014 s. 1650). Tällöin ohjelmisto osaa ilmoittaa ylläpitäjälle automaattisesti mikäli se havaitsee ongelmia varmuuskopioiden luettavuudessa tai niiden palautuksissa. Joissakin tapauksissa

se myös osaa korjata esimerkiksi kevyesti korruptoituneen varmuuskopion. On kuitenkin huomioitava että varmuuskopiointiohjelmiston tekemät palautustestit eivät ikinä korvaa oikeita palautustestejä, jotka varmuuskopioiden ylläpitäjän tulee suorittaa säännöllisesti toimivuuden varmistamiseksi. Säännöllisistä palautustesteistä on myös hyötyä ohjelmiston käyttäjälle siten että palautusprosessi on valmiiksi muistissa todellisen tilanteen sattuessa. Esimerkiksi ohjelmistoon julkaistut päivitykset voivat muuttaa palautusprosessia tai sen vaiheita, säännöllinen testaus pitää täten käyttäjän ajan tasalla.

2.3 Varmuuskopioiden säilytys

Varmuuskopioiden tallennuspaikka, ja mahdollisten siirrettävien tallennusmedioiden säilytyspaikka on myös tärkeä osa varmuuskopiointijärjestelmää. Eri ohjelmistojen tekemät tilapäiset varmuuskopiotiedostot tallennetaan yleensä samaan paikkaan kuin alkuperäistiedosto, mutta kun puhutaan varsinaisesta tiedon varmistamisesta, halutaan varmuuskopiot kuitenkin yleisesti ottaen tallentaa eri paikkaan (Bosworth et al. 2014 s. 1628). Tallennusmedian fyysinen sijoitus on myös tärkeää, paikalliselle kiintolevylle tallennetuista varmuuskopioista on harvemmin hyötyä tulipalon, varkauden tai vesivahingon sattuessa.

2.3.1 Tallennusmedian sijainti

Fyysisesti erillään olevat, tai irrotettavat tallennusmediat ovat siis suositeltavia paikkoja tallentaa varmuuskopiot. Ideaalitilanteessa varmuuskopiointi on järjestelty niin että kopiot tallennetaan mahdollisimman moneen, toisistaan mahdollisimman erillään olevaan, paikkaan. Yksinkertainen ja varsinkin kotikäytössä suosittu ratkaisu on ulkoiset USB-liitännäiset kiintolevyt.

Koska suurin osa varmuuskopioidun tiedon palautuksista koskee muutoksia jotka ovat vähemmän kuin 14 päivää vanhoja (Buffington 2010 s. 69), on hyvä olla ainakin yksi paikallinen tallennusmedia josta tietoja saadaan palautettua nopeasti ja vaivattomasti. Katastrofitilanteita varten säilytettävät varmuuskopiot eivät välttämättä tarvitse olla yhtä nopeasti saatavilla. Koska paikallinen nopea tallennustila on yleensä kallista verrattuna

hitaampiin medioihin, onkin syytä säilyttää varmuuskopioiden arkisto muualla myös taloudellisista syistä.

Tilat joissa varmuuskopioita säilytetään tulee olla turvallisia ja tarkkaan harkittuja. Tiloihin pääsy tulee olla rajoitettu vain asiaankuuluville henkilöille, esimerkiksi tukeva lukittava kaappi voi olla yksinkertainen ja kustannustehokas ratkaisu. Pelkkä pääsyn rajoittaminen ei kuitenkaan ole riittävä suoja. Tulipaloihin ja vesivahinkoihinkin on varauduttava. Tarjolla onkin monenlaisia säilytyskaappeja paperisten dokumenttien säilyttämiseen, ja nämä soveltuvat usein hyvin myös erilaisten tallennusmedioiden säilyttämiseen. Pitkäaikaisessa säilytyksessä on otettava huomioon myös lämpötila ja kosteusvaihtelut. Jotkut mediat, kuten esimerkiksi magneettinauhat, saattavat myös vaurioitua vahvoista magneettikentistä. (Wallace et al. 2001 s. 330)

Kiinteistön ulkopuolella ja maantieteellisesti erillään sijaitseva varmuuskopioarkisto tarjoaa tiedoille paremman suojan fyysisiä vahinkoja vastaan kuin mikä tahansa paloturvakaappi tai muu vastaava tila. Ulkopuoliset tallennustilat ovat täten tärkeä osa varmuuskopiointijärjestelmää (Wallace et al. 2001 s. 330). Jos yrityksellä on monia toimitiloja voi varmuuskopioita säilyttää toisessa toimitilassa kuin missä alkuperäisdata sijaitsee, olettaen että nämä toimitilat ovat tarpeeksi erillään toisistaan. On myös olemassa yrityksiä jotka tarjoavat säilytyspalveluja tallennusmedioille (Wallace et al. 2001 s. 330). Siirrettäessä varmuuskopioita pois omista tiloista on kuitenkin huomioitava tietoturva. On hyvin tärkeää että varmuuskopioitu tieto salataan ennen kuljettamista, tapahtuipa siirto miten tahansa (Wallace et al. 2001 s. 325). Internetin yli siirrettäessä on helppoa ymmärtää miksi salaus on tärkeää, eikä vastaanottajapäässäkään sijaitseva salaamaton tieto ole turvassa. Myös fyysisillä tallennusmedioilla sijaitseva data saattaa joutua vääriin käsiin siirron aikana.

Varmuuskopioidun tiedon siirtäminen Internetin yli on helppo tapa toimittaa tieto maantieteellisesti eri paikalla sijaitsevaan tallennustilaan, riippuen tietenkin datan määrästä ja käytössä olevan Internet-yhteyden nopeudesta. Pilvipalveluna tarjottavat tallennusratkaisut ovat suosittuja varmuuskopioiden tallennuspaikkoja. On myös kehitetty menetelmiä jotka mahdollistavat vain muuttuneen datan kopioimisen, tällöin tarvitaan kuitenkin aluksi kokonainen kopio johon muuttunut data sitten siirretään. Vaikka pelkäs-

tään muuttuneen datan siirtäminen nopeuttaakin varmuuskopiointiprosessia siirrettäessä Internetin yli, se ei kuitenkaan nopeuta palautusta siinä tilanteessa että tieto tuhoutuu kokonaan alkuperäisessä lähteessä esimerkiksi laitteen rikkoutumisen vuoksi. (Crump 2013)

2.3.2 NAS ja SAN

Kustannustehokkuuden ja helpon eristettävyyden ansioista erilaiset verkkotallennusjärjestelmät ovatkin suosittuja tallennusratkaisuja varmuuskopiointikäytössä. Verkon yli siirtäminen ei vaadi henkilökunnalta toimenpiteitä ja järjestelmä voi olla hyvin automatisoitu. Koska saatavilla on valmiita ratkaisuja jotka on suunniteltu juurikin suurien tietomäärien tallentamiseen, ovat nämä ratkaisut usein vaivattomia käyttää ja tarjoavat monia hyödyllisiä ominaisuuksia varmuuskopiointia varten. Laitteet hyödyntävät yleensä RAID-tekniikkaa, ja ne osaavat usein esimerkiksi tarkkailla kiintolevyjensä kuntoa ja ilmoittaa vikaantuneista levyistä automaattisesti tiedon menetyksen välttämiseksi.

Sekä SAN- että NAS-ratkaisut tarjoavat verkkoon liitettyä tallennustilaa. SAN-ratkaisut ovat perinteisesti olleet enemmän suuryritysten käytössä, ja tarjoavat suuria kapasiteetteja, nopeuksia sekä erinomaista skaalautuvuutta. SAN-ratkaisut liitetään yleensä palvelimiin valokuitutekniikkaa hyödyntäen. NAS-ratkaisut taas toimivat tiedostopohjaisilla protokollilla, tyypillisesti normaalin ethernet-yhteyden yli ja tarjoavat kustannustehokkaampaa tallennustilaa sekä helpompaa hallittavuutta. Nykyisin on tosin havaittavissa konvergenssia näiden teknologioiden välillä, SAN-ratkaisuista osa ovat siirtyneet käyttämään ethernet–pohjaista tiedonsiirtoa ja NAS-ratkaisut ovat kiintolevy- ja tiedonsiirtoteknologien kehittymisestä johtuen pystyneet alkamaan tarjoamaan suuria kapasiteetteja ja nopeampaa tiedonsiirtoa. (Mitchell 2014)

2.3.3 Magneettinauhat

Jo yli 30 vuoden ajan on puhuttu magneettinauhan kuolemasta (Rola 2002). Silti magneettinauhat ovat varsin yleinen näky yrityksissä, varsinkin varmuuskopiointi- ja arkistointikäytössä. Magneettinauhan pitkä historia on ehkä syy miksi magneettinauhat nähdään tuttuna ja turvallisena vaihtoehtona tiedon tallentamiselle. Nauhat ovat suhteellisen

helppoja kuljettaa ja säilyttää, yleisimmin käytetyt formaatit ovat kasettimuotoisia, jossa itse nauha ja kelat sijaitsevat suojaavan kotelon sisällä.

Magneettinauhojen tyypillinen heikkous, peräkkäinen tiedon luku ja tallennus, eivät välttämättä haittaa arkistointi- ja varmuuskopiointikäytössä. Magneettinauhan kymmenien sekuntien haku-aika ei huomattavasti hidasta kerran vuorokaudessa ajettavaa varmuuskopiointiprosessia varsinkaan kun magneettinauhojen luku- ja kirjoitusnopeudet ovat varsin nopeita. Esimerkiksi jo vuonna 2010 julkaistun ”LTO-5”-standardin mukaiset magneettinauhat tarjoavat 1,5 teratavua tallennustilaa, ja jopa 140 Mt/s nopeuksia (The LTO Program 2014). Verrattuna esimerkiksi 1000 Mb/s lähiverkon teoreettiseen maksimisiirtonopeuteen, 125 Mt/s, ja kun erilaisten NAS-järjestelmien luku- ja kirjoitusnopeudet käytännössä jäävät kauas näistä, ei magneettinauhaa voida kutsua hitaaksi. Kirjoitushetkellä uusin, 2012 julkaistu ”LTO-6”-standardi, tarjoaa jopa 2.5 teratavua tallennustilaa ja 160 Mt/s siirtonopeuksia (The LTO Program 2014). LTO-standardin mukaiset kasetit ovat myös varsin kompakteja ulkomitoiltaan ja sopivat siksi varsin hyvin esimerkiksi paloturva- tai kassakaapissa säilöttäviksi. Magneettinauhat ovat myös suosittuja tallennusmedioita kun halutaan siirtää varmuuskopioita eri kiinteistöön.

2.3.4 Magneettinauhojen korvaajat

Magneettinauhojen helpon siirreltävyyden ja erinomaisen kestävyyden vuoksi on myös kehitetty joitakin levypohjaisia magneettinauhojen korvaamiseen tarkoitettuja ratkaisuja. Aiemmin mainitut USB-liitännäiset ulkoiset kiintolevyt voivat olla erinomainen ratkaisu kotikäytössä, mutta yrityksissä ne nähdään kuitenkin yleensä liian hitaina ja epäluotettavina. Vaikka oikeanlaisella liitännällä varustettu ulkoinen kiintolevy olisikin yhtä nopea, tai kuten vaikka ei-peräkkäisen tiedon lukemisen ja kirjoittamisen tapauksessa, jopa nopeampi, kärsii se kuitenkin heikommasta kestävyydestä. Ulkoisissa kiintolevyissä on yleisesti ottaen tavallinen kiintolevy sisällä joka vaatii oman ohjauselektroniikkansa kun taas magneettinauhat eivät usein sisällä minkäänlaista elektroniikkaa. Suurin heikkous on kuitenkin perinteinen pyörivä kiintolevy, jonka kestävyys varsinkin siirreltävässä laitteessa on vähintäänkin kyseenalainen. Yleistyvät SSD-massamuistit saattavat

olla ratkaisu tähän ongelmaan, tosin niiden hinta on vielä moninkertainen verrattuna perinteisiin pyöriviin kiintolevyihin.

