JATKUVUUDEN HALLINTA ASIAKASYRITYKSESSÄ

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Ammattikorkeakoulututkinnon opinnäytetyö

Tietojenkäsittelyn koulutus, Hämeenlinnan korkeakoulukeskus
syksy, 2021

Jouko Laine

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Tietojenkäsittelyn koulutus — Tiivistelmä

Hämeenlinnan korkeakoulukeskus

Tekijä	Jouko Laine	Vuosi 2021
Työn nimi	Jatkuvuuden hallinta asiakasyrityksessä	
Ohjaajat	Lasse Seppänen	

TIIVISTELMÄ

Tässä opinnäytetyössä käsiteltiin jatkuvuuden hallintaa asiakasyrityksessä varmistuksen näkökulmasta. Työn tarkoituksena oli selkeästi kuvata ja selvittää mitä tarkoittaa toipumispiste (RPO) sekä toipumisaika (RTO). Näitä hyödyntäen toteutettiin asiakasyritykselle BIA-analyysi, jolla voidaan parantaa tuotannon jatkuvuutta. Lisäksi BIA-analyysin avulla pystytään jatkossa paremmin hallitsemaan liiketoiminnan jatkuvuutta IT-järjestelmän näkökulmasta sekä parantamaan toipumista poikkeustilanteesta. Käyttöön otettiin monitorointi- ja raportointisovellus Veeam ONE, jolla monitoroidaan toipumispisteitä sekä ympäristöä kokonaisvaltaisesti. Asiakasyritys sai käyttöönsä opinnäytetyön aikana heille määritellyn BIA-analyysin, joka on käyty asiakkaan kanssa läpi. RTO ja RPO ovat todella hyödyllisiä määrittelyitä jatkuvuuden hallinnassa, ja niitä seuraamalla päästään parempiin lopputuloksiin poikkeustilanteissa. Tutkimusmenetelminä käytettiin demoympäristössä testauksia sekä aiheeseen liittyvien artikkeleiden ja dokumenttien tutkintaa.

Avainsanat	Tietoturva, Tietotekniikka, Tietotekniikka-arkkitehtuuri, Varmistus, BIA
Sivut	45 sivua ja liitteitä 3 sivua

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Degree Programme in Business Information Technology
Hämeenlinna University Campus

Abstract

Author Jouko Laine
Year 2021
Subject Continuity management in customer company
Supervisors Lasse Seppänen

ABSTRACT

The thesis deals with continuity management in a customer company from the perspective of backup. The purpose of the work was to clearly describe and explain what the recovery point objective (RPO) and recovery time objective (RTO) mean. Utilizing these, a BIA analysis was performed for the customer company to improve the continuity of production. BIA analysis will help to better manage business continuity from an IT system perspective and improve recovery from emergencies. The Veeam ONE monitoring, and reporting application was introduced, which monitors recovery points and the environment holistically. During the thesis, the client company received the business impact (BIA) analysis defined for them, which has been reviewed with the client. RTO and RPO are useful definitions for continuity management and following them will lead to better results in exceptional situations. The research methods used were tests in a demo environment and the examination of related articles and documents.

Keywords Backup, Security, Information technology, Information technology architecture, BIA
Pages 45 pages and appendices 3 pages

Sisällys

Kuvat, taulukot ja kaavat

Liitteet

Liite 1 Aineistonhallintasuunnitelma

Liite 2 BIA-analyysi

Käsitteet ja termit

Veeam Backup & Replication

Opinnäytetyössä käytettävä varmistusohjelmisto.

Veeam ONE

Opinnäytetyössä käytettävä raportointi ja monitorointiohjelmisto.

RTO (Recovery Time Object)

Termi, jolla mitataan aikaa vikatilanteen alkamisajasta siihen, milloin järjestelmä on käytettävissä.

RPO (Recovery Point Object)

Termi, jolla joka ilmaisee tavoitellun toipumispisteen ajan.

Liiketoimintavaikutusten analyysi (BIA-analyysi)

BIA-analyysi, jolla havainnollisestaan palvelimien kriittisyyttä liiketoiminnan näkökulmasta.

Deduplikointi

Deduplikointi on käsittelyteknologia toistuvien tietojen kopioiden poistamiseen.

Domain Controller

Windows-toimialueen ohjauskone.

SQL Server

Relaatiotietokantapalvelin, jota opinnäytetyössä käytetään

Transaktioloki

SQL-palvelimen lokitiedosto

SLA (Service Level Agreement)

Sopimus, jossa määritellään asiakkaan tarvitsema palvelutaso

VMWare vCenter Server

VMWaren virtualisointialustan ohjauspalvelin

Hyper-V Host

Microsoftin virtualisointialusta

Failover Cluster

Microsoftin korkean käytettävyyden virtualisointiratkaisu.

SCVMM Server

Microsoftin System Center Virtual Machine Manager joka on virtualisointialustan hallintatyökalu.

1 Johdanto

Opinnäytetyössä tutkitaan, kuinka asiakasyrityksessä voidaan parantaa jatkuvuuden hallintaa. Tähän käytetään BIA-analyysiä ja siihen tehtyä vaikutusarviotyökalua. Opinnäytetyön aikana otetaan käyttöön Veeam ONE monitorointi- ja raportointisovellus tukemaan jatkuvuudenhallintaa ja parantamaan ympäristön tiedonkulkua ylläpidosta vastaaville henkilöille. Jatkuvuudenhallintaa käytetään organisaatioissa mahdollisimman häiriöttömien toimintojen takaamiseksi. Lisäksi sillä varmistetaan organisaation avaintoimintoja, jolloin tuottavuus voidaan säilyttää myös poikkeustilanteissa. (Väestörekisterikeskus, 2019, s. 29)

Jatkuvuuden hallinta on jatkuvasti kehitettävä ja kehittyvä prosessi, jonka tulisi olla osa organisaation normaalia toimintaa varautumisen ohella.
Jatkuvuudenhallintaprosessissa luodaan ja päivitetään määrittelyjä palveluiden ja palvelimien kriittisyydestä, voidaan hyödyntää esimerkiksi varmistusratkaisuissa varmistustiheyden määrittelyssä, toipumisaikamäärittelyyn tai varmistuksien säilytyksessä. (Väestörekisterikeskus, 2019, s. 29)

Opinnäytetyössä tutkitaan BIA-analyysitukityökalua ja luodaan erillinen BIA-analyysitukityökalu, johon on tiivistetty asiakasyrityksen tarpeet.
Järjestelmän varmistus suoritetaan asiakkaalla olemassa olevalla Veeam Backup & Replication -ohjelmistolla. Monitorointia ja raportointia hallinnoidaan Veeam ONE -ohjelmistolla. Opinnäytetyön aikana ei ole tarkoitusta päivittää Veeam Backup & Replication -ohjelmistoa, mutta Veeam ONE - ohjelmisto päivitetään versiosta V10 versioon V11. Version päivittäminen uudempaan mahdollistaa laajemmat raportointityökalut. Raportointia otetaan laajemmin käyttöön opinnäytetyön aikana tuotantoympäristöön.

Opinnäytetyön tarkoituksena on visualisoida ja dokumentoida asiakasympäristön palvelut ja palvelimet toipumisaika (RTO) ja toipumispiste (RPO) määrittelyllä sekä määrittelemällä palvelutasot (SLA). Tavoitteiden saavuttamiseen käytetään BIA Analyysiä tukityökaluna.

Tavoitteena on saada järjestelmään parempi saatavuus parantamalla varmistuksia tuomalla mukaan raportointia ja monitorointia hyväksikäyttäen tukityökalua palvelun kriittisyysasteen määrittelyyn.

Tutkimuskysymykset

- Kuinka kehitetään toiminnan jatkuvuutta ja varaudutaan poikkeustilanteisiin?
- Miten priorisoidaan palvelut jatkuvuuden hallinnan suunnittelussa?
- Mihin käytetään toipumispistettä (RPO) ja toipumisaikaa (RTO)?
- Kuinka hyödyntää toipumispistettä ja toipumisaikaa asiakasympäristössä?

2 Tutkimusmenetelmät

Tässä opinnäytetyössä tutkitaan aiheeseen liittyvää materiaalia eri lähteistä sekä käytetään testausvaiheessa käytännön testausta demoympäristössä. Testauksella varmistetaan aineistojen paikkansa pitävyys ja mahdollisesti voidaan löytää uusia tapoja, joita ei aineistossa ole esitelty. Tutkimuksessa löydetyt ratkaisut, mitkä eivät ole aineistosta poimittuja, dokumentoidaan ja validoidaan Veeamin teknisen tuen kanssa, jolloin varmistutaan toimivuudesta myös poikkeustilanteissa tuotantoympäristössä.

Opinnäytetyön kirjoittaja on käynyt Veeam VMCE- ja VMCE-A-sertifiointikokeisiin oikeutettavat kurssit, joista ratkaisuja tuodaan opinnäytetyön käytännön osuuteen, lisäksi työskentelee erilaisten Veeam ympäristöjen kanssa päivittäin. Muina lähteinä käytetään Mastering Veeam Backup & Replication -kirjaa, jonka on kirjoittanut Chris Childerhose. Kirjan kirjoittaja on VMCE- sekä VMCE-A-sertifioinnin suorittanut henkilö, joka toimii Veeam Vanguardin jäsenenä.

3 Jatkuvuudenhallinnan teknologioita

Luku käsittelee yleistä teoriaa ja siinä syvennytään tarkemmin opinnäytetyön alussa esiteltyihin käsitteisiin ja termeihin.

3.1 Domain Controller

Active Directory on Microsoftin Windows Server-käyttöjärjestelmien päällä toimiva palvelu. Palvelun pääasiallinen tehtävä on hallinnoida Windows-pohjaisten verkkojen käyttäjien ja tietokoneiden oikeuksien varmentamista ja oikeuksien jakamista (Antti Eteläaho, 2015, s. 21).

3.2 SQL Server

SQL on lyhenne englannin kielen sanoista structured query language. Alunperin kyselykielen on kehittänyt IBM 70-luvulla (2K, ei pvm.). Kirjallisuudessa on todettu että SQL:ää voidaan pitää eniten käytettynä neljännen sukupolven ohjelmointikielenä (Hovi, 2004).

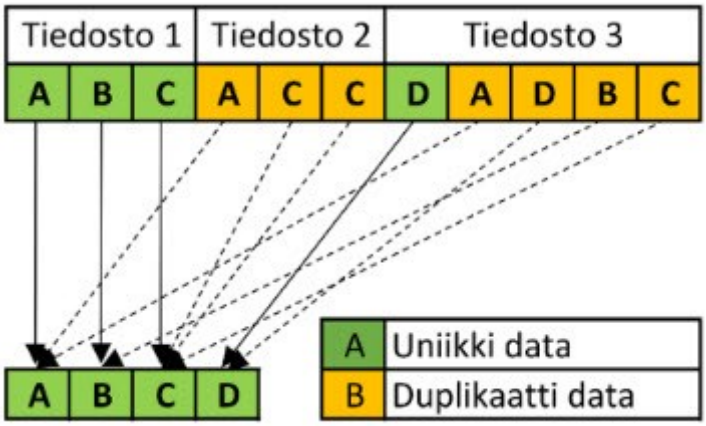
SQL-prosessin aikana tuotetaan transaktiolokeja, jotka sisältävät lokitietueita. Ne ovat tärkein osa SQL Server -tietokantaa hätätilanteiden varalta ja niiden tulee säilyä vahingoittumattomina. (Stankovic, 2014)

3.3 Deduplikointi

Deduplikointi on datan pakkaamiseen tarkoitettu tekniikka. Vuonna 2021 deduplikointiratkaisuja löytyy monelta eri valmistajalta. Deduplikointia voidaan tehdä lähdepalvelimen toimesta, joka tarkoittaa sitä, että datan deduplikointi tehdään lähdepäässä. Tällä vähennetään dataliikennettä verkossa varmistuksen aikana. Negatiivisena puolena ratkaisussa on prosessoritehon tarve varmistuksen aikana ja lisäksi tarvitaan useimmiten sovellus, joka toiminnon hoitaa. Kohdededuplikointi tapahtuu varmistuskohteen päässä. Tämä tapa vähentää prosessorikuorman tarvetta lähdepäässä, mutta kuormittaa enemmän verkkoa, kun data kulkee deduplikoimattomana. Inline-deduplikointitapa mahdollistaa, että data deduplikoidaan ennen kuin se kirjoitetaan varmistuskohteeseen.

Vaihtoehto vähentää siirrettävän datan määrää ja vähentää kapasiteetin tarvetta varmistuskohteessa.(Andrew Maclen, ei pvm.) Varmistuksen jälkeisellä deduplikoinnilla tarkoitetaan että data prosessoidaan varmistuskohteessa varmistustyön valmistuttua. Ratkaisua käytetään yleisesti virtuaalisissa nauhakirjastoissa sekä joissain deduplikoivissa varmistuskohteissa. (Määttä, 2013) Nauhakirjastolla tarkoitetaan varmistuskohdetta, jossa varmistettava tieto tallennetaan nauhalle.
Esimerkkeinä deduplikoivista varmistuskohteista on EMC DataDomain, Exagrid, HPE Storeonce ja Quantum DXi. Eri valmistajien ratkaisuissa on eroja datan käsittelytavoissa.

Kuva 1. Deduplikointia havainnollistava piirros (Määttä, 2013, s. 23)



3.4 Virtualisointialustat

Virtualisointialustoja on saatavilla eri valmistajilta. Virtualisoinnin tärkeimpiä etuja on fyysisen palvelinlaitteiston tehokkaampi käyttö (IBM, 2021). Opinnäytetyössä käsitellään kahta eri virtualisointialustaratkaisua. Virtualisointialustojen hallintapalvelimella tarkoitetaan palvelinta, jonka kautta virtualisointialustoja voidaan hallita keskitetysti.

3.4.1 VMware vSphere Hypervisor (ESXi)

VMWaren virtualisointialustaratkaisu. VMWare on tuonut markkinoille ensimmäisen virtualisointialustan nimellä VirtualServer vuonna 2007 (VMWare, 2021a).
VMWaren vCenter server on palvelimien keskitetty hallintaportaali, jolla voidaan hallinnoida palvelinkokonaisuuksia yhdestä pisteestä. Kuvassa 2 havainnollistetaan miten VMWare virtualisointi visuaalisesti esitetään. Alin kerros kuvassa 2 havainnollistaa fyysista rautaa. vSphere-kerros havainnollistaan VMWaren kerrosta fyysisen raudan päällä. OS merkitsee käyttöjärjestelmätasoa vSphere-tason päällä ja APP tarkoittaa sovelluskerrosta virtuaalisen käyttöjärjestelmän päällä. (Kuva 2)

Kuva 2. Havaintokuva virtualisoinnista (VMWare, 2021b).

3.4.2 Hyper-V

Hyper-V on Microsoftin tarjoama virtualisointialusta (Posey, ei pvm.). Hyper-V:stä on saatavilla kolme eri versiota. Saatavilla on itsenäinen Hyper-V-käyttöjärjestelmä, Hyper-V For Windows 10 sekä Hyper-V For Windows Server (DNS Stuff, 2020). Windows 10 sekä Server-käyttöjärjestelmässä Hyper-V-rooli sisältyy käyttöjärjestelmään ja voidaan ottaa käyttöön palvelinkäyttöjärjestelmässä asentamalla Hyper-V-rooli tai Windows 10 -käyttöjärjestelmässä käyttöönottamalla ominaisuutena.

Microsoft System Center Virtual Machine Manager on Microsoftin System Center-tuoteperheen virtualisointialustan hallintasovellus. Hallintasovelluksen tarkoitus on Hyper-V-virtualisointialustojen ylläpito ja hallinta. (Lee, 2019)

3.5 Veeam

Kappaleessa esitellään opinnäytetyössä käytettävää ohjelmaa ja siihen liittyviä keskeisiä aiheita.

