TAMPEREEN
AMMATTIKORKEAKOULU

VIRTUALISOIDUN PALVELINYMPÄRISTÖN VARMENTAMINEN

Lauri Itävuori

Opinnäytetyö
Marraskuu 2015
Tietojenkäsittelyn koulutusohjelma
Tietoverkkopalvelut

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tietojenkäsittelyn koulutusohjelma
Tietoverkkopalvelut

ITÄVUORI, LAURI:
Virtualisoidun palvelinympäristön varmentaminen

Opinnäytetyö 47 sivua
Marraskuu 2015

Tämän opinnäytetyön tavoitteena oli kehittää Prima Pet Premium Oy:n virtualisoidun palvelinympäristön varmistusratkaisua luotettavammaksi, tehokkaammaksi ja helpommin hallittavaksi. Palvelinvarmistusten toimivuus ja varmuuskopioiden palautuskyky ovat yritystoiminnan jatkuvuuden kannalta merkityksellisiä, koska sähköisessä muodossa oleva tieto on osa yritysten tärkeintä pääomaa. Siksi varmistusratkaisujen ylläpitoon ja kehittämiseen tulee panostaa osana yritysten IT-toimintojen kehittämistä.

Työn tarkoituksena oli etsiä Prima Pet Premium Oy:n tarpeita vastaava varmistusohjelmisto yrityksen nykyisen varmistusratkaisun korvaajaksi. Tavoitteen saavuttamiseksi opinnäytetyössä määritellään vaatimukset uudelle varmistusratkaisulle, suunnitellaan tarvittavat ohjelmisto- ja laitehankinnat, suoritetaan asennukset, otetaan varmistusratkaisu käyttöön ja testataan sen toimivuus eri tilanteissa.

Työssä syvennytään uuden varmistusratkaisun vaatimusmäärittelyyn, varmistusympäristön luomiseen valittuun ohjelmistoon, palvelinvarmistustöihin sekä palautusten testaukseen. Opinnäytetyön valmistuttua varmistusohjelmiston käytöstä laaditaan ohjeistus toimeksiantajayrityksen IT-osaston työntekijöiden käyttöön sekä kehitetään toipumissuunnitelma palvelinympäristön katastrofitilanteisiin.

Asiasanat: varmuuskopiointi, palvelinvarmistus, virtualisointi, palvelin

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
Degree Programme in Business Information Systems
Network Services

ITÄVUORI, LAURI:
Backing Up a Virtualized Server Environment

Bachelor's thesis 47 pages
November 2015

This thesis was commissioned by Prima Pet Premium Oy. The main goal was to improve in-place backup solution for virtualized server environment in a way that the overall solution would be easier to manage, more reliable and performing better.

The purpose of this thesis was to search for a suitable server backup solution which would then be used to replace Prima Pet Premium Oy's former backup software. In order to achieve these goals a requirement definition for new backup software was drawn up, compulsory software and hardware purchases were planned and installations and server restoration tests performed according to plan.

The main focus of this thesis is the requirements for a new solution, building a backup environment for the chosen backup software, creating server backup tasks and restoring servers and objects from backup files. A usage guide of the chosen backup software for employees' will be conducted in the near future along with disaster recovery plan.

Key words: backup, server backup, virtualization, server

SISÄLLYS

1 JOHDANTO 7
2 VIRTUALISOINTI JA TIEDON VARMISTAMINEN 8
2.1 Virtualisointi 8
2.2 Tiedon varmistaminen 9
3 TOIMEKSIANTAJAYRITYKSEN VARMISTUSYMPÄRISTÖ 10
3.1 Palvelinympäristön kuvaus 10
3.2 Korvattava palvelinvarmistusratkaisu 11
4 VARMISTUSRATKAISUN VAATIMUKSET JA HANKINTA 13
4.1 Vaatimukset uudelta varmistusratkaisulta 13
4.2 Valittu varmistusratkaisu 14
4.2.1 Palautuspisteiden lukumäärä 15
4.2.2 Varmistustavan valinta 16
4.2.3 Tallennusjärjestelmän tallennustilavaatimukset 17
4.3 Laitteisto- ja ohjelmistohankinnat 20
5 PALVELINYMPÄRISTÖN VALMISTELU 22
5.1 Tiedonsiirtotavan valinta 22
5.2 Muuttuneiden sektorien seuraaminen 24
6 VARMISTUSPALVELIMEN ASENNUS JA SUORITUSKYKY 26
6.1 Palvelimen asennus 26
6.2 Kiintolevyjärjestelmän suorituskyvyn mittaaminen 27
7 VARMISTUSRATKAISUN KÄYTTÖÖNOTTO 30
7.1 Varmistusohjelmiston asennus ja yhdistäminen palvelinympäristöön 30
7.2 Veeam Backup Proxy -tiedonsiirtopalvelinten luominen 31
7.3 Veeam Backup Repository -tallennussijainnin luominen 32
7.4 Veeam Tape Server -palvelinroolin luominen 33
8 PALVELINVARMISTUSTÖIDEN LUOMINEN 35
9 PALAUTUSTÖIDEN TESTAUS 37
10 KEHITYSEHDOTUKSET 39
11 POHDINTA 41
LÄHTEET 43

LYHENTEET JA TERMIT

AAIP	*Application-Aware Image Processing* - Varmistustyön asetus, jolla luodaan transaktioyhtenäinen varmuuskopio
Active Full Backup	Täysi varmuuskopio, joka otetaan käynnissä olevasta palvelimesta
Backup Proxy	Tiedonsiirtäjä lähde- ja kohdejärjestelmän välillä
Backup Repository	Varmuuskopiotiedostojen tallennussijainti
CBT	*Changed Block Tracking* - Tekniikka, jolla seurataan palvelinten virtuaalilevyillä tapahtuneita muutoksia
CIFS	*Common Internet File System* - Protokolla tiedostojen jakoon tietoverkoissa
Deduplication	Menetelmä, jossa tietolohkoja vertaillaan keskenään ja vain poikkeavat lohkot tallennetaan
GFS	*Grandfather-Father-Son* - Varmistusrakenne, jossa luodaan eritasoisia varmuuskopioita
GPT	*GUID Partition Table* - Kiintolevyn osiointijärjestelmä
GRT	*Granular Recovery Technology* - Mahdollistaa yksittäisen objektin palauttamisen varmuuskopiosta ilman koko varmuuskopion palauttamista
HBA	*Host Bus Adapter* - Laajennuskortti isäntä- ja tallennuslaitteen yhdistämiseen
Incremental Backup	Varmuuskopio, joka sisältää vain edellisestä varmuuskopiosta muuttuneen tiedon
Media Pool	Looginen ryhmä, johon magneettinauhat kuuluvat
Media Set	Jatkuva tietovirta, joka voi lomittua useille yksittäisillä magneettinauhoille
NBD	*Network Block Device* - Protokolla kiintolevyjärjestelmän simuloimiseen asiakaslaitteelle verkkoyhteyden yli
NFS	*Network File System* - Protokolla tiedostojen käsittelyyn verkkoyhteyden yli paikallisen tiedostojärjestelmän tapaan
NTFS	*New Technology File System* - Windows-käyttöjärjestelmän tiedostojärjestelmä
Restore Point	Palautuspiste

Retention Period	Säilytettävien palautuspisteiden lukumäärä
SAN	*Storage Area Network* - Verkko, joka yhdistää tallennuslaitteet niitä käyttäviin palvelimiin
SAS	*Serial Attached SCSI* - Tietokoneväylä kiintolevyjen liittämiseen isäntälaitteeseen
Sequential Write	Tallennettavat tietolohkot kirjoitetaan kiintolevylle peräkkäin
Snapshot	Tilannevedos, jolla tallennetaan virtuaalipalvelimen nykytila ja johon voidaan palata
Synthetic Full Backup	Täysi varmuuskopio, joka luodaan yhdistämällä inkrementaalit varmuuskopiot edelliseen täyteen varmuuskopioon
Thick Provision	Virtuaalipalvelimen virtuaalilevyn koko määritetään palvelinta luotaessa
VMDK	*Virtual Machine Disk* - Virtualisointijärjestelmän käyttämien virtuaalilevyjen tiedostomuoto

1 JOHDANTO

Tämän opinnäytetyön tavoitteena on kehittää Prima Pet Premium Oy:n *virtualisoidun* palvelinympäristön varmistusratkaisua. Työn tarkoituksena on löytää toimeksiantajayrityksen tarpeita vastaava varmistusohjelmisto, jolla yrityksen nykyinen varmistusratkaisu korvataan. Tavoitteen saavuttamiseksi opinnäytetyössä määritellään vaatimukset uudelle varmistusratkaisulle, suunnitellaan tarvittavat ohjelmisto- ja laitehankinnat, suoritetaan asennukset, otetaan varmistusratkaisu käyttöön ja testataan sen toimivuus eri tilanteissa.

Prima Pet Premium Oy on vuonna 1999 perustettu pirkkalalainen, täysin kotimaisessa omistuksessa oleva, lemmikkieläinten ruoka- ja tarvikemaahantuojayritys. Yrityksen tunnetuimpia omia tuotemerkkejä ovat Hau Hau Champion, PrimaCat ja Planet Pet Society. Prima Pet Premium Oy:n myyntiverkosto kattaa koko Suomen ja vientiä harjoitetaan useisiin Euroopan maihin sekä Venäjälle. Hankinnat tapahtuvat pääasiassa Euroopan ja Aasian alueilta. Yrityksen vuoden 2014 liikevaihto oli yli 25 miljoonaa euroa. (Prima Pet Premium Oy 2015.)

Toimeksiantajayrityksen sisäinen IT-osasto vastaa yrityksen tieto- ja viestintäteknisestä toiminnasta. Palvelin- ja verkkoympäristö ovat suurelta osin yrityksen omassa omistuksessa ja hallinnassa. Osa tarvittavasta sovelluskehityksestä sekä haastavasta suunnittelu- ja asiantuntijapalvelusta hankitaan yrityksen ulkopuolelta. (Prima Pet Premium Oy 2015.)

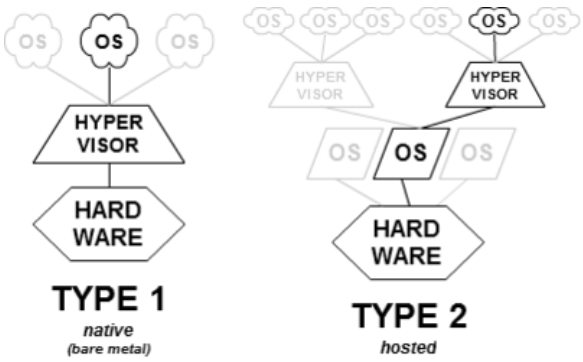
Opinnäytetyö painottuu uuden varmistusratkaisun vaatimusmäärittelyyn, varmistusympäristön luomiseen valittuun ohjelmistoon, palvelinvarmistustöihin sekä palautusten testaukseen. Työssä ei syvennytä asennuksessa käytettäviin Windows Server -palvelinkäyttöjärjestelmiin tai varmistusohjelmiston asennusvaiheisiin. Opinnäytetyön valmistuttua varmistusohjelmiston käytöstä laaditaan ohjeistus yrityksen IT-osaston työntekijöiden käyttöön sekä kehitetään toipumissuunnitelma palvelinympäristön katastrofitilanteisiin.

2 VIRTUALISOINTI JA TIEDON VARMISTAMINEN

2.1 Virtualisointi

Virtualisointi on teknologiaresurssien yhteen kokoamista ja jakamista. Sen tavoitteena on helpottaa tietoteknisten resurssien hallintaa ja lisätä niiden käyttöastetta vastaamaan liiketoiminnan haasteita nopeasti muuttuvassa toimintaympäristössä. (Golden 2011, 3.)

Palvelinympäristössä virtualisointia käytetään yhden fyysisen omaisuuden (asset) toiminnan muuntamiseen niin, että se näyttäytyy useana omaisuutena (Golden 2008, 10). Tämä saavutetaan hyödyntämällä niin sanottuja *hypervisoreita*. Hypervisori on tietokoneohjelma, laiteohjelmisto tai laitteisto, jonka avulla useat vieraskäyttöjärjestelmät voivat jakaa yhden fyysisen laitteen resursseja. Hypervisori ohjaa laitteiston laiteresursseja kohdistaen niitä vieraskäyttöjärjestelmille, joita kutsutaan myös virtuaalikoneiksi, varmistaakseen niiden keskeytyksettömän toiminnan. (Rouse 2006.) Hypervisorit voidaan jakaa tyypin 1 ja 2 hypervisoreihin niiden toimintatavan mukaisesti. Tyypin 1 hypervisoria suoritetaan suoraan isäntälaitteessa kun taas tyypin 2 hypervisori toimii isäntälaitteen käyttöjärjestelmässä (kuva 1). (Virtzone 2015.)



KUVA 1. Hypervisoreiden toimintatavat (Wikipedia-käyttäjä Scsami 2011)

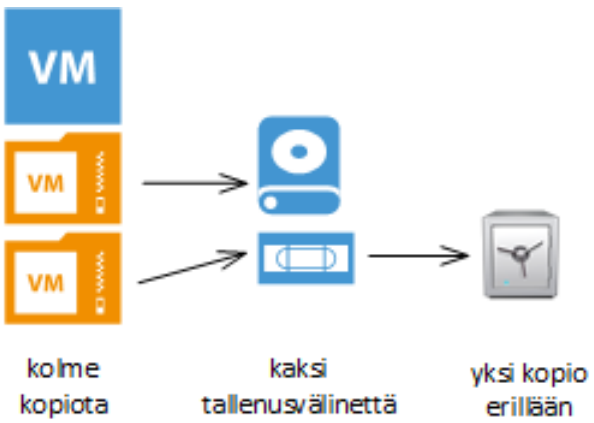
Virtualisointi on nykyaikainen ratkaisu palvelinkapasiteetin hallintaan. Sen avulla laiteresurssien jakaminen on helpompaa ja yli- sekä aliprovisiointia pystytään välttämään kohdentamalla virtuaalipalvelimille vain tarvittava määrä resursseja. Lisäksi virtualisointi vähentää tarvittavan laitteiston määrää, mikä tuo säästöjä laitehankinnoissa, sähkönkulutuksessa ja palvelintilojen kokovaatimuksissa. (Golden 2011, 4-11).

2.2 Tiedon varmistaminen

Sähköinen tieto on osa yritysten tärkeintä pääomaa ja tarve sen varmistamiseen lisääntynyt (Hewlett-Packard 2004). Tieto tulee olla aina saatavilla, luottamuksellista ja eheää (Mäkelä 2014). Varmistuksilla pyritään huolehtimaan tiedon saatavuudesta tilanteissa, joissa alkuperäinen tieto ei ole käytettävissä tai se on muuttunut ei-toivotulla tavalla. Syitä alkuperäisen tiedon käyttökelvottomuuteen voivat olla esimerkiksi laiterikko, haittaohjelma tai inhimillinen virhe. (Krogh 2015.)

Varmuuskopiointi on yksi tiedon varmistustavoista. Siinä tietoa kopioidaan ja talletetaan, jotta se voidaan tarvittaessa palauttaa varmuuskopiosta (Krogh 2015). Varmuuskopioinnissa käytettävät tallennusvälineet voivat olla esimerkiksi kiintolevyjä, magneettinauhoja tai optisia levyjä. Nykyaikaisilla varmistusohjelmistoilla varmuuskopioita voidaan tallentaa myös julkisten tietoverkkojen välityksellä esimerkiksi IT-palveluntarjoajan konesaliin tai yrityksen toiseen toimipisteeseen. (Ward 2015.)