Näiden heikkouksien ratkaisemiseksi on kehitetty tekniikoita jotka muistuttavat magneettinauhoja mutta käyttävät kuitenkin muuta tallennustekniikkaa. Näissä ratkaisuissa on pyritty siirtämään mahdollisimman paljon komponentteja pois itse siirrettävältä tallennusmedialta erilliseen asemaan, jolla pyritään emuloimaan magneettinauhajärjestelmän asettelua jossa on yksi asema useita nauhoja kohtaan. Tällöin tallennusmedian kestävyys parantuu, ja koko pienenee. Myös välttämällä usean samanlaisen komponentin käyttöä (esimerkiksi oma levyohjain jokaisessa mediassa), voidaan tehdä järjestelmästä kustannustehokkaampi.

Yksi näistä tekniikoista oli Iomegan kehittämä REV. REV-tekniikan ideana oli eriyttää itse levy ja sen moottori lopuista kiintolevyn komponenteista. Levy ja sen moottori oli sijoitettu siirrettävään muoviseen koteloon ja muut komponentit sijaitsivat itse asemassa. Tällä järjestelyllä saatiin valmistajan mukaan hyvä kestävyys ja alhainen hinta. REV kärsi kuitenkin joidenkin lähteiden mukaan heikosta luotettavuudesta, ja muihin tekniikoihin verrattuna korkeasta hinnasta ja sen valmistus lopetettiin (Curtis 2015). (Iomega 2014)

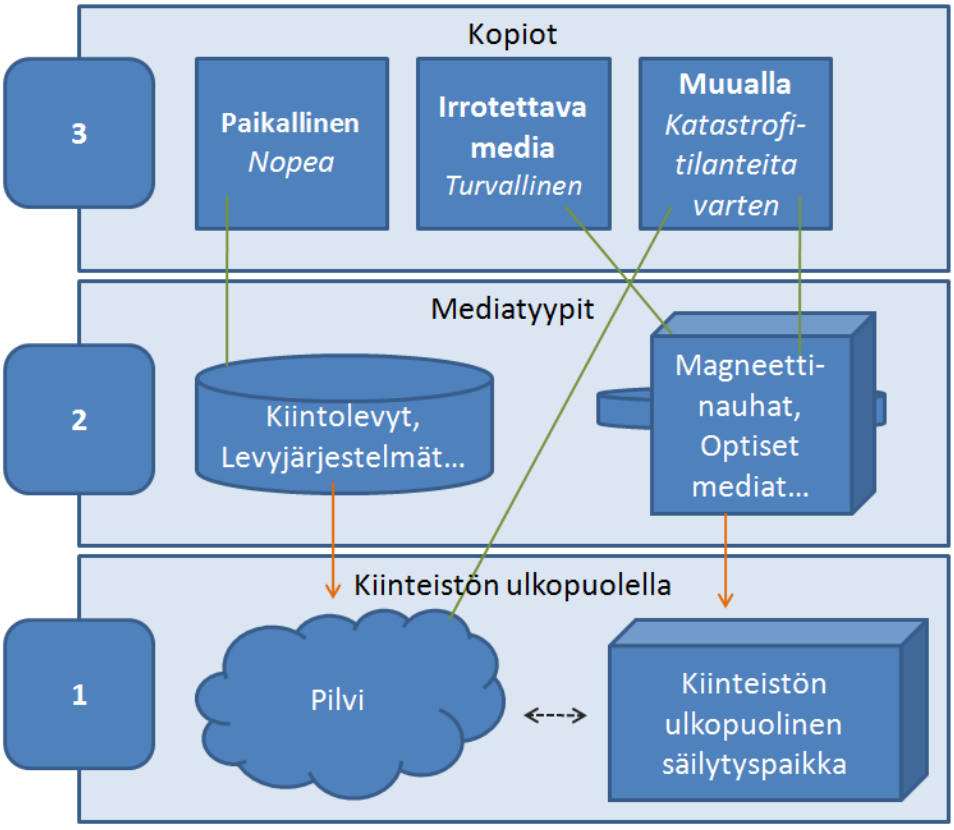
2.4 Varmuuskopiointikäytännöt

Varmuuskopiointijärjestelmä kokonaisuutena koostuu fyysisten laitteiden ja ohjelmistojen lisäksi useista eri vaiheista ja käytännöistä. Hyvin pitkälle automatisoitu järjestelmä vaatii aina vähintään valvontaa, mutta usein myös muita toimenpiteitä sen käyttäjiltä. Tällaiset toimenpiteet voivat olla esimerkiksi tallennusmedioiden kuljettaminen yhdestä paikasta toiseen varmuuskopiointistrategiasta riippuen.

2.4.1 ”3-2-1”-käytäntö

Kuten IT-alalla on tavallista, on myös varmuuskopioinnille muodostunut yleisesti hyväksyttyjä parhaita käytäntöjä. Yksi tunnetuimmista on ns. ”3-2-1”-käytäntö. Tämä käytäntö koskee varmuuskopioiden tallennusmedioita ja niiden sijoittelua. Ideana on että varmuuskopioita tehdään kahdelle eri mediatyypille kolme kappaletta, joista yksi sijaitsee kiinteistön ulkopuolella, kuten havainnollistetaan kuvassa 1.

”3-2-1”-käytännön tavoitteena on saavuttaa hyvä tasapaino nopeuden, vikasietoisuuden ja resurssienkäytön välillä. Ensimmäinen kopio on tarkoitettu nopeaa palauttamista varten, toinen toimii turvallisempana kopiona lisäten vikasietoisuutta, ja kolmas kiinteistön ulkopuolella sijaitseva kopio turvaa tiedon säilymisen katastrofitilanteissa. (QStar Technologies 2013)



Kuva 1 – ”3-2-1”-käytäntö

2.4.2 Varmuuskopiointistrategia

Varmuuskopiointistrategia rakentuu useimmiten ennalta määritellyn aikajakson ympärille, joka riippuu organisaation tuottaman tiedon määrästä, varmuuskopiointiarkiston tavoitellun säilytysajan pituudesta sekä käytössä olevista resursseista. Modernit varmuuskopiointijärjestelmät tarjoavat erilaisia varmuuskopiointityyppejä, jotka helpottavat varmuuskopiointistrategian luomista ja mahdollistavat tehokkaamman tallennustilan käytön. Varmuuskopiointityypit eroavat toisistaan sekä kopioidun tiedon määrän että sen sisällön suhteen (Bosworth et al. 2014 s. 1645).

2.4.3 Varmuuskopiointityypit

Yksinkertaisin varmuuskopiointityyppi on ns. ”täysi” varmuuskopio. Tällä termillä tarkoitetaan alkuperäisen tallennuspaikan kaikkien tiedostojen täydellistä kopioimista siten että prosessin päätyttyä alkuperäistiedostoista on, mahdollista pakkausta lukuun ottamatta, olemassa täysin identtinen kopio. (Bosworth et al. 2014 s. 1645)

Täysi varmuuskopio vie varmuuskopiointityypeistä eniten tallennustilaa ja aikaa. Täydestä varmuuskopiosta puhutaan joskus myös referenssivarmuuskopiona ja se luodaan pisimmällä aikavälillä varmuuskopiointistrategiassa. Jos varmuuskopiointistrategia perustuu esimerkiksi viikon mittaiseen sykliin alkaa se useimmiten täydestä varmuuskopiosta. Koska täysi varmuuskopio vie eniten resursseja on se tällöin järkevää ajoittaa sellaiselle ajankohdalle jolloin järjestelmän käyttö on vähäistä, tavallisesti lauantaille tai sunnuntaille.

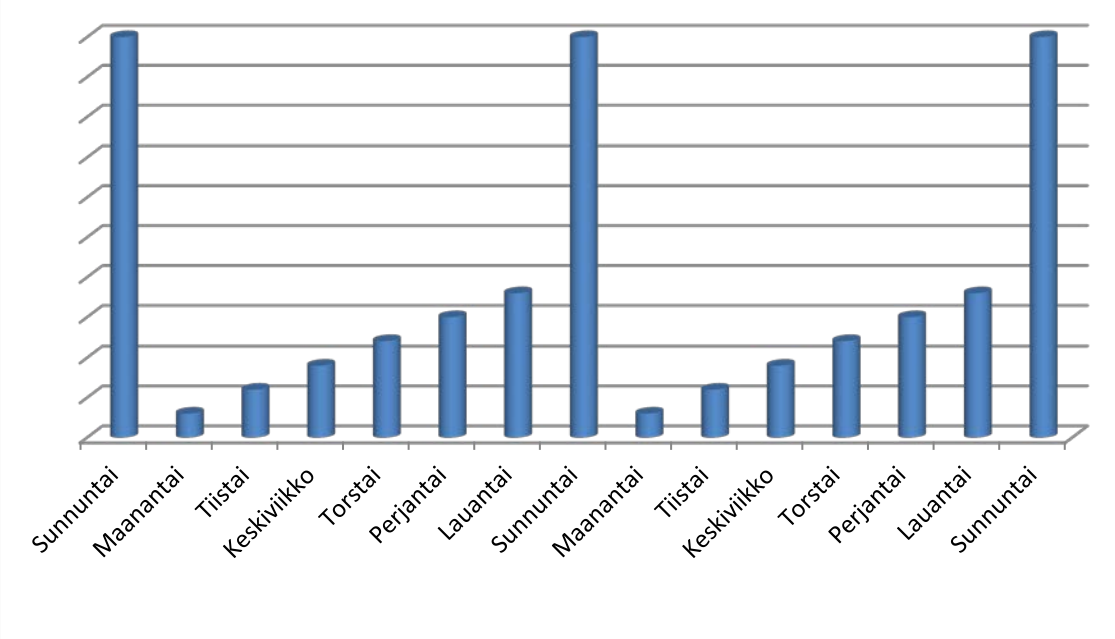
Täysien varmuuskopioiden erittäin suuren tilan- ja resurssienkäytön vuoksi on kehitetty muita varmuuskopiointityyppejä. Näiden kaikkien ideana on lisätä mahdollisten palautuspisteiden määrää kasvattamatta tilantarvetta kohtuuttoman isoksi.

Differentiaalisella varmuuskopioinnilla tarkoitetaan muuttuneen datan kopioimista määrätystä pisteestä alkaen, toisin sanoen varmuuskopioon päätyy vain se data joka muuttunut määrätyn ajankohdan jälkeen. Tämä piste on useimmiten edellinen täysi varmuuskopio (Bosworth et al. 2014 s. 1645). Jos muuttunutta dataa on vähän voi tällä järjeste-

lyllä luoda huomattavasti enemmän palautuspisteitä kuin täysillä varmuuskopioilla yksinään. Varmuuskopioitaessa esimerkiksi kokonaisia virtuaalipalvelimia on tästä huomattavan paljon hyötyä, sillä itse käyttöjärjestelmä ja ohjelmat vievät suuren osan tilasta ja muuttuvat harvoin verrattuna muihin tiedostoihin jos kyseessä on esimerkiksi verkkolevypalvelin.