3.5.1 Backup & Replication

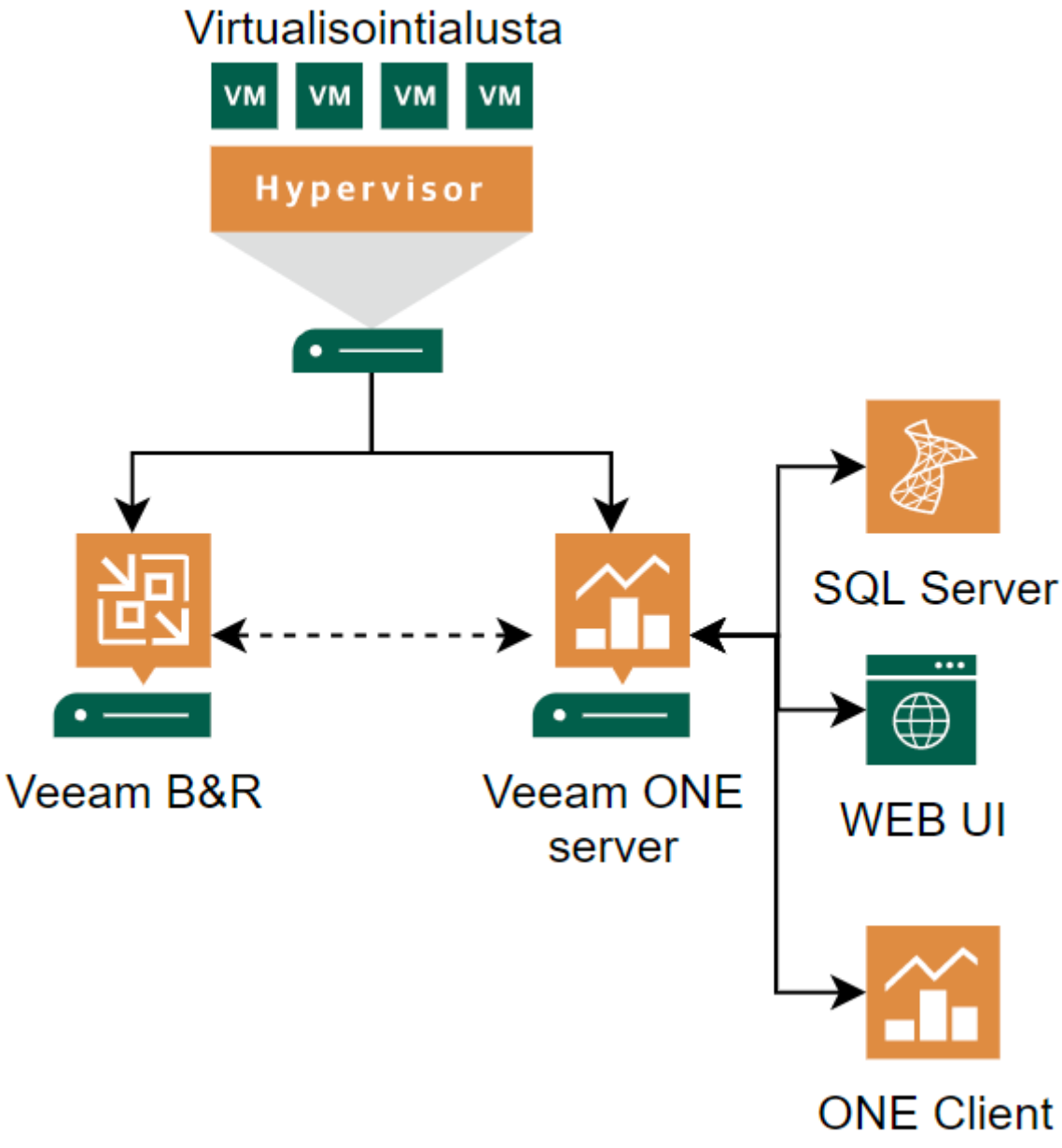
Veeam Backup & Replication -varmistus- ja replikointiohjelmisto koostuu erilaisista komponenteista, joilla kaikilla oma roolinsa. Ohjelmiston komponentteja ovat varmistuspalvelin (Backup server), varmistettavan tiedon välityspalvelin (Proxy server), liityntäpalvelin (Mount server) sekä varmistuskohde (Backup repository). Varmistuspalvelin voidaan asentaa joko fyysiseen tai virtuaaliseen Windows-palvelimeen ja se toimii konfigurointi- ja hallintaliittymänä. Varmistettavan tiedon välityspalvelin prosessoi ja suorittaa datan siirron lähteestä varmistuskohteeseen. Liityntäpalvelin on olennainen osa palautusprosessia. Palautusprosessissa liityntäpalvelin liittää varmistusajankohdan palautustiedostot ja toimii tiedostojen tai kohteen palautusprosessissa suorittavana palvelimena. Varmistuskohde toimii varmistustöiden säilönä. Varmistuskohteena voi toimia Windows-palvelin, Linux-palvelin, levyjärjestelmä tai deduplikoiva varmistuskohde. Toissijaisena varmistuskohteena tai varmistuksien arkistointiin voidaan käyttää pilvitallennuskapasiteettia kuten Amazon S3, Azure Blob storage, muu S3-yhteensopiva tai IBM Cloud storage. (Veeam, 2020a)

3.5.2 Veeam ONE

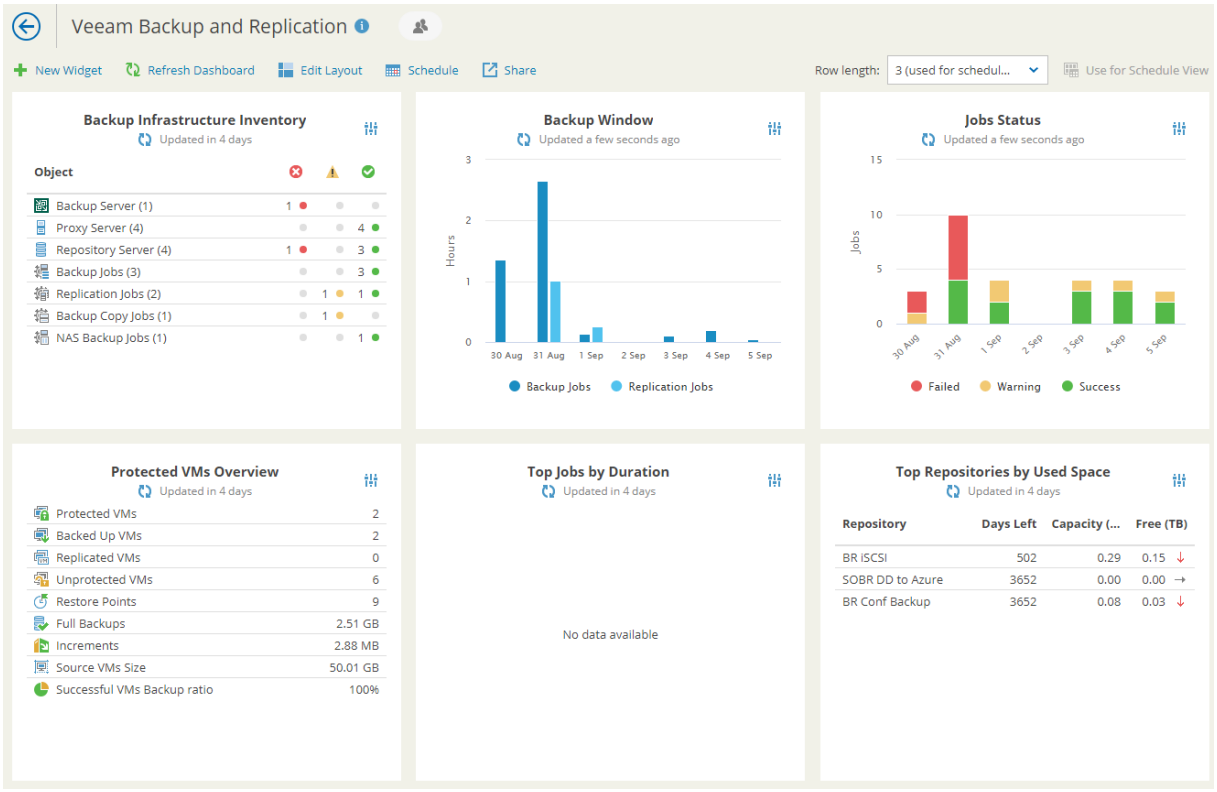
Veeam ONE -monitorointi- ja raportointiohjelma. Käytössä oleva versio on V11. Ohjelmisto integroituu Veeam Backup & Replicationin kanssa ja mahdollistaa kokonaisvaltaisen ympäristön reaaliaikaisen sekä historian monitoroinnin ja raportoinnin. Kuvassa 3 on esitetty yleinen arkkitehtuurikuva, kuinka ONE toimii. ONE sisältää myös käyttöliittymänäkymän liiketoiminnan näkökulmasta. Tällä voidaan tehdä ryhmiä, joita voidaan monitoroida.

ONE:sta saa myös reaaliaikaisia hälytyksiä esimerkiksi sähköpostiin mahdollisista poikkeuksista tai vikatilanteista. Ohjelmassa on kaksi käyttöliittymää. Sovelluspohjaisella käyttöliittymällä, pääosin konfiguroidaan ja selainpohjainen käyttöliittymä, muodostaa erilaisia näkymiä, joita halutaan seurata. Kuvassa 4 esitetään esimerkkikuva selainkäyttöliittymän tarjoamasta tiedosta koskien esimerkkitapauksessa varmistuksien tietoa. Kuvassa 5 on esimerkkikuva sovelluspohjaisesta käyttöliittymästä. ONE:lla voi myös tehdä keskeisimpiä hallintatöitä yhdestä näkymästä, Esimerkkinä snapshottien yhdistäminen. ONE koostuu komponenteista, jotka ovat ONE Server, Web UI, monitor-ohjelmisto sekä SQL-server. (Veeam, 2020a)

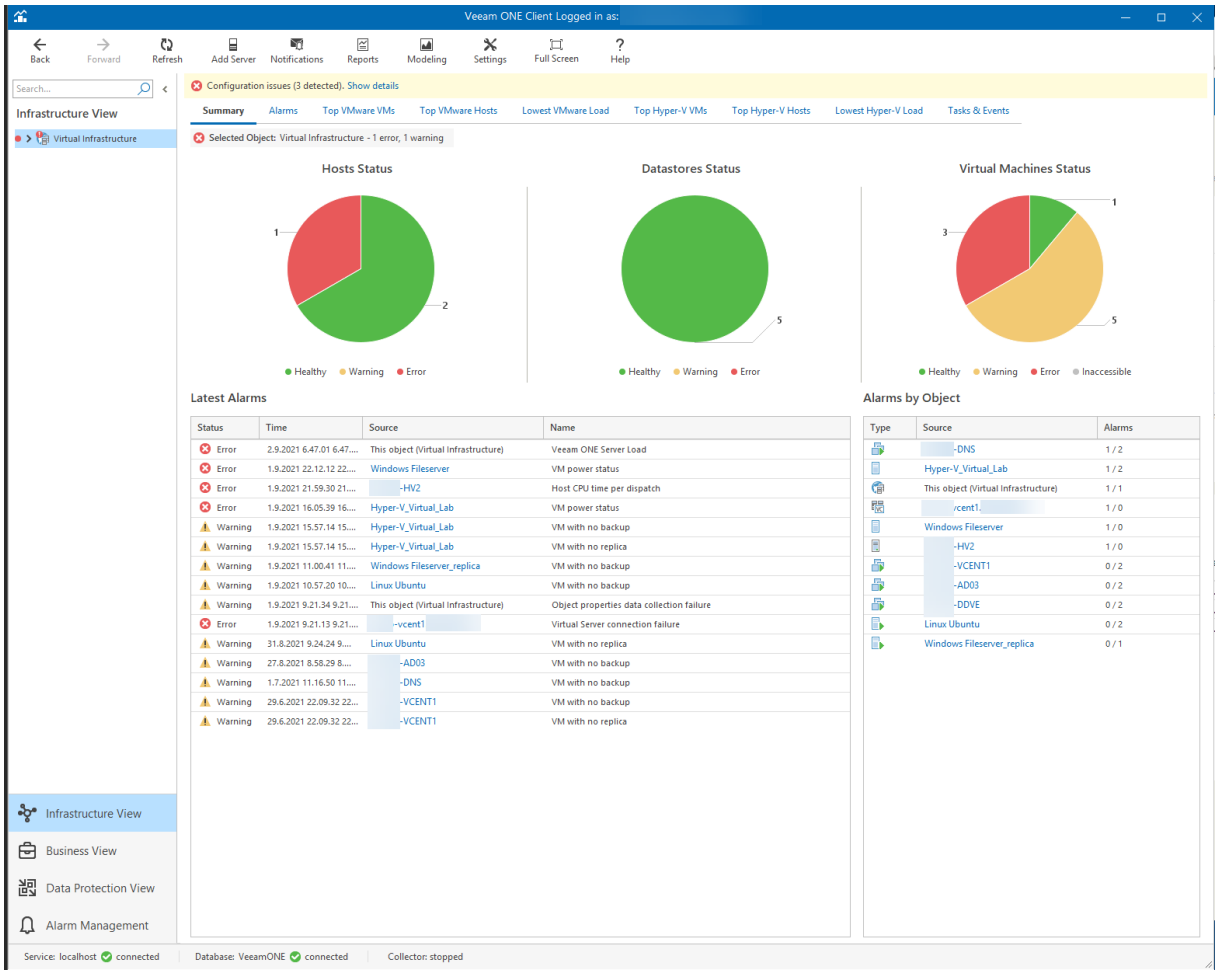
Kuva 3. Arkkitehtuurikuva ratkaisusta



Kuva 4. Esimerkkikuva selainkäyttöliittymän näkymästä



Kuva 5. Esimerkkikuva sovelluspohjaisesta käyttöliittymästä



3.5.3 Veeam ONE lisenssivaihtoehdot

ONE lisensoidaan joko täydellisenä versiona tai vaihtoehtoisesti community-versiona, joka on maksuton. Maksullinen täysversio lisensoidaan serverin prosessorikohtaisesti, instanssipohjaisesti tai vuokramallina. Instanssi tarkoittaa tässä kohtaa esimerkiksi monitoroitavaa kohdetta. Vuokramallisena lisensointi tapahtuu myös instanssipohjaisesti. Maksuttomassa community-versiossa on joitain rajoituksia verrattuna täysversioon, kuten esimerkiksi monitoroitavien palvelimien määrän rajaus ja suppeammat sähköposti-ilmoitukset. (Veeam, 2021c)

3.6 Virtuaalikoneiden merkintä virtualisointiympäristöön

VMWare tarjoaa mahdollisuuden määrittää virtuaalikoneille tunnisteita (tag). Vaatimuksena on, että käytössä on vCenter server. Tunnisteiden käyttö helpottaa virtuaalikoneiden hallintaa ja ryhmittelyä. Veeamin varmistuksissa tunnisteita voidaan käyttää hyödyksi esimerkiksi määrittelemällä toipumisaikojen tai SLA:n perusteella. Varmistustyöt toimivat dynaamisesti, mikäli varmistustyöhön on määritelty, että valintaperusteena käytetään tunnistetta tai tunnisteita.