Varmistusratkaisuilla luotuja varmuuskopiotiedostoja tulee testata aika ajoin niiden palautuskyvyn varmistamiseksi. Varmuuskopioita suositellaan säilytettävän useilla eri tallennusvälineillä ja fyysisesti toisista erillään. Hyvän varmistuskäytännön mukaisesti tiedon varmistuksessa suositellaankin noudatettavan niin sanottua 3-2-1 -sääntöä, jossa tiedosta tulee olla vähintään kolme kopiota, kahdella eri tallennusvälineellä ja yhtä varmuuskopioista säilyttää erillään muista (kuva 2). (Levkina 2014.)



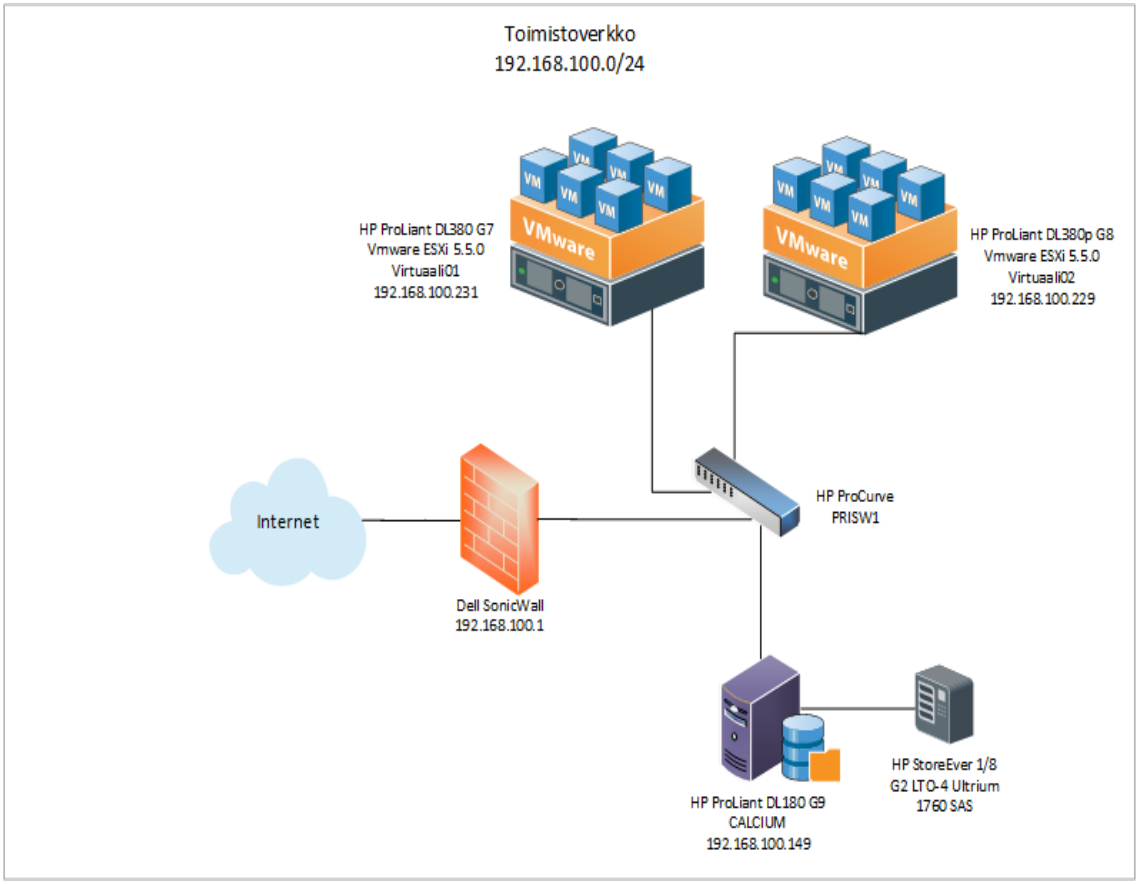
KUVA 2. 3-2-1 -varmistussääntö

3 TOIMEKSIANTAJAYRITYKSEN VARMISTUSYMPÄRISTÖ

3.1 Palvelinympäristön kuvaus

Prima Pet Premium Oy:n palvelinympäristö on suurelta osin virtualisoitu. Käytetty virtualisointialusta on VMware ESXi 5.5, joka on VMware-ohjelmistoyhtiön kehittämä tyypin 1 hypervisoriohjelmisto. Toimeksiantajan virtualisoitu palvelinympäristö koostuu kolmesta fyysisestä ESXi-isäntäpalvelimesta, jotka on liitetty yrityksen lähiverkkoon HP ProCurve -kytkimen avulla.

Lisäksi palvelinympäristöön kuuluu kaksi fyysistä palvelinta. Niistä toinen on yrityksen vanha varmistuspalvelin ja toinen tässä opinnäytetyössä tehdyn vaatimusmäärittelyn mukaan hankittu uusi varmistuspalvelin nimeltään ”CALCIUM”. Kaikki palvelimet kuuluvat aliverkkoon 192.168.100.0/24. Kuvassa 3 on esitetty toimeksiantajayrityksen palvelinympäristö varmistusratkaisun oleellisimmilta osin.



KUVA 3. Prima Pet Premium Oy:n tietoverkkotopologia

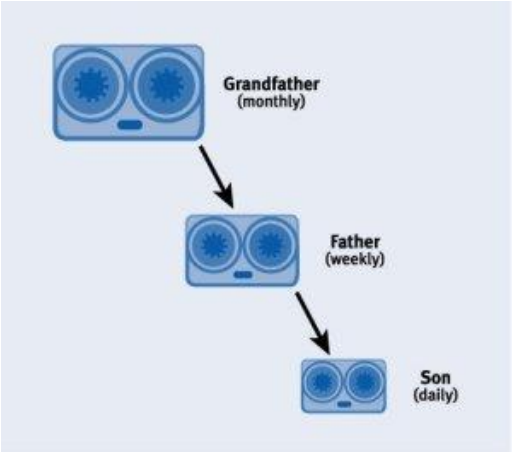
3.2 Korvattava palvelinvarmistusratkaisu

Yrityksen palvelinvarmistus oli toteutettu Symantec Backup Exec -varmistusohjelmistolla. Backup Exec on agenttiavusteinen varmistusohjelmisto, mikä tarkoittaa, että jokaiselle varmistettavalle palvelinkäyttöjärjestelmälle tulee asentaa ohjelmiston käyttämä agenttikomponentti. Se lukee tietoa varmistettavan palvelimen kovalevyltä ja lähettää sitä varmistuspalvelimelle. (Lewis 2012.)

Varmistuspalvelin kirjoitti luodut varmuuskopiot magneettinauhoille, joita käytettiin niiden ainoana tallennusvälineenä. Magneettinauhat ovat perinteinen ja edelleen käytetty tapa tiedon pitkäaikaiseen säilytykseen, vaikka kiintolevyperusteinen varmuuskopiointi on lisääntynyt. Nauhojen arvo suhteessa niiden tallennuskapasiteettiin on kiintolevyjä parempi, vaikka levyjen hinnat ovat laskeneet ja tallennustila kasvanut. Nykyaikaisissa varmistusympäristöissä nauhoja suositellaan käytettävän varmuuskopioiden toissijaisena tallennusvälineenä niiden suuren tallennuskapasiteetin ja korkean kirjoitusnopeuden ansiosta. Nauhojen heikkoutena vastaavasti nähdään palautusoperaatioiden hitaus, koska niiden lukunopeus on matala. (Lock 2010.)

Toimeksiantajayrityksen varmistusratkaisussa magneettinauhoja ohjattiin HP StoreEver 1/8 G2 LTO-4 Ultrium 1760 SAS -nauha-asemalla. Asemassa on kahdeksan nauhapaikkaa LTO-4 -tekniikan mukaisille magneettinauhoille. Yhdessä paikoista säilytettiin puhdistusnauhaa aseman kirjoitinpään puhdistamiseen. Nauha-asema oli yhdistetty varmistuspalvelimeen SAS-tekniikalla (Serial Attached SCSI). Nauha-aseman yhdistämiseksi varmistuspalvelimen PCI Express -väylään oli asennettu HBA -laajennuskortti (Host Bus Adapter). Se on tiedon lukemis- ja kirjoitustyöhön (I/O) kykenevä piirikortti, joka yhdistää isäntäjärjestelmän tallennuslaitteeseen (Sliwa 2015).

Varmistustöissä sovellettiin GFS-varmistusrakennetta (Grandfather-Father-Son), joka on käytetyimpiä tallennusvälineiden kierrätyssuunnitelmia nauhatallennusympäristöissä. GFS-rakenteessa eritasoisia varmuuskopioita säilytetään eri ajanjaksoja. Niitä voivat olla esimerkiksi päivittäiset, viikoittaiset ja kuukausittaiset varmuuskopiot (kuva 4). (Veeam Help Center 2015.) Toimeksiantajayrityksen varmistusrakenne koostui kuukausittaisista (Grandfather), viikoittaisista (Father) ja päivittäisistä (Son) varmistuksista.



KUVA 4. GFS-varmistusrakenne (Niktips 2012)

Magneettinauhoja kierrätettiin kierrätyssuunnitelman mukaisesti. Viikkonauhat (kahdeksan kappaletta) vaihdettiin viikoittain ja kuukausinauhat (kuusi kappaletta) kuukausittain. Viikkovarmistustyöt käyttivät *inkrementaalia* varmistustapaa, jossa vain edellisestä varmistuskerrasta muuttunut tieto tallennetaan uuteen varmuuskopioon (Microsoft TechNet 2015). Inkrementaalit varmuuskopiot luotiin ajastetusti arkisin vuorokauden vaihduttua ja täydet varmuuskopiot joka viikon perjantaina. Kuukausivarmistustyöt oli ajastettu luomaan täydet varmuuskopiot kuukauden viimeisenä lauantaina. 3-2-1 -varmistussäännön mukaisesti kierrätettyjä nauhoja säilytettiin muista varmuuskopioista erillään toimiston ulkopuolella.

4 VARMISTUSRATKAISUN VAATIMUKSET JA HANKINTA

4.1 Vaatimukset uudelta varmistusratkaisulta

Toimeksiantajayrityksen toiveena oli korvata Symantec Backup Exec varmistusratkaisulla, joka hyödyntää paremmin virtualisoidun palvelinympäristön luomia mahdollisuuksia. Ratkaisun haluttiin keskustelevan palvelinten virtualisointijärjestelmän kanssa ja toimimaan ilman vieraskäyttöjärjestelmille asennettavia ohjelmistoagentteja. Oli tärkeää, että ratkaisu loi varmuuskopiot suoraan varmistettavan palvelimen virtuaalilevytiedostosta, joka sisältää kaikki perinteisen kiintolevyn rakenneominaisuudet (VMware Virtual Disks 2007, 2). Lisäksi toimeksiantaja toivoi, että varmistusratkaisu tukee varmuuskopiointia magneettinauhoille, koska yrityksellä on vaadittava laitteisto nauhatallennukseen. (Majamäki 2015.)

Kehityspäällikkö Majamäen (2015) mukaan uuden varmistusratkaisun piti helpottaa luotujen varmuuskopioiden palautuskyvyn testausta, koska sitä ei ollut tehty järjestelmällisesti. Vaikka tiedostotason palautukset vanhalla varmistusratkaisulla onnistuivat, ei tiedetty olivatko luodut täydet varmuuskopiot palautuskykyisiä. Varmuuskopiotiedostojen palautuskyky haluttiin varmistaa esimerkiksi tiedostojen korruptoitumisen havaitsemiseksi.

Uuden varmistusratkaisun tavoitteena oli varmistaa yritystoimintaan ja palvelinympäristön toimintakykyyn eniten vaikuttavat palvelimet (taulukko 1). Lisäksi toiveena oli, että varmistusratkaisu *skaalautuu* palvelinympäristön kasvuun, jotta uusia palvelimia kyetään varmistamaan tarvittaessa. Skaalautuvuus tuli huomioida soveltuvan ratkaisun valinnassa ja hankintojen suunnittelussa niin, että lisähankintoja ei tarvita lähitulevaisuudessa. (Majamäki 2015.)

TAULUKKO 1. Toimeksiantajayrityksen varmistettavat virtuaalipalvelimet

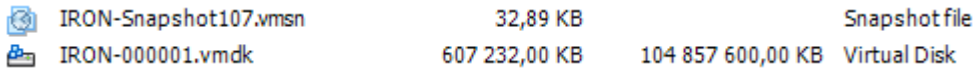
Isäntänimi	Käyttöjärjestelmä	Roolit
Iron	Windows Server 2012	Tietokanta, toiminnanohjausjärjestelmä, tiedostojako, raportointi, tilaussanomanvälitys
Carbon	Windows Server 2012	Tilausjärjestelmä, Domain Controller
Cobalt	Windows Server 2012 R2	Virustorjunta, pikaviestin, tulostimet
Gold	Windows Server 2008 R2	Sähköposti
Helium	Windows Server 2012 R2	Verkkokaupat
Oxygen	Windows Server 2012 R2	Toiminnanohjausjärjestelmä

4.2 Valittu varmistusratkaisu

Opinnäytetyössä syvennytään tutkimaan Veeam Backup and Replication -varmistusohjelmiston soveltuvuutta yrityksen palvelinympäristöön. Ratkaisuvaihtoehtoja tutkittaessa tutustuttiin myös muihin varmistusohjelmistoihin, mutta niitä ei käsitellä tässä opinnäytetyöraportissa.

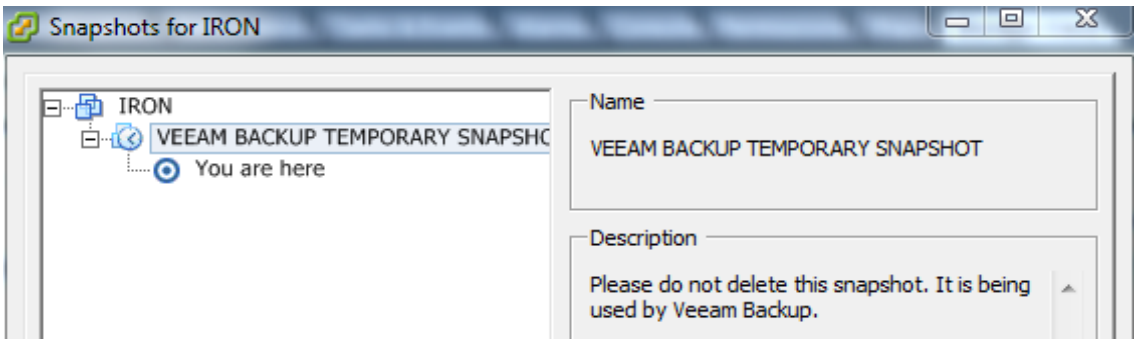
Veeam Backup and Replication, myöhemmin Veeam B&R, on kiintolevyperusteinen varmistusohjelmisto. Se tarkoittaa, että luotujen varmuuskopiotiedostojen ensisijaisena tallennusvälineenä on kiintolevyjärjestelmä. Kiintolevyperusteisuuden etu muihin tallennusvälineisiin on levyjärjestelmien korkea lukunopeus, mikä johtaa tehokkaampiin palautusoperaatioihin. (Fellows 2008.) Kiintolevyperusteinen varmistusratkaisu edellyttää, että varmuuskopiot tallennetaan ensin kiintolevyjärjestelmään, josta ne voidaan siirtää esimerkiksi magneettinauhoille tai toissijaiseen levyjärjestelmään.