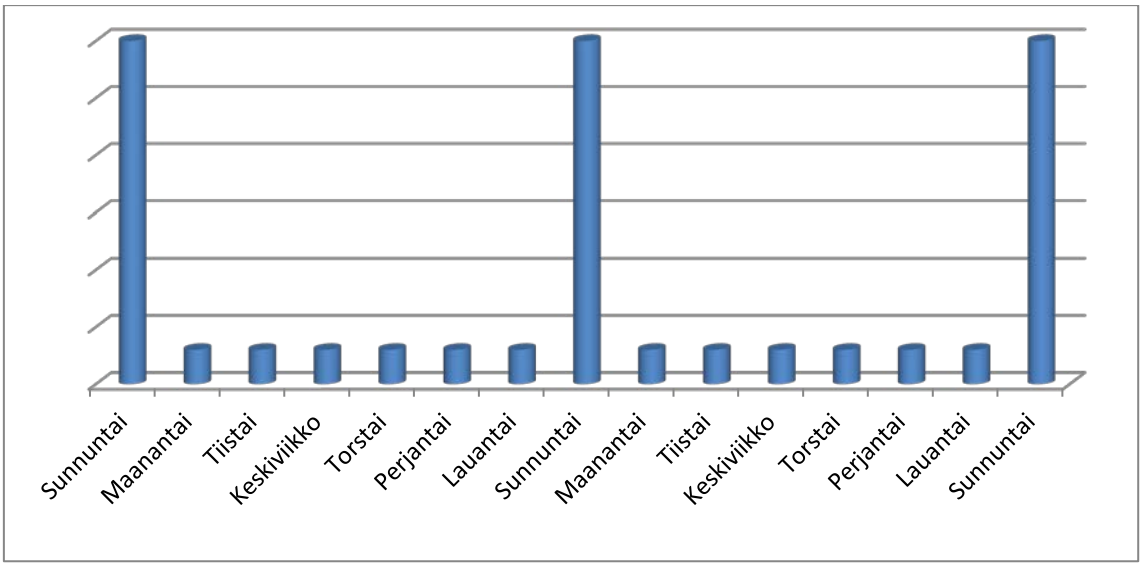
Haittapuolena differentiaalisessa varmuuskopioinnissa on palautuksien vaikeutuminen ja hidastuminen. Jos sunnuntaina täysin varmuuskopioitu ja muina viikonpäivinä differentiaalisesti varmuuskopioitu järjestelmä pitää palauttaa esimerkiksi perjantaina tapahtuvaa ongelmatilannetta edeltävään aikaan, on palautuksessa käytettävä sekä sunnuntain täyttä varmuuskopiota että torstain differentiaalivarmuuskopiota. Tällöin palautetaan ensin täydestä varmuuskopiosta kaikki tiedot pohjaksi, jonka differentiaalivarmuuskopio sitten ylikirjoittaa muuttuneiden tiedostojen osalta. Koska eri varmuuskopiot voivat sijaita eri tallennusmedioilla on palautus hitaampaa kuin täysistä varmuuskopioista. (Bosworth et al. 2014 s. 1646)

Differentiaalivarmuuskopioinnissa varmuuskopion koko kasvaa ajan myötä kunnes tehdään seuraava täysi varmuuskopio, kuvan 2 osoittamalla tavalla. Kaikki uudet differentiaalivarmuuskopiot sisältävät aina myös edellisten differentiaalivarmuuskopioiden datat. Jotta yksittäisen varmuuskopion tilantarvetta saadaan pienennettyä vieläkin enemmän, ja siten myös palautuspisteiden määrä mahdollisimman suureksi on kehitetty inkrementaaliset varmuuskopiot.



Kuva 2 – Varmuuskopion koko differentiaalisella varmuuskopioinnilla jossa sunnuntaina tehdään täysi varmuuskopio

Inkrementaalisissa varmuuskopioissa kopioidaan vain se data joka on muuttunut edellisen varmuuskopiointikerran jälkeen. Tämä koskee kaikkia varmuuskopioita eikä vain täysiä varmuuskopioita. Tämä tarkoittaa että inkrementaalinen varmuuskopio ei sisällä samaa dataa kuin edellinen inkrementaalinen varmuuskopio eikä varmuuskopioiden koko täten kasva yhtä nopeasti kuin differentiaalisessa varmuuskopioinnissa. Kuva 3 kuvastaa tilannetta jossa muuttunutta dataa syntyy päivittäin saman verran. Tämänkin varmuuskopiointityypin haittapuolena on palautuksen hidastuminen. Pahimmassa tapauksessa tarvitaan palautusta varten kaikki varmuuskopiot jotka ovat syntyneet sitten edellisen täyden varmuuskopion. (Bosworth et al. 2014 s. 1646)



Kuva 3 – Varmuuskopion koko inkrementaalisella varmuuskopioinnilla jossa sunnuntaina tehdään täysi varmuuskopio

2.4.4 Deduplikointi

Deduplikoinnilla tarkoitetaan tekniikoita joilla pyritään välttämään saman tiedon tallentamista ja siirtämistä useaan kertaan. Verrattuna tavalliseen pakkaukseen deduplikoinnilla tunnistetaan isompia tietoalueita, esimerkiksi kokonaisia levyosioita tai tiedostoja, kun taas pakkauksella tunnistetaan yksittäisen tiedoston sisällä toistuvia alueita, yksittäisiä bittijonoja. (Fu, Y et al. 2013)

Deduplikoinnista on erityisen paljon hyötyä varmuuskopioitaessa virtualisoituja ympäristöjä joissa saattaa olla useita virtuaalipalvelimia jotka käyttävät samaa käyttöjärjestelmää. Tällaisessa tapauksessa voidaan deduplikoinnilla säästää huomattava määrä tallennustilaa koska virtuaalipalvelimet sisältävät keskenään paljon samaa dataa. Deduplikointia käytetään usein yhdessä tavallisen pakkauksen kanssa.

Käyttämällä pakkausta ja deduplikaatiota sekä tämän lisäksi yhdistelemällä eri varmuuskopiointityyppejä voidaan tallennustilan tarvetta alentaa ja tiedonsiirtoa nopeuttaa. Hyvän varmuuskopiointijärjestelmän tulee siis tukea näitä tekniikoita.

3 VARMUUSKOPIOINTIRATKAISUN VALINTA

Sopivan varmuuskopiointiratkaisun löytymiseksi on ensiksi selvitettävä toimeksiantajan tarpeet ja vaatimukset. Toimeksiantajan nykyistä varmuuskopiointiratkaisua on hyvä käyttää vertailupohjana. Siinä esiintyneet puutteet ja vahvuudet edesauttavat vaatimusten määrittelyä. Tarpeiden ja vaatimusten perusteella toimeksiantaja pyytää tarjouksia valitsemiltaan omat kriteerinsä täyttäviltä toimittajilta ja kilpailuttaa ne.

3.1 Nykyinen varmuuskopiointiratkaisu

Toimeksiantajan nykyinen varmuuskopiointiratkaisu on toteutettu ”Symantec Backup Exec 2012”-ohjelmistolla, NAS-verkkolevypalvelimella, ulkoisilla kiintolevyillä, sekä magneettinauhoilla. Ulkoiset kiintolevyt ovat USB-liitännällä suoraan kytketty Hyper-V alustapalvelimiin eivätkä ne ole varsinaisen varmuuskopiointiohjelmiston hallinnassa vaan niihin tehdään täydet varmuuskopiot päivittäin käyttöjärjestelmän omalla varmuuskopiointityökalulla ”Windows Server Backup”.

Varmuuskopiointiohjelmisto tekee varmuuskopiot sekä magneettinauhoille että verkkolevyasemalle. Magneettinauhat ovat ”LTO-4”-standardin mukaisia (tallennuskapasiteetti 800 Gt) ja niihin kirjoitetaan palvelinhuoneessa sijaitsevalla yksipesäisellä nauhaasemalla josta ne sitten siirretään paloturvakaappiin käsin. Nykyisen varmuuskopiointistrategian mukaisesti magneettinauhalle tehdään täysi varmuuskopio joka lauantai, ja differentiaaliset varmuuskopiot tiistaisin ja torstaisin. Käytännössä tämä tarkoittaa että kasetti on vaihdettava maanantaisin, keskiviikkoisin ja perjantaisin. Paloturvakaappi on järjestelty siten että lauantain, tiistain ja keskiviikon varmuuskopioille on omat hyllyrivit. Lisäksi on olemassa erillinen hyllyrivi kuukauden ensimmäisen lauantain varmuuskopioille.

Verkkolevypalvelin toimii varmuuskopioiden päätallennuspaikkana. Verkkolevypalvelin sijaitsee palvelinhuoneessa varsinaisen palvelinkaapin vieressä. Verkkolevylle tehdään täysi varmuuskopio joka sunnuntai, ja differentiaaliset varmuuskopiot maanantaisin, keskiviikkoisin ja perjantaisin. Verkkolevypalvelin on liitetty iSCSI-tekniikalla lähiverkkoyhteyden yli yhteen alustapalvelimeen johon itse varmuuskopiointiohjelmisto

on asennettu. Verkkolevypalvelimelle tehtävät varmuuskopiot eivät vaadi valvonnan lisäksi muita toimenpiteitä henkilökunnalta.

3.1.1 Nykyisen varmuuskopiointiratkaisun vahvuudet

Nykyisen ratkaisun vahvuuksiksi tunnistettiin seuraavat kohdat:

- Varmuuskopioita on yhteensä kolme kappaletta
- Varmuuskopioita tehdään sekä kiintolevyille että magneettinauhalle
- Kaikki varmuuskopiot eivät ole riippuvaisia samasta ohjelmistosta
- Magneettinauhat säilytetään paloturvakaapissa
- Kohtuullisen kustannustehokas ratkaisu
- Varmuuskopiointistrategia on melko selkeä
- Ohjelmisto ja verkkolevypalvelin osaavat tarkkailla varmuuskopiointien etenemistä ja ilmoittaa sähköpostitse virhetilanteista
- Järjestelmä skaalautuu melko hyvin, tallennustilan kasvattaminen on yksinkertaista

3.1.2 Nykyisen varmuuskopiointiratkaisun heikkoudet

Seuraavat kohdat koettiin nykyisen järjestelmän heikkouksina:

1. Ei kiinteistön ulkopuolista varmuuskopiota
2. Sekä verkkolevypalvelin että ulkoiset kiintolevyt sijaitsevat palvelinhuoneessa
3. Varmuuskopiointiohjelman käyttöä pidettiin hankalana
4. Magneettinauhat vaativat paljon manuaalista työtä

Kohta 1 koettiin olevan järjestelmän suurin heikkous. Kiinteistön ulkopuolella sijaitsevan varmuuskopion puuttuminen ei ole parhaiden käytäntöjen mukaista ja sellaisen järjestäminen olikin uudistusprojektin ensimmäinen tavoite.

Tallennusratkaisujen fyysinen sijainti havaittiin olevan toinen ongelmakohta. Paikallisen vahingon sattuessa, esimerkiksi tulipalo palvelinhuoneessa, jättäisi varmistuksen ainoastaan magneettinauhojen varaan. Paloturvakaapin sijainti samassa kerroksessa kuin palvelinhuone lisää entisestään ulkopuolisen varmuuskopion tärkeyttä. Verkkolevypalvelimen uudelleensijoitus kiinteistön sisällä osoittautui vaivattomaksi ensiratkaisuksi siihen sopivan tilan olemassa olosta johtuen, joten uudelleensijoitus suoritettiin jo projektin alkuvaiheessa.

Nykyinen varmuuskopiointiohjelmisto mahdollistaa monipuolisuudellaan halutun varmuuskopiointistrategian toteuttamisen, mutta ohjelmiston käyttö koettiin hankalana. Ohjelman konfigurointi ja valvonta on ulkoistettu. Ohjelmiston konfiguraatiota tutkiessa paljastui, että nykyinen konfiguraatio ei vastannutkaan toimeksiantajan varmuuskopiointistrategiaa. Syyksi koettiin ohjelmiston hankala käyttölogiikka. Ohjelmistossa moitittiin erityisesti pakkoa luoda erilliset varmuuskopiointitehtävät jokaiselle palvelimelle. Virtualisoidussa ympäristössä jossa on paljon palvelimia, ja joiden määrä elää aiheuttaa tämä paljon lisätyötä. Ohjelmisto vaatii lisäksi että jokaiselle varmuuskopioitavalle palvelimelle asennetaan asiakasohjelma joka myös lisää tarvittavan työn määrää uutta virtuaalipalvelinta luodessa.