Esimerkkinä Veeamin dokumentaatiossa kerrotaan rajoituksista, jotka on hyvä huomioida tunnisteiden käytössä. Dokumentaatiossa kuvaillaan kategorialuokan ”prioriteetti” luominen ja sille annetaan arvoksi yksi tunniste yhtä objektia kohden. Esimerkkinä kategorialuokassa on kaksi tunnistetta **normaali** ja **korkea**. Määritellessä virtuaalikoneiden kansion tunnisteeksi **normaali** ja kansion sisällä olevan virtuaalikoneen tunnisteeksi **korkea**. Mikäli varmistustyössä käsitellään objektia **normaali** -tunnisteella, niin myös virtuaalikone, jolla on **korkea** -tunniste, sisällytetään tähän työhön. Veeam Backup & Replication tulkitsee, että virtuaalikoneen säilössä olevat virtuaalikoneet perivät säilölle määritetyn tunnisteen. (Veeam, 2021e)

3.7 Toipumispiste ja toipumisaika (RPO / RTO)

RPO (Recovery Point Objective) tarkoittaa toipumispistettä. Termillä kuvataan pistettä mihin vikatilanteessa päästään palautumaan.
RTO (Recovery Time Objective) on termi, jolla mitataan aikaa vikatilanteen alkamisajasta siihen, milloin järjestelmä tulisi olla käytettävissä häiriötilanteen jälkeen. (VAHTI, 2016)

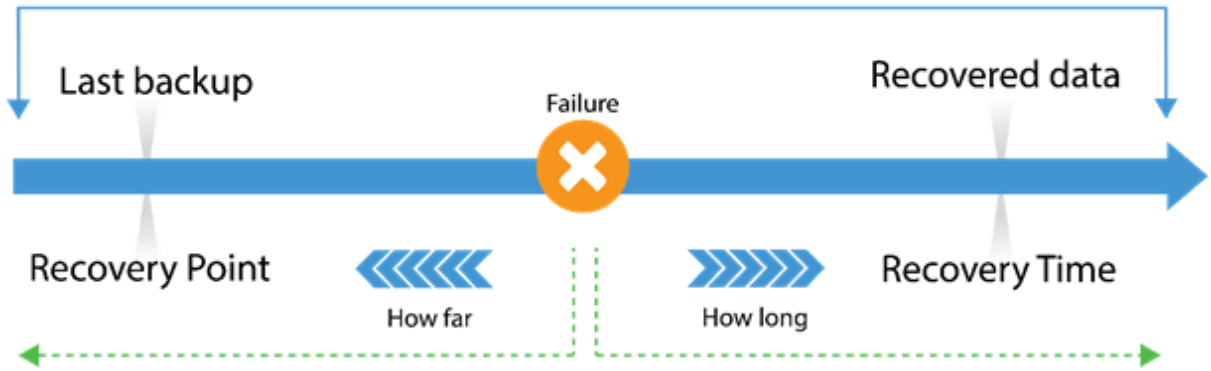
Termeillä havainnollistetaan ja määritellään palvelimien tai palveluiden kriittisyysaste eli kuinka nopeasti palvelin tai palvelu pitää olla käytettävissä mahdollisen vikatilanteen jälkeen. RPO määrittää varmistussyklin, kuinka monta kertaa päivässä palvelu tai palvelin varmistetaan. Yleisesti toipumispiste ja toipumisaika kuvataan (Kuva 3) mukaisesti. Yksityiskohtaisemmin aikajana (Kuva 4) voidaan lohkoa pienempiin osiin, jolloin kokonaisuutta voidaan tarkistella tarkemmin.

Yleisesti toipumispiste ja toipumisaika kuvataan yksinkertaisemmalla havainnekuvalla (Kuva 6). Kuva 7 on yksityiskohtaisemmin havainnollistava kuva toipumisajasta ja toipumispisteestä (kuva 7). Erityinen yksityiskohta kuvan 7 aikajanassa on reaktioaika. Reaktioajalla kuvataan sitä, miten nopeasti poikkeustilanteeseen reagoidaan. Reaktioaikaan vaikuttaa se, miten nopeasti työhön saadaan tekijä, joka pystyy aloittamaan palautustoimenpiteet. Toinen reaktioaikaan vaikuttava asia on organisaation sisäinen rakenne siitä, kuinka nopeasti palautukseen tarvittava lupa saavuttaa palautusta suorittavan henkilön. Yleisesti reaktioajan hitaus johtuu siitä, että palautusta suorittavalla henkilöllä ei ole valtuuksia palauttaa ilman ylemmän tason lupaa.

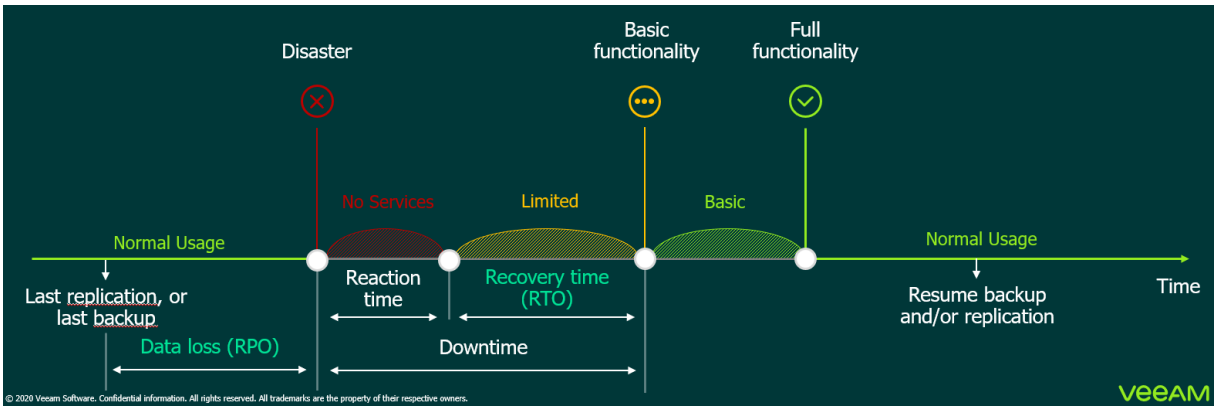
Havainnollistavana esimerkkinä käytetään poikkeustilaa organisaatiossa, jossa palautuksista päättää tietohallintopäällikkö. Organisaatiossa kriittisimmät palvelut varmistetaan kahden tunnin välein, toipumispiste on kaksi tuntia ja toipumisaika kriittisimmille palveluille on neljä tuntia. Jatkuvuuden hallinnan suunnittelussa ei ole huomioitu toipumisajassa reaktioaikaa. Palautustestissä kriittisten palveluiden palautus tuotantoon on kaksi tuntia. Arkipäivänä klo. 13.00 tapahtuu kriittinen vikatilanne ja palautustoimet joudutaan aloittamaan varmuuskopiosta. Organisaation IT-asiantuntijalla ei ole valtuuksia päättää palautuksesta vaan valtuutuksen palautukseen antaa tietohallintopäällikkö. Tietohallintopäällikkö on tavoittamattomissa kaksi tuntia ja palautusta ei pystytä aloittamaan, vaikka IT-asiantuntija olisi valmiina aloittamaan palautustyöt. Tämä pitkittää palautustyön aloittamista ja tavoiteaika saattaa ylittyä.

Jatkuvuuden suunnittelussa pidetään tärkeänä osana myös reaktioajan huomiointia. On kyse sitten sisäisestä IT-osastosta, joka palautuksen suorittaa tai ensisijaisesti palautuksista vastaavasta ulkoisesta palveluntarjoajasta, täytyy myös reaktioaika huomioida toipumisajan määrittelyssä.

Kuva 6. Yleinen havainnepiirros toipumisajasta ja toipumispisteestä(Veeam, 2017).



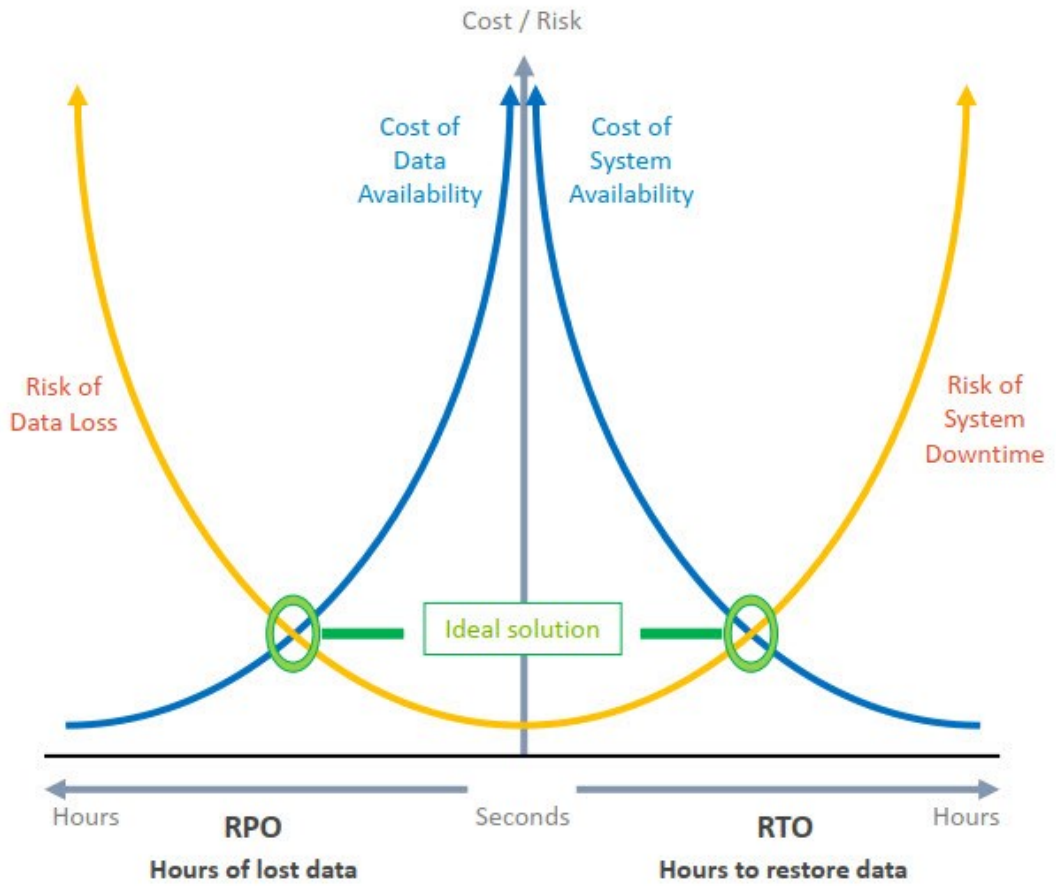
Kuva 7. RPO / RTO havainnollistava piirros (Veeam Key concepts, 2020).



3.8 Riskien ja kustannusten balanssi

Kuvan 8 piirroksella havainnollisestaan sitä miten lyhyemmät toipumisaika ja toipumispiste ajat vaativat suuremmat kustannukset. Korkeammat toipumisaika ja toipumispiste ajat madaltavat kustannuksia mutta samalla riski tietojen menettämiseen kasvaa ja järjestelmän odottamattomat käyttökatkojen määrä saattaa nousta. Optimaalinen ratkaisu täyttää tai ylittää toipumisajan ja toipumispisteen kustannusvaatimukset, jotka eivät ylitä investoinnin arvoa tai odottamattomasta käyttökatkosta aiheutuvaa kustannusta.

Kuva 8. Havainnollistava piirros riskien ja kustannuksien balanssista (Jensen, 2017).



3.9 Palvelutaso (SLA)

Palvelutasosopimuksessa määritellään kahden osapuolen välillä mitkä IT-palvelut sopimukseen sisällytetään, kuinka sopimukseen sisällytettyjen palveluiden palvelutasot määritellään ja miten palvelutasojen toteutumista seurataan. Sopimusta tehdessään osapuolet määrittelevät palvelutasotavoitteet. (Julkisen hallinnon tietohallinnon neuvottelukunta JUHTA, 2019, s. 14) JUHTA:n suosituksessa (2019 s.14) kuvaillaan palvelutasotavoitteita seuraavasti: ”Palvelutasotavoitteet määritellään sellaisiksi, että ne ovat mahdollistaa saavuttaa ja ne tukevat asiakkaan liiketoimintaa.” BIA-analyysityökalussa SLA-tasot määritellään esimerkin omaisesti viiteen eri tasoon. Tasoihin määritellään palveluaika, käytettävyys, palveluvaste sekä ratkaisuaika. Käytettävyydellä tarkoitetaan prosenttiarvoa, jolla kuvataan käytettävyystasoa. Esimerkkinä voidaan käyttää 99,9 % arvoa, joka tarkoittaa päivätasolla yhtä minuuttia ja kahtakymmentä kuutta sekuntia. Viikkotasolla sama SLA-arvo tarkoittaa kymmentä minuuttia ja neljää sekuntia (Uptime, ei pvm.).

3.10 Liiketoimintavaikutusten analyysi (BIA, Business Impact Analysis)

Kyseessä on yleismaailmallinen termi liiketoimintavaikutusten analyysista. Analyysillä selvitetään ja tutkitaan palveluiden tai palvelimien kriittisyyttä liiketoiminnan näkökulmasta. Internetistä löytyy valmiita malleja, joita voidaan käyttää yrityksen tarpeisiin lainaamalla ja muokkaamalla.

Kangas (2016, s. 3) kiteyttää vaikutustyökalun käytön seuraavasti:

> Vaikutusanalyysiä käytetään mm. toiminnan jatkuvuuden ja järjestelmien toipumisen tukityökaluna, jolla selvitetään mm. tietoturvan merkitystä ja häiriöiden (esim. käyttökatkokset tai tietojen menetys tai tietojen päivittymättömyys) vaikutusten arviointiin.

Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä VAHTI:n internet-sivulta löytyy valmis BIA-analyysipohja, jonka on luonut Arto Kangas. Aluksi käydään läpi Kankaan tekemää vaikutusarviotyökalua. Vaikutusarviotyökalulla määritellään analyysin kohde, kohteen sijainti ja palveluntarjoaja. Valmiiseen työkalupohjaan täytetään lisäksi arvioinnin teettäjä, suorittamisajankohta ja arviointiin osallistuvien henkilöiden nimet, työroolit sekä organisaatio. (Kangas, 2016)

3.10.1 ICT-varautumisen luokitukset

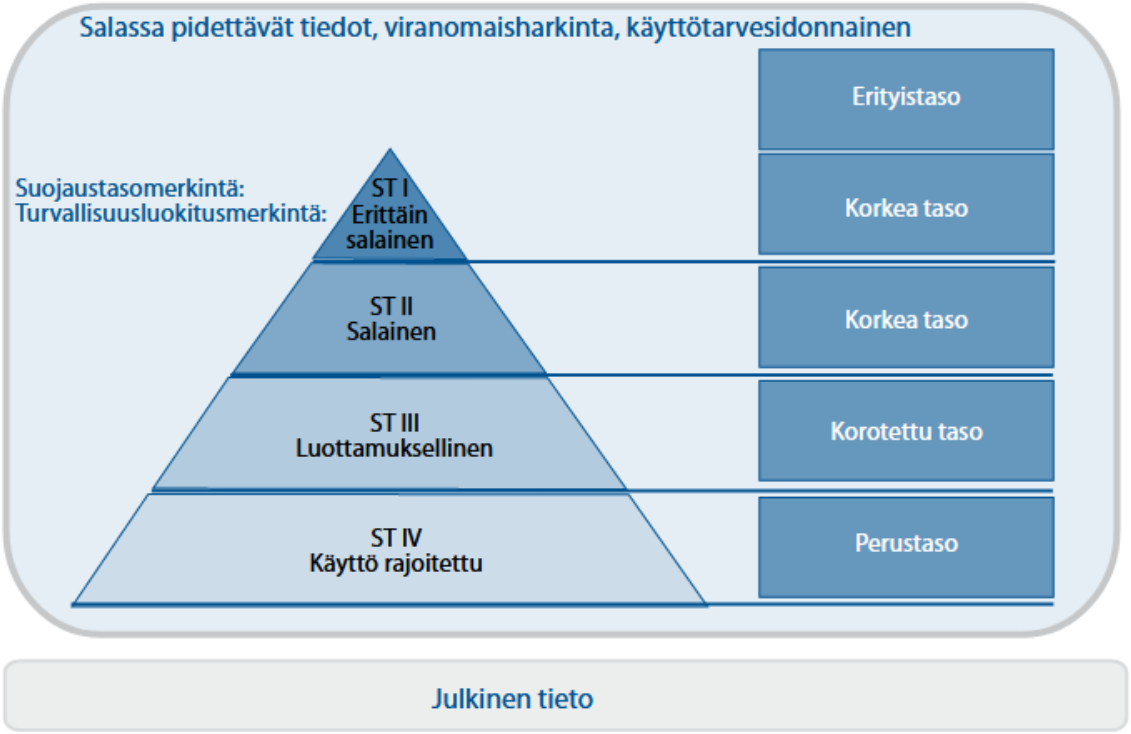
Vaikutusarviotyökalun toisessa vaiheessa määritellään kohteen, siinä käsiteltävien tietojen ja ICT-varautumisen luokitukset (Valtionvarainministeriö, 2020). Suojaustasot on määritelty ennalta arviotyökaluun ja näiden selitykset löytyvät Teknisen ICT-ympäristön tietoturvataso-ohje-julkaisusta (Valtiovarainministeriö, 2012, s. 27).