Varmistusohjelmisto hyödyntää palvelinvarmistuksessa virtualisointijärjestelmän tilannevedosominaisuutta (Veeam Knowledge Base 2015). Käynnissä oleva virtuaalipalvelin voidaan varmuuskopioida luotettavasti vain silloin, kun palvelimen virtuaalilevyllä ei tapahdu muutoksia. Muutokseton tila saavutetaan käyttämällä tilannevedosta, joka sisältää osittaisen kopion palvelimen virtuaalilevystä ja muutoslokitiedostoja. Tilannevedosta suoritettaessa palvelimen alkuperäinen virtuaalilevytiedosto muuttuu kirjoitussuojatuksi ja palvelimella tapahtuvat muutokset tallennetaan muutoslokeihin (kuva 5). Tilannevedoksen sulkeutuessa ne yhdistetään jälleen alkuperäiseen levytiedostoon. (VMware Knowledge Base 2010.)



KUVA 5. Tilannevedos- ja muutoslokitiedosto varmistettavan palvelimen tietovarastossa

Ohjelmisto käskyttää virtualisointijärjestelmää luomaan tilannevedoksen varmistettavasta palvelimesta varmistustyön alussa ja poistamaan sen työn päätyttyä (kuva 6) (Veeam Knowledge Base 2015). Tilannevedostoimintoa käytettäessä tulee huomioida, että muutoslokitiedostot voivat kasvaa jopa alkuperäisen virtuaalilevytiedoston kokoisiksi ja täyttää palvelimen tietovaraston (Datastore) kokonaan (Klee 2013).



KUVA 6. Tilannevedos varmistettavasta palvelimesta

Varmistusratkaisu tukee magneettinauhatallennusta varmuuskopiotiedostojen toissijaisena tallennusvälineenä. Koska ratkaisu on kiintolevyperusteinen, palautustyö nauhalta vaatii laskeutumisalueen (Landing Zone) palautettavalle varmuuskopiotiedostolle. Laskeutumisalue tarkoittaa tyhjää kiintolevytilaa, johon varmuuskopio ensin palautetaan. (Veeam Help Center 2014.) Toimeksiantajayrityksen edeltävästä varmistusohjelmistosta poiketen Veeam B&R ei tue GRT-tekniikkaa (Granular Recovery Technology) nauhatallennuksesta palautettaessa (Veeam Community Forums 2014). GRT-tekniikka mahdollistaa yksittäisen objektin palauttamisen varmuuskopiosta ilman koko varmuuskopion palauttamista (Ward 2009).

Veeam B&R -varmistusohjelmisto osoittautui soveltuvaksi varmistusratkaisuksi yrityksen palvelinympäristöön. Muita perusteita ohjelmiston valinnalle olivat sen lisensointimalli, hyvä tekninen dokumentaatio, aktiivinen käyttäjäyhteisö ja suositukset. Ohjelmisto päätettiin hankkia yrityksen ESXi-isäntäpalvelinten lukumäärän mukaisesti kolmena Veeam Backup Essentials Enterprise -ohjelmistolisenssinä kolmen vuoden ohjelmistotuella.

4.2.1 Palautuspisteiden lukumäärä

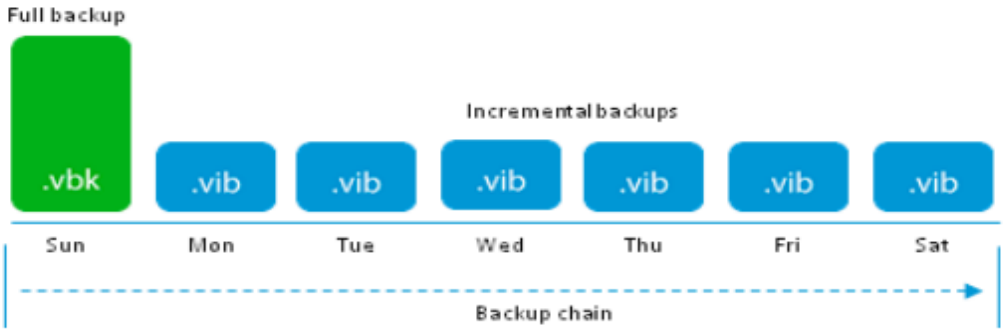
Varmistettavat palvelimet päätettiin varmuuskopioida kerran päivässä, joten palautuspisteiden määräksi (Restore Point) muodostui yksi palautuspiste vuorokaudessa. Kiintolevyllä säilytettävien palautuspisteiden lukumäärä (Retention Period) määritettiin 14 palautuspisteeseen, joten levyltä oli mahdollista palauttaa varmuuskopiot kahden viikon ajalta. Majamäen (2015) mukaan palvelinvarmistustyöt tuli ajastaa arkisen toimistotyöajan ulkopuolelle niin, että palvelinympäristöön ei kohdistu ylimääräistä kuormitusta.

Toissijaisena tallennusvälineenä toimiville magneettinauhoille päätettiin tallentaa vain viikoittaiset täydet varmuuskopiot. Nauhojen kierrätyssykliä ei määritetty ennen kuin tiedettiin täysien varmuuskopiotiedostojen koot varmistuspalvelimen kiintolevyjärjestelmässä. Tiedostojen koot määrittivät, montako täyttä varmuuskopiota nauhoille oli mahdollista tallentaa.

4.2.2 Varmistustavan valinta

Valittu varmistusohjelmisto mahdollistaa eri varmistustapojen käytön palvelinten varmistustöissä. Toimeksiantajayrityksen varmistusympäristön varmistustavaksi valittiin Forward Incremental -tapa ja täydet varmuuskopiot luotiin Active Full -tavalla. Forward Incremental -tapaa suositellaan käytettävän ympäristöissä, joissa toissijaisena tallennusvälineenä toimii magneettinauhajärjestelmä (Dell'Oca 2012). Active Full -tavalla varmistettiin, että luotu täysi varmuuskopio vastaa varmistettavan palvelimen nykytilaa, koska se otetaan suoraan tuotantoympäristössä suoritettavasta palvelimesta (Veeam Help Center 2015).

Varmistustyön ensimmäisellä suorituskerralla varmistettavasta palvelimesta luodaan täysi varmuuskopio, jota seuraavat inkrementaalit varmuuskopiot, kunnes ajastettu täysi varmuuskopio aloittaa varmistusketjun jälleen alusta (kuva 7). Täysi varmuuskopio voidaan luoda kahdella tavalla. Synthetic Full Backup yhdistää varmistusketjun inkrementit edelliseen täyteen varmuuskopioon. Active Full Backup puolestaan ottaa varmuuskopion suoraan tuotantoympäristössä suoritettavasta palvelimesta. (Veeam Help Center 2015.)



KUVA 7. Forward Incremental -varmistusketju (Dell'Oca 2015)

4.2.3 Tallennusjärjestelmän tallennustilavaatimukset

Varmistettavien palvelinten, valitun varmistustavan ja palvelinkohtaisten palautuspisteiden lukumäärän perusteella laskettiin suuntaa-antavasti varmistuspalvelimen tarvitseman kiintolevytilan määrä. Tarvittavan kiintolevytilan laskennassa suositellaan käytettävän palvelinympäristöstä saatavia tarkkoja lukuarvoja tai arvoja, jotka pätevät useimmissa palvelinympäristöissä (Dell'Oca 2015, 3). Tarvittavan kiintolevytilan laskemiseen käytettiin palvelinympäristöstä saatavaa tietoa.

Laskennassa käytetyt lukuarvot saatiin Veeam ONE -ohjelmistosta ja palvelinten virtualisointijärjestelmästä. Veeam ONE on raportointi- ja kapasiteetinsuunnitteluohjelmisto, jolla pystytään seuraamaan ja analysoimaan palvelinympäristöjä. Sen testiversio asennettiin virtuaalikoneelle ja yhdistettiin yrityksen palvelinympäristöön. Ohjelmiston VM Change Rate Estimation -raportilla selvitettiin palvelinten virtuaalilevyillä päivittäin tapahtuvien muutosten määrä gigatavuissa (taulukko 2). (Veeam Help Center 2015.) Palvelinten päivittäisistä muutoksista laskettiin keskiarvo, jota käytettiin inkrementaalien varmuuskopiotiedostojen koon arviointiin. Muutosten keskiarvoksi saatiin noin 150 gigatavua muuttunutta tietoa vuorokaudessa.

TAULUKKO 2. Varmistettavien palvelinten päivittäiset muutokset

VM	tiistai	keskiviikko	torstai	perjantai	lauantai	sunnuntai
IRON	94,38 GB	91,18 GB	98,57 GB	94,56 GB	84,59 GB	84,58 GB
GOLD	28,71 GB	22,79 GB	25,29 GB	18,79 GB	7,47 GB	5,71 GB
CARBON	6,77 GB	4,36 GB	15,08 GB	17,05 GB	14,90 GB	12,94 GB
COBALT	17,31 GB	16,57 GB	14,09 GB	9,11 GB	4,88 GB	3,43 GB
OXYGEN	4,50 GB	3,05 GB	4,48 GB	2,68 GB	1,94 GB	1,28 GB
HELIUM	1,41 GB	1,77 GB	1,14 GB	2,91 GB	< 1 GB	< 1 GB

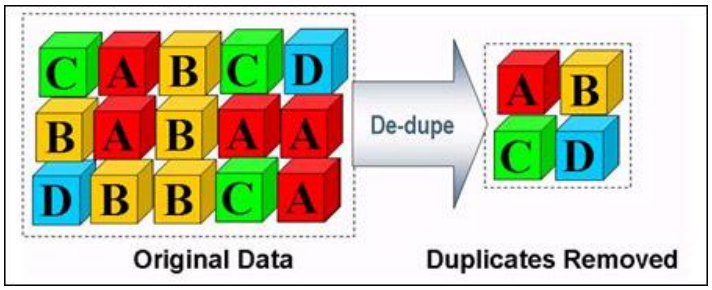
Kiintolevytilan laskennassa käytettyjen täysien varmuuskopiotiedostojen koot saatiin selville yrityksen virtualisointijärjestelmästä. Ne vastasivat varmistettavien virtuaalipalvelinten virtuaalilevyjen kokoa (taulukko 3). Palvelinten virtuaalilevyt sisälsivät myös tyhjää tilaa, koska ne oli luotu virtualisointijärjestelmän Thick Provision -tavalla. Siinä virtuaalilevyn koko määritetään jo palvelinta luotaessa, ottamatta kantaa palvelimen todelliseen levytilan tarpeeseen. Virtuaalilevyjen tyhjä tila katoaa varmuuskopiotiedostosta, kun palvelinta varmistetaan. (VMware Community 2013.)

TAULUKKO 3. Palvelinten virtuaalilevyjen koot virtualisointijärjestelmässä

Isäntänimi	Virtuaalipalvelimen koko / GB
Iron	3180 GB
Carbon	56 GB
Cobalt	104 GB
Gold	512 GB
Helium	110 GB
Oxygen	92 GB

Tarvittavaa kiintolevytilaa laskettaessa tuli huomioida, että kahden viikon varmistussykli Forward Incremental -varmistustavalla säilyttää kiintolevyllä kolmen viikon varmuuskopiotiedostot. Täysiä varmuuskopioita ei voida poistaa, mikäli kaikkia varmuuskopioon viittaavia inkrementtejä ei poisteta samalla. Inkrementaalien varmuuskopioiden tulee aina viitata varmistusketjun edellisiin inkrementteihin ja täyteen varmuuskopioon. (Veeam Recorded Webinars 2014.)

Varmistusohjelmiston käyttämien *deduplikointi*- ja pakkauskeinojen avulla kiintolevylle tallennettavien varmuuskopiotiedostojen koko saattaa jopa puolittua niiden alkuperäisestä koosta (Veeam Recorded Webinars 2014). Deduplikointi on tekniikka, jossa tietopalasia vertaillaan ja vain samanlaiset tiedon osat tallennetaan (kuva 8) (Pentikäinen 2009). Deduplikoinnin tehokkuuteen vaikuttaa esimerkiksi yhteen varmistustyöhön lisättyjen samankaltaisten palvelinten lukumäärä. Mitä enemmän yhteneväisiä palvelimia varmistetaan samassa varmistustyössä, sen korkeampi on varmuuskopiotiedostojen deduplikointisuhde. Varmuuskopiotiedostojen pakkaustehoon vaikuttavat puolestaan varmistettavan palvelimen sisältämän tiedon määrä ja laatu. Esimerkiksi tiedostopalvelimet pakkautuvat usein huonosti, koska ne sisältävät runsaasti pieniä tiedostoja. (Veeam Recorded Webinars 2014.)



KUVA 8. Deduplikointi (Poelker 2009)

Varmistettavien palvelinten koon ja niillä tapahtuvien muutosten keskiarvon perusteella laskettiin tarvittavan kiintolevytilan määrä. Laskennassa huomioitiin levyllä säilytettävien palautuspisteiden lukumäärä ja varmistusohjelmiston käyttämien deduplikointi- ja pakkaustapojen vaikutukset. Saatuun lopputulokseen lisättiin vielä ylimääräistä kiintolevytilaa, koska varmistettaviin palvelimiin voi tulla muutoksia ja nauhatallennusominaisuus vaatii kiintolevytilaa laskeutumisalueeksi (kuva 9).

Restore point = 24h (1/vuorokausi)										
Retention period = 14 vuorokautta (2 viikkoa)										
Palvelinten koot (GB):										
Iron	3180									
Carbon	56									
Cobalt	104									
Gold	512									
Helium	110									
Oxygen	92									
Yht.	4054	≈ 4000 GB								
Palvelinten täysi varmuuskopio yhteensä ≈ 4000 GB										
Palvelinten päivittäinen muutos eli inkrementaali varmuuskopio yhteensä ≈ 150 GB										
Deduplikointi ja pakkaus pienentävät varmuuskopioden koon puoleen:										
→	Täysi varmuuskopio ≈ 2000GB ja inkrementaali ≈ 75GB									
1 täysi varmuuskopio + 6 inkrementtiä = 2000 GB + 6 * 75 GB ≈ 2500 GB										
Retention period 2 viikkoa, lasketaan kolmella viikolla = 2500 GB * 3 = 7500 GB										
Retention period + nauhalta täysien varmuuskopioiden palautukseen vaadittu tila = 7500 GB + 2000 GB ≈ 10 000 GB										
Levytilaa tarvitaan VÄHINTÄÄN 10 TB + kasvuvaraa/liikkumatilaa										

KUVA 9. Arvioitu tarvittava kiintolevytilan määrä

Varmuuskopiotiedostojen tallennussijaintiin tarvittavan kiintolevytilan määrä osoittautui niin suureksi, että se pystyttiin saavuttamaan ainoastaan useasta yksittäisestä kiintolevystä muodostettavalla kiintolevyjärjestelmällä. Levyjärjestelmä luotiin RAID-tekniikalla (Redundant Array of Independent Disks), jossa useita yksittäisiä kiintolevyjä yhdistetään yhdeksi loogiseksi levykokonaisuudeksi (Lynn 2014). RAID-tekniikan tasoksi valittiin taso viisi, jossa yhden kiintolevyn tallennuskapasiteetti käytetään hajautetun *pariteettidatan* tallentamiseen kaikille järjestelmän levyille. RAID 5 -taso parantaa levyjärjestelmän vikasietoisuutta niin, että järjestelmä kestää yhden kiintolevyn hajoamisen ilman tietojen menetystä. Useamman levyn yhtäaikainen hajoaminen johtaa koko levyjärjestelmän tuhoutumiseen. RAID 5 -tasoon päädyttiin, koska se on kustannustehokas ratkaisu suurta tallennuskapasiteettia vaativissa levyjärjestelmissä, joiden toimintakyky ei ole päivittäisen yritystoiminnan kannalta kriittistä. RAID 5 -taso parantaa levyjärjestel-

män tiedonlukunopeutta, koska sen kaikki levyt osallistuvat lukuoperaatioihin. Järjestelmän heikkoutena nähdään puolestaan sen matala kirjoitusnopeus ja pariteettidatan hidas uudelleenlaskenta hajonneen kiintolevyn korvaamisen jälkeen. (Lynn 2014.)