Magneettinauhajärjestely on perehtymättömälle vaikeaselkoinen. Kasettia vaihtaessa pitää olla tietoinen järjestelystä, ja että hyllyrivien merkinnät vastaavat varmuuskopiointipäivää eikä kasetin vaihtopäivää sekä huomioida oliko lauantai kuukauden ensimmäinen. Lisäksi kasetin vaihto kolmesti viikossa on melko työlästä, eikä saman henkilön voida olettaa olevan paikalla vaihtamassa kasettia joka kerta. Toimeksiantajan mukaan onkin syntynyt tilanteita jossa kasetti on jäänyt vaihtamatta inhimillisten erehdysten takia, esimerkiksi lomakausien aikana.

3.2 Kiinteistön ulkopuolella sijaitseva varmuuskopio

Aiemmin mainitun perusteella todettiin siis yhden varmuuskopion sijoittaminen kiinteistön ulkopuolelle olevan uudistusprojektin ensisijainen tavoite. Ulkopuolisen varmuuskopion voi sijoittaa moneen paikkaan, seuraavaksi vertaillaan eri sijoituspaikkoja.

3.2.1 Kodit

Varsinkin pienissä yrityksissä saattaa tuntua luontevalta ja vaivattomalta ratkaisulta sijoittaa yksi varmuuskopioista jonkun luotettavana pidetyn henkilön kotiin, esim. IT-päällikkö, toimitusjohtaja tai vastaava. Tämä järjestely ei kuitenkaan ole suositeltava eikä turvallinen. Vaikka kyseinen henkilö olisikin luotettava, ei tämä välttämättä päde muihin kodin asukkaisiin. Lisäksi kodin suojausta murtovarkauksia vastaan on vaikeasti arvioitavissa. (Bosworth et al. 2014 s. 1654)

Mediatyypistä riippuen eivät kodin säilytysolosuhteetkaan usein ole oikeanlaiset ja niitä on vaikea valvoa. Kodin lämpötilat ja ilmankosteus saattavat olla haitallisia tallennusmedioille. Myös vakuutukset voivat olla ongelmallisia, kotivakuutus ei todennäköisesti korvaa työnantajan omaisuutta. (Bosworth et al. 2014 s. 1654)

3.2.2 Tallelokerot ja holvit

Pankkien tallelokerot ovat usein hyvin suojattuja ja niissä on hyvät olosuhteet tallennusmedioita varten (Bosworth et al. 2014 s. 1655). Monella yrityksellä, kuten myös toimeksiantajalla, on jo tallelokeroita joissa säilytetään yrityksen tärkeimpiä dokumentteja. Vaikka pankin tallelokero voikin olla hyvä ja edullinen ratkaisu monelle organisaatiolle, on sillä kuitenkin myös huonoja puolia. Kuljetuksen järjestäminen tallelokerolle ja takaisin säännöllisesti on vaivalloista, lisäksi pankkien aukioloajat rajoittavat suuresti kopion saatavuutta. Usein yllättävät ongelmatilanteet jolloin varmuuskopiota juuri olisi tarvittu osuvatkin pankkien aukioloaikojen ulkopuolelle.

On myös olemassa yrityksiä jotka tarjoavat tallennusmedioiden säilytystä palveluna. Palveluun voi kuulua kaikki kuljetuksesta säilytykseen ja valvontaan. Etuna näissä palveluissa on että palveluntarjoaja on erikoistunut juuri digitaalisten tallennusmedioiden säilytykseen joten heillä on siihen sopivat tilat ja osaaminen. (Bosworth et al. 2014 s. 1655)

Tallennusmedioiden säilyttämisen kokonaisvaltaisena palveluna tarjoavia yrityksiä ei tosin Suomesta juuri löydy, tai ainakaan palveluja ei markkinoida kovin aktiivisesti. Uudistusprojektissa vertailluista palveluntarjoajista ei yksikään tarjonnut tällaista palvelua, kaikki palveluntarjoajat tarjosivat tietovarastointipalvelun pilvipalveluna.

3.2.3 Pilvipalvelut

Pilvipalveluna toteutetut varmuuskopiointiratkaisut ovat kätevä tapa saada varmuuskopio myös kiinteistön ulkopuolelle. Pilvipalveluiden edut ovat selkeitä. Fyysisten medioiden kuljetusta ei tarvitse järjestää ja palveluntarjoaja vastaa tiedon säilyttämisestä. Palveluntarjoajien konesalit ovat usein hyvin valvottuja ja ne usein täyttävätkin Viestintäviraston asettamat tärkeän tilan vaatimukset ja ne ovat asianmukaisesti auditoidut. Tämä tarkoittaa käytännössä ettei asiakasorganisaation tarvitse huolehtia varmuuskopioista lähettämisen jälkeen, kunhan ne ovat asianmukaisesti salattu jo ennen lähetystä.

Periaatteessa kaikki varmuuskopiot voidaan sijoittaa pilveen, riippuen tietysti tiedon määrästä ja saatavilla olevan Internet-yhteyden nopeudesta. Yhteyksien rajoitetut nopeudet ovat käytännössä suurin haaste pilvipalveluna toteutetuissa varmuuskopiointiratkaisuissa (Crump 2013). Toimeksiantajalla on käytössä symmetrinen 100 Mbps valokuituliittymä. Kaikkien toimeksiantajan virtuaalipalvelimien levykapasiteetti yhteensä on noin 6Tt. Toimeksiantajan jo olemassa olevan laitteiston ja tiedon suuresta määrästä johtuen päätettiin kuitenkin varmuuskopioiden päätallennuspaikka pitää toimeksiantajan omissa tiloissa.

Tiedon suuresta määrästä johtuen todettiin parhaaksi ratkaisuksi eriyttää tuotantokriittinen data muusta datasta ulkopuolista tallennusta varten. Näin toteutettuna osoittautui pilvipalvelu toimeksiantajan kannalta vaivattomimmaksi ja kustannustehokkaimmaksi ratkaisuksi. Tällaista ratkaisua voidaan kutsua hybridipilviratkaisuksi, ja vastaavat ratkaisut ovatkin kasvattaneet suosiotaan viime aikoina (Crump 2013).

3.3 Varmuuskopiointiohjelmisto

Vaikkei varmuuskopiointiohjelmiston korvaaminen ollutkaan projektin ensisijaisimpia vaatimuksia, päätettiin sen korvaaminen selvittää saatujen tarjousten perusteella. Valituista toimittajista kaikki tarjosivat vaihtoehtona nykyiselle varmuuskopiointiohjelmistolle ”Veeam Backup & Replication”-ohjelmistoa. Toiseksi vaihtoehdoksi jäi pitää nykyinen varmuuskopiointiohjelmisto tai sen korvaaminen uudemmalla versiolla.

3.3.1 Symantec Backup Exec 2014

Uusin versio toimeksiantajan nykyisestä varmuuskopiointiohjelmistosta on ”Symantec Backup Exec 2014” ja se sisältää joitakin toimeksiantajan kannalta tärkeitä uudistuksia. Suurimpana hankaluutena nykyisessä versiossa koettiin vaatimusta luoda erillinen varmuuskopiointitehtävä jokaista palvelinta kohden. Uusimassa versiossa tätä vaatimusta ei enää ole, joten yhteen varmuuskopiointitehtävään voi sisällyttää useita palvelimia. (Symantec Corporation 2015)

Ohjelmiston valmistajan mukaan ohjelmiston käyttöä ja valvontaa on myös selkeytetty uuden kaikki varmuuskopiointitehtävät sisältävän näkymän lisäämisellä (Symantec Corporation 2015). Tämä saattaisi myös helpottaa toimeksiantajalla koettua käytön hankaluutta ja epäselkeyttä.

Muita huomattavia uudistuksia edelliseen versioon verrattuna ovat ohjelmiston valmistajan lupaama jopa 100 % parannus varmuuskopioinnin ja deduplikoinnin nopeuteen.

Ohjelmisto tukee nyt myös Windows Server 2012 ja 2012 R2 versioita josta voi olla hyötyä tulevaisuutta ajatellen. (Symantec Corporation 2015)

Etuna muiden valmistajien tuotteisiin verrattuna voidaan myös pitää valmistajan lupaamaa helppoa päivitettävyyttä toimeksiantajan nykyisestä versiosta (Symantec Corporation 2015). Tosin asetusten suoraan tuominen nykyisestä asennuksesta ei olisi suotavaa jos nykyisen asennuksen monimutkaisuudesta haluttaisiin päästä eroon hyödyntämällä uusia ominaisuuksia, esimerkiksi sisällyttämällä useita palvelimia samaan varmuuskopiointitehtävään.

3.3.2 Veeam Backup & Replication

Veeam Backup & Replication on Veeam Softwaren kehittämä varmuuskopiointiohjelmisto virtualisoituja palvelinympäristöjä varten. Veeam Backup & Replication on tarkoitettu käytettäväksi kokonaan virtualisoiduissa ympäristöissä eikä se siten tue fyysisten palvelimien varmuuskopiointia ollenkaan. Ohjelmisto tukee VMwaren vSphere sekä Microsoftin ”Windows Server Hyper-V”-virtualisointialustoja. (Veeam Software 2014b)

Veeam Software korostaa markkinoinnissaan tuotteensa nopeutta ja sen helppoa käyttöä. Ohjelmiston käyttö ei vaadi ohjelmistokomponenttien erikseen asentamista jokaiselle virtuaalipalvelimelle. Veeam Backup & Replication osaa myös käynnistää varmuuskopioidun virtuaalipalvelimen suoraan varmuuskopiosta ja tarvittaessa palauttaa vain muuttuneet tiedot palautusprosessin nopeuttamiseksi. (Veeam Software 2014c)

Veeam Backup & Replication osoittautui toimeksiantajan kannalta sopivimmaksi ratkaisuksi. Veeam Software on sekä tuotekehityksessään että markkinoinnissaan selvästi hyödyntänyt ”Symantec Backup Exec”-ohjelmiston saamaa kritiikkiä. Veeam Software on myös hinnoitellut tuotteensa houkuttelevasti.

4 TOTEUTETTU RATKAISU

Tehtyjen valintojen perusteella päätettiin toimeksiantajalla toteuttaa varmuuskopiointiratkaisu yhden toimittajan antaman tarjouksen perusteella. Tarjous sisälsi varmuuskopiointiohjelmiston, pilvireplikointipalvelun, asennuksen ja valvontapalvelun. Muita toimenpiteitä olivat aiemmin mainittu NAS-palvelimen siirtäminen sekä myöhäisemmässä vaiheessa toteutettu NAS-palvelimen ja magneettinauha-aseman uudistaminen.

4.1 Käyttöönoton suunnittelu

Käyttöönotto toteutettiin yhdessä palveluntarjoajan konsultin kanssa. Suunnitteluvaiheessa päätettiin missä sijaitsevat tuotantokriittisimmät tiedot joiden varmuuskopiot replikoitaisiin myös pilvipalveluun.

Tällaisia kohteita olivat:

- Päätietokantapalvelimella olevien tietokantojen varmuuskopiot
- CRM-järjestelmän omalla tietokantapalvelimella olevan tietokannan varmuuskopio
- Sähköpostipalvelimen varmuuskopio
- Tiedostopalvelimella sijaitsevien tiettyjen tuotantokriittisten kansioiden varmuuskopiot

Varmuuskopiointiohjelmisto päätettiin asentaa samalle palvelimelle jossa aikaisempi ohjelmisto sijaitsi. Näin voidaan hyödyntää olemassa olevaa magneettinauha-asemaa ja NAS-palvelinta ilman että laitteita tarvittaisiin siirtää, yhteyksiä luoda uudelleen tai ajureita asentaa toiseen palvelimeen. Tämä on myös suotavaa sellaisen tilanteen kannalta jossa vanhan ohjelmiston tekemiä varmuuskopioita pitäisi palauttaa magneettinauhalta. Vanha ohjelmisto päätettiin myös pitää asennettuna niin kauan kunnes kaikki vanhat magneettinauhalla olevat varmuuskopiot ovat uuden varmuuskopiointiohjelmiston ylikirjoittamia. Nauhoja siirretään siis uuteen järjestelmään sitä mukaan kun niillä olevat varmuuskopiot vanhenevat.