3.10.2 Tietoturvallisuuden tärkeys, palvelutasotavoitteet

Vaikutusarviotyökalussa käytetään esimerkinomaisesti viranomaisasiakirjojen luokitteluun kohdistettua suojaustaso- ja turvallisuusluokitusta. Työkalu antaa mahdollisuuden kirjoittaa vapaamuotoisen luokittelun, joka voidaan määritellä analyysin luontivaiheessa asiakaskohtaisesti. Tietoturvan tärkeyteen ja palvelutasotavoitteisiin määritellään arvot kolmeen eri kategoriaan; luottamuksellisuus, eheys ja saatavuus. Käytettäviä vaihtoehtoja on

neljä. Esimerkkinä käytetään tasoa neljä joka on määritelty erittäin tärkeäksi voidaan käyttää (VAHTI, 2012, s. 27) mukaisesti ST I- tai ST II-tason luokittelua. Tietoturvan tärkeydessä pohditaan luottamuksellisuutta, saatavuutta ja eheyttä. Luottamuksellisuuden tärkeydellä tarkoitetaan sitä, kuinka hyvin tieto on saatavilla vain niille käyttäjille, joille tieto kuuluu. Kangas (2016, s. 7) kirjoittaa ”Pääsääntöisesti tämän arvioinnissa eniten vaikuttaa se, miten paljon tietojen oikeellisuuteen (informaationa ja/tai datana) pitää pystyä luottamaan.” Saatavuuden tärkeydellä tarkoitetaan, miten helposti ja häiriöttömästi data tai palvelu on saatavilla ja käytettävissä. Saatavuuden tärkeyden arvioinnissa on otettava huomioon myös palvelutason kriittisyydestä johtuvat kustannusvaikutukset (Kangas, 2016, s. 8).

Kuva 9. Suojaustaso ja turvallisuusluokitus diagrammi (VAHTI, 2012, s. 27).



3.10.3 Käyttökatkokset, tiedon vanhenemisen vaikutukset ja tiedon menetys

Työkalun ohjeissa käydään läpi vaikutukset eri osapuolille. Vaikutukset on kategorisoitu seuraavasti: oma organisaatio, kumppanit tai alihankintatahot, asiakkaat tai loppukäyttäjät ja muut osapuolet. Muut osapuolet osiota voidaan tarpeen mukaan vaikutusarviotyökalussa muokata riippuen niiden vaikutuksista esimerkiksi terveyteen tai henkeen, lakisääteisten

tehtävien hoitamiseen, suoriin taloudellisiin menetyksiin tai maineen menetykseen. (Kangas, 2016, s. 10)

3.10.4 Keskeiset riippuvuudet

Kankaan BIA-analyysin viidennessä osiossa arvioidaan riippuvuuksia kahdesta eri kulmasta. Analyysissä luetellaan ensimmäiseksi keskeiset riippuvuudet, joista arviointikohde on riippuvainen ja merkitään kuinka tärkeitä riippuvuudet ovat. Toisesta suunnasta keskeisiä riippuvuuksia tarkastellaan palveluista, prosesseista tai tahoista nähden, joista toiminto on riippuvainen. (Kangas, 2016, s. 13)

3.10.5 Yhteiskunnan turvallisuusstrategian (YTS 2010) uhkakuvien vaikutukset

Kankaan vaikutusarviotyökalun käyttöohjeen kuudennessa osiossa käsitellään yhteiskunnan turvallisuusstrategian uhkakuvien, kuten tietoliikenteen ja tietojärjestelmien vakavien uhkien tai sotilaallisen voimankäytön vaikutuksia. Osiossa arvioidaan kohteen tärkeyttä yhteiskunnalle elintärkeille tehtäville. Osiossa tarkastellaan ja arvioidaan, onko kohteella varautumisvelvollisuuksia YTS 2010 mukaisesti. (Kangas, 2016, s. 14)

BIA-analyysi vaikutustukityökalun tekohetkellä on käytetty yhteiskunnan turvallisuusstrategiadokumenttia vuodelta 2010. Uudempi yhteiskunnan turvallisuusstrategiadokumentti on kirjattu vuodelta 2017.

4 Jatkuvuudenhallinta ja ONE:n käyttöönotto

Käytännön osuudessa perehdytään käytännön testaukseen, ratkaisun tuotantoon vientiin, BIA-analyysin suunnitteluun, määrittelyyn ja käytettävän tukityökalun valintaan.

4.1 Yleistä raportoinnista, monitoroinnista ja ilmoituksista

Opinnäytetyön kirjoittajan kuudentoista vuoden kokemus IT-työstä on se, että raportointiin ja monitorointiin kiinnitetään nykyisin enemmän huomiota kuin esimerkiksi vuonna 2005. Kysyntää monitoroinnille on paljon enemmän. Tästä kertoo se, että edellisen kahden vuoden aikana palveluna tuotettavan raportointi- ja monitorointituotteen sensorien määrä on kasvanut yli 50 prosenttia.
Aikaisemmin raportointi- ja monitorointityökalut ovat olleet vain isompien organisaatioiden saatavilla. Ohjelmien sisäiset raportointi- ja monitorointityökalut ovat olleet kankeita ja puutteellisia. Nykyisin on paljon valmistajia, joiden raportointi- ja monitorointityökalut ovat saatavilla laajoilla ominaisuuksilla. Ohjelmistojen omat työkalut ovat parantuneet ja näistä saadaan automatisoituja raportteja lähetettyä.

Monitorointi sekä raportointi ovat keskeisiä rooleja, kun valvotaan järjestelmän toimintaa sekä näillä voidaan ennaltaehkäistä tuotantokatkoja, jotka voivat aiheuttaa pahimmillaan datan häviötä. Esimerkkinä voidaan käyttää opinnäytetyössäkin keskeisessä roolissa olevaa SQL-tietokantapalvelinta. SQL kirjoittaa transaktiolokia ja mikäli tätä transaktiolokia ei varmisteta ja tyhjennetä varmistuksen jälkeen, täyttää se SQL-lokiosiota. Lokiosion täyttyessä SQL-transaktiot eivät enää onnistu. Tällöin järjestelmä, joka käyttää SQL-tietokantapalvelua menee vikatilaan ja tästä seuraa tuotantokatko.
Ilmoituksiin voidaan määritellä, että levytilaa seurataan ja raja-arvon täyttyessä siitä lähtee hälytys, jolloin voidaan tehdä ennaltaehkäiseviä toimia kuten kasvattaa levyä ja selvittää mistä ongelma johtuu. Raja-arvojen määrittely Veeam ONEssa tapahtuu prosenteilla. Raja-arvoja hälytyksessä on kaksi kappaletta. Ensimmäinen on varoitustaso, jolle oletuksena on määritetty 10 prosenttia. Toisena on virhetaso, joka oletuksena on määritetty viiteen prosenttiin. Nämä toimivat yleisesti hyvin oletusasetuksina, mutta niitä voidaan myös tarvittaessa hienosäätää.

Monitorointi tuottaa ennusteita, esimerkiksi siitä milloin varmistuskohteen kapasiteetti alkaa loppua. Ennusteiden avulla voidaan myös etukäteen budjetoida mahdollista varmistuskohteen lisäkapasiteetin tarvetta.

Raportointi mahdollistaa hyvän katsauksen ympäristön sekä varmistuksen kokonaistilasta. Automatisoituna tämä helpottaa normaalia arkirutiinia. Tällä vältytään esimerkiksi rutiininomaiselta varmistuspalvelimen tarkastelulta esimerkiksi varmistuksien poikkeamien suhteen. Varmistusohjelmistossa itsessään on varmistustyöraportointi integroituna mikä kertoo varmistustyökohtaisesti, onko poikkeuksia. Isoissa ympäristössä varmistustöitä voi olla kymmeniä tai satoja. Tästä aiheutuu sähköpostitulva, mikäli kaikki varmistustyöt ilmoittavat oman tilatietonsa sähköpostilla päivittäin. Veeam ONE mahdollistaa tiedon koostamisen yhteen postiin, joka sisältää oleellisen tiedon. Esimerkkinä raportista on varmistustöiden aikatrendit. Trendit näkyvät punaisena tai vihreänä nuolena. Tästä voidaan myös nähdä, onko varmistusaika ollut normaalia pidempi. Trendimuutoksesta voidaan päätellä, onko varmistushetkellä ollut suorituskykyongelmaa tai onko datan määrä kasvanut edellisestä varmistuksesta merkittävästi, joka näkyy varmistuksen pituudessa.

Ilmoituksien ja hälytyksien konfigurointiin saa käytettyä paljon aikaa. Se on kuitenkin kannattavaa. Määrittelyllä ja konfiguroinnilla säästetään työaikaa ja henkilöresursseja voidaan käyttää tehokkaammin muualla, kun resurssia ei sidota jokapäiväisiin rutiinin omaisiin tarkastuksiin.
Kappaleessa tuodaan esille näkökulma, joka on muodostunut useista keskusteluista IT-ammattilaisten kanssa. Jokapäiväinen rutiinitarkastus monessa tilanteessa menee rutiinilla ja tarkistuksen tekevä henkilö saattaa tulla sokeaksi ilmoituksille ja hän ei välttämättä huomaa poikkeusta mikä taas saattaa aiheuttaa pidemmässä juoksussa pahimmassa tapauksessa datahäviötä tai tuotantokatkon. Raportointisovellus tekee pyyteettömästi joka päivä rutiinityön työntekijän puolesta.

Sovelluksesta saadaan myös liiketoimintalähtöisiä raportteja, joka voidaan automatisoida ja lähettää henkilölle joka kuukausi, kvartaaleittain tai vuosittain. Automatisoinnilla liiketoiminnasta vastaava henkilö saa haluamansa raportin automaattisesti ja tätä ei tarvitse erikseen hänelle muodostaa. Tällä saadaan myös vapautettua resurssia muihin tehtäviin.

4.2 Pohdintaa valmiin ja oman BIA-analyysin välillä

Osiossa pohditaan valmiin ja opinnäytetyön ohella tehdyn BIA-analyysin välillä. Kankaan vaikutusarviotyökalussa on paljon hyviä osioita, joita voi käyttää ja hyödyntää. Kankaan vaikutusarviotyökalu on kuitenkin ensisijaisesti tarkoitettu julkishallintoon vaikkakin siinä on osioita, joita voidaan hyödyntää myös yritysmaailmassa. Kankaan luoma vaikutusarviotyökalu ei soveltunut tämän opinnäytetyön loppuasiakkaan käyttöön sillä se oli liian raskas laajuudestaan ja yksityiskohdistaan johtuen. Käyttöohjeessa, opinnäytetyön kirjoittajan mielestä jotkut kohdat oli kirjoitettu epäselvästi tai puutteellisesti, joka vaikeutti dokumentin ja vaikutusarviotyökalun tulkintaan ja käytettävyyteen. Tätä opinnäytetyötä varten käytiin läpi erityyppisiä BIA-analyysimalleja ja vertailtiin näiden ominaisuuksia. Ulosrajatut BIA-analyysityökalut olivat ominaisuuksiltaan puutteellisia eivätkä ne vastanneet asiakkaan tarpeita. Kankaan BIA-vaikutusarviotyökalu otettiin tarkempaan tarkasteluun, sillä se sisälsi eniten asiakkaan tarpeiden kannalta hyödynnettäviä ominaisuuksia. Kangas on tehnyt erittäin hyvän ja kattavan BIA-vaikutusarviotyökalun, joka on saatavilla Suomidigin internetsivuilta (Valtionvarainministeriö, 2020).

Ensisijainen tarkoitus oli räätälöidä hyvä ja helppokäyttöinen analysointityökalu asiakkaalle, jolle opinnäytetyö toteutetaan. BIA-analyysityökalusta toteutettiin myös englanninkielinen versio. Analyysityökalussa haluttiin keskittyä asiakkaalle tärkeisiin ja hyödyllisiin osioihin. Opinnäytetyöprosessin aikana luotiin BIA-vaikutusarviotyökalu, joka mukailee hyviksi havaittuja käytäntöjä ja tätä varten jo olemassa olevista vaikutusarviotyökaluista lainattiin hyväksi havaittuja osioita. Arviointikriteerejä on muutettu niin että ne palvelevat parhaimmalla mahdollisella tavalla yritystä, jonka käyttöön analyysi tuotettiin.

Saatavuus-, eheys- ja suojaustasojen määrittelyssä on käytetty erilaisia variaatioita. Yleinen käytäntö monessa BIA-analyysin ohjeistuksessa on määritelty, että vähäisen merkityksen tai merkityksettömyyden voi jättää merkitsemättä tai määrittelemättä mikä hieman keventää analyysin luontiprosessia.

Opinnäytetyön edetessä havaittiin, että asiakaskohtaisesti kohdennettu BIA-analyysi palvelee paremmin tarkoitustaan ja BIA-analyysissä voidaan keskittyä keskeisiin palvelu- ja palvelinkomponentteihin. Opinnäytetyössä luodussa BIA-analyysityökalussa (Liite 1)

keskitytään ensisijaisesti tarkastelemaan asiakasympäristöä ja käyttämällä niitä komponentteja analyysissä, jotka on koettu asiakkaan kanssa käydyissä keskusteluissa tärkeäksi heille liiketoiminnan ja IT-näkökulmasta.

4.3 BIA-analyysin esittely

Seuraavissa kappaleissa perehdytään tarkemmin opinnäytetyön aikana toteutettuun BIA-analyysiin. Tarkoituksena on selkeyttää lukijalle analyysityökalun käytön vaikutuksia asiakkaan tietojärjestelmien käytettävyyteen, sekä kuinka saatavuus- ja eheystasoja on suunniteltu käytettäväksi.

4.3.1 Yleiset tiedot

Yleiset tiedot-kentässä määritellään perustiedot, jotka seuraavat läpi dokumentin elinkaaren. Analyysin kohde voi olla kokonaiskuva palveluympäristöstä, tietty palveluympäristö tai yksittäinen palvelu, jota tarkastellaan. Analyysin kohde vaikuttaa siihen miten syvälle analyysissä paneudutaan. Kuvassa 10 esitellään esimerkinomaisesti, kuinka lomaketta täytetään (Kuva 10).

Kohteen sijainnin voi dokumentin täyttäjä määrittää omalla, riittävän tarkalla määrittelyllä. Yleisesti voi riittää kaupunki tai vaihtoehtoisesti esimerkiksi pilvipalvelualusta Microsoft Azure tai Amazon AWS.