Varmistusratkaisujen kiintolevyjärjestelmänä suositellaan käytettävän jopa RAID 5 -tasoa vikasietoisempia järjestelmiä (Spiceworks Community 2012). Vikasietoisuuden tarve tulee kuitenkin määrittää tapauskohtaisesti. Toimeksiantajan tapauksessa koko levyjärjestelmän tuhoutuminen usean yhtäaikaisen kiintolevyrikon seurauksena oli hyväksyttävää, sillä viikoittaiset täydet varmuuskopiot tallennetaan toissijaiseen tallennusvälineeseen ja Veeam Configuration Backup -toiminnolla varmistusohjelmistoon määritetyt asetukset voidaan palauttaa uuteen ohjelmistoasennukseen hyvin nopeasti.

Veeam Configuration Backup -työ noutaa varmistusohjelmiston asetustiedot varmistuspalvelimen tietokannasta ja kirjoittaa ne XML-tiedostoihin, jotka tallennetaan varmuuskopiotiedostoon. Configuration Backup -työn suorittaminen voidaan ajastaa halutusti ja varmuuskopiotiedoston tallennussijainti määrittää itse. Asetustiedostoja on suotavaa säilyttää erillään varmistuspalvelimesta, jotta palvelimen mahdollinen rikkoutuminen ei tuhoa niitä (Veeam Help Center 2015).

4.3 Laitteisto- ja ohjelmistohankinnat

Koska varmistussuunnitelman mukaista vapaata kiintolevytilaa ei yrityksen olemassa olevilla laiteresursseilla pystytty toteuttamaan, toimeksiantajayrityksen tuli tehdä tarvittavat laitteistohankinnat. Vaihtoehtoina uuden varmistusratkaisun laitteistokokoonpanolle olivat vanhan varmistuspalvelimen käyttöönotto ja kiintolevytilan lisääminen erillisellä levykehikolla (Disk Enclosure) tai uuden, tallennuskapasiteetiltaan riittävän, palvelimen hankkiminen.

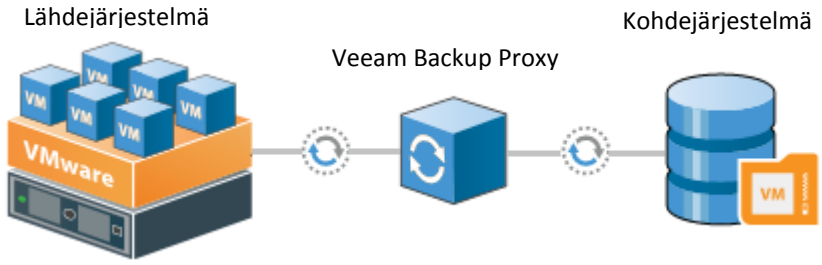
Konsultoimme toimeksiantajayrityksen pitkäaikaista palvelinlaitetoimittajaa ja päädyimme ratkaisuun, jossa yritys hankkii uuden varmistuspalvelimen ja tarvittavan määrän kiintolevyjä. Toimeksiantajan toimintatapojen mukaisesti varmistusratkaisu haluttiin toteuttaa paikallisena asennuksena ja ohjelmistolla luodut varmuuskopiot säilyttää yrityksen omissa tiloissa (Majamäki 2015).

Uudeksi varmistuspalvelimeksi valittiin HP ProLiant DL180 Gen9 -palvelin ja kiintolevyiksi kahdeksan kahden teratavun levyä. Varmistuspalvelimen sisäistä levyjärjestelmäohjainta ei haluttu korvata ennen kuin sen suorituskyky päästiin testaamaan tuotantoympäristössä. Levyjärjestelmäohjain ei ole täysin laitteistopohjainen vaan se hyödyntää isäntäkäyttöjärjestelmän resursseja (HP QuickSpecs 2014). Jotta nauha-asema ja varmistuspalvelin voitiin yhdistää, HBA-laajennuskortti siirrettiin vanhasta varmistuspalvelimesta uuteen. Palvelimen keskusmuistia lisättiin kahdeksasta gigatavusta 32 gigatavuun.

5 PALVELINYMPÄRISTÖN VALMISTELU

5.1 Tiedonsiirtotavan valinta

Veeam B&R -varmistusratkaisussa tiedonsiirron lähde- ja kohdejärjestelmän välillä suorittaa Veeam Backup Proxy -komponentti. Tiedonsiirtäjä noutaa varmistettavan virtuaalipalvelimen tiedot tietovarastosta, pakkaa ne ja lähettää tallennussijaintiin (kuva 10). Varmistusohjelmiston asennuksessa tiedonsiirtäjän rooli osoitetaan varmistuspalvelimelle, mutta tiedonsiirron kuormantasauksen ja suorituskyvyn parantamiseksi se suositellaan siirrettävän jollekin palvelinympäristön Windows-palvelimista. Tiedonsiirtäjäksi osoitetulla Windows-palvelimella voi olla myös muita tehtäviä, sillä varmistusratkaisu käyttää tiedon siirtämiseen Windows-käyttöjärjestelmässä suoritettavaa kevyttä taustapalvelua (Service). Varmistusympäristöissä suositellaan käytettävän useita tiedonsiirtopalvelimia varmistusratkaisun parhaan suorituskyvyn saavuttamiseksi. (Veeam Help Center 2015.)

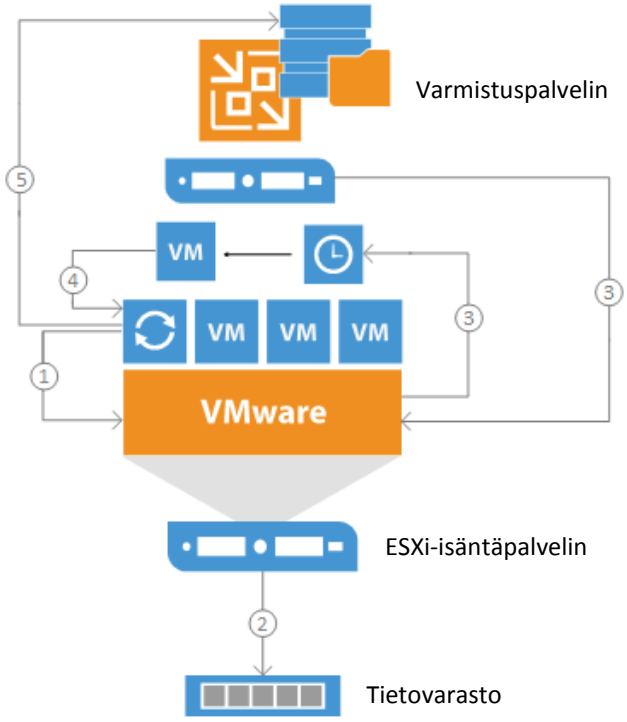


KUVA 10. Backup Proxy -palvelimen rooli varmistusratkaisussa

Varmistustöiden tehokkuuteen ja suoritusaikaan vaikuttaa tiedonsiirtopalvelimen käyttämä tiedonsiirtotapa. Varmistusohjelmisto mahdollistaa kolmen vaihtoehtoisen siirtotavan käyttämisen. Ne ovat tehokkuusjärjestyksessä Direct SAN Access, Virtual Appliance ja Network. Toimeksiantajan palvelinympäristössä Direct SAN Access -siirtotapaa ei pystytty hyödyntämään, koska se vaatii varmistettavien palvelinten virtuaalilevyjen sijaitsemisen SAN-arkkitehtuuriin (Storage Area Network) perustuvissa tallennusjärjestelmissä. (Veeam Help Center 2015.)

Virtual Appliance -siirtotavassa varmistusohjelmisto hyödyntää virtualisointijärjestelmän kykyä yhdistää laitteita käynnissä olevaan palvelimeen. Varmistustyötä suoritettaessa

varmistettavan palvelimen virtuaalilevyt yhdistetään tiedonsiirtopalvelimeen, josta levyjen tiedot luetaan suoraan varmistuspalvelimeen ilman, että tietoa siirretään lähiverkkoyhteyden yli (kuva 11). Virtual Appliance -tapaa suositellaan käytettävän ympäristöissä, joissa tiedonsiirtopalvelin on virtualisoitu. Lisäksi tulee huomioida, että ESXi-isäntäpalvelimella, jolla tiedonsiirtopalvelinta suoritetaan, tulee olla pääsy kaikkiin tietovarastoihin, joissa varmistettavien palvelinten virtuaalilevyt sijaitsevat. (Veeam Help Center 2015).



1. Backup Proxy -virtuaalipalvelin pyytää ESXi-isäntäpalvelinta paikantamaan varmistettavan virtuaalipalvelimen virtuaalilevyn tietovarastosta.

2. ESXi paikantaa virtuaalilevyn.

3. Varmistusohjelmisto käskyttää virtualisointijärjestelmää luomaan tilannevedoksen varmistettavasta palvelimesta.

4. Varmistettavan palvelimen virtuaalilevy yhdistetään tiedonsiirtopalvelimeen.

5. Varmistuspalvelin lukee varmistettavat tiedot suoraan tiedonsiirtopalvelimeen yhdistetyltä virtuaalilevyltä, irrottaa levyn työn päätyttyä ja ohjeistaa virtualisointijärjestelmää poistamaan luodun tilannevedoksen.

KUVA 11. Virtual Appliance -tiedonsiirtotapa

Network-siirtotavassa tiedonsiirtopalvelin noutaa varmistettavan palvelimen tietoja ESXi-isäntäpalvelimelta lähiverkon yli käyttäen NBD-protokollaa (Network Block Device). Network-tapaa ei suositella käytettävän, mikäli muita siirtotapoja voidaan hyödyntää, koska lähiverkon tiedonsiirtonopeus on usein matala. Lisäksi varmistustyöt saattavat ruuhkauttaa lähiverkkoa, jos tiedonsiirtopalvelimen suurinta mahdollista kaistanleveyttä ei ole määritetty. (Veeam Help Center 2015.)

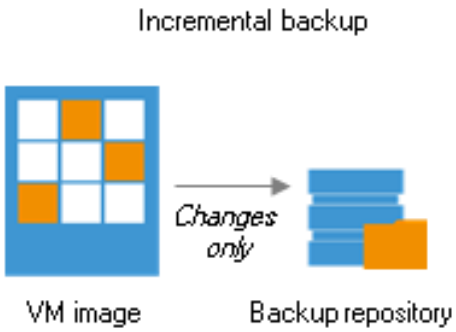
Toimeksiantajayrityksen varmistettavat virtuaalipalvelimet sijaitsivat ESXi-isäntäpalvelimilla Virtuaali01 ja Virtuaali02. Niillä ei ollut pääsyä toistensa tietovarastoihin, joten molemmille isäntäpalvelimille määritettiin oma Backup Proxy -palvelimensa. Virtuaali01:n tiedonsiirtopalvelin luotiin käyttämättömästä Windows Server 2008 R2 -virtuaalipalvelimesta. Virtuaali02:lla ei ollut ylimääräistä palvelinta tiedonsiirtopalvelimeksi.

Siksi palvelinympäristön kolmannelta ESXi-isäntäpalvelimelta poistettiin käyttämätön Windows Server 2008 R2 -virtuaalipalvelin ja sen käyttöjärjestelmälisenssillä aktivoitiin Virtuaali02:lle luotu palvelin. Virtuaalipalvelinten luontia virtualisointijärjestelmään ei kuvata tässä opinnäytetyössä.

5.2 Muuttuneiden sektorien seuraaminen

Varmistusohjelmisto hyödyntää virtualisointijärjestelmän CBT-ominaisuutta (Changed Block Tracking), joka tehostaa inkrementaalien varmuuskopioiden suorittamista (Veeam Help Center 2015). Sen avulla ESXi-isäntäpalvelimilla suoritettavat virtuaalipalvelimet kykenevät seuraamaan virtuaalilevyillään tapahtuvia muutoksia. CBT-ominaisuus tunnistaa muuttuneet tietolohkot kahden toisistaan poikkeavan muutostunnisteen (ID) avulla. (VMware Knowledge Base 2015.)

Ohjelmisto kutsuu CBT-ominaisuutta VADP (vSphere APIs for Data Protection) -rajapinnan avulla. Virtualisointijärjestelmä vastaa kutsuun palauttamalla palvelimen viimeisimmän varmuuskopiotilannevedoksen jälkeen muuttuneet tietolohkot, jotka kirjoitetaan inkrementaaliin varmuuskopiotiedostoon (kuva 12). (Veeam Help Center 2015.)



KUVA 12. CBT-ominaisuus inkrementaaleissa varmuuskopiotöissä (Veeam Help Center)

CBT-ominaisuuden käyttöönotto vaatii varmistettavan virtuaalipalvelimen *konfiguraatiotiedostoon* (.vmx) tehtäviä muutoksia (kuva 13) (VMware Knowledge Base 2015). Virtuaalipalvelin, jonka asetustiedostoa muutetaan, tulee sammuttaa ennen konfiguraatiomuutoksia. CBT-ominaisuus otetaan käyttöön palvelimella komennolla:

ctkEnabled = "TRUE"

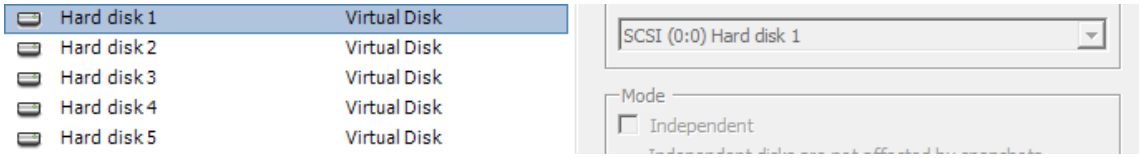
ja palvelimen virtuaalilevy määritetään käyttämään ominaisuutta komennolla:

scsi0:0.ctkEnabled = "TRUE"

SCSI0:0.ctkEnabled	true
ctkEnabled	true

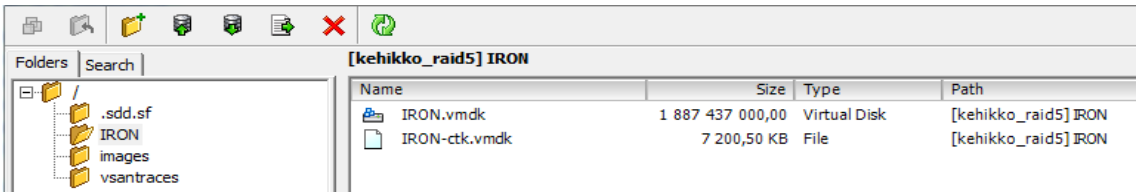
KUVA 13. CBT-ominaisuuden käyttöönottoon vaaditut komennot

Jokaiselle virtuaalipalvelimeen liitetylle virtuaalilevylle on osoitettu yksilöllinen SCSI-laite, joka näyttäytyy palvelimen ominaisuuksissa esimerkiksi nimellä *scsi0:0*, *scsi0:1* tai *scsi1:1* (kuva 14). Mikäli palvelimeen on liitetty useita levyjä, tulee CBT-ominaisuus ottaa käyttöön jokaiselle levylle erikseen. Sen käyttöönotossa tulee kuitenkin huomioida, että konfiguraatiotiedostoon tehdyt muutokset astuvat voimaan, kun virtuaalipalvelin on käynyt läpi niin sanotun *stun-unstun -syklin* eli esimerkiksi uudelleenkäynnistyksen. (VMware Knowledge Base 2013).