Alustapalvelimissa kiinni olleet USB-kiintolevyt ja niihin tehtävät varmuuskopiot päätettiin pitää ennallaan. Koska kiintolevyjä ei voida pitää erityisen luotettavina, eivätkä ne ole millään lailla yhteydessä varsinaiseen varmuuskopiointiohjelmistoon, ei niitä nähdä oleellisena osana varsinaista varmuuskopiointijärjestelmää ja sen tuomaa turvaa, vaan ne toimivat lähinnä nopeuttajina tilanteessa jossa alustapalvelin joudutaan asentamaan uudelleen.

Toimeksiantajalla on kaksi DC-palvelinta jotka molemmat ovat asennettu fyysisille palvelimille. Uusi varmuuskopiointiohjelmisto ei tue fyysisten palvelimien varmuuskopiointia joten yksi DC-palvelimista päätettiin virtualisoida. Tällainen järjestely mahdollistaa nopeat palautukset virtualisoidun DC-palvelimen osalta, mutta on myös Microsoftin Windows Server 2008R2 koskevien suositusten mukainen joiden mukaan kannattaa säilyttää ainakin yksi fyysinen DC-palvelin virtualisointialustassa mahdollisesti esiintyvän ongelmatilanteen vaikutusten minimoimiseksi (Microsoft 2013).

4.1.1 Varmuuskopiointistrategian uudelleenmäärittely

Toimeksiantajan nykyisen varmuuskopiointistrategian uudistaminen tehtiin yhdessä toimittajan konsultin kanssa jotta se rakentuisi mahdollisimman hyvin uuden varmuuskopiointiohjelmiston tarjoamien ominaisuuksien ympärille.

Varmuuskopiointistrategia yksinkertaistui huomattavasti entisestä. Kaikki palvelimet varmuuskopioidaan joka yö NAS-palvelimelle inkrementaalisesti, ja lauantaisin tehdään täysi varmuuskopio. Pilvipalveluun vietävät varmuuskopiot tehdään joka yö. Magneettinauhalle siirretään lauantain täysi varmuuskopio sen valmistuttua, ja nauha vaihdetaan viikon aikana uuteen. Paloturvakaappi järjestellään niin että magneettinauhoja on kaksi rivillistä, yksi kuukauden ensimmäisen lauantain varmuuskopioita varten ja toinen muiden lauantaiden varmuuskopioita varten.

Uusi magneettinauhajärjestely vähentää huomattavasti manuaalisen työn määrää. NAS-palvelimen uudelleen sijoittaminen, joka yö tehtävät varmuuskopiot ja pilvivarmuuskopiot parantavat ratkaisun vikasietoisuutta joten magneettinauhojen ensisijaiseksi tehtäväksi jää toimia pidempiaikaisena arkistona. Täten allokoitiinkin suurin osa magneetti-

nauhoista kuukauden ensimmäisen lauantain varmuuskopioita varten mahdollisimman pitkän arkistointiajan saavuttamiseksi, ja muiden lauantaiden magneettinauhat toimivat vain vikasietoisuutta lisäävänä tekijänä, ”3-2-1”-käytännön mukaisesti. Koska magneettinauhavarmuuskopiointitehtävä käytännössä vain siirtää jo tehdyn täyden varmuuskopion magneettinauhalle käyttää järjestelmä myös vähemmän resursseja.

4.2 Ohjelmistojen asennus

Pääasiallinen varmuuskopiointiohjelmisto, Veeam Backup & Replication, asennettiin siis olemassa olevan varmuuskopiointiohjelmiston rinnalle. Pilvipalvelun asiakasohjelmisto asennettiin jokaiselle palvelimelle jolta haluttiin siirtää varmuuskopioita pilveen. Käytännössä tämä tarkoitti kahta tietokantapalvelinta, tiedostopalvelinta sekä palvelinta jolla päävarmuuskopiointiohjelmisto sijaitsee. Päävarmuuskopiointiohjelmisto ja pilvipalvelun ohjelmisto ovat riippumattomia toisistaan.

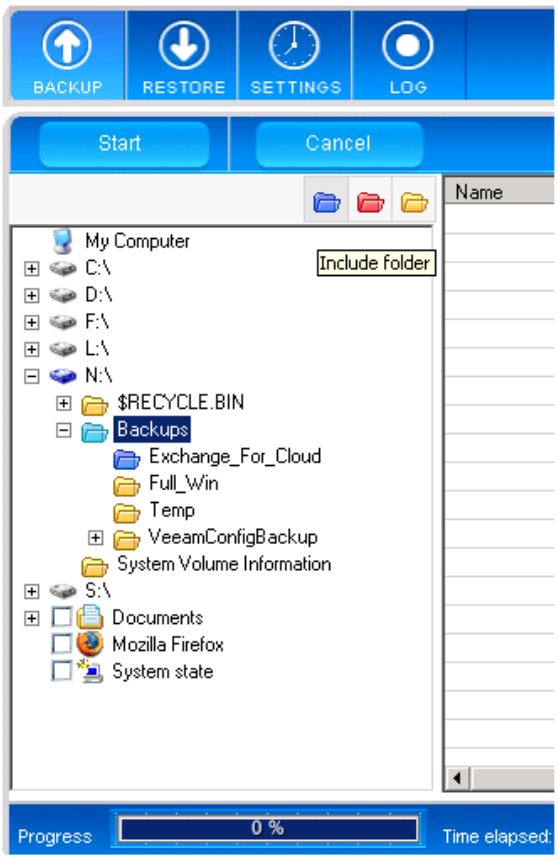
Asennus sujui ongelmitta. Asennustyöt eivät vaatineet käyttökatkoksia ja ne voitiin suorittaa normaalina toimistotyöaikana. Itse asennukset kestivät alle tunnin. Asennusten valmistuttua ohjelmistot konfiguroitiin vastaamaan suunniteltua varmuuskopiointistrategiaa.

4.3 Ohjelmistojen konfigurointi

Konfigurointivaiheessa liitettiin tallennusmediat varmuuskopiointiohjelmistoon, luotiin varmuuskopiointitehtävät ja määriteltiin niiden asetukset sekä luotiin pilvipalvelun salausavaimet. Salausavaimia tarvitaan jos pilvipalvelun asiakasohjelmisto asennetaan uudelleen, esimerkiksi laiterikon seurauksena. Salausavaimista tehtiin kaksi kopiota paperille joista yhtä säilytetään pankkiholvissa ja toista toimeksiantajan omassa kassakaapissa.

4.3.1 Pilvipalvelun asiakasohjelmisto

Salausavaimen asettamisen jälkeen pilvipalvelun asiakasohjelmistoon määriteltiin kuvan 4 mukaisesti mitkä kansiot huomioitaisiin varmuuskopiossa. Tietokantapalvelimilla kansioiksi määriteltiin tietokannan oman varmuuskopiointitehtävän kohdekansiot. Päävarmuuskopiointiohjelmiston palvelimelta valittiin kansio johon myöhemmin luotavan sähköpostipalvelimen varmuuskopiointitehtävän tuottamat tiedostot sijoitetaan, joten pilvipalveluun viedään koko sähköpostipalvelimen varmuuskopio.



Kuva 4 – Kansioiden valinta

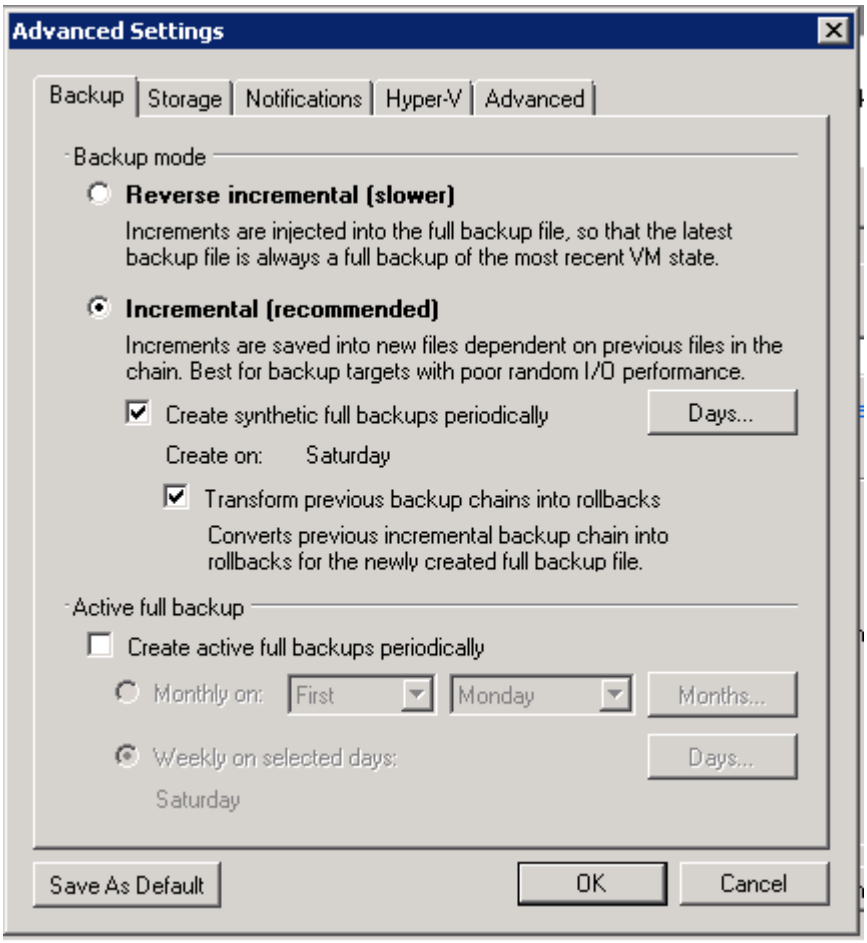
Asiakasohjelmistoon määritellään myös ne sähköpostiosoitteet johon ohjelmisto lähettää raportteja ja virheilmoituksia. Aikatauluasetuksissa asetettiin varmuuskopiointiajaksi joka yö. Varmuuskopioinnin käynnistymisen kellonajat jaksotettiin niin, ettei jokainen palvelin siirtäisi varmuuskopioitaan pilvipalveluun yhtäaikaisesti kaistankäytön mini-

moimiseksi. Asetuksissa oli myös huomioitava ohjelmiston käyttämä väliaikaiskansio varmuuskopiointitöitä varten. Erityisesti palvelimella jolta sähköpostipalvelimen varmuuskopiot siirretään käyttää ohjelmisto huomattavan määrän levytilaa välikasitiedostoja varten kun se pakkaa ja salakirjoittaa varmuuskopiot ennen siirtoa.

Pilvipalvelussa sijaitsevan varmuuskopion on tarkoitus toimia varakopiona tilanteessa jossa kaikki NAS-palvelimella, magneettinauhoilla ja palvelimissa kiinni olevilla USB-kiintolevyillä olevat varmuuskopiot tuhoutuvat tai eivät ole saatavissa. Täten ohjelmistosta kytkettiin pois päältä arkistointiominaisuudet ja versiointi koska pilvipalvelussa säilytetään vain tiedostojen uusimmat versiot. Ohjelmisto asetettiin myös poistamaan lähdepalvelimelta poistetut tiedostot pilvipalvelusta jotta tilankäyttö ei kasva jatkuvasti. Tällaista varmuuskopiointia kutsutaan peilaukseksi.