Palveluntarjoaja voidaan määrittää sen mukaan, miten tarkasti analyysin kohde on rajattu. Esimerkkinä voidaan käyttää kokonaisvaltaista ja pintapuolista BIA-analyysiä yrityksen IT-ympäristöstä. Näin ollen palveluntarjoaja voi olla ulkopuolinen yritys tai vaihtoehtoisesti yrityksen sisäinen IT-organisaatio.

Dokumentaatioon kirjataan ne henkilöt, jotka ovat olleet mukana tekemässä ja arvioimassa analyysia. Mikäli dokumentin elinkaari on pitkä, voidaan käyttää tarkentavana lisäkenttänä vielä mukana versiossa-kenttää, johon voidaan eritellä, kuka on ollut määrittelemässä mitäkin versiota. Versioinnissa kuitenkin tärkeintä on pitää yhdenmukaisuus läpi dokumentin elinkaaren.

Organisaatio-kentässä voidaan käyttää yritystä, tai esimerkiksi tiettyä liiketoimintayksikköä yrityksen sisällä. Dokumentissa määritellään, kuka arvioinnin on teettänyt sekä mikä hänen roolinsa on yrityksessä.

Kuva 10. Yleiset tiedot

1. Yleiset tiedot

Analyysin kohde	**Ympäristö A / Palvelu A**	**Organisaatio**	**Yritys A**
Kohteen sijainti	**Kaupunki / Konesali**	**Arvioinnin teettäjä**	**Matti Malli**
Palveluntarjoaja	**Palveluntarjoaja A**	**Rooli**	**IT Manager**

Arvioinnissa mukana olleet henkilöt

Nimi	Rooli	Organisaatio	Mukana versiossa
Matti Malli	IT Manager	Yritys A	1
Mikko Mallikas	Specialist	Yritys B	1
Teppo Testi	Specialist	Yritys B	1

Dokumentin versiointi

Versio	Päivämäärä	Päivittäjä	Muutos
1	28.4.2021	Mikko Mallikas	Ensimmäinen versio

4.3.2 Palvelutasojen määrittely

Palvelutasoissa määritellään eri palvelutasot palveluille. Palvelutasoja voi olla enemmän tai vähemmän mikäli analyysi sitä vaatii ja se koetaan tarpeellisena. Esimerkkinä kuvassa 11 on käytetty viittä eri palvelutasoa (Kuva 11).

4.3.3 Eheystasot

Eheystasolla tarkoitetaan sitä, kuinka tietojen oikeellisuuteen täytyy pystyä luottamaan. Samoin kuin palvelutasoissa, voidaan eheystasojen määrävaatimusta tarkastella analyysin hahmottelu- tai aloitusvaiheessa. Esimerkissä eheystasoja on kolme, jotka ovat erittäin tärkeä, merkityksellinen sekä vähäinen merkitys (Kuva 11).

4.3.4 Saatavuustasot

Saatavuustasoilla arvioidaan, kuinka kriittinen palvelu on kyseessä ja kuinka paljon saatavuuden heikkeneminen vaikuttaa tuotantoon. Esimerkissä saatavuustasot ovat määritelty kolmeen eri kategoriaan (Kuva 11).

4.3.5 Koontinäkymä palvelutasoista

Koontinäkymään on kerätty toipumisaika, toipumispiste, palvelutaso, eheys- sekä saatavuustasot. Toipumisaika määritellään näkymään palvelukohtaisesti ja vaikutusarviotyökaluun on luotu indikaattori tason mukaan, joka näyttää värillä kuinka kriittisestä palvelusta on kyse. Punainen väri merkitsee lyhyttä toipumisaikaa ja vihreä tarkoittaa pidempää toipumisaikaa. Toipumispiste-kentässä määritellään, miten pitkä toipumispiste palvelulla on. SLA on lyhennetty palvelutasosta. Eheys-sarakkeessa määritellään palvelun eheyden kriittisyys. Saatavuus sarakkeessa määritellään palvelun saatavuuden kriittisyys.

Kuva 11. Palvelutason määrittely

2. Palvelutason määrittely

Palvelutaso (SLA)	Palveluaika	Käytettävyys	Palveluvaste	Ratkaisuaika
5	24/7	99,9 %	30min	2h
4	24/7	99,5 %	60min	4h
3	työpäivinä 6-24	99 %	90min	12h
2	työpäivinä 6-24	99 %	4h	24h
1	työpäivinä 6-24	99 %	8h	48h

Eheystasot	Kriittisyys
3	Erittäin tärkeä
2	merkityksellinen
1	Vähäinen merkitys

Saatavuustasot	Kriittisyys
3	Erittäin tärkeä
2	merkityksellinen
1	Vähäinen merkitys

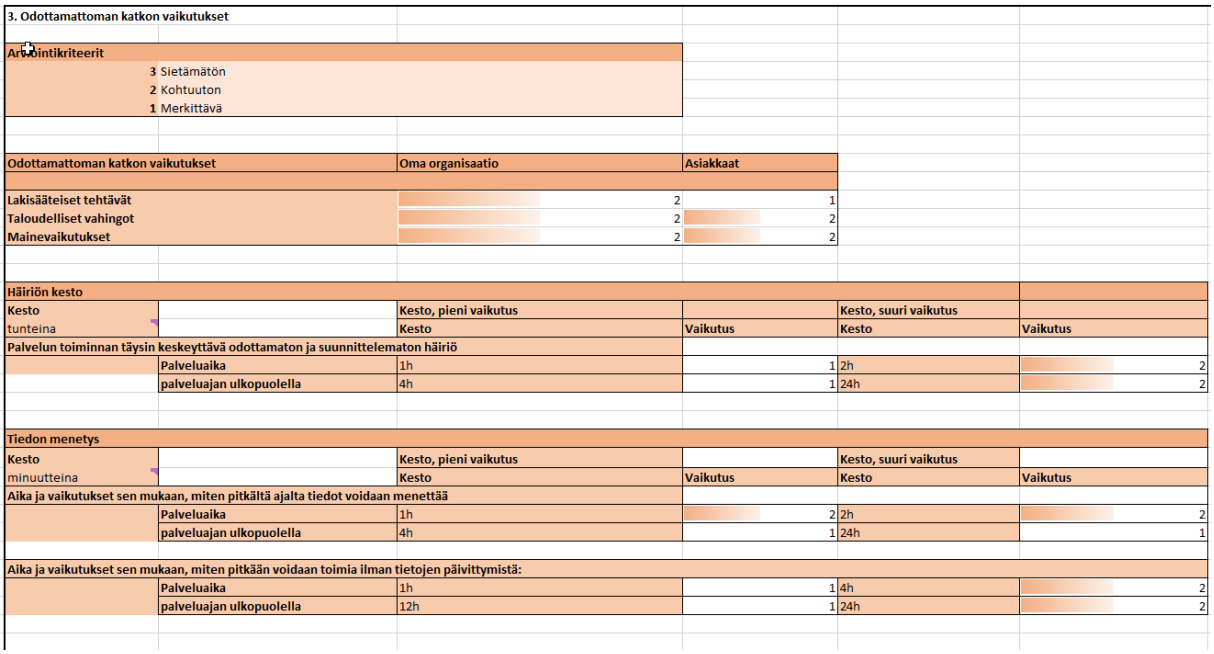
Palvelu	RTO (h)	RPO (h)	SLA	Eheys	Saatavuus
Palvelu 1	5	24	5	2	3
Palvelu 2	1	0,25	4	3	3
Palvelu 3	1	0,25	4	3	3
Palvelu 4	1	24	5	3	2
Integraatiopalvelu 1	2	24	2	2	1
Integraatiopalvelu 2	3	24	4	2	2
Integraatiopalvelu 3	4	24	2	2	1
Integraatiopalvelu 4	4	24	2	2	1
Integraatiopalvelu 5	4	24	4	2	2
Integraatiopalvelu 6	4	24	5	3	3
Integraatiopalvelu 7	4	24	5	3	3

4.3.6 Odottamattomien katkojen vaikutukset

Odottamattomien katkojen vaikutuksia analyysissä tarkastellaan vastaavin arviointikriteerein kuin saatavuus tai eheystasoissa. Esimerkissä arviointikriteereissä on käytetty kolmea (Kuva 12). Odottamattomien katkojen vaikutuksia on määritelty useita riippuen siitä mistä BIA-analyysivaikutusarviotyökalusta on kyse, mutta tässä opinnäytetyössä käytettävään vaikutusarviotyökaluun on määritelty kolme arviointialuetta, jotka vaikuttavat tapahtuessaan eniten yritykseen jolle analyysi tehtiin. Arviointikriteeristö on jaettu kolmeen eri kategoriaan.

Häiriön kestossa arvioidaan häiriön vaikutusta tuotantoon. Häiriön kesto on eritelty kahteen eri kategoriaan, kesto, jolla on pieni vaikutus sekä kesto, jolla on suuri vaikutus (Liite 1). Häiriön vaikutukset tarkastellaan aina analyysin alussa asiakaskohtaisesti. Keston määreenä voidaan käyttää esimerkiksi minuuttia, tuntia tai päivää. Päivä on melko harvinainen määre, mutta mahdollinen esimerkiksi palvelulle, jota käytetään kerran kuukaudessa. Tiedon menetyksessä käytetään samankaltaista aikamäärettä kuin häiriön kestossa. Häiriön kestossa arvioidaan vaikutusta ajalta miltä tieto katoaa. Pieni vaikutus voi olla yksi tunti ja silloin esimerkin omaisesti se on merkittävä. Suurella vaikutuksella esimerkissä kuvataan kahta tuntia, jolloin vaikutus on kohtuuton. Kolmantena arvioidaan aikaa ja vaikutuksia sen mukaan, kuinka pitkään voidaan toimia ilman tietojen päivittymistä. Tällä arvioidaan tilannetta, miten pitkään tuotantoa voidaan pitää käynnissä ilman tietojen syöttämistä tai tietojen saamista tietojärjestelmästä.

Kuva 12. Odottamattoman katkon vaikutukset

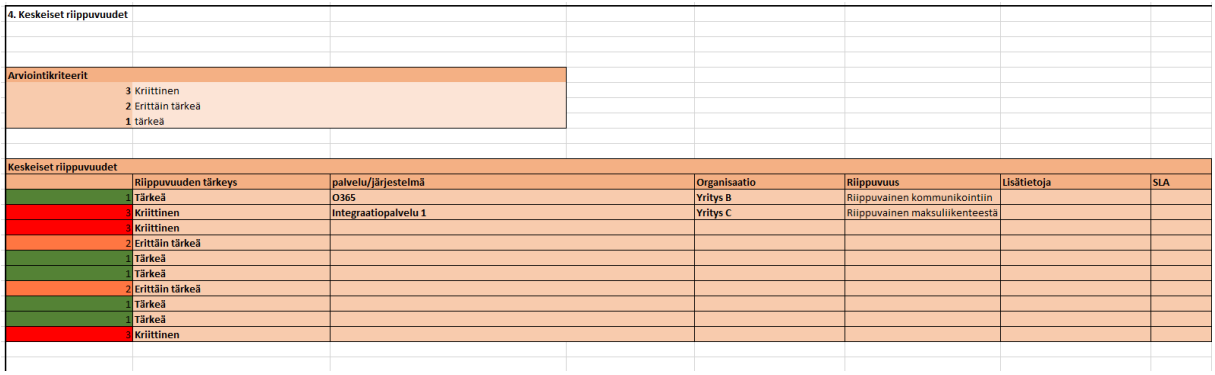


3. Odottamattoman katkon vaikutukset						
Arviointikriteerit						
3 Sietämätön						
2 Kohtuuton						
1 Merkittävä						
Odottamattoman katkon vaikutukset		Oma organisaatio		Asiakkaat		
Lakisääteiset tehtävät			2	1		
Taloudelliset vahingot			2	2		
Mainevaikutukset			2	2		
Häiriön kesto						
Kesto		Kesto, pieni vaikutus			Kesto, suuri vaikutus	
tunteina		Kesto		Vaikutus	Kesto	Vaikutus
Palvelun toiminnan täysin keskeyttävä odottamaton ja suunnittelematon häiriö						
	Palveluaika	1h		1	2h	2
	palveluajan ulkopuolella	4h		1	24h	2
Tiedon menetys						
Kesto		Kesto, pieni vaikutus			Kesto, suuri vaikutus	
minuutteina		Kesto		Vaikutus	Kesto	Vaikutus
Aika ja vaikutukset sen mukaan, miten pitkältä ajalta tiedot voidaan menettää						
	Palveluaika	1h		2	2h	2
	palveluajan ulkopuolella	4h		1	24h	1
Aika ja vaikutukset sen mukaan, miten pitkään voidaan toimia ilman tietojen päivittymistä:						
	Palveluaika	1h		1	4h	2
	palveluajan ulkopuolella	12h		1	24h	2

4.3.7 Keskeiset riippuvuudet

Keskeisten riippuvuuksien arviointikriteereissä on määritelty esimerkissä kolme kriteeriä. BIA-analyysin esimerkissä arvioinnin kohteena on koko yrityksen IT-infrastruktuuri, joten keskeisiä riippuvuuksia monesti koko ympäristössä on useampia (Kuva 13). Näitä yleisimpiä ovat kommunikointiratkaisut sekä erilaiset integraatiopalvelut. Esimerkissä on käytetty näitä kahta kuvaamaan arviointia (Kuva 13). Tärkeys määritellään arviointikriteerien mukaisesti, palvelu- tai järjestelmäsarake täytetään riittävän tarkasti kuvaamaan palvelua tai järjestelmää. Organisaatiolla tarkoitetaan sitä, kuka palvelun tai järjestelmän on toimittanut sekä tuntee tai ylläpitää järjestelmää. Riippuvuudella kuvataan mistä palvelu tai järjestelmä on riippuvainen. Lisätietokenttään voidaan kirjoittaa tarkentavia lisätietoja. Viimeisenä palveluille määritellään palvelutaso. Palvelutasossa voidaan käyttää samaa kriteeristöä kuin aiemmin palvelutasomäärittelyssä tai voidaan tehdä erillinen palvelutasokriteeristö.