KUVA 14. Virtuaalipalvelimen virtuaalilevylle osoitettu SCSI-laite

CBT-ominaisuuden käyttöönoton onnistuminen varmistetaan virtuaalipalvelimen kotikansiosta, joka sijaitsee palvelimen käyttämässä tietovarastossa (kuva 15). Siellä palvelimen jokaista virtuaalilevyä tulee vastata *vmname-ctk.vmdk* -tiedosto, jossa *vmname* vastaa kyseisen virtuaalipalvelimen nimeä. Mikäli palvelin koostuu useista virtuaalilevyistä eri tietovarastoissa, tarkastus tulee suorittaa jokaiseen tietovarastoon erikseen. (VMware Knowledge Base 2015).



KUVA 15. IRON-virtuaalipalvelimen kotikansio

6 VARMISTUSPALVELIMEN ASENNUS JA SUORITUSKYKY

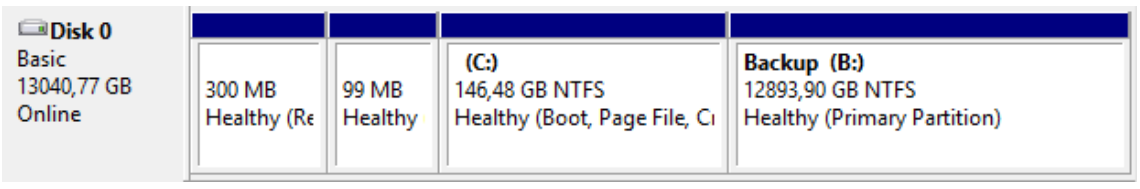
6.1 Palvelimen asennus

Varmistuspalvelimen käynnistystavaksi asetettiin UEFI (Unified Extensible Firmware Interface). UEFI määrittelee ohjelmistorajapinnan käyttöjärjestelmän ja laitteiston laiteohjainten välille. Se tuli ottaa käyttöön, jotta kiintolevyt pystyttiin osioimaan GPT-osiointijärjestelmällä, joka tukee yli kahden teratavun kiintolevyjä. (Hoffman 2014.)

Palvelimen kiintolevyjärjestelmä luotiin HP ACU (HP Array Configuration Utility) -toiminnolla, jossa määritettiin loogiseen kiintolevyjärjestelmään kuuluvat levyt ja järjestelmän RAID-taso. Levyjärjestelmän raitakooksi asetettiin 64 kilotavua. Se on suurin mahdollinen palvelimen levyjärjestelmäohjaimella käytettävä raitakoko. Levyraita on pienin viitattava tiedon osa kiintolevyjärjestelmässä. Sen koko vaikuttaa levyjärjestelmän suorituskykyyn ja tulee valita käyttötarkoituksen mukaisesti. (Kozierok 2001.)

Varmistuspalvelimelle asennettiin Windows Server 2012 R2 -palvelinkäyttöjärjestelmä. HP ACU -toiminnolla luotu kiintolevyjärjestelmä saatiin näkymään käyttöjärjestelmän asennusvelhossa asentamalla palvelimelle levyjärjestelmäohjaimen ajuriohjelmisto. Palvelinkäyttöjärjestelmäasennuksen vaiheita ei käsitellä tarkemmin tässä opinnäytetyössä.

Varmuuskopiotiedostojen tallennussijaintina käytettävä kiintolevyosio luotiin ja alustettiin käyttöjärjestelmäasennuksen jälkeen. Levyosion lohkokooksi valittiin Windows-käyttöjärjestelmän NTFS (New Technology File System) -tiedostojärjestelmän suurin mahdollinen lohkokoko, joka on 64 kilotavua (Microsoft Support 2015). Kiintolevyjärjestelmän raitakoon ja käyttöjärjestelmän levyosion lohkokoon suositellaan vastaavan toisiaan, jotta tallennettava tieto kohdistuu niille oikein (Randal 2009). Varmuuskopiotiedostoille luodun kiintolevyosion kirjaintunnukseksi asetettiin (B:\) ja sille annettiin noin 13 teratavua kiintolevytilaa (kuva 16).



KUVA 16. Varmistuspalvelimen kiintolevyosiot

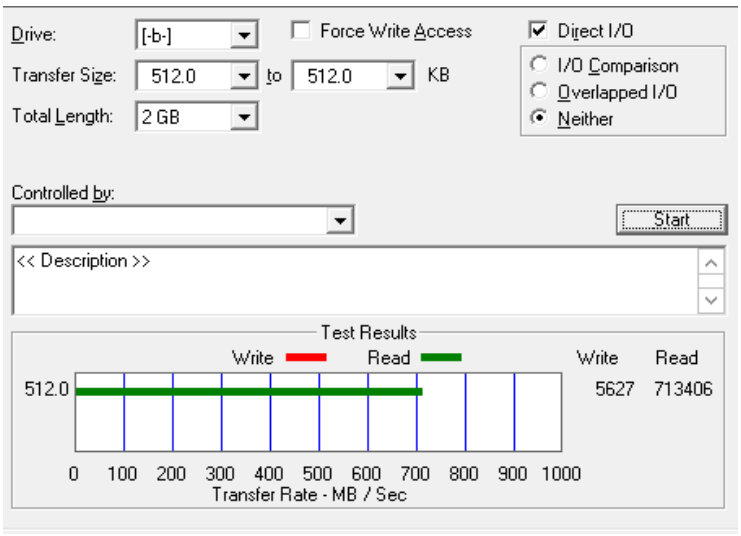
Tiedostojärjestelmän lohkokoko esittää pienintä levytilankäytön yksikköä levyosiolla. Riippumatta tallennettavan tiedon koosta, järjestelmä varaa määritetyn lohkokoon mukaisen määrän levytilaa sen tallentamiseen. (Fitzpatrick 2013.) Ennen varmistusohjelmiston käyttöönottoa tiedettiin, että ohjelmistolla luotujen varmuuskopiotiedostojen lohkokoko tallennussijainnissa tulee olemaan 512 kilotavua (Dell'Oca 2015). Tiedostojärjestelmän lohkokoon valinnalla (kuva 17) varmistettiin, että tallennettava varmuuskopiotiedosto täyttää mahdollisimman vähän lohkoja levyosiolla, koska vähäinen käytettyjen lohkojen määrä parantaa levyjärjestelmän suorituskykyä (Fitzpatrick 2013).

```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>fsutil fsinfo ntfsinfo B:
NTFS Volume Serial Number :       0x3ec02396c0235405
NTFS Version   :                  3.1
LFS Version    :                  2.0
Number Sectors :                  0x000000064bbcafff
Total Clusters :                  0x0000000000c97795f
Free Clusters  :                  0x0000000001da4344
Total Reserved :                  0x0000000000000000
Bytes Per Sector  :               512
Bytes Per Physical Sector :       512
Bytes Per Cluster :               65536
Bytes Per FileRecord Segment    : 1024
Clusters Per FileRecord Segment : 0
Mft Valid Data Length :           0x0000000000340000
Mft Start Lcn  :                  0x000000000000c000
Mft2 Start Lcn :                  0x0000000000000001
Mft Zone Start :                  0x0000000000000c020
Mft Zone End   :                  0x0000000000000ccc0
Resource Manager Identifier :     8BD2126C-F96A-11E4-80B6-9CB65475C12D

C:\Windows\system32>_
```

KUVA 17. Kiintolevyosio (B:\) alustettu 64 kilotavun lohkokoolla

6.2 Kiintolevyjärjestelmän suorituskyvyn mittaaminen

Varmuuskopiotiedostojen tallennukseen luodun kiintolevyosion suorituskykyä kokeiltiin ennen varmistusohjelmiston asennusta. Koe suoritettiin ATTO Disk Benchmark -ohjelmistolla. Se on levyjen ja levyjärjestelmien suorituskykymittaukseen kehitetty työkalu, jolla pystytään mittaamaan järjestelmän kirjoitus- ja tiedonlukunopeutta eri parametrein (ATTO 2015). Tallennussijainnin suorituskykykokeeseen valittiin asetukset, jotka vastasivat mahdollisimman tarkasti varmistusympäristön todellista tilannetta. Kokeessa levyosiolle kirjoitettavien tietolohkojen kooksi määritettiin 512 kilotavua. Se asetettiin luomaan kahden gigatavun tiedosto ja järjestelmän puskurointi ja välimuisti poistettiin käytöstä (kuva 18).



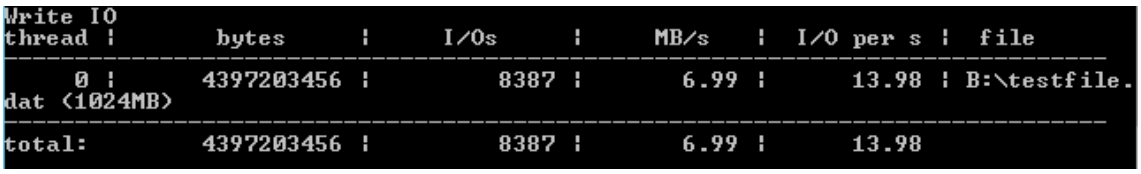
KUVA 18. Kiintolevyosion (B:\) suorituskykymittaus ATTO Disk Benchmark -ohjelmistolla

Kirjoitusnopeuskoe toistettiin Microsoft DiskSpd -työkalulla. Se on Veeam-ohjelmistoyhtiön suosittelema väline levyjärjestelmien suorituskyvyn mittaamiseen. Veeam on luonut työkalulle useita valmiita *profiileja*, joita soveltamalla eri varmistustapojen vaikutuksia tiedonsiirtonopeuksiin levyjärjestelmissä voidaan kokeilla. (Veeam Knowledge Base 2015.)

Toimeksiantajayrityksen varmuuskopiotiedostojen tallennussijainnin kirjoitusnopeutta kokeiltiin Forward Incremental- ja Active Full -varmistustapoja imitoivalla profiililla. Siinä tallennussijaintiin (*B:*) kirjoitetaan yhden gigatavun (*-c1G*) kokoinen tiedosto (*testfile.dat*). Sen kirjoittamiseen käytetään 512 kilotavun lohkokokoa (*-b512K*), täysin peräkkäisellä (sequential) kirjoitustavalla (*-w100*), ilman käyttöjärjestelmän ja laitteiston välimuistia (*-h*) yhteensä kymmenen minuutin ajan (*-d600*):

diskspd.exe -c1G -b512K -w100 -h -d600 B:\testfile.dat

Koetuloksista selvisi, että varmistuspalvelimen levyjärjestelmän kirjoitusnopeus on suhteellisen matala (kuva 19), sillä molemmat kokeet antoivat järjestelmän kirjoitusnopeudeksi alle kymmenen megatavua sekunnissa (ATTO Disk Benchmark 5,62 megatavua sekunnissa ja DiskSpd 6,99 megatavua sekunnissa). Vastaavasti järjestelmän lukunopeus oli hyvin korkea (ATTO Disk Benchmark 713,41 megatavua sekunnissa).



KUVA 19. Kiintolevyosion (B:\) kirjoitusnopeustestin tulos Microsoft DiskSpd-työkalulla

Suorityskykymittaukset vahvistivat käsityksen siitä, että RAID 5 -levyjärjestelmän kirjoitusnopeus on huomattavasti lukunopeutta matalampi (Lynn 2014). Synteettisiä suorituskykymittareita käytettäessä tulee kuitenkin huomioida, että järjestelmän todelliset siirtonopeudet voivat poiketa suorityskykymittausten tuloksista huomattavasti (Veeam Knowledge Base 2015).

7 VARMISTUSRATKAISUN KÄYTTÖÖNOTTO

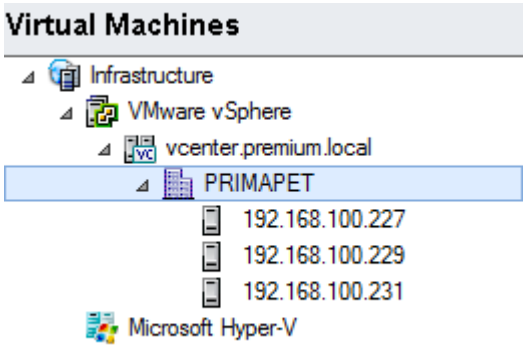
7.1 Varmistusohjelmiston asennus ja yhdistäminen palvelinympäristöön

Toimeksiantajayrityksen uusi varmistusohjelmisto asennettiin ohjelmiston kehittäjän verkkosivuilta ladattavasta levykuvatiedostosta. Windows Server 2012 R2 -palvelinkäyttöjärjestelmä mahdollisti levykuvatiedoston liittämisen (Disk Mounting) suoraan varmistuspalvelimen käyttöjärjestelmään ilman kolmannen osapuolen ohjelmistoja. Levykuvatiedostosta käynnistettiin varmistusohjelmiston asennustiedosto, joka avasi ohjelmiston asennusvelhon. Varmistusohjelmiston asennusvaiheeseen ei syvennytä tarkemmin tässä opinnäytetyössä.

Varmistusympäristön luominen varmistusohjelmistoon aloitettiin asennetun ohjelmiston yhdistämisellä yrityksen palvelinympäristöön. Tämän jälkeen ohjelmistoon lisättiin varmistusympäristön oleelliset järjestelmäkomponentit. Varmistusympäristön luomisvaiheessa tehtävät valinnat vaikuttavat varmistusratkaisun suorituskykyyn, joten ne suunniteltiin tarkasti ennen ratkaisun käyttöönottoa.

Varmistusohjelmisto yhdistettiin yrityksen palvelinympäristöön vCenter-palvelimella. Se on VMware-virtualisointijärjestelmän keskitetty hallintatyökalu ESXi-virtualisointialustoille (VMware Datasheet 2015). Sen avulla varmistusohjelmisto saa tiedon yrityksen virtualisoidusta palvelinympäristöstä, joten palvelimia ei tarvitse lisätä ohjelmistoon yksitellen. Palvelinympäristössä tapahtuvat muutokset päivittyvät varmistusohjelmistoon automaattisesti, mikä helpottaa varmistusympäristön ylläpitoa.

Yhdistäminen vCenter-palvelimeen tapahtui ohjelmiston Add Server -asennusvelholla. Siinä ohjelmisto määritettiin etsimään vCenter-palvelinta yrityksen lähiverkosta palvelimen DNS (Domain Name System) -isäntänimellä. Tämän jälkeen asennusvelhoon syötettiin vCenter-palvelimen ylläpitäjätasoinen käyttäjätunnus. Kun yhdistäminen palvelimeen onnistui, yrityksen virtualisoitu palvelinympäristö näyttäytyi varmistusohjelmiston Virtual Machines -näkymässä (kuva 20).