4.3.2 Veeam Backup & Replication

Ohjelmiston konfigurointi aloitettiin lisäämällä NAS-palvelin ohjelmiston käytössä oleviin tallennuspaikkoihin. NAS-palvelin on liitetty palvelimeen iSCSI-tekniikalla ja näkyy siten normaalina levyasemana käyttöjärjestelmässä joten sen lisääminen ohjelmistoon oli yksinkertaista. Ohjelmistoon luotiin kolme varmuuskopiointitehtävää. Ensin luotiin kaikki virtuaalipalvelimet kattava tehtävä joka ajetaan joka yö. Ohjelmistossa voitiin varmuuskopiointitehtävään valita suoraan alustapalvelin, jolloin kaikista alustapalvelimella olevista virtuaalipalvelimista tehdään varmuuskopiot. Tehtävä asetettiin luomaan inkrementaalisia varmuuskopioita sekä luomaan täysi varmuuskopio joka lauantai. Täyden varmuuskopion muodostamiseen hyödynnettiin ohjelmiston ”Synthetic Full Backup”-ominaisuutta. Kuvassa 5 näkyvät varmuuskopiointityön lisäasetukset kokonaisuudessaan.



Kuva 5 – Varmuuskopiointitehtävän lisäasetukset

Tämän ominaisuuden ollessa kytkettynä ohjelmisto muodostaa täyden varmuuskopion ottamalla ensin normaalisti inkrementaalisen varmuuskopion ja hyödyntää tämän jälkeen sitä, sekä aikaisempia varmuuskopioita täyden varmuuskopion luomiseen. Koska inkrementaalisen varmuuskopion ottaminen on huomattavasti nopeampaa kuin täyden, ei synteettisen täyden varmuuskopion luominen kuormita palvelimia juuri ollenkaan. Varmuuskopion luomiseen menee edelleenkin paljon aikaa, mutta se kuormittaa vain varmuuskopioiden tallennusmediaa eikä suoraan palvelimia. Lopputuloksena on täysi varmuuskopio joka sisältää samat tiedot kuin jos täysi varmuuskopio otettaisiin suoraan palvelimilta. Ohjelmisto mahdollistaa myös perinteisen täyden varmuuskopion ottamisen, jolloin tiedot kopioidaan suoraan palvelimilta. Tällaista varmuuskopiota kutsutaan ohjelmistossa nimellä ”Active Full Backup”.

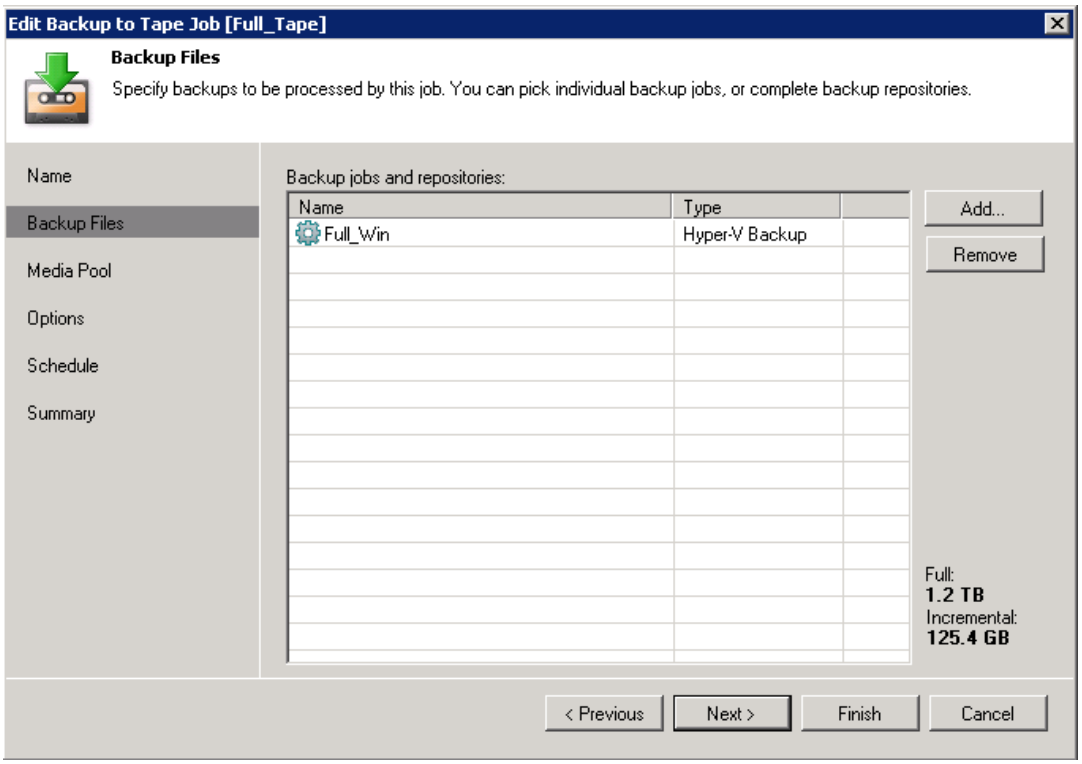
Varmuuskopiointiyössä kytkettiin myös päälle ominaisuus ”Transform previous backup chains into rollbacks”. Tämän ominaisuuden tarkoituksena on säästää levytilaa säilyttämällä levyllä ainoastaan yhden täyden varmuuskopion kahden sijaan. Tällöin inkrementaaliset varmuuskopiot luodaan aina edellistä täyttä varmuuskopiota vasten, ja sitä vanhemmat varmuuskopiot muunnetaan ketjuksi taaksepäin inkrementaalisia varmuuskopioita. Ominaisuuden käyttämisen haittapuolena on että täyden varmuuskopion muodostamisen jälkeinen muuntaminen kestää kauemmin kuin pelkän täyden varmuuskopion muodostaminen, mutta ominaisuuden mahdollistama tilansäästö on merkittävä.

Sähköpostipalvelimen pilvivarmuuskopiota varten luotiin erillinen varmuuskopiointitehtävä, joka asetettiin päävarmuuskopiointitehtävän tavoin luomaan viikoittainen täysi varmuuskopio, ja päivittäiset inkrementaaliset varmuuskopiot, mutta palautuspisteiden määräksi asetettiin vain yksi. Pilvipalvelun asiakasohjelmisto siirtää tämän varmuuskopion pilvipalveluun.

Magneettinauhavarmuuskopioita varten lisättiin ohjelmistoon ensin palvelimeen jo ennestään liitetty magneettinauha-asema. Ohjelmistossa käytetään käsitettä ”media-pool” jolla tarkoitetaan magneettinauhojen loogista ryhmää. Ohjelmistossa on valmiiksi joitakin ryhmiä kuten ”Free” ja ”Retired”. Valmiiden ryhmien lisäksi voidaan ohjelmistoon luoda uusia ryhmiä ja määritellä näille omat säännöt, esimerkiksi ylikirjoittamisen suoja-aika tai eri salausasetuksia. Koska ohjelmistoon lisätään magneettinauhoja sitä mukaan kun niillä olevat vanhan järjestelmän tuottamat varmuuskopiot vanhenevat, aiheuttaa viikoittainen magneettinauhojen lisääminen ja numeroiminen hieman lisätyötä siirtymisvaiheen ajan.

Magneettinauhavarmuuskopiointitehtävä on ajastettu lauantai-illaksi, jolloin voidaan olla varmoja siitä että lauantain aamuyöllä käynnistyvän päävarmuuskopiointitehtävän muodostama täysi varmuuskopio on valmis. Ohjelmistossa on myös mahdollista ajastaa varmuuskopiointitehtävä käynnistymään automaattisesti toisen varmuuskopiointitehtävän päätyttyä. Tätä ominaisuutta käytettiin aluksi, mutta ohjelmiston versionpäivityksen jälkeen esiintyneiden ongelmien jälkeen siirryttiin käyttämään normaalia ajastusta. Kuten kuvasta 6 käy ilmi voidaan varmuuskopiointitehtävän lähteeksi valita ohjelmistossa suoraan päävarmuuskopiointitehtävä käyttämällä varmuuskopiointityyppiä ”Backups to

Tape” ja määrittää se kopioimaan magneettinauhalle ainoastaan täysiä varmuuskopioita kytkemällä pois valinta ”Process incremental backup files”. Tehtävään ei siis tarvitse määritellä kopioitavia kansioita tai tiedostoja, vaan ohjelmisto löytää ne itse kun lähteeksi on valittu toinen varmuuskopiointitehtävä. Ohjelmistossa on myös mahdollista luoda perinteisiä magneettinauhavarmuuskopioita suoraan palvelimien tiedostoista, valitsemalla tehtävän tyypiksi ”Files to Tape”.



Kuva 6 – Varmuuskopiointitehtävän lähteen valinta

4.4 Järjestelmän jatkokehitys

Uuden järjestelmän tuotantokäyttöön ottamisen jälkeen kehitettiin sitä edelleen. Suurin osa muutoksista oli tuotantokäytössä esiintyneiden asioiden kehittämistä ja korjaamista. Aiemmin mainittu magneettinauhavarmuuskopion ajastuksen muuttaminen sekä tietokantojen pilvipalveluun siirrettävien kopioiden määrän hienosäätäminen ovat esimerkkejä tällaisista toimenpiteistä. Myös itse päävarmuuskopiointitehtävän palautuspisteiden määrää on hiljalleen nostettu optimaalisen tilankäytön takaamiseksi.

4.4.1 Magneettinauha-aseman uudistaminen

Käytössä ollut ”LTO-4”-standardin mukainen asema ja sen kasetit alkoivat olla elinkaarensa lopussa. Kasettien 800 Gt tallennuskapasiteetti aiheutti sen että runsaan teratavun kokoinen varmuuskopio jouduttiin jakamaan useammalle kasetille aiheuttaen ylimääräisiä kasetinvaihtoja. Aiemmin tehdyn selvitystyön perusteella todettiin, että magneettinauha-aseman korvaaminen uudemmalla ”LTO-6”-standardin mukaisella vastaavalla asemalla oli sopivin ja kustannustehokkain ratkaisu. Uusien kasettien tarjoama 2,5 Tt tallennuskapasiteetti riittää hyvin nykyisiin tarpeisiin ja jättää myös kasvuvaraa. Varmuuskopiointiohjelmisto asetettiin luomaan korkeintaan yksi varmuuskopio yhdelle nauhalle. Jos ohjelmiston asetukset olisivat vanhan aseman asetusten mukaiset, olisi käytettävissä oleva tallennuskapasiteetti ollut huomattavasti suurempi. Asetuksia päätettiin kuitenkin muuttaa helpomman hallittavuuden, riittävän kasvuvaran ja paremman turvallisuustason saavuttamiseksi. Järjestely takaa sen että paloturvakaapissa on korkeintaan viikon vanha varmuuskopio. Magneettinauhojen huokea hinta merkitsi että niitä voitiin hankkia riittävä määrä joten palautuspisteiden määrää ei jouduttu pienentämään järjestelyn vuoksi.

4.4.2 NAS-palvelimen uudistaminen

Alkuperäinen NAS-palvelin päätettiin siirtää sisäiseen käyttöön ja tilalle hankittiin uusi vastaavanlainen palvelin suuremmalla tallennuskapasiteetilla ja modernimmalla laitteistolla. Uuden palvelimen käytettävissä oleva tallennuskapasiteetti on 8 Tt. Tallennuskapasiteetti on moninkertainen verrattuna edellisen palvelimen 3 Tt tallennuskapasiteettiin joka sekin oli toimeksiantajalle riittävä. Uusi palvelin asetettiin myös RAID10 (1+0) tilaan joka tarjoaa edellisen palvelimen käyttämään RAID5 tilaan verrattuna hieman korkeampaa suorituskykyä ja joissakin tilanteissa parempaa vikasietoisuutta käytettävissä olevan tallennuskapasiteetin kustannuksella (Bosworth et al. 2014 s. 1631).