Kuva 13. Keskeiset riippuvuudet



4. Keskeiset riippuvuudet

Arviointikriteerit	
3	Kriittinen
2	Erittäin tärkeä
1	tärkeä

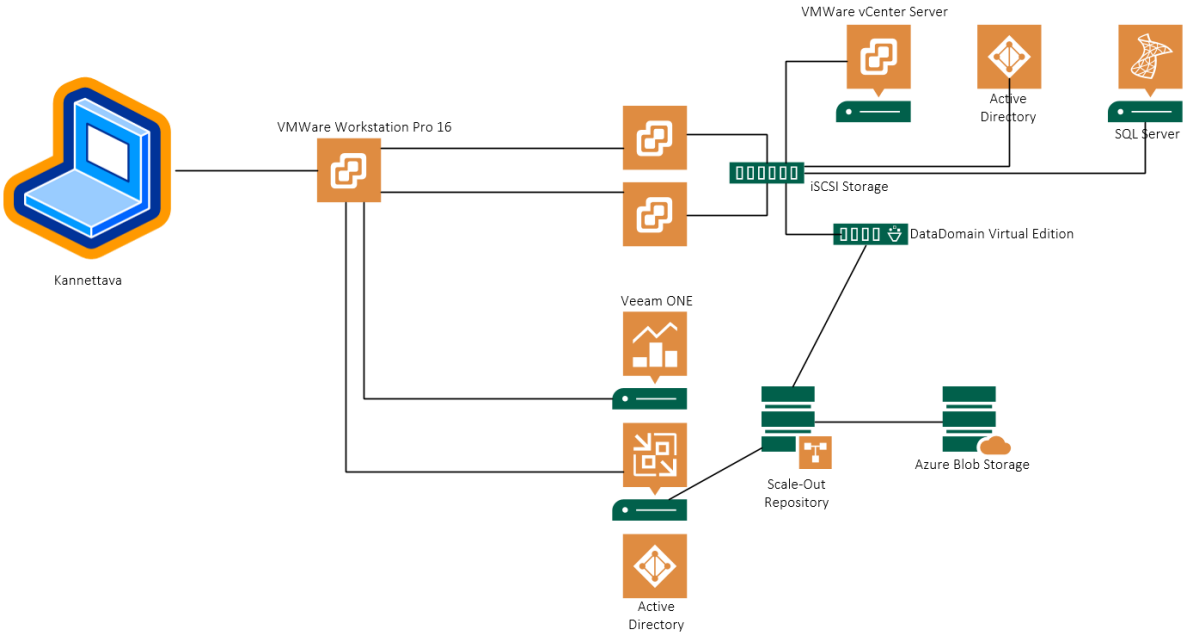
Keskeiset riippuvuudet

	Riippuvuuden tärkeys	palvelu/järjestelmä	Organisaatio	Riippuvuus	Lisätietoja	SLA
1	Tärkeä	O365	Yritys B	Riippuvainen kommunikointiin		
3	Kriittinen	Integraatiopalvelu 1	Yritys C	Riippuvainen maksuliikenteestä		
3	Kriittinen					
2	Erittäin tärkeä					
1	Tärkeä					
1	Tärkeä					
2	Erittäin tärkeä					
1	Tärkeä					
1	Tärkeä					
3	Kriittinen					

4.4 Demoympäristö testaukselle

Demoympäristönä toimii tietokone, johon on asennettu VMWare Workstation Pro 16. VMWare Workstationin alustalla pyörii kolme VMWare ESXI 7.0.1-virtualisointialustaa, jotka simuloivat todellista tuotantoympäristöä. Virtuaalialustojen päällä pyörii virtualisoitu VMWare vCenter Server -hallintaohjelmisto. Virtuaaliympäristö on eristetty erillisellä pfSense -palomuurilla. Verkko on segmentoitu erilliseen verkkoon. Levyjärjestelmää ympäristössä simuloi TrueNAS-ohjelmisto, joka esittää levyä VMWarelle iSCSI-protokollalla. Demoympäristö koostuu useista virtuaalipalvelimista, joita ovat Active Directory, SQL, Veeam Backup & Replication, Veeam ONE sekä tiedostopalvelin. Ympäristöllä voidaan simuloida, testata ja luoda erilaisia skenaarioita koskematta tuotantoympäristöön. Varmistuskohteena toimii virtualisoitu Dell EMC DataDomain Virtual Edition, joka duplikoidaan Microsoft Azuressa sijaitsevaan blob storageen.

Kuva 14. Demoympäristö



4.5 Veeam ONEn asennus

Asennus aloitetaan määrittelemällä palvelin tai palvelimet, joihin palvelut asennetaan. Chris Childerhose kuvaa kirjassaan prosessin olevan hyvin suoraviivainen. Ennen asennuksen aloittamista, suositellaan tarkistamaan alustan ja järjestelmän vaatimukset. Lisäksi on tärkeää käydä läpi käyttäjätilien oikeudet sekä verkkoportit. (Childerhose, 2021, s. 273) Optiona asennuksessa voidaan perustaa SQL-tietokanta jo ennen asennuksen aloitusta. Järjestelmän vaatimukset ja suositukset riippuvat siitä, miten monta palvelinta on monitoroitavana. Vaatimukset ja suositukset ovat Veeamin määrittelemiä (Veeam, 2021d).

Esimerkkinä tässä opinnäytetyössä käytetään 100 palvelimen vaatimuksia ja suosituksia. Suoritinvaatimus on vähintään 4 vCPU:ta ja suositus on 8 vCPU:ta. Muistivaatimus palvelulle on 4 GB ja valmistaja suosittelee vähintään 8 GB. Kiintolevysuositus on vähintään 50 GB. Valmistaja tarjoaa laskentakaavan millä helpotetaan palvelimen kapasiteetin tarpeen määrittelyä (Veeam, 2021d). Tuetut käyttöjärjestelmät sekä tuettujen SQL- palvelimien listaus löytyy Veeam:in ohjesivuilta (Veeam, 2021a). Childerhose suosittelee palvelun komponenttien osoittamisen eri levyasemille; järjestelmälevy, ohjelmisto, tietokanta ja suorituskyvyn välimuisti jokainen omalle levyasemalleen (Childerhose, 2021, s. 274). Parhaita käytäntöjä käyttämällä levyasemia tarvitaan neljä, ja näin toimimalla palvelun käyttöön saadaan nopeutta ja suorituskykyä.

Asennuksessa voidaan valita tilanteeseen sopivampi asennustyyppi kahdesta vaihtoehdosta. Pienempiin ympäristöihin suositellaan tyypillistä asennusta ja suurempiin ympäristöihin suositellaan kehittyneempää asennusta. Kehittyneempi asennus antaa mahdollisuuden hajauttaa ONE:n palveluita eri palvelimille. Asennusohjelma tarkistaa, onko palvelimelle asennettuna jo vaadittavat oheissovellukset. Mikäli oheissovelluksia ei ole, asennusohjelma asentaa oheissovellukset automaattisesti. Tarkempi lista oheissovelluksista löytyy ohjesivustolta (Veeam, 2021b). Asennusohjelma kysyy mihin asemalle palvelu asennetaan. Oletuksena asennusohjelma tarjoaa käyttöjärjestelmän Program Files -kansiota. Palvelu tarvitsee palvelutilin (service account). Tietoturvanäkökulmasta suositellaan käyttämään erillistä palvelutiliä, jolla ei ole oikeuksia muualle kuin palveluun tarvittaviin palveluihin. Asennusohjelma kysyy seuraavaksi SQL-palvelimen osoitetta ja instanssia mihin ONE tallentaa tiedon. SQL-palvelimeen voi kirjautua joko Windows-käyttäjätunnuksilla tai SQL:n

omalla sa-tunnuksella (Childerhose, 2021, s. 279). Asennuksessa voidaan määritellä lisenssi, jolla palvelu aktivoidaan. Mikäli lisenssi on saatavilla, osoitetaan lisenssitiedosto asennusohjelmalle tai jos ONE asennetaan samalle palvelimelle kuin Veeam Backup & Replication, löytää asennusohjelma lisenssin automaattisesti.

Asennusohjelmassa määritellään yhteyden muodostukseen käytettävät portit sekä varmenteen. Oletuksena ONE käyttää raportoinnin web-rajapintaan HTTPS 1239 ja Veeam ONE agent käyttää porttia TCP 2805. Mikäli halutaan muuttaa portteja esimerkiksi tietoturvan vuoksi, voidaan nämä portit muuttaa.

Asennusohjelman viimeisessä vaiheessa määritellään suorituskyvyn datan välimuistikansio. Oletuksena asennusohjelma tarjoaa käyttöjärjestelmä osiota, mutta suosituksien mukaan se on hyvä olla erikseen sille varatulla levyosiolla (Childerhose, 2021, s. 273). Asennusohjelma kysyy virtuaalisen infrastruktuurin tyyppiä. Vaihtoehdot ovat VMWare vCenter Server tai Hyper-V host, Failover cluster tai SCVMM Server. Ohjeistuksessa suositellaan ohittamaan tämä vaihe ja jatkamaan asennusta.

Asennuksen edistyessä määritellään datan keräämismuoto ympäristöstä. Vaihtoehtoja on kolme. Optimoitu tyypilliseen käyttöönottoon, optimoitu skaalautuvaan käyttöönottoon tai vain varmistusdatan keräämiseen. Tyypillinen käyttöönotto on suunnattu pienempiin ympäristöihin, joissa on vähemmän kuin 100 fyysistä virtualisointialustaa ja alle 1500 virtuaalikonetta. Skaalautuvaa käyttöönottoa suositellaan, kun tyypillisen käyttöönoton rajat ylittyvät. Lopuksi asennusohjelma näyttää koosteen määrittelyistä josta voidaan tarkastaa asennusmäärityksien oikeellisuus ennen asentamista.(Childerhose, 2021, s. 283).

Ohjelman ensimmäisellä käynnistyskerralla käynnistyy ohjattu määrittely, jolla osoitetaan sähköpostin lähettämiseen käytettävä palvelin, osoitteet joihin ilmoitukset toimitetaan sähköpostilla ja lähetystiheys. Ohjattu määrittely voidaan myös ohittaa ja konfiguroida myöhemmin.

Ohjatun määrittelyn jälkeen aukeaa itse ohjelma, joka on lähes tyhjä, kun konfigurointeja ei ole tehty eikä tietoa ole vielä kerätty ympäristöstä. Monitoroitavan ympäristön liittämisen jälkeen muodostuu näkymään yleiskuvaus ympäristöstä.

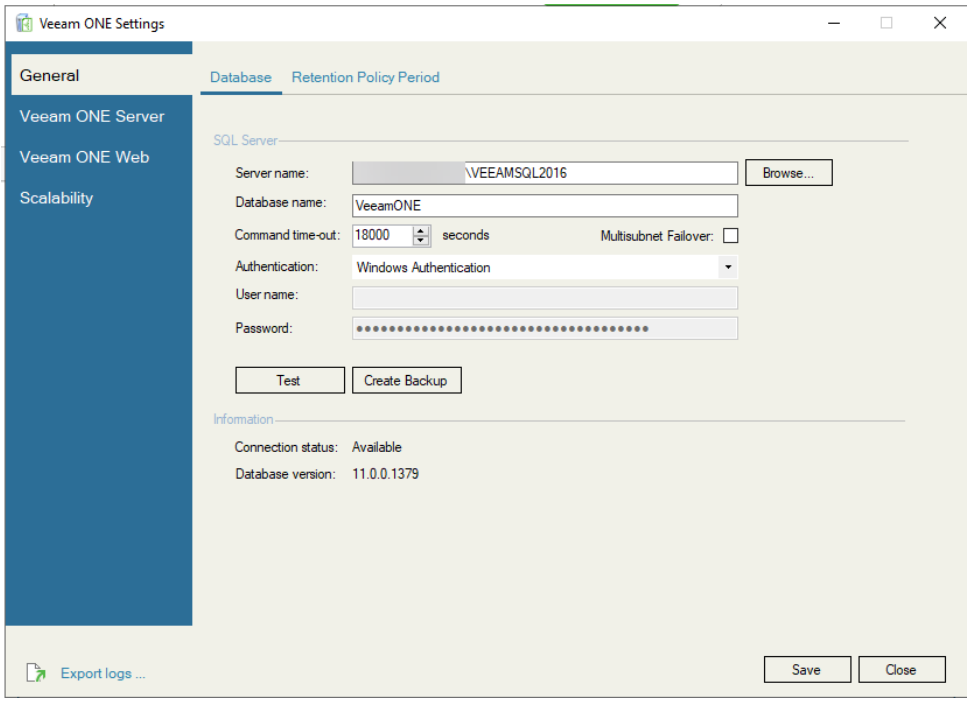
4.6 Veeam ONE päivitys

Luvussa kerrotaan päivitysprosessista demoympäristön sekä tuotantoympäristön päivityksestä versioon V11. ONE:n päivityksellä saavutetaan paremmat monitorointi- ja raportointiominaisuudet verrattuna edelliseen versioon.

4.6.1 Testiympäristön päivitys

Ensimmäisessä vaiheessa päivitetään demoympäristön Veeam ONE versioon 11. Opinnäytetyön kirjoitushetkellä ONEsta on tullut päivitys, joka mahdollistaa asiakkaan näkökulmasta paremman raportoinnin ja monitoroinnin. Päivitysprosessi aloitetaan ottamalla olemassa olevasta tietokannasta varmuuskopio. ONE:n työkaluista löytyy varmistusosio, jolla tietokannasta johon data tallennetaan, otetaan varmistus ennen päivitystä.

Kuva 15. Tietokannan varmistaminen



4.6.2 Veeam ONE päivitys tuotantoympäristössä

Tuotantoympäristön päivittäminen aloitetaan varmistamalla nykyinen Veeam ONE:n SQL-kanta Veeamin omalla tietokannan varmistustyökalulla. Varmistuksessa kesti jonkin verran kauemmin verrattuna demoympäristön varmistamiseen. Demoympäristön tietokannan koko oli 1,2GB kun taas tuotantotietokannan koko oli lähes 4 GB. Tietokannan varmistus sujui hyvin. Tietokannan varmistuksen palautusta testattiin demoympäristössä toimivaan SQL-palvelimeen ja ajamalla SQL-komentojonon, joka tulosti saman tiedon mitä tuotantotietokannasta saatu tuloste oli.

4.7 Virtuaalikoneiden merkintä

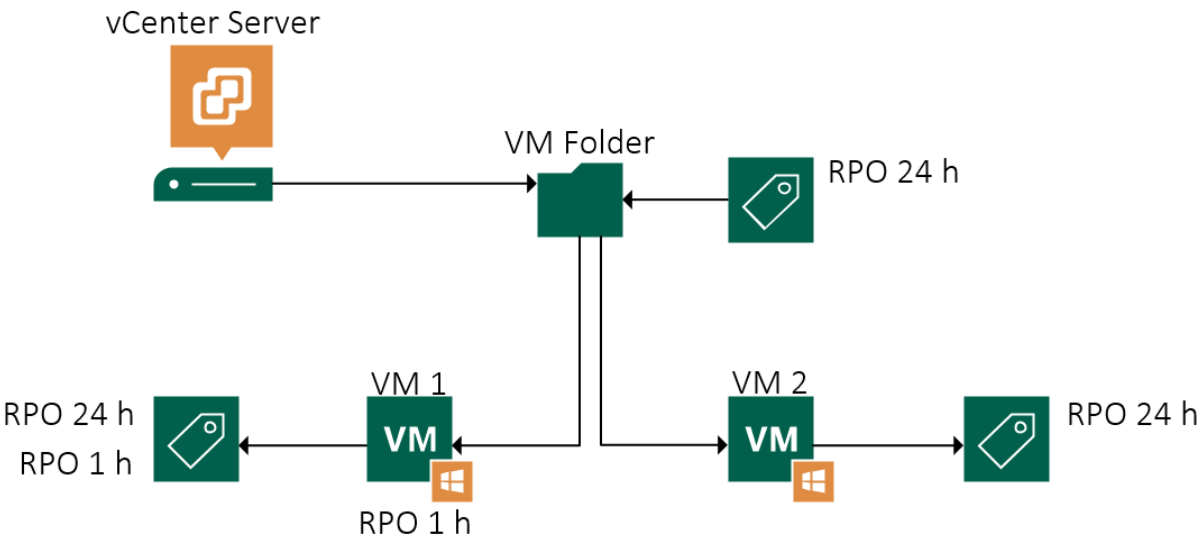
Merkintä aloitetaan testausympäristössä, jolloin nähdään merkintöjen toimivuus, toimintaperiaate sekä vaikutukset. Teoriaosuudessa käsiteltiin merkintöjen rajoituksia ja nyt rajoitukset haluttiin testata demoympäristössä, jotta voitiin nähdä, kuinka merkinnät toimivat. Demoympäristössä määriteltiin VMWare vCenterissä kategorian RPO, jonka sisälle määriteltiin merkinnät RPO 1 h sekä RPO 24 h. Merkinnät kuvaavat kuinka usein palvelimesta halutaan tehtävän varmuuskopio ja mahdollisessa poikkeustilanteessa, miten lähelle vikaantumispistettä päästään palautumaan varmuuskopiolla.