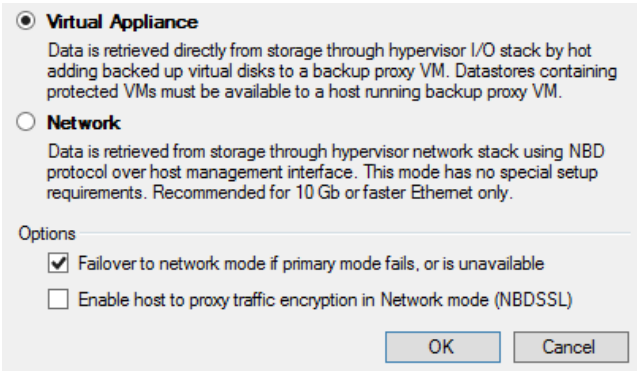


KUVA 20. Toimeksiantajayrityksen virtualisoitu palvelinympäristö varmistusohjelmistossa

7.2 Veeam Backup Proxy -tiedonsiirtopalvelinten luominen

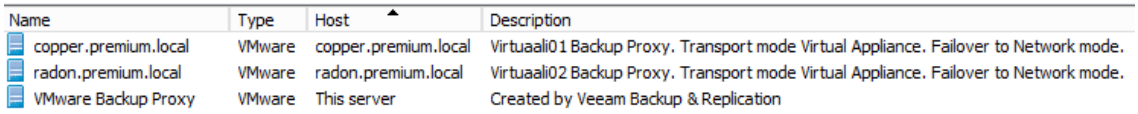
Varmistusohjelmiston yhdistäminen yrityksen palvelinympäristöön mahdollisti Backup Proxy -roolin asentamisen tiedonsiirtopalvelimiksi luoduille virtuaalipalvelimille. Varmistuspalvelin asensi tiedonsiirtopalvelimille kaikki tarvittavat ohjelmistokomponentit, kun palvelimet oli luotu varmistusohjelmistoon. Vaaditut komponentit ovat Windows-käyttöjärjestelmässä suoritettavia taustapalveluita, jotka vastaavat tiedon siirrosta lähde- ja kohdejärjestelmien välillä. (Veeam Help Center 2015.)

Tiedonsiirtopalvelimet luotiin ohjelmiston Add Proxy -asennusvelholla, jossa varmistustöissä käytettäväksi tiedonsiirtotavaksi valittiin Virtual Appliance ja toissijaiseksi siirtotavaksi Network (kuva 21). Näin varmistettiin, että tiedonsiirtopalvelin siirtyy käyttämään toissijaista siirtotapaa, mikäli ensisijainen siirtotapa ei ole käytettävissä.



KUVA 21. Tiedonsiirtopalvelimille valittu siirtotapa-asetus

Palvelimet asetettiin tunnistamaan automaattisesti kaikki tietovarastot, joista ne pystyvät varmuuskopioimaan virtuaalipalvelimia. Yhtäaikaisesti suoritettavien varmuuskopiotöiden määrä rajoitettiin yhteen työhön kerrallaan, koska sillä pyrittiin takaamaan varmistuspalvelimen korkea suorituskyky. Tiedonsiirtopalvelinten luomaa verkkoliikenteen määrää ei rajoitettu, koska ensisijainen tiedonsiirtotapa ei käytä lähiverkkoyhteyttä varmuuskopiotiedostojen siirtoon. Kuvassa 22 on esitetty toimeksiantajayrityksen varmistusohjelmistoon luodut tiedonsiirtopalvelimet.



Name	Type	Host	Description
copper.premium.local	VMware	copper.premium.local	Virtuaali01 Backup Proxy. Transport mode Virtual Appliance. Failover to Network mode.
radon.premium.local	VMware	radon.premium.local	Virtuaali02 Backup Proxy. Transport mode Virtual Appliance. Failover to Network mode.
VMware Backup Proxy	VMware	This server	Created by Veeam Backup & Replication

KUVA 22. Varmistusohjelmistoon luodut tiedonsiirtopalvelimet

7.3 Veeam Backup Repository -tallennussijainnin luominen

Varmistusohjelmistoon määritettiin varmuuskopiotiedostojen tallennussijaintina käytettävä ensisijainen tallennusjärjestelmä. Toimeksiantajayrityksen tapauksessa tiedostojen tallennussijainniksi osoitettiin varmistuspalvelimen paikallinen kiintolevyjärjestelmä, joka oli osioitu niin, että varmuuskopiotiedostot tallennettiin omalle kiintolevyosiolleen. Varmistusohjelmistoon määritettiin myös ohjelmiston Configuration Backup -asetustiedostojen tallennukseen käytettävä tallennussijainti.

Ensisijainen tallennussijainti luotiin varmistusohjelmiston Add Repository -asennusvelholla, jossa tallennussijaintipalvelimen tyypiksi määritettiin paikallinen Windows-palvelin ja varmuuskopiotiedostot osoitettiin tallennettavaksi palvelimen kiintolevyosioon (B:\). Tallennussijaintiin samanaikaisesti kirjoitettavien varmistustöiden määrä rajoitettiin yhteen työhön kerrallaan, eikä korkeinta sallittua tiedonsiirtomäärän tasoa asetettu.

Varmistusratkaisun vPower NFS -palvelinrooli asetettiin ensisijaiseen tallennussijaintiin. Se mahdollistaa deduplikoidun ja pakatun varmuuskopiotiedoston liittämisen varmistuspalvelimelta suoraan ESXi-isäntäpalvelimeen tavallisen virtuaalilevytiedoston tapaan. Ominaisuutta hyödynnetään varmistusohjelmiston Instant VM Recovery -palautustavassa. Siinä alkuperäinen varmistettu palvelin muuttuu kirjoitussuojatuksi ja kaikki muu-

tokset tallennetaan tallennussijainnista käynnistettyyn palvelimeen. Kun tallennussijainnista käynnistetty palvelin yhdistetään takaisin alkuperäiseen palvelimeen, tallennetut muutokset yhdistetään siihen ja väliaikainen palvelin poistetaan virtualisointijärjestelmästä. (Veeam Help Center 2015.)

Veeam Configuration Backup -asetustiedostojen tallennussijainniksi osoitettiin opinnäytetyön tekijän henkilökohtaiselta kannettavalta tietokoneelta toimeksiantajayrityksen tietoverkkoon jaettu kansio. Tallennussijainnin tyypiksi määritettiin CIFS (Common Internet File System), joka on standardoitu tapa tiedostojen jakamiseen tietoverkoissa (Microsoft TechNet 2015). Kuvassa 23 on esitetty toimeksiantajayrityksen varmistusohjelmistoon luodut tallennussijainnit.

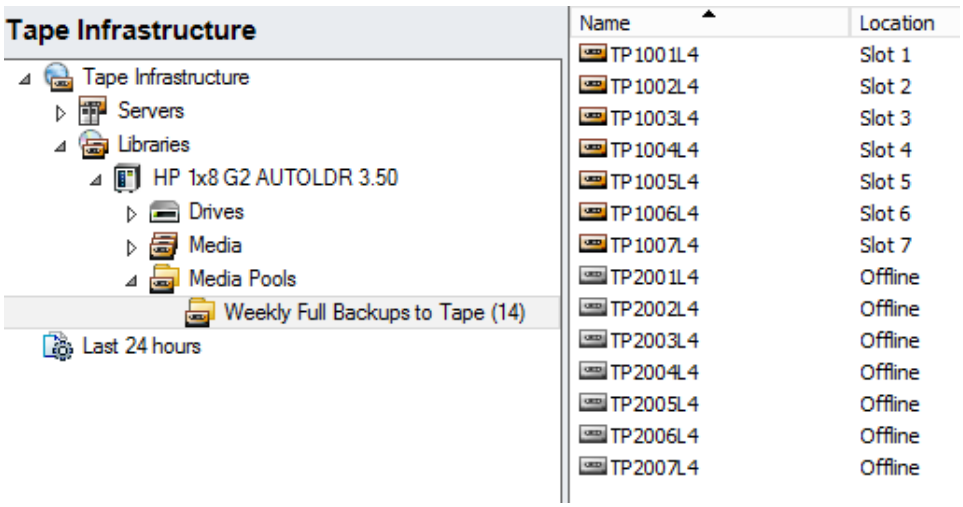
Name	Type	Host	Path	Capacity	Free	Description
Backup Repository	Windows	This server	B:\Backup	12,6 TB	4,4 TB	Backup Repository
Veeam Config Backup	CIFS		\\LAURI7\C$	119,1 GB	12,6 GB	Veeam Configuration Backup file to host LAURI7

KUVA 23. Varmistusohjelmistoon luodut tallennussijainnit

7.4 Veeam Tape Server -palvelinroolin luominen

Nauhatallennusjärjestelmän käyttöönotto varmuuskopiotiedostojen toissijaisena tallennusvälineenä edellytti Veeam Tape Server -palvelinroolin asentamista jollekin palvelinympäristön Windows-palvelimista (Veeam Help Center 2015). Toimeksiantajayrityksen varmistusratkaisussa nauhatallennuspalvelinrooli asennettiin varmistuspalvelimelle ratkaisun hallittavuuden parantamiseksi.

Kun nauhatallennusrooli oli asennettu palvelimelle, varmistusohjelmisto havaitsi varmistuspalvelimeen yhdistetyn nauha-aseman automaattisesti. Tallennuksessa käytettävien magneettinauhojen yksilölliseen tunnistukseen luotiin viivakoodit, jotka kiinnitettiin nauhoihin. Nauha-aseman viivakoodinlukija havaitsi asemaan syötetyt nauhat ja esitti ne varmistusohjelmistossa. Varmistusohjelmistoon luotiin looginen nauhavaranto (Media Pool) Weekly Full Backups to Tape, johon ohjelmiston havaitsemat nauhat liitettiin (kuva 24) (Veeam Help Center 2015).



KUVA 24. Varmistusohjelmistoon luotu nauhavaranto ja siihen liitetyt magneettinauhat

Varmistusohjelmistoon luodun nauhavarannon asetuksissa määritettiin varmuuskopiotiedostojen tallennukseen käytettävä jatkuva tietovirta (Media Set), joka nimettiin Weekly Full Backups:ksi. *Media Set* tarkoittaa jatkuvaa tietovirtaa (Data Stream), kuten esimerkiksi viikoittainen täysi varmuuskopio, joka jakautuu useille yksittäisille magneettinauhoille (Veeam Help Center 2015). Media Set asetettiin kirjoittamaan viikoittaiset varmistustyöt nauhoille edellisten viikkovarmistustöiden jälkeen. Nauhavarannon ylikirjoitussuojaksi määritettiin kahdeksan päivää, jotta varmuuskopiotiedostot eivät ylikirjoita nauhoille edellisen viikon varmuuskopioita.

8 PALVELINVARMISTUSTÖIDEN LUOMINEN

Varmistustyöt luotiin ensisijaisena tallennussijaintina toimivaan kiintolevyjärjestelmään varmistusohjelmiston Create Backup Job -varmistustyövelholla. Jokaiselle varmistettavalle palvelimelle tehtiin oma varmistustyönsä ja ne ajastettiin suoritettavaksi peräkkäin yksi kerrallaan. Varmistustöiden asetuksissa huomioitiin varmistettavien palvelinten erityispiirteet.

Toimeksiantajayrityksen tietokanta- ja tiedostonjakopalvelimen varmistustyössä otettiin huomioon, että palvelimen tietokannat varmistetaan Microsoft SQL -tietokantaohjelmiston omilla varmistustavoilla (Majamäki 2015). Varmistusohjelmiston erillistä tietokantojen varmistustapaa ei otettu käyttöön. Tiedostonjakopalvelimen varmistustyön asetuksissa otettiin kuitenkin käyttöön varmistusohjelmiston tiedostotason palautusominaisuus, jolla yksittäisiä tiedostoja voitiin palauttaa varmuuskopiosta ilman, että koko palvelin palautetaan (Veeam Help Center 2015). Tiedostotason palautusominaisuus otettiin lopulta käyttöön kaikkien varmistettavien palvelinten varmistustöissä.

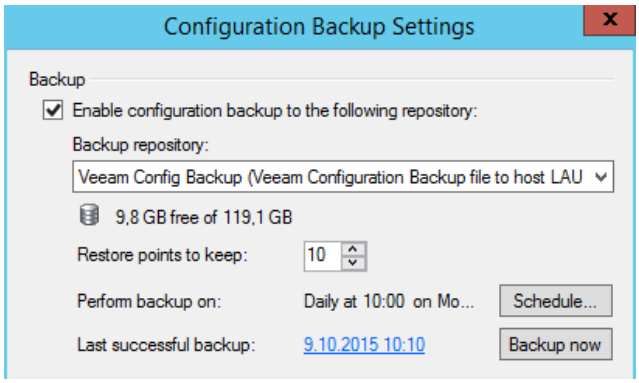
Sähköpostipalvelimen varmistustyö asetettiin käyttämään varmistusohjelmiston Microsoft Exchange -sähköpostiohjelmiston yksittäisen viestin palautusominaisuutta. Se mahdollistaa sähköpostiviestien ja kalenterimerkintöjen palauttamisen varmuuskopiosta ilman, että koko sähköpostipalvelin palautetaan (Veeam Product Features 2015). Kuvassa 25 on esitetty toimeksiantajayrityksen varmistusohjelmiston ensisijaiseen tallennussijaintiin luodut palvelinkohtaiset varmistustyöt.

Name	Type	Status	Last result	Next run	Target	Objects in job
CARBON	VMware Backup	Stopped	Success	After [IRON]	Backup Repository	1
COBALT	VMware Backup	Stopped	Success	After [CARBON]	Backup Repository	1
GOLD	VMware Backup	Stopped	Success	After [HELIUM]	Backup Repository	1
HELIUM	VMware Backup	Stopped	Success	After [OXYGEN]	Backup Repository	1
IRON	VMware Backup	Stopped	Success	13.10.2015 16:05:00	Backup Repository	1
OXYGEN	VMware Backup	Stopped	Success	After [COBALT]	Backup Repository	1

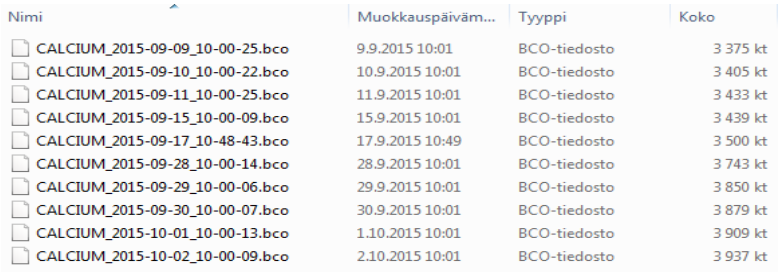
KUVA 25. Varmistusohjelmiston ensisijaiseen tallennussijaintiin luodut varmistustyöt

Varmistusohjelmiston asetustiedot varmuuskopioitiin Veeam Configuration Backup -varmistustyöllä. Varmuuskopioiden tallennussijainniksi määritettiin asetustiedostoille luotu CIFS-tallennussijainti ja varmistustyö ajastettiin suoritettavaksi arkisin kello kym-

menen aamupäivällä. Varmistustyön asetuksissa määritettiin, että tallennussijainnissa säilytetään kymmenen tuoreinta varmuuskopiotiedostoa (kuva 26). Kuvassa 27 on opinnäytetyön tekijän kannettavalle tietokoneelle tallennettuja Configuration Backup -varmuuskopiotiedostoja.