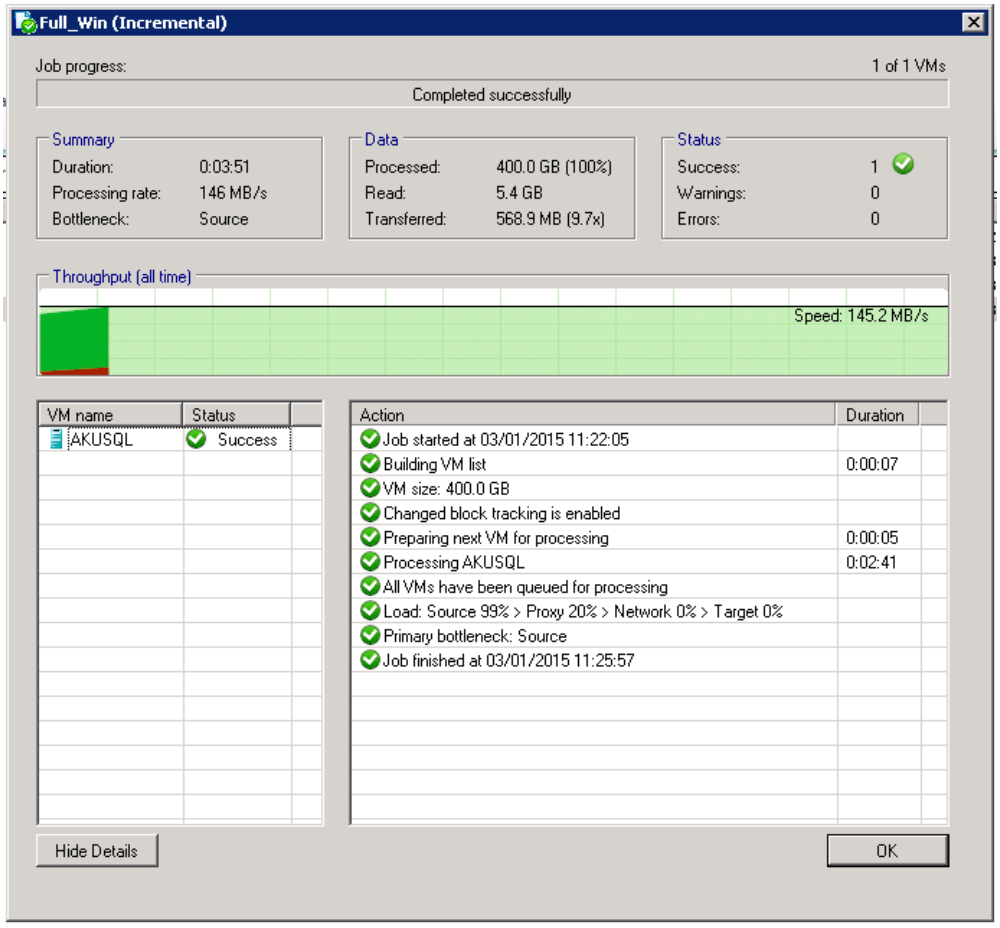
5 JOHTOPÄÄTÖKSET

Modernisoitu varmuuskopiointijärjestelmä on kirjoitushetkellä ollut tuotantokäytössä noin vuoden. Työn tavoitteena oli modernisoida toimeksiantajan varmuuskopiointijärjestelmä ja saada se tuotantokuntoon. Tämä tavoite on saavutettu.

Lähes jokainen järjestelmän komponentti uudistettiin. Varmuuskopiointiohjelmisto vaihtui kokonaan toisen valmistajan tuotteeseen. Päätallennuspalvelin sekä magneettinauhajärjestelmä vaihdettiin nykyaikaisempaan, mutta vastaavaan laitteistoon. Lisäksi otettiin käyttöön kiinteistön ulkopuolella sijaitseva varmuuskopio katastrofitilanteita varten. Varmuuskopiointistrategia perustuu edelleen viikon mittaiseen sykliin, mutta strategiaa yksinkertaistettiin ja selkeytettiin. Päätallennuspaikasta löytyy nyt jokaiselle päivälle palautuspiste yli 90 päivää taaksepäin, ja palautuspisteiden määrää on vielä mahdollista nostaa. Magneettinauha-arkistossa on tilaa kuukausittaisille palautuspisteille yli vuoden taaksepäin. Uusi magneettinauhajärjestely vaatii vähemmän manuaalista työtä ja se on selkeämpi myös asiaan perehtymättömälle.

Uusi varmuuskopiointiohjelmisto on osoittautunut joitakin ongelmia lukuun ottamatta toimivaksi. Ongelmat ovat liittyneet versiopäivityksissä ilmenneisiin ongelmiin, joista olisi voitu välttyä odottamalla ensimmäisen korjauspäivityksen ilmentymistä ennen uuteen versioon siirtymistä. Ongelmat kielivät kuitenkin riittävän testauksen puutteesta valmistajan osalta. Valmistajan tukipalvelut ovat kuitenkin osoittautuneet erinomaisiksi ja korjauksia ongelmiin on aina saatu samana päivänä. Hyvänä uudistuksena verrattuna toimeksiantajan vanhaan varmuuskopiointiohjelmistoon on että jokaisessa varmuuskopioinnissa kopioidaan koko virtuaalipalvelin eikä vain palvelimella olevia tiedostoja. Kuten kuva 7 osoittaa menee yhden kokonaisen virtuaalipalvelimen varmuuskopioimiseen noin 5 minuuttia, joten koko virtuaalipalvelimen varmuuskopioiminen aina ennen huoltotyön aloittamista on osoittautunut erinomaiseksi käytännöksi. Oivana esimerkkinä on tilanne jossa erään taloushallinnon käyttämän ohjelmiston päivityksessä ilmeni ongelma. Mahdollisuus palauttaa ohjelmiston tietokanta sekä jokin tai kaikki ohjelmiston tiedostoista päivityksen aloitusta edeltävään tilaan minuuteissa helpotti ongelmanratkontaprosessia huomattavasti. Myös tilanteessa jossa yksi alustapalvelimista ei levyohjaimen ohjelmistopäivityksen epäonnistumisen jälkeen enää käynnistynyt oli helppoa

palauttaa virtuaalipalvelinten varmuuskopiot toiselle alustapalvelimelle alkuperäisen palvelimen huoltotöiden ajaksi.



Kuva 7 – Yksittäisen virtuaalipalvelimen varmuuskopiointi

Pilvivarmuuskopiointipalvelu on toiminut moitteetta. Asiakasohjelmisto ei ole vaatinut toimenpiteitä eikä palautuksia ole tarvittu testauksia lukuun ottamatta tehdä pilvipalvelusta.

Järjestelmästä löytyy toki vielä kehitettävää. Itse varmuuskopiointiohjelmisto on tällä hetkellä asennettu yhdelle alustapalvelimista. Tämä ei ole hyvien käytäntöjen mukaista, ja se asennettiin kyseiselle palvelimelle lähinnä historiallisista syistä käyttöönoton nopeuttamiseksi. Koska Veeam Backup & Replication ei varmuuskopioi fyysisiä palvelimia, joutuisi ohjelmiston asentamaan uudelleen toiselle palvelimelle tilanteessa jossa alustapalvelin rikkoutuisi. Ohjelmisto varmuuskopioi tosin omat asetuksensa päivittäin,

ja ohjelmiston asennus on nopeaa, joten palautuminen ei kestäisi kauaa. Alustapalvelin on toki myös mahdollista palauttaa USB-kiintolevyltä, mutta tuotantoon palaaminen olisi todennäköisesti nopeampaa jos virtuaalipalvelimet voitaisiin palauttaa suoraan toiselle alustapalvelimelle varmuuskopiointiohjelmistolla. Ohjelmiston asennuksen jälkeen siihen lisätään vain varmuuskopioiden sijainti, jonka jälkeen ohjelmistoon palautetaan asetusten varmuuskopio. Palautuminen olisi vielä nopeampaa, jos ohjelmisto asetettaisiin pitämään toisella alustapalvelimella ajan tasalla olevaa kopiota virtuaalipalvelimesta jolla ohjelmisto on asennettu. Tällöin voitaisiin rikkoutumistilanteessa vain käynnistää virtuaalipalvelimen kopio ja käyttää sitä suoraan. Koska tällainen ominaisuus löytyy ohjelmistosta eikä sen käyttöönotto ole hankalaa tullaan ohjelmisto todennäköisesti asentamaan omalle virtuaalipalvelimelle tulevaisuudessa.

LÄHTEET

Apple Inc. 2014.*OS X Recovery*. Luettavissa: https://www.apple.com/osx/recovery/ Haettu: 13.9.2014

Bosworth, Seymour Kabay, Michel E. Whyne, Eric. 2014, *Computer Security Handbook, Sixth Edition Set (6th Edition)*, Somerset, NJ, USA: John Wiley & Sons, Incorporated, 2207s.

Buffington, Jason. 2010, *Data Protection for Virtual Data Centers*, Hoboken, NJ, USA, John Wiley & Sons, 530s.

Crump, George. 2013 *Cloud Backup Vs. Tape: Think Hybrid*, Informationweek - Online, Manhasset, United States, UBM LLC.

Curtis, Jason. 2015, *Iomega REV (2004-2010)* Musem Of Obsolete Media. Luettavissa: http://www.obsoletemedia.org/rev/29 Haettu: 27.2.2015.

Fu, Y., Xiao, N., Liao, X. & Liu, F. 2013, *Application-Aware Client-Side Data Reduction and Encryption of Personal Data in Cloud Backup Services*, Journal of Computer Science and Technology, vol. 28, no. 6, s. 1012-1024.

Iomega. *Iomega® REV™ 35GB/90GB* Drive General Questions*. Luettavissa: https://web.archive.org/web/20130725030913/http://iomega.com/rev/rev-faq.html Haettu 18.10.2014.

Microsoft 2014. *Backup and Restore*. Luettavissa: http://windows.microsoft.com/en-us/windows7/products/features/backup-and-restore Haettu: 13.9.2014.

Microsoft 2013. *Running Domain Controllers in Hyper-V*. Luettavissa: https://technet.microsoft.com/en-us/library/virtual_active_directory_domain_controller_virtualization_hyperv%28v=ws.10%29.aspx Haettu 13.9.2014.

Mitchell, Bradley. 2014, SAN *vs. NAS What is the Difference?* Luettavissa: http://compnetworking.about.com/od/networkstorage/f/san-vs-nas.htm Haettu: 20.9.2014.

Red Hat, Inc. 2014.*Backup Technologies*. Luettavissa: https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/4/html/Introduction_To_System_Administration/s2-disaster-backups-tech.html Haettu: 13.9.2014.

Rola, Monika. 2002, *Rumours of death of tape exaggerate,*. Computing Canada;17: s.8

Skeppstedt Jonas. 2015, Back-up. *Nationalencyclopedin.* Luettavissa: www.ne.se/uppslagsverk/encyklopedi/lång/back-up Haettu: 27.2.2015.

Smith, D. 2003, *The Cost of Lost Data.* Graziadio Business Review, no. 3. Luettavissa: http://gbr.pepperdine.edu/2010/08/the-cost-of-lost-data/ Haettu 18.10.2014.

Symantec Corporation 2011.*Symantec Backup Exec 2012 datasheet.* Luettavissa: http://www.symantec.com/content/en/us/enterprise/fact_sheets/b-backup_exec_2012_overview_DS_21218370.en-us.pdf Haettu: 13.9.2014.

Symantec Corporation 2015. *Introducing Backup Exec 2014*. Haettu: 22.1.2015. Luettavissa: http://www.symantec.com/page.jsp?id=introducing-backup-exec-2014

The LTO Program. 2014, *LTO Ultrium Roadmap.* Luettavissa: http://www.lto.org/wp-content/uploads/2014/09/LTO_10GenChart_2014-e1410340087608.jpeg Haettu: 21.9.2014.

Veeam Software 2014a. *Veeam Backup and replication datasheet*. Haettu: 5.2.2014. Luettavissa: http://www.veeam.com/veeam_vas_8_hyperv_datasheet_en_ds.pdf

Veeam Software 2014b. *Product Overview*. Luettavissa: http://www.veeam.com/veeam_backup_8_overview_en_ds.pdf Haettu: 5.2.2014.

Veeam Software 2014c. *Veeam Availability Suite Editions Comparison.* Luettavissa: http://www.veeam.com/veeam_vas_8_editions_comparison_en_ds.pdf Haettu: 5.2.2014.