Merkintöjen käyttöön virtuaalikoneiden kategorioinnissa on muutama eri tapa. VMWare vCenterissä voidaan määritellä kansiotasolla merkinnät, jolloin kaikki virtuaalipalvelimet, jotka sijaitsevat kansion alla, saavat automaattisesti merkinnän. Merkinnät siirtyvät ja tulevat näkyville Veeamin ohjelmistoihin. Merkintöjen mukaan voidaan sijoittaa virtuaalikoneita palautustöihin tai hyödyntää kategorisointia raportoinnissa ja monitoroinnissa.

Toinen vaihtoehto on määritellä virtuaalikoneille merkinnät yksittäin VMWare vCenterissä. Tämä on ylläpidon kannalta työläämpi vaihtoehto käyttää merkintää. Virheellisten merkintäkonfigurointien välttämiseksi ei kannata merkitä virtuaalikoneita ja kansioita. Sekoitettaessa merkintöjä virtuaalikonetasolla ja kansiotasolla, saattaa se aiheuttaa ristiriitoja varmistuksissa.

Esimerkkinä tästä käytetään demoympäristössä tehtyä varmistustyötestiä, joka varmistaa palvelimet, joilla on RPO 24 h -merkintä. VMWare vCenterin hallinnassa on luotu kansio, jonka sisällä on kaksi virtuaalipalvelinta. Kansiotasolla kansio on merkitty RPO 24 h. Merkintä periytyy kansiolta virtuaalikoneille, jolloin molemmat virtuaalikoneet tulevat varmistustyöhön, jolle on määritetty merkintä RPO 24 h. Toiselle virtuaalikoneelle asetetaan merkintä RPO 1 h ja luodaan toinen varmistustyö. Varmistustyö varmistaa palvelimen, jolla on merkintä RPO 1 h. Virtuaalikoneelle erikseen määritelty merkintä RPO 1 h, ei kumoa ylempää perittyä merkintää vaan lisää sen. Näin ollen virtuaalikoneella on kaksi merkintää, RPO 24 h sekä RPO 1 h. Tästä saattaa aiheutua ristiriitoja, mikäli varmistustyöt ajetaan päällekkäin ja virtuaalipalvelin, jolla on kaksi merkintää, varmistetaan kahteen kertaan.

Kuva 16. Havainnekuva merkintöjen periytymisestä



4.8 Raportointi (määrittely ja testaus)

Tiedon saaminen automaattisesti ja ajastetusti on keskeinen osa ratkaisua, joka mahdollistaa paremman jatkuvuuden hallinnan varmistusnäkökulmasta. Veeam ONE antaa erittäin hyvät ja kattavat työkalut raportointiin, monitorointiin sekä raportoinnin automatisointiin. Pääsääntöisesti raportointia hallitaan selainkäyttöliittymällä. Työpöytäsovelluksessa on käytössä raportointikuvake, kuvake ohjaa automaattisesti selainhallintaan.

Ensimmäisenä tutustuttiin Veeam ONE 11 version julkaisutietoihin, jotta voitiin paremmin hahmottaa miten versiota 11 on paranneltu. Yhtenä tärkeänä toiminnallisuutena versiossa 11 on tullut SQL-lokien varmistuksen raportointi. Versiossa 10 SQL-lokivarmistushistorian raportti ei näytä SQL-lokivarmistusta, mikäli varmistustyö on tehty agenttivarmistuksena. Agenttivarmistuksella tarkoitetaan sovellusta, jonka kautta varmistus suoritetaan palvelimesta. (Yakovlyuk.A, Henkilökohtainen tiedonanto, 22.3.2021) Tieto perustuu Alex Yakovlyukin kanssa käytyyn sähköpostikeskusteluun. Yakovlyuk työskentelee Veeam asiakaspalvelussa järjestelmäasiantuntijana.

Opinnäytetyön kohteen kannalta SQL-lokivarmistushistoria on kriittinen raportti, jotta voidaan seurata että, SQL-palvelimien lokivarmistukset toimivat ja tästä saadaan automaattisesti raportti. Raportoinnin määrittelyssä ja käyttöönotossa on huomioitava, miten pitkältä ajalta raportti halutaan muodostettavan. Raportti on mahdollista lähettää sähköpostilla tai ONE voi muodostaa sen tiedostona määriteltyyn verkkojakoon. Tiedostomuotoisia raportteja voidaan muodostaa PDF:ksi, Microsoft Word -dokumentiksi, Microsoft Excel -työkirjaksi, CSV-tiedostoksi tai XML-tiedostoksi. Tiedostomuotoisena tätä voidaan jatkojalostaa ja viedä esimerkiksi IT-osaston omaan intranet-sivustoon, jolloin tieto tavoittaa suuremman määrän henkilöitä.

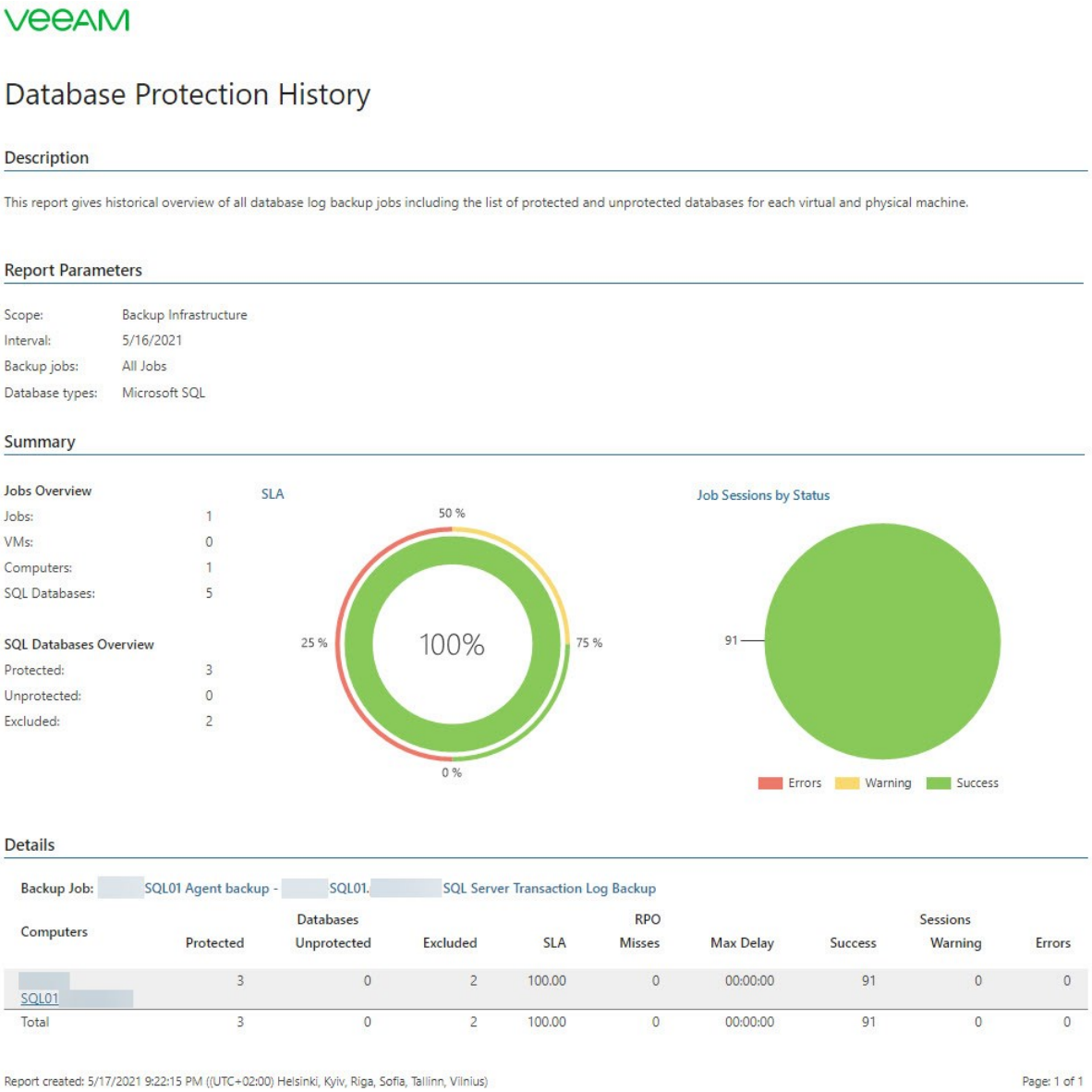
Määrittelyssä käytetään esimerkkinä tietokantojen varmistusraportteja, joita määritellään kaksi. Ensimmäisessä raportissa käytetään ajanjaksona edellistä päivää, jolloin nähdään päivätasolla lokivarmistuksien toimivuus sekä SLA. Toinen raportti määritellään muodostamaan raportti tietokantojen varmistuksesta kuluvalta kuukaudelta.

Raportin lähettämisen ja muodostamisen voi määritellä eri vaihtoehdoin. Vaihtoehtoina ovat tietty aikaväli, jonka jälkeen järjestelmä muodostaa tai lähettää sähköpostina raportin, kerran päivässä tiettynä kellon aikana tai kuukausittain. Tässä on hyvä huomioida, että raportin määrittelyssä käytetään sopivaa ajanjaksoa, jolloin esimerkiksi kuluvan kuukauden raportti lähetetään tai muodostetaan kuukauden viimeisenä päivänä.

Esimerkkiraportissa (Kuva 17) esitetään edellisen päivän varmistuksien onnistumista. Lokivarmistuksien kokonaismäärä on 91 kappaletta, ja näiden onnistumisprosentti on 100 %. Raportti on määritelty lähetettäväksi automaattisesti jokaisena arkipäivänä kello yhdeksän,

jolloin nähdään edellisen päivän tieto ja poikkeamiin voidaan reagoida mahdollisimman nopeasti.

Kuva 17. Esimerkkimalli tietokannan varmistuksesta saatavasta raportista



VEEAM

Database Protection History

Description

This report gives historical overview of all database log backup jobs including the list of protected and unprotected databases for each virtual and physical machine.

Report Parameters

Scope:	Backup Infrastructure
Interval:	5/16/2021
Backup jobs:	All Jobs
Database types:	Microsoft SQL

Summary

Jobs Overview

Jobs:	1
VMs:	0
Computers:	1
SQL Databases:	5

SQL Databases Overview

Protected:	3
Unprotected:	0
Excluded:	2

Details

Backup Job: SQL01 Agent backup - SQL01. SQL Server Transaction Log Backup

Computers	Databases Protected	Databases Unprotected	Databases Excluded	SLA	RPO Misses	Max Delay	Sessions Success	Sessions Warning	Sessions Errors
SQL01	3	0	2	100.00	0	00:00:00	91	0	0
Total	3	0	2	100.00	0	00:00:00	91	0	0

Report created: 5/17/2021 9:22:15 PM ((UTC+02:00) Helsinki, Kyiv, Riga, Sofia, Tallinn, Vilnius)

Page: 1 of 1

4.8.1 Raportoinnin käyttöönotto tuotantoympäristössä

Opinnäytetyön aikana suoritettiin raportoinnin ensimmäinen käyttöönotto. Pääasiassa seurataan kriittisten SQL-palvelimien varmistuksia ja ilmoituksia poikkeuksista. Kerran viikossa koostetaan raportti, joka kertoo edellisen viikon varmistuksen toiminnasta. Toinen tärkeä raportti, joka ensimmäisessä vaiheessa on otettu käyttöön, on virtuaalikoneiden snapshottien seuranta. Snapshotteja hyödynnetään paljon päivitys- ja testaustilanteissa ja

näin ollen vanhoja snapshotteja saattaa jäädä turhaan levyjärjestelmään, mikä aiheuttaa levykuormaa levyjärjestelmälle tai paikallisille kiintolevyille. Heräte hälyttää, mikäli snapshot on yli seitsemän vuorokautta vanha. Kerran kuukaudessa tästä koostetaan automatisoidusti raportti, joka kertoo, onko snapshotteja ollut edellisen kuukauden aikana ja miten ne on siivottu pois.

Toisessa käyttöönottovaiheessa määritellään sovelluspalvelimet, toimialueen ohjauskoneet sekä muut kriittiset palvelimet, joiden toimintaa halutaan valvoa ja joista halutaan saada herätteitä sekä raportteja. Opinnäytetyön aikana käyttöönoton toinen vaihe oli vasta suunnitteluasteella, jonka vuoksi se rajautui ulos opinnäytetyöstä.

4.8.2 Integrointi kommunikointi- ja tiedonvälitysalustoihin

Herätteiden ja raporttien integrointi kommunikointi- ja tiedonvälitysalustoille parantaa tiedon saatavuutta ja tavoittaa suuremman jakelun. Teamsiin ja Slackiin Veeamilta löytyy ratkaisu, jolla herätteet voidaan toimittaa myös nykyaikaiseen kommunikointi- ja tiedonvälitysympäristöön. ONE:ssa ei itsessään ole suoraa ratkaisua herätteiden integroimiseksi. Jorge De La Cruz on vuonna 2019 julkaissut artikkelin, jossa on esitelty tapa, kuinka tieto voidaan integroida esimerkiksi Teamsiin webhookin avulla. Tapa on edelleen täysin käyttökelpoinen ja toimiva, mutta nykyisin mm. Teamsissa kanavilla on sähköpostiosoite, eli tieto voidaan välittää myös ONE:sta sähköpostilla Teamsiin.

Informatiiviset ilmoitukset ja ei-kriittiset ilmoitukset voidaan ilmoittaa yksinkertaisella lähetystavalla esimerkiksi sähköpostilla. Kriittisimmät ilmoitukset voidaan toimittaa esimerkiksi kahta eri väylää esimerkiksi webhookin kautta kuten Jorge De La Cruzin esimerkissä kuvasi sekä sähköpostin kautta. Kahdennetulla tiedonsiirrolla ennaltaehkäistään esimerkiksi postin liikennöinnin epäonnistumista tai viivettä, kuten myös päinvastoin. (De La Cruz, 2019)

Yleisesti näissä konfiguroinneissa tapahtuu yritys ja erehdys -tilanteita esimerkiksi kaikki informatiivinen ja ei-kriittiset ilmoitukset aiheuttavat informaatiotulvan mikä aiheuttaa sen, että kriittinen tieto saattaa hukkua näiden muiden ilmoituksien joukkoon. On hyvä tarkastella siitä mikä tieto tulkitaan yrityksen järjestelmän kannalta kriittiseksi ja luodaan näistä ilmoitukset useampaan kohteeseen. Näiden ilmoituksien konfigurointiin ja

läpikäymiseen suositellaan käytettäväksi aikaa ja perehtymään näihin. Silloin herätteisestä ja ilmoituksista saadaan paras hyöty.

4.9 Monitorointi

Veeam ONE on tehokas apuväline reaaliaikaisen sekä historian tiedon monitorointiin tai tarkasteluun. Riippuen missä tyypissä ONE on asennettu, määrittää se tietyt aikajaksot suorituskykydatan keräämiselle. Esimerkkinä opinnäytetyössä on käytetty tyypillistä asennustapaa, joka kerää suorituskykydataa virtualisointialustalta kahdenkymmenen sekunnin välein ensimmäisen tunnin. Suorituskyvyn historiatieto viikon taaksepäin kerätään viiden minuutin välein. Viikon jälkeen vuoden taaksepäin suorituskyvyn historiadata on saatavilla kahden tunnin välein. Suorituskykydatan keruusykliesimerkit ovat VMWaresta. Hyper-V-virtualisointialustassa keruusykli on hieman erilainen tyypillisessä asennustavassa. Ympäristön koon kasvaessa, mikäli käytetään laajennettua asennustapaa, muuttuu keruusykli pidemmäksi. Arvot ovat oletusarvoja ja näitä voi muuttaa. (Veeam, 2020b) Yleisesti virtualisointialustoissa on omat suorituskykymonitorit ja ONE koostaa monitorit saman hallintapaneelin alle, joka helpottaa ympäristön monitorointia.