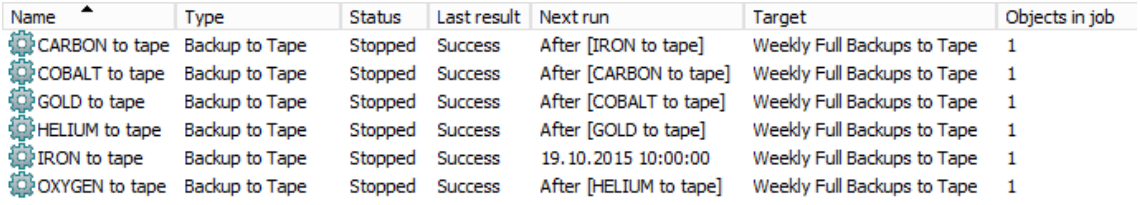
KUVA 26. Asetustietojen varmistustyön asetukset



Nimi	Muokkauspäivämäärä	Tyyppi	Koko
CALCIUM_2015-09-09_10-00-25.bco	9.9.2015 10:01	BCO-tiedosto	3 375 kt
CALCIUM_2015-09-10_10-00-22.bco	10.9.2015 10:01	BCO-tiedosto	3 405 kt
CALCIUM_2015-09-11_10-00-25.bco	11.9.2015 10:01	BCO-tiedosto	3 433 kt
CALCIUM_2015-09-15_10-00-09.bco	15.9.2015 10:01	BCO-tiedosto	3 439 kt
CALCIUM_2015-09-17_10-48-43.bco	17.9.2015 10:49	BCO-tiedosto	3 500 kt
CALCIUM_2015-09-28_10-00-14.bco	28.9.2015 10:01	BCO-tiedosto	3 743 kt
CALCIUM_2015-09-29_10-00-06.bco	29.9.2015 10:01	BCO-tiedosto	3 850 kt
CALCIUM_2015-09-30_10-00-07.bco	30.9.2015 10:01	BCO-tiedosto	3 879 kt
CALCIUM_2015-10-01_10-00-13.bco	1.10.2015 10:01	BCO-tiedosto	3 909 kt
CALCIUM_2015-10-02_10-00-09.bco	2.10.2015 10:01	BCO-tiedosto	3 937 kt

KUVA 27. Veeam Configuration Backup -varmistustyöllä varmistettuja asetustiedostoja

Toissijaisena tallennussijaintina toimivaan nauhatallennusjärjestelmään tallennettiin vain viikoittaiset täydet varmuuskopiot. Nauhavarmistustyöt luotiin varmistusohjelmiston Create Tape Job -varmistustyövelholla, jossa määritettiin varmistettavien palvelinten varmuuskopiotiedostojen tallennuskohteena käytettävä looginen nauhavaranto. Jokaiselle varmuuskopioitavalle palvelimelle luotiin oma varmistustyönsä, jotka ajastettiin suoritettavaksi peräkkäin. Kuvassa 28 on esitetty toimeksiantajayrityksen varmistusohjelmistoon luodut palvelinkohtaiset nauhavarmistustyöt.



Name	Type	Status	Last result	Next run	Target	Objects in job
CARBON to tape	Backup to Tape	Stopped	Success	After [IRON to tape]	Weekly Full Backups to Tape	1
COBALT to tape	Backup to Tape	Stopped	Success	After [CARBON to tape]	Weekly Full Backups to Tape	1
GOLD to tape	Backup to Tape	Stopped	Success	After [COBALT to tape]	Weekly Full Backups to Tape	1
HELIUM to tape	Backup to Tape	Stopped	Success	After [GOLD to tape]	Weekly Full Backups to Tape	1
IRON to tape	Backup to Tape	Stopped	Success	19.10.2015 10:00:00	Weekly Full Backups to Tape	1
OXYGEN to tape	Backup to Tape	Stopped	Success	After [HELIUM to tape]	Weekly Full Backups to Tape	1

KUVA 28. Nauhavarmistustyöt varmistusohjelmistossa

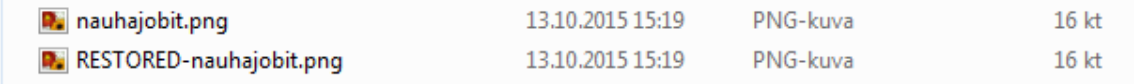
9 PALAUTUSTÖIDEN TESTAUS

Varmuuskopiotiedostojen palauttamista testattiin sekä ensisijaisena tallennussijaintina toimivasta kiintolevyjärjestelmästä että nauhatallennuksesta. Varmistettujen palvelinten palauttaminen tapahtui varmistusohjelmiston Restore-palautusvelholla. Siinä määriteltiin palautustyössä käytettävä palautustapa, valittiin haluttu palautuspiste ja määritettiin palvelimen palautussijainti palvelinympäristössä.

Virtuaalipalvelimen palautusta palvelinympäristöön testattiin koekäyttöisellä palvelimella. Palautustestejä ei suoritettu vaatimusmäärittelyn mukaisesti varmistetuilla palvelimilla, koska riskiä testin mahdollisesta epäonnistumisesta ei haluttu ottaa. Testipalvelimen palautuksen epäonnistuminen ei olisi ollut merkityksellistä palvelinympäristön toimintakyvylle.

Testipalvelimen palautustyöt suoritettiin onnistuneesti molemmilla varmistusohjelmiston täyden palvelimen palautustavoilla. Full VM Recovery -palautustavalla palvelin palautettiin suoraan alkuperäiseen sijaintiinsa palvelinympäristössä. Instant VM Recovery -tavalla palvelin puolestaan käynnistettiin ESXi-isäntäpalvelimella suoraan varmuuskopiotiedostosta, jonka jälkeen se yhdistettiin alkuperäiseen palvelimeen palvelinympäristössä.

Ohjelmistolla palautettiin onnistuneesti myös yksittäisiä tiedostoja tiedostonjakopalvelimelta sekä sähköpostiviestejä ja kalenterimerkintöjä sähköpostipalvelimelta. Tiedostotason palautustyö käynnisti varmistusohjelmistossa tiedostoselainikkunan, jolla palvelimen tiedostorakennetta voitiin selata. Palautetuilla tiedostoilla sekä korvattiin alkuperäinen tiedosto että luotiin kopio siitä (kuva 29) (Veeam Help Center 2015).

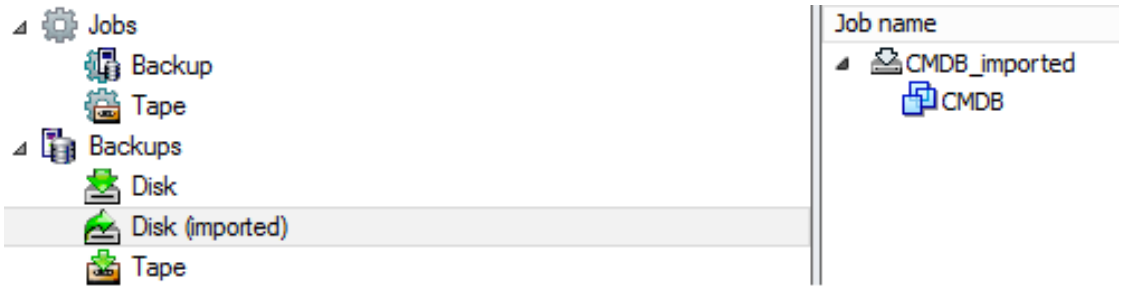


KUVA 29. Alkuperäisen tiedoston viereen palautettu tiedostokopio

Myös sähköpostiviestitason palautustyö käynnisti selainikkunan varmistusohjelmistossa. Selainikkuna esitti sähköpostipalvelimen sähköpostilaatikkotietokannan, josta palautettavat sähköpostiobjektit etsittiin. Palautukset tehtiin sekä lähettämällä palautettu viesti suoraan käyttäjän sähköpostiin että tallentamalla sähköpostiviesti varmistuspalvelimen työpöydälle. (Veeam Help Center 2013).

Testipalvelin palautettiin suoraan palvelinympäristöön myös nauhatallennusjärjestelmästä. Nauhapalautustyövelhossa tuli määrittää varmuuskopiotiedoston laskeutumisalueena käytettävä kiintolevyjärjestelmä, josta varmuuskopio palautettiin edelleen palvelinympäristöön.

Lisäksi palvelin palautettiin nauhalta varmistusohjelmiston mahdollistamalla vaihtoehtoisella palautustavalla ensin varmistuspalvelimen kiintolevyjärjestelmään. Sieltä se palautettiin palvelinympäristöön erillisellä levypalautustyöllä. Nauhalta levyjärjestelmään palautettu varmuuskopiotiedosto näyttäytyy varmistusohjelmistossa nimellä (imported) ja käyttäytyy ohjelmistossa kuten mikä tahansa muu kiintolevyjärjestelmään tallennettu varmuuskopiotiedosto (kuva 30).



KUVA 30. Nauhatallennusjärjestelmästä kiintolevyjärjestelmään palautettu virtuaalipalvelimen varmuuskopio

10 KEHITYSEHDOTUKSET

Varmistusratkaisun nauhatallennusominaisuus osoittautui toimintakyvyltään vajaaksi ja ohjelmiston käyttöönottovaiheessa havaitut puutteet heikensivät sen täysimittaista hyödyntämistä. Merkittävin puute nauhatallennusominaisuudessa oli sen kyvyttömyys tallentaa varmistettavan palvelimen viimeisin täysi varmuuskopio magneettinauhoille viikoittaisissa varmistustöissä.

Varmistustyön asetuksissa pystytään määrittämään, tallennetaanko ensimmäisellä suorituskerralla nauhalle ainoastaan varmistettavan palvelimen uusin täysi varmuuskopio vai kaikki varmuuskopiot. Olipa valinta kumpi tahansa, ensimmäisen varmistustyön jälkeen ohjelmisto tallentaa nauhoille automaattisesti palvelimen kaikki täydet varmuuskopiot, riippumatta siitä, onko se tarkoituksenmukaista vai ei. Varmistusohjelmiston kehittäjä onkin luvannut korjauspäivityksen ongelmaan varmistusohjelmiston uudessa ohjelmistoversiossa. (Veeam Community Forums 2015.) Päätimme yhdessä opinnäytetyön toimeksiantajan kanssa, että varmistusohjelmisto päivitetään uusimpaan versioon heti, kun se julkaistaan.

Ohjelmisto mahdollistaa niin sanotun hiekkalaatikkoympäristön rakentamisen. Sen avulla jokaisen ohjelmistolla luodun varmuuskopiotiedoston palautuskyky voidaan varmistaa käynnistämällä se tuotantoympäristöstä eristetyssä hiekkalaatikkoympäristössä. Varmuuskopiosta pystytään testaamaan esimerkiksi varmistetun palvelimen käynnistymiskyky ja verkkoyhteyksien sekä sovellusten toimivuus (Veeam Help Center 2015). *Virtuaalilaboratorion* käyttöönoton mahdollisuutta osana yrityksen varmistusratkaisua tutkitaan tulevaisuudessa, sillä se yksinkertaistaisi ja helpottaisi varmuuskopioiden palautuskyvyn testaamista.

Varmistuspalvelimen kiintolevyjärjestelmän suorituskykyä pystytään parantamaan. Mahdollisia parannuskeinoja ovat esimerkiksi kiintolevyjärjestelmätason muuttaminen tai tehokkaamman levyjärjestelmäohjaimen hankkiminen. Levyjärjestelmätason muutos tarkoittaisi käytännössä pariteettidataa hyödyntävän RAID-tason vaihtamisen peilausta ja lomitusta hyödyntäviin tasoihin. Niissä levyjärjestelmään tallennettavaa tietoa kirjoitetaan tasaisesti järjestelmän kaikille kiintolevyille ja levyistä luodaan toistensa kopioita (Lynn 2014). Jotta tarvittava kiintolevytila saavutettaisiin uudella levyjärjestelmätasolla,

yrityksen tulisi hankkia lisää kiintolevyjä tai luopua nykyisestä ylimääräisestä vapaasta tallennustilasta.

Kustannustehokkain tapa kirjoitusnopeuden kasvattamiseen olisi luultavasti uuden levyjärjestelmäohjaimen hankkiminen, sillä varmistuspalvelimen sisäinen järjestelmäohjain ei mahdollista kirjoitusvälimuistin käyttöä. Kirjoitusvälimuisti parantaa levyjärjestelmän kirjoitusnopeutta keräämällä kirjoituskomentoja ohjaimen lyhytkestoiseen muistiin, jossa niitä säilytetään, kunnes hitaampi tallennusväline, esimerkiksi kiintolevy, on valmis ottamaan ne vastaan. (Fischer 2015.)

Täysien varmuuskopiotöiden suoritusnopeutta pystytään kasvattamaan siirtymällä *synteettiseen* varmistustapaan täysien varmuuskopioiden luonnissa. *Aktiivisella* varmuuskopiointitavalla erityisesti tiedostonjakopalvelimen suoritusaika on pitkä, joten varmistettavan palvelimen tilannevedosta joudutaan pitämään auki pitkään. Palvelimilla, joilla tapahtuu paljon päivittäisiä muutoksia, tämä voi pahimmassa tapauksessa aiheuttaa käytettävän tietovaraston täyttymisen ja varastoa hyödyntävien palvelinten kaatumisen (Klee 2013).

Varmistusratkaisua tullaan kehittämään niin, että se hyödyntää GFS-varmistusrakennetta. Käytettävä varmistusrakenne koostuu nyt päivittäisistä inkrementaaleista varmuuskopioista varmistuspalvelimen kiintolevyjärjestelmässä ja viikoittaisista täysistä varmuuskopioista sekä levyjärjestelmässä että magneettinauhoilla. GFS-varmistusrakenteen mukaiset kuukausittaiset varmuuskopiot vaativat ainoastaan neljä uutta magneettinauhaa, joille täydet varmuuskopiotiedot tallennetaan. Tällä hetkellä nauhoilta on mahdollista palauttaa neljän viikon takaiset varmuuskopiot, joten kuukausitason varmuuskopiotyöt tulee asettaa suoritettavaksi vähintään kahden kuukauden välein.

11 POHDINTA

Varmistusohjelmisto osoittautui lopulta luotettavaksi ja toimivaksi ratkaisuksi toimeksiantajayrityksen virtualisoidun palvelinympäristön varmentamiseen. Ohjelmiston puutteet nauhatallennuksessa olivat kuitenkin harmittavia, joten uuden ohjelmistoversion julkaisemisen toivotaan tapahtuvan mahdollisimman pian.

Ohjelmiston käyttöliittymä on visuaalisesti selkeä. Varmistus- sekä palautustöiden oleelliset toiminnot ovat helposti saatavilla. Ohjelmiston kehittäjä on ilmaissut halunsa madaltaa kynnystä palvelinvarmuuskopioinnin käyttöönottoon myös pienissä ja keskisuurissa yrityksissä yksinkertaistamalla ohjelmiston käyttöä niin, että se pystytään ottamaan käyttöön jopa hyvin vähäisin asetusmuutoksin (Veeam Products 2015). On kuitenkin suositeltavaa, että palvelinympäristön valmistelutoimet ja ohjelmiston asetukset suunnitellaan huolellisesti etukäteen. Tosin suunnittelusta huolimatta varmistusohjelmiston todellista suorituskykyä ei tiedetä täysin etukäteen ja vasta ohjelmiston käyttöönoton jälkeen pystytään tekemään sitä parantavia täsmällisiä toimenpiteitä.

Virtuaalipalvelinten varmuuskopiointi ja palvelinvarmistusten konseptit olivat opinnäytetyön tekijälle ennestään tuntemattomia. Siksi työn tekeminen valitusta aiheesta oli mielenkiintoista ja tulevaisuudessa pystyn hyödyntämään opittuja asioita erilaisissa palvelinympäristöissä. Toimeksiantajayrityksen käyttöön valittu varmistusohjelmisto on käytössä myös monissa muissa yrityksissä ja voidaan sanoa, että siitä on tullut standardiratkaisu virtuaalipalvelinten varmuuskopiointiin (Kilpinen 2015).