Wallace, Michael Webber, Lawrence. 2004, *Disaster Recovery Handbook,* New York, NY, USA: AMACOM Books, 416s.

LIITE - SAMMANDRAG PÅ SVENSKA

1 INLEDNING

Konstant sjunkande priser på lagringsutrymme har orsakat en explosiv ökning i lagrat data. Innehavandet av en stor mängd data medför också en ökad risk för dataförlust, något man försöker undvika med hjälp av säkerhetskopiering. Detta examensarbete baserar sig på uppdateringen av uppdragsgivarens säkerhetskopieringssystem för att uppfylla dagens krav och behov.

Målet är att modernisera uppdragsgivarens existerande lösning för säkerhetskopiering av en virtualiserad servermiljö. Med lösning menas inte endast apparatur och programvara utan även praxis och strategi. Arbetet är indelat i en teoretisk del och i en del som beskriver det praktiska arbetet. I teoridelen behandlas säkerhetskopieringens teknik och i den praktiska delen beskrivs moderniseringsprojektet. Den teoretiska delen baserar sig på en litteraturundersökning och fungerar som grund för de val som görs i den praktiska delen.

Uppdragsgivaren är Kiinko, som är ett sammansatt namn för Kiinteistöalan Koulutuskeskus Oy och Kiinteistöalan koulutussäätiö. Kiinko arrangerar utbildning för fastighetsbranschen. Aktiebolaget är grundat år 1978 och stiftelsen år 1989.

Uppdragsgivaren har två kontor. Det ena finns i Malm i Helsingfors och det andra i centrum av Helsingfors på Annegatan. Servrarna som behandlas i detta arbete finns i kontoret i Malm. Uppdragsgivarens produktionsservrar är virtualiserade på tre ”Windows Server 2008R2 Hyper-V”-servrar. Förutom dessa har uppdragsgivaren även två virtualiserade molnservrar vilkas säkerhetskopiering tjänsteleverantörer ansvarar för och behöver inte därmed beaktas i säkerhetskopieringslösningen.

2 SÄKERHETSKOPIERINGENS TEKNIK

Med säkerhetskopiering menas att man för att minska på risken för dataförlust kopierar data till ett eller flera ställen. Vanligtvis vill man kopiera ursprungliga filerna till ett fysiskt separerat lagringsmedium för att skydda sig mot hårdvarufel.

Egentligen kan man säga att det finns två huvudsakliga orsaker till säkerhetskopiering. Den första orsaken är återhämtning av data vid total dataförlust och den andra är återhämtning av data från en tidigare tidpunkt. Säkerhetskopiorna fungerar då som en typ av arkiv. Det finns ett flertal orsaker till dataförlust. Mänsklig påverkan är vanligt, men även mer oförväntade situationer såsom brand och naturkatastrofer kan orsaka dataförlust. Inbrott kan leda till dataförlust och även andra former av brott såsom dataintrång bör beaktas då man planerar ett säkerhetskopieringssystem.

Det finns flera olika sätt att skapa säkerhetskopior. Den enklaste formen av säkerhetskopiering som går att automatisera är ett enkelt skript som kopierar data till ett säkrare ställe. De flesta operativsystem erbjuder även någon form av verktyg för säkerhetskopiering. När dessa verktyg inte längre uppfyller de ställda kraven använder man sig av specialiserad programvara som sköter om hela säkerhetskopieringsprocessen. Dessa program kan schemalägga säkerhetskopieringen och krypterar, komprimerar och deduplikerar data automatiskt. Programmen kan själv övervaka säkerhetskopiorna och anmäla automatiskt om felsituationer uppstår. Man bör dock alttid även kontrollera säkerhetskopiornas integritet regelbundet för hand. Regelbundna teståterhämtningar bidrar även till att hålla återhämtningsprocessen i färskt minne inför en riktig situation. Säkerhetskopieringsprogrammen har oftast stöd för magnetband och kan upprätthålla magnetbandsarkiv.

Säkerhetskopieringsprogrammet har en central roll i ett säkerhetskopieringssystem och bör därför väljas med eftertanke. Eftersom programmet fungerar som ett gränssnitt mot arkivet av säkerhetskopior bör det sättas minst lika stor vikt på återhämtningsfunktionaliteten som på själva säkerhetskopieringsegenskaperna.

Säkerhetskopior kan förvaras på många olika sätt. Den enklaste och minst säkra formen är kopior som lagras lokalt på samma ställe som ursprunglig data. En sådan säkerhetskopia kan t.ex. vara en temporär fil som ett program skapar och kan användas för att återhämta data efter att det har skett ett elavbrott medan ursprunglig data hanterades. Ett annat lite säkrare sätt är att lagra kopian på ett annat lagringsmedium som ändå är kopplat lokalt till samma maskin t.ex. som en nätverksenhet eller som en annan lokal hårddisk. Även om en sådan säkerhetskopia har ett bättre skydd mot hårdvarufel är den i lika stor fara som den ursprunglig data om maskinen drabbas av ett skadligt program eller ett dataintrång. Säkerhetskopian kan dock vara till stor nytta om man snabbt vill återhämta en fil som t.ex. raderats av misstag. De flesta återhämtningarna gäller dataändringar som är under 14 dagar gamla.

Ännu bättre skydd ger en säkerhetskopia på ett löstagbart lagringsmedium, t.ex. ett magnetband eller en löstagbar hårddisk. I hemmabruk är hårddiskar vanliga, men magnetband är hållbarare för transport p.g.a. sin enkla uppbyggnad, mer kostnadseffektiva för större datamängder och går bra att förvara t.ex. i brandsäkra skåp p.g.a. sin kompakta storlek. Det bästa skyddet ger en säkerhetskopia som finns i en helt annan fastighet som i bästa fall är geografiskt separerad från ursprungsplatsen. Transporten blir då mer problematisk och kan medföra datasäkerhetsrisker, men kryptering och transport över Internet minskar sådana risker. Återhämtningen blir så klart aldrig lika snabb som från en lokal säkerhetskopia.

För att uppnå en bra balans mellan säkerhet och återhämtningsflexibilitet har man utvecklat ett säkerhetskopieringssystem som kallas ”3-2-1”. I sin korthet betyder det att man har totalt 3 säkerhetskopior, som man lagrar på minst 2 olika typer av lagringsmedium och en säkerhetskopia lagras utanför den fastighet där ursprunglig data finns.

För att skapa så många återhämtningspunkter som möjligt för givet lagringsutrymme har man utvecklat olika typer av säkerhetskopior. Den enklaste formen av säkerhetskopia är en s.k. full säkerhetskopia. Kopian är som namnet antyder en total kopia på all ursprunglig data. Denna typ av säkerhetskopia kräver mycket lagringsutrymme och belastar infrastrukturen och ursprungsdatorn märkbart. Man brukar schemalägga säkerhetskopieringen omkring ett visst tidsintervall, oftast en vecka beroende på organisatio-

nens verksamhet. Man vill då skapa fulla säkerhetskopior under en tid som minst påverkar verksamheten, t.ex. under veckoslut. För att kunna skapa återhämtningspunkter inne i veckan kan man sedan använda sig av andra typer av säkerhetskopior, som belastar infrastrukturen mindre och kräver mindre lagringsutrymme på bekostnad av återhämtningstiden.

Differentiella säkerhetskopior innehåller de filer som modifierats sedan den förra fulla säkerhetskopian. Detta betyder att en differentiell säkerhetskopia alltid innehåller filerna från den förra differentiella säkerhetskopian och därmed växer den enda tills nästa fulla säkerhetskopia tas. För att återhämta all data krävs då alltså den förra fulla säkerhetskopian on den nyaste differentiella säkerhetskopian. En annan form av säkerhetskopior är inkrementella säkerhetskopior. En inkrementell säkerhetskopia innehåller de filer som modifierats sedan den förra säkerhetskopian togs oberoende av vilken typ av säkerhetskopia den var. Detta betyder att man i värsta fall behöver ha hela kedjan av inkrementella säkerhetskopior och den ursprungliga fulla säkerhetskopian för att återhämta all data. De olika formerna av säkerhetskopior lämpar sig olika bra för olika lagringsmedium. En kedja av inkrementella säkerhetskopior på olika magnetband är sällan en lämplig lösning, men för lokala säkerhetskopior erbjuder en sådan kedja effektiv användning av lagringsutrymme.

3 VAL AV SÄKERHETSKOPIERINGSLÖSNING

För att skapa en kravspecifikation kartlades det nuvarande systemet. Systemet var uppbyggt kring programvaran ”Symantec Backup Exec 2012”. Den huvudsakliga lagringsplatsen var en NAS-server och förutom den lagrades även på ”LTO-4”-magnetband med 800 GB lagringskapacitet säkerhetskopior, som sedan förvarades i ett brandsäkert skåp. De fysiska ”Hyper-V”-servrarna säkerhetskopieras sedan av säkerhetskopieringsverktyget i Windows till lokala USB-hårddiskar.

Avsaknaden av en säkerhetskopia belägen utanför fastigheten identifierades som det största problemet, vars lösning blev projektets huvudsakliga mål. NAS-servern var stationerad i serverrummet och ett enkelt sätt att öka på säkerheten var att flytta den till ett

annat lämplingt rum i andra ändan av byggnaden. Säkerhetskopieringsprogrammet upplevdes vara svåranvänt och vid närmare granskning upptäcktes felkonfigureringar, som enligt leverantören berodde på att programmet var svårare att använda än tidigare versioner.

4 DEN VALDA LÖSNINGEN

En molnbaserad tjänst för att transportera och lagra säkerhetskopior utanför fastigheten togs i bruk. Till denna molntjänst speglas varje natt data som identifierades vara produktionskritiskt.

Säkerhetskopieringsprogrammet ersattes av ”Veeam Backup & Replication”, som är ett program avsett för säkerhetskopiering av virtualiserade servermiljöer. Eftersom programmet inte stöder säkerhetskopiering av fysiska servrar virtualiserades uppdragsgivarens ena DC-server. Programmet konfigurerades att skapa inkrementella säkerhetskopior varje natt och att varje veckoslut skapa en s.k. syntetisk full säkerhetskopia som sedan kopieras till magnetband. Denna syntetiska fulla kopia innehåller samma data som en full säkerhetskopia skulle innehålla, men programmet bildar den genom att först ta en inkrementell säkerhetskopia och sedan utnyttja den och tidigare säkerhetskopior för att skapa den fulla säkerhetskopian. Därmed belastas endast säkerhetskopiornas huvudsakliga lagringsenhet, NAS-servern, istället för värd- och virtualservrarna.

Magnetbanden ersattes av ”LTO-6”-band med 2,5 TB lagringskapacitet och säkerhetskopieringsstrategin för magnetbanden förenklades märkbart. NAS-servern ersattes av en motsvarande modernare server med större lagringskapacitet.

Installationen och konfigurationen gick smidigt och krävde inga avbrott, arbetet kunde utföras under normal arbetstid. Den nya programvaran kräver inte att någon klientprogramvara installeras på virtualservrarna utan en hel server kan kopieras genom att man helt enkelt inkluderar den i den schemalagda säkerhetskopieringen.

5 SAMMANFATTNING

Arbetets mål var att modernisera uppdragsgivarens säkerhetskopieringssystem. Målet är uppnått.

Trots att det huvudsakliga målet för projektet var att skapa en säkerhetskopia belägen utanför fastigheten förnyades så gott som alla delar av systemet. Det nya systemet möjliggör daglida återhämtningspunkter över 90 dagar bakåt, och månatliga över ett år. Det tar under 5 minuter att ta en säkerhetskopia på en enskild virtualserver vilket möjliggör att man kan ta en säkerhetskopia på hela servern alltid innan man gör ändringar.

Systemets uppbyggnad kunde ytterligare utvecklas genom att virtualisera servern för själva säkerhetskopieringsprogramvaran vilket skulle möjliggöra en flexiblare återhämtningsprocess.