Monitorointiin on käytännössä kaksi käyttöliittymää, näitä ovat työpöytäsovellus sekä selainpohjainen käyttöliittymä. Työpöytäsovellus keskittyy hallintaan ja konfigurointiin. Selainpohjainen käyttöliittymä on enemmän informatiivinen käyttöliittymä, jossa voidaan luoda näkymiä, joihin saadaan keskeisiä informaatiokomponentteja, joita halutaan seurata. Selainpohjainen käyttöliittymä on hyvä ympäristön kokonaiskuvan kannalta.

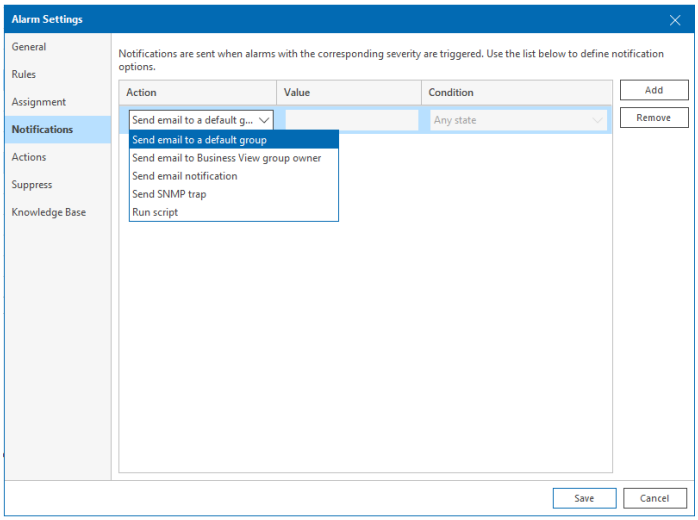
4.10 Herätteiden hallinta

Herätteillä tarkoitetaan sähköpostilla, SNMP:llä tai ponnahdusikkunasta tulevaa ilmoitusta virheestä tai varoituksesta. Herätteillä pyritään kiinnittämään valvovan tahon huomio poikkeustilanteeseen, jolloin voidaan reagoida proaktiivisesti. Tämä vähentää palvelukatkoksia tuotantoympäristöissä.

Veeam ONE sisältää ennalta määritettyjä herätteitä, joita voidaan muokata monipuolisesti. Herätteiden hallinnalla on ONEssa oma hallintapaneeli, joka on käytettävissä työpöytäversiossa. Selainversiossa ei ole erillistä herätteiden hallintaa. Opinnäytetyössä keskitytään VMWaren herätteisiin ja niiden toimintaan.

Esimerkkinä luvussa käydään läpi virtuaalikoneen uudelleen käynnistystä ja sen ilmoitusta. Prosessi on hyvin yksinkertainen, testiympäristössä käynnistetään virtuaalikone uudelleen mikä laukaisee herätteen. Herätteeseen on määritelty oletuksena, että lähettää ONEn asennuksen yhteydessä määritettyyn oletusryhmään sähköpostia. Herätteen ilmoitustoiminnoista voidaan lisätä eri toiminnoilla esimerkiksi lähettämällä sähköposti-ilmoitus erilliseen sähköpostiosoitteeseen, liiketoimintanäkymän ryhmän omistajalle, lähettämällä SNMP-syöte tai suorittamalla komentosarja.

Kuva 18. Havainnekuva herätteen ilmoitustoiminnoista



Esimerkkiratkaisuna voidaan käyttää yrityksen IT-osastoa, joka käyttää Microsoft Teamsin kanavaa, jonne kaikki ilmoitukset toimitetaan keskitetysti tai vaihtoehtoisesti kategorisoituna eri kanaviin.

5 Tulokset

Opinnäytetyön aikana tehdyn BIA-analyysin perusteella on tehty tuotannon jatkuvuuden hallintaan parannuksia. Tätä tukemaan on otettu käyttöön Veeam ONE -ohjelmisto, joka monitoroi palveluita, ilmoittaa herätteillä poikkeuksista sekä luo raportteja, josta nähdään mahdolliset poikkeukset. ONE:n päivitys testi- sekä tuotantoympäristössä meni läpi poikkeuksitta mikä nopeutti edistymistä määrittelyvaiheeseen. Tärkeimmät palvelut tuotiin valvonnan piiriin ja näille määriteltiin herätteet mikä mahdollistaa nopeamman reagoinnin poikkeustilanteessa. BIA-analyysin perusteella tehdyn dokumentin perusteella kriittisimmät palvelimet ovat määritelty tunnisteilla ja näiden varmistussykliä on muutettu tiheämmäksi, jolloin toipumispiste ja toipumisaika -määrittelyt toteutuvat. Ennen muutoksia palvelimien varmistussykli oli kerran päivässä. Määrittelyjen jälkeen tärkeimmät palvelimet varmistetaan neljä kertaa päivässä. Varmistuksia seurataan automatisoiduilla raporteilla ja poikkeuksista toimitetaan herätteitä henkilöille, jotka vastaavat ratkaisusta. Ilmoitukset toimitetaan valvontaryhmälle, josta luodaan myös tukitiketti tikettijärjestelmään, jolloin tieto tavoittaa henkilöt, jotka toimivat ympäristön kanssa ja voivat reagoida ennakoivasti mahdolliseen poikkeukseen.

Poikkeustilanteeseen on varauduttu laajentamalla osaamista yrityksen sisällä palauttamisen suhteen ja käyty läpi yleisimmät palautusskenaariot, jotka ovat myös dokumentoitu ohjemuotoon. Reagointiajat lyhenevät, kun tieto tavoittaa nopeasti useamman asiantuntijan ja toimenpiteet voidaan aloittaa nopeallakin aikataululla.

Kriittisimpiin palveluihin voidaan hyödyntää myös poikkeustilanteissa välitöntä palautustoimenpidettä, joka mahdollistaa palvelimen käynnistämisen suoraan varmistuskohteelta, jolloin aikaa säästetään tiedon palauttamiselta tuotantoympäristöön ja siirto tuotantoympäristöön voidaan suorittaa myöhemmässä vaiheessa tai mikäli VMWare:n lisensointi antaa myöden, voidaan siirto tehdä myös katkotta Storage vMotionin avulla.

BIA-analyysi onnistui hyvin ja asiakas sai tästä pohjan kokonaisvaltaiselle vaikutusarviotukityökalulle, jota opinnäytetyön jälkeen tullaan hyödyntämään asiakkaalla muutoksien yhteydessä. Analyysillä pystyttiin määrittelemään palveluille toipumispisteet

sekä toipumisajat, jotka käsiteltiin ja tullaan viemään tuotantoon suuremmassa mittakaavassa.

6 Yhteenveto

Prosessi aiheen parissa oli mielenkiintoinen ja opetti uutta. Teknologianäkökulmasta tuli jonkun verran uutta syventävää asiaa ONE:n osalta sekä uusia ratkaisutapoja, kuinka hyödyntää ONE:a paremmin tulevaisuudessa ja miten ONE voidaan integroida erilaisiin nykyaikaisiin kommunikointipalveluihin kuten Microsoft Teams. BIA-analyysi oli mielenkiintoinen ja toi paljon uutta näkökulmaa. Prosessi opetti myös kirjoittamaan enemmän yleiskielisillä termeillä, mikä tietotekniikka-alalla on mielestäni melko haastavaa. Eniten haasteita yleisesti toi termit ja käsitteet, jotka yleisesti käsitellään englanninkielisenä.

Tutkimuskysymyksiin vastaaminen onnistui hyvin ja kattavasti. Toiminnan jatkuvuuden kehittämistä saadaan parannettua hyödyntämällä BIA-analyysiä ja pitämällä vaikutusarviotyökalua ajantasalla. Poikkeustilanteisiin varautumiseen otettiin käyttöön ONE:n ilmoitukset ja herätteet, jolla saadaan tietoa ympäristöstä, jolloin voidaan toimia ennaltaehkäisevästi tai myös tilanteissa saadaan tietoa, mikäli poikkeustila syntyy. Palveluiden priorisointiin jatkuvuudenhallintasuunnittelussa otettiin käyttöön palvelimien merkinnät, jotka osoittavat varmistustiheyttä sekä priorisointia poikkeustilanteessa. Toipumispiste ja toipumisaika käsiteltiin mihin näitä tarvitaan ja miten näitä hyödynnetään jatkuvuudenhallinnassa. Työssä on käsitelty myös paljon näiden keskeisten kysymyksien rinnalta oleellisia termejä, käsitteitä ja teknologioita, jolloin lukijalla tulee parempi yleiskäsitys opinnäytetyön sisällöstä.

Työn keskeinen lähtökohta aiheen valinnalle oli työelämälähtöisyys ja kuinka opinnäytetyön aikana opittua tietoa voin hyödyntää työelämässä prosessin jälkeen. Tulevaisuudessa pystyn hyödyntämään näitä opinnäytetyössä oppimiani asioita työelämässä. Kokonaisuutena opetti myös tunnistamaan, havaitsemaan ja ymmärtämään paremmin asiakasympäristöjen tarpeita liiketoiminnan ja IT:n näkökulmasta.

Lähteet

2K, M. (ei pvm.). *Johdatus SQL:n maailmaan*. Noudettu 13. huhtikuuta 2021, osoitteesta https://www.2kmediat.com/sql/alkeet.asp

Andrew Maclen. (ei pvm.). *Data Deduplication and different types*. Noudettu 7. huhtikuuta 2021, osoitteesta https://www.slideshare.net/AndrewMaclen/data-deduplication-and-its-different-types

Antti Eteläaho. (2015). *Windows Server 2012 ja Active Directory*. https://www.theseus.fi/bitstream/handle/10024/91949/Etelaaho_Antti.pdf?sequence=2&isAllowed=y

Childerhose, C. (2021). *Mastering Veeam Backup & Replication 10*. Packt.

De La Cruz, J. (2019). *Veeam: Using Microsoft Teams for our Veeam ONE notifications when alerts are being generated*. https://jorgedelacruz.uk/2019/11/20/veeam-using-microsoft-teams-for-our-veeam-one-notifications-when-alerts-are-being-generated/

DNS Stuff. (2020). *What Is Hyper-V Software and Hardware Virtualization Technology?* https://www.dnsstuff.com/hyper-v-virtualization

Hovi, A. (2004). *SQL pikaopas*. https://www.arihovi.com/materiaalit/sql-pikaopas-e-kirja/

IBM. (2021). *5 Benefits of Virtualization*. https://www.ibm.com/cloud/blog/5-benefits-of-virtualization

Jensen, J. (2017). *The 3 C's of Data Protection*. https://www.quest.com/community/blogs/b/data-protection/posts/the-3-c-s-of-data-protection

JUHTA. (2019). *JHS 212 ICT-palvelujen palvelutasonhallinta (SLM)*.

Kangas, A. (2016). *Vaikutusanalyysi (BIA, Business Impact Analysis) käyttäjän ohje*. https://www.lausuntopalvelu.fi/FI/Proposal/DownloadProposalAttachment?attachmentId=911

Lee, B. (2019). *System Center Virtual Machine Manager 2019 – Part 1 : Overview and Installation*. https://www.vembu.com/blog/install-system-center-virtual-machine-manager-2019-step-by-step/

Määttä, T. (2013). *Tuomas määttä palvelinten varmistusjärjestelmät*.

Posey, B. (ei pvm.). *An absolute beginner's guide to Microsoft Hyper-V*. Noudettu 26. huhtikuuta 2021, osoitteesta https://techgenix.com/beginners-guide-microsoft-hyper-v/

Stankovic, I. (2014). *A beginner's guide to SQL Server transaction logs*. https://www.sqlshack.com/beginners-guide-sql-server-transaction-logs/

Uptime. (ei pvm.). *SLA & Uptime Calculator*. Noudettu 13. huhtikuuta 2021, osoitteesta https://uptime.is/

Väestörekisterikeskus. (2019). *Digitaalisen turvallisuuden projektiopas*. 1–60. https://dvv.fi/documents/2252790/13076333/Digiturvallisuuden_projektiopas_v100_1206_2019.pdf/a32ddf0b-a8c5-d61d-000e-a798cd9fe312/Digiturvallisuuden_projektiopas_v100_1206_2019.pdf

VAHTI. (2012). *Teknisen ICT-ympäristön tietoturva taso-ohje*. https://www.suomidigi.fi/sites/default/files/2020-06/VAHTI_3_2012_pdf.pdf

VAHTI. (2016). *Toiminnan jatkuvuuden hallinta*. https://julkaisut.valtioneuvosto.fi/handle/10024/75168

Valtionvarainministeriö. (2020). *BIA-vaikutusarviotyökalu*. https://www.suomidigi.fi/bia-vaikutusarviotyokalu

Veeam. (2017). *Demystifying Recovery Objectives*. https://www.veeam.com/blog/rto-rpo-definitions-values-common-practice.html

Veeam. (2020a). *Availibity Suite V10 Configuration and Management*.

Veeam. (2020b). *Data Retention*. https://helpcenter.veeam.com/docs/one/deployment/data_retention.html?ver=110

Veeam. (2021a). *System Requirements*. https://helpcenter.veeam.com/docs/one/deployment/system_requirements.html?ver=110

Veeam. (2021b). *System Requirements Veeam ONE Server*. https://helpcenter.veeam.com/docs/one/deployment/system_requirements.html?ver=110

Veeam. (2021c). *Veeam Backup & Replication v11 Veeam ONE v11 Feature comparison*. 1–18.

Veeam. (2021d). *Veeam ONE 11 Deployment Guide*. https://helpcenter.veeam.com/docs/one/deployment/system_requirements.html?ver=110

Veeam. (2021e). *VM Tags*. https://helpcenter.veeam.com/docs/backup/vsphere/vm_tags.html?ver=110

VMWare. (2021a). *Build numbers and versions of VMware vCenter Server (2143838)*.

https://kb.vmware.com/s/article/2143838

VMWare. (2021b). *What is a vSphere Hypervisor?*

https://www.vmware.com/products/vsphere-hypervisor.html

Liite 1: Aineistonhallintasuunnitelma

Työn aikana kerättävä julkistesti saatavilla oleva lähdemateriaali säilytetään Mendeleyssä, jolla hallitaan opinnäytetyön aikana lähteitä sekä lähdeviitteitä. Prosessin ohessa tehty BIA-analyysi toimitetaan asiakkaalle ja heille annetaan tähän käyttöoikeus. Liitteenä olevaan BIA-analyysiin on täytetty tietoja esimerkinomaisesti. Asiakasyrityksen tietoja ei käsitellä opinnäytetyön aikana materiaaleissa. Prosessin aikana tiedot tallennetaan HAMK:n henkilökohtaiseen Onedrive -pilvipalveluun, joka kopioidaan käsin toiseen Onedrive -pilvipalveluun tiedon varmistamiseksi. Toinen Onedrive -pilvipalvelu varmuuskopioidaan kolmannen osapuolen tuotteella.

Opinnäytetyöprosessin jälkeen HAMK:n Onedrive -pilvipalvelussa olevat tiedot tuhotaan kuuden kuukauden kuluttua prosessin loppumisesta. Lopullinen hävittäminen tapahtuu HAMK:n toimesta, kun kirjoittajan Office 365 -pilvipalvelu suljetaan.

Liite 2: BIA analyysi

BIA-analyysi

1. Yleiset tiedot

Analyysin kohde	**Ympäristö A / Palvelu A**	**Organisaatio**	**Yritys A**
Kohteen sijainti	**Kaupunki / Konesali**	**Arvioinnin teettäjä**	**Matti Malli**
Palveluntarjoaja	**Palveluntarjoaja A**	**Rooli**	**IT Manager**

Arvioinnissa mukana olleet henkilöt

Nimi	Rooli	Organisaatio	Mukana versiossa
Matti Malli	IT Manager	Yritys A	1
Mikko Mallikas	Specialist