Haastavaa opinnäytetyön tekemisessä oli työn vastuullisuus ja ratkaisujen suunnitteleminen itsenäisesti. Työn vaativimmat ja ajankäytöllisesti pisimmät vaiheet olivat varmistusratkaisun käyttöönoton suunnittelu, suorituskyvyn etukäteisoptimointi ja suunnitelmien perusteella tehtävien hankintojen valmistelu. Opinnäytetyön tekijän mielestä varmistusohjelmiston käyttöönotto ja sen tehokas käyttö edellyttävät ohjelmiston ominaisuuksiin ja vaatimuksiin perehtymistä, teknistä taitoa ja varmistettavan palvelinympäristön tuntemusta. Varmistusohjelmiston asennukseen ja käyttöönottoon laaditut suunnitelmat osoittautuivat melko onnistuneiksi, sillä suuria vastoinkäymisiä tai yllätyksiä ei koettu, lukuun ottamatta nauhatallennusominaisuuden vajavaisuutta.

Vaikka työn toteutusvaihe sujuikin kokonaisuudessaan hyvin, kohdattiin myös muutamia tilanteita, joita suunnittelussa ei osattu huomioida. Niihin ei ollut varauduttu, koska kaikkien ohjelmisto- ja laitteistoasetusten vaikutuksia toisiinsa ja varmistusratkaisun kokonaisuuteen ei tiedetty. Työn suorittamisen aikana havaitut ongelmat eivät kuitenkaan estäneet ratkaisun käyttöönoton toteutumista vaan lähinnä hidastivat itse asennusprosessia.

Opinnäytetyön teoriapohjaksi löytyi vain muutama kirjallinen lähde. Lähteinä jouduttiin käyttämään runsaasti varmistusohjelmiston kehittäjän omaa teknistä dokumentaatiota sekä internetin keskustelupalstoja ja blogikirjoituksia. Julkisiin keskustelupalstoihin ja blogikirjoituksiin tulee suhtautua lähdekriittisesti, vaikka varmistusohjelmiston omaa palstaa voidaankin pitää melko luotettavana tietolähteenä. Ohjelmiston kehittäjän dokumentaatiota tarkasteltaessa tulee kuitenkin muistaa, että se esittää ratkaisun ominaisuudet ohjelmiston kannalta edullisella tavalla, mikä ei välttämättä vastaa täysin todellisuutta.

Opinnäytetyön valmistuttua toimeksiantajayrityksen käyttöön laaditaan varmistusohjelmiston käyttö- ja päivitysohjeet ja kirjataan toiminta- ja toipumissuunnitelma palvelinympäristön katastrofitilanteisiin. Varmuuskopioista palautus ja palautustöiden luominen on dokumentoitu erikseen, koska ne ovat salaista tietoa.

Kun uusi varmistusohjelmistoversio on saatavilla, nauhatallennusympäristö viimeistellään viikoittaisten ja kuukausittaisten varmuuskopiotöiden osalta. Ensisijaisten varmuuskopiotöiden täysi varmistustapa muutetaan aktiivisesta synteettiseen. Varmistustapaa muuttamalla varmistusratkaisun suorituskykyä saadaan luultavasti kasvatettua niin, että muutoksia levyjärjestelmään ei tarvita. Virtuaalilaboratorion rakentamista varmistusohjelmistoon tutkitaan, mutta sen käyttöönotto ei ole välttämätön ajatelleen varmistusratkaisun kokonaisuutta.

LÄHTEET

ATTO. Disk Benchmark. Luettu 20.9.2015. https://www.attotech.com/disk-benchmark/

Dell'Oca, L. 2012. Veeam backup methods and the impact on destination storage I/O. Luettu 20.9.2015. http://www.virtualtothecore.com/en/veeam-backup-methods-and-the-impact-on-destination-storage-io/

Dell'Oca, L. 2015. Veeam Backup & Replication v8: Designing and planning backup repository performance. Luettu 26.9.2015. http://www.veeam.com/wp-veeam-backup-replication-v8-designing-planning-backup-repository-performance.html

Dell'Oca, L. 2015. Your Veeam backups are slow? Check the stripe size! Luettu 16.9.2015. http://www.virtualtothecore.com/en/veeam-backups-slow-check-stripe-size/

Dell'Oca, L. & Mendoza, J. 2014. How to properly size your backup repository. Webinaaritallenne. Katsottu 28.8.2015. http://www.veeam.com/videos/how-properly-size-your-backup-repository-4116.html

Fellows, R. 2008. Four ways to streamline your data backup process. Luettu 5.10.2015. http://searchdatabackup.techtarget.com/tip/Four-ways-to-streamline-your-data-backup-process

Fischer, W. 2015. RAID Controller and Hard Disk Cache Settings. Luettu 21.9.2015. https://www.thomas-krenn.com/en/wiki/RAID_Controller_and_Hard_Disk_Cache_Settings

Fitzpatrick, J. 2013. What Should I Set the Allocation Unit Size to When Formatting? Luettu 16.9.2015. http://www.howtogeek.com/136078/what-should-i-set-the-allocation-unit-size-to-when-formatting/

Golden, B. 2008. Virtualization FOR DUMMIES. Indianapolis: Wiley Publishing.

Golden, B. 2011. Virtualization FOR DUMMIES - 3RD HP SPECIAL EDITION. Luettu 16.9.2015. https://ssl.www8.hp.com/de/de/pdf/virtualisation_tcm_144_1147500.pdf

Hewlett-Packard. 2004. Why back up? http://static.highspeedbackbone.net/pdf/hp_why_backup.pdf

Hoffman, C. 2014. What's the Difference Between GPT and MBR When Partitioning a Drive? Luettu 14.9.2015. http://www.howtogeek.com/193669/whats-the-difference-between-gpt-and-mbr-when-partitioning-a-drive/

Isoweli. Varmuuskopiointipalvelut. Luettu 2.10.2015. http://www.isoweli.fi/varmuuskopiointi

Kilpinen, J. 2015. System Specialist. Decens Oy. Palaverikeskustelu 24.9.2015.

Klee, D. 2013. Keep VMware snapshot growth from wrecking your day. Luettu 21.9.2015. http://www.davidklee.net/2013/02/19/keep-vmware-snapshot-growth-from-wrecking-your-day/

Kozierok, C. 2001. Stripe Width and Stripe Size. Luettu 15.9.2015. http://www.pcguide.com/ref/hdd/perf/raid/concepts/perfStripe-c.html

Krogh, P. 2015. Backup Overview? Luettu 4.10.2015. http://dpbestflow.org/node/262

Levkina, M. 2014. How to follow the 3-2-1 backup rule with Veeam Backup & Replication. Luettu 5.10.2015. http://www.veeam.com/blog/how-to-follow-the-3-2-1-backup-rule-with-veeam-backup-replication.html

Lewis, K. 2012. Agent and Agentless VM Backup and Recovery – Unraveling the myths. Luettu 6.10.2015. http://www.symantec.com/connect/blogs/agent-and-agentless-vm-backup-and-recovery-unraveling-myths

Lock, I. 2010. Tape backup vs disk backup. Luettu 16.9.2015. http://www.computerweekly.com/podcast/Tape-backup-vs-disk-backup

Lynn, S. 2014. RAID Levels Explained. Luettu 13.9.2015. http://www.pcmag.com/article2/0,2817,2370235,00.asp

Majamäki, L. 2015. Kehityspäällikkö. Prima Pet Premium Oy. Henkilökohtainen keskustelu.

Microsoft Support. Default cluster size for NTFS, FAT, and exFAT. Luettu 15.9.2015. https://support.microsoft.com/en-us/kb/140365

Microsoft TechNet. Backup types. Luettu 2.10.2015. https://technet.microsoft.com/en-us/library/cc938478.aspx

Microsoft TechNet. Common Internet File System. Luettu 8.9.2015. https://technet.microsoft.com/en-us/library/cc939973.aspx

Niktips. 2012. GFS backup scheme in Symantec Backup Exec. Luettu 9.9.2015. https://niktips.files.wordpress.com/2012/03/ps4q01se-mncluster2.jpg?w=300&h=264

Nykänen, P. 2014. Tietoturva – tietosuoja tietojärjestelmien suunnittelussa. Tampereen yliopisto. Luettu 23.9.2015. http://www.uta.fi/sis/tie/tjsum/index/TJSUM_Luento6_2014_PirkkoNyk%C3%A4nen.pdf

Pentikäinen, J. 2009. Deduplikointi lääkitsee dataturvotusta. Luettu 18.9.2015. http://www.tivi.fi/Arkisto/2009-08-17/Deduplikointi-l%C3%A4%C3%A4kitsee-dataturvotusta-3174673.html

Poelker, C. 2009. How to Leverage Data Deduplication to Green Your Data Center. Luettu 15.9.2015 http://www.eweek.com/c/a/Data-Storage/How-to-Leverage-Data-Deduplication-to-Green-Your-Data-Center

Prima Pet Premium Oy. 2015. Yrityksen sisäinen tiedonanto.

QuickSpecs. 2014. HP Dynamic Smart Array Controller. Luettu 3.9.2015. http://www8.hp.com/h20195/v2/GetPDF.aspx/c04390743.pdf

Randal, P. 2009. Are your disk partition offsets, RAID stripe sizes, and NTFS allocation units set correctly? Luettu 16.9.2015. http://www.sqlskills.com/blogs/paul/are-your-disk-partition-offsets-raid-stripe-sizes-and-ntfs-allocation-units-set-correctly/

Rouse, M. 2006. Hypervisor definiton. Luettu 3.10.2015. http://searchservervirtualization.techtarget.com/definition/hypervisor

Scsami. 2011. Hyperviseur. Luettu 15.9.2015. https://upload.wikimedia.org/wikipedia/commons/e/e1/Hyperviseur.png

Sliwa, C. 2015. Host bus adapter (HBA) definition. Luettu 13.9.2015. http://searchstorage.techtarget.com/definition/host-bus-adapter

Spiceworks Community. 2012. What type of raid do you use for a backup server? Luettu 11.9.2015. https://community.spiceworks.com/topic/191976-what-type-of-raid-do-you-use-for-a-backup-server

Veeam Community Forums. 2014. Recovery from Tape - Needs major work. Luettu 28.9.2015. http://forums.veeam.com/tape-f29/recovery-from-tape-needs-major-work-t22438.html.

Veeam Community Forums. 2015. Backup to Tape only last backup with reversed incremental. Luettu 1.10.2015. http://forums.veeam.com/tape-f29/backup-to-tape-only-last-backup-with-reversed-incremental-t17617.html

Veeam Help Center. Active Full Backup. Luettu 29.9.2015. http://helpcenter.veeam.com/backup/80/hyperv/active_full_backup.html

Veeam Help Center. Backup Proxy. Luettu 25.8.2015. http://helpcenter.veeam.com/backup/80/vsphere/backup_proxy.html

Veeam Help Center. Changed Block Tracking. Luettu 1.9.2015. http://helpcenter.veeam.com/backup/80/vsphere/changed_block_tracking.html

Veeam Help Center. Creating Configuration Backups. Luettu 19.9.2015. http://helpcenter.veeam.com/backup/80/hyperv/export_vbr_config.html

Veeam Help Center. Forward Incremental Backup. Luettu 26.9.2015. http://helpcenter.veeam.com/backup/80/hyperv/forward_incremental_backup.html

Veeam Help Center. GFS Retention Policy. Luettu 18.9.2015. http://helpcenter.veeam.com/backup/80/vsphere/backup_copy_gfs.html

Veeam Help Center. Network Mode. Luettu 27.8.2015. http://helpcenter.veeam.com/backup/80/vsphere/network_mode.html

Veeam Help Center. Overview. Luettu 15.9.2015. http://helpcenter.veeam.com/backup/70/vsphere/vee_overview.html

Veeam Help Center. Restore from Tape. Luettu 23.9.2015. http://helpcenter.veeam.com/backup/70/bp_vsphere/hiw_tape_restore.html

Veeam Help Center. Restoring VM Guest OS Files (Microsoft Windows). Luettu 19.9.2015. http://helpcenter.veeam.com/backup/80/hyperv/performing_guest_restore.html

Veeam Help Center. Step 4. Specify Media Set Options. Luettu 19.9.2015. http://helpcenter.veeam.com/backup/80/vsphere/add_media_pool_set.html

Veeam Help Center. Step 6. Save Restored Files. Luettu 23.9.2015. http://helpcenter.veeam.com/backup/80/hyperv/guest_restore_save_hv.html

Veeam Help Center. System Requirements. Luettu 25.8.2015. http://helpcenter.veeam.com/backup/80/vsphere/system_requirements.html

Veeam Help Center. Veeam vPower NFS Service. Luettu 13.9.2015. http://helpcenter.veeam.com/backup/80/vsphere/vpower_nfs_service.html

Veeam Help Center. Virtual Appliance. Luettu 27.8.2015. http://helpcenter.veeam.com/backup/80/vsphere/virtual_appliance.html

Veeam Help Center. Virtual Lab. Luettu 20.9.2015. http://helpcenter.veeam.com/backup/80/vsphere/virtual_lab.html

Veeam Help Center. VM Change Rate Estimation. Luettu 16.9.2015. http://helpcenter.veeam.com/one/80/reports/vm_change_rate_estimation.html

Veeam Help Center. Working with Media Pools. Luettu 19.9.2015. http://helpcenter.veeam.com/backup/80/vsphere/working_with_pools.html

Veeam Knowledge Base. 2013. Veeam Backup Temporary Snapshot. Luettu 20.9.2015. http://www.veeam.com/kb1790

Veeam Knowledge Base. 2015. How to use DiskSpd to simulate Veeam Backup & Replication disk actions. Luettu 20.9.2015. http://www.veeam.com/kb2014

Veeam Products. 2015. Backup Essentials for VMware and Hyper-V. http://www.veeam.com/smb-vmware-hyper-v-essentials.html

Veeam Product Features. 2015. E-discovery and granular recovery for Microsoft Exchange. Luettu 19.9.2015. http://www.veeam.com/microsoft-exchange-recovery.html

Virtzone. What's the difference between a 'Type 1′ hypervisor and a 'Type 2′ hypervisor? Luettu 24.9.2015. http://www.virtzone.net/the-difference-between-a-type-2-hypervisor-and-a-type-1-hypervisor/

VMware Community. 2013. What Is The Difference Between Eager Zero And Lazy Zero Thick Provision Disks? https://communities.vmware.com/message/2199576

VMware Knowledge Base. Changed Block Tracking (CBT) on virtual machines (1020128). Luettu 1.9.2015. http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1020128

VMware Knowledge Base. 2010. Understanding virtual machine snapshots in VMware ESXi and ESX (1015180). Luettu 25.9.2015. http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1015180

VMware Knowledge Base. 2013. Enabling or disabling Changed Block Tracking (CBT) on virtual machines (1031873). Luettu 2.9.2015. http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1031873

VMware Products. 2015. VMware vCenter Server datasheet. Luettu 8.9.2015. https://www.vmware.com/files/pdf/products/vCenter/VMware-vCenter-Server-Datasheet.pdf

VMware Virtual Disks. 2007. Virtual Disk Format 1.1. Tallennettu 15.9.2015.

Ward, M. 2009. Granular application and system recovery. Luettu 25.9.2015. http://www.itworld.com/article/2782369/storage/granular-application-and-system-recovery.html

Ward, S. Data Backup is The Best Data Protection. Luettu 3.10.2015. http://sbinfocanada.about.com/cs/management/a/databackup.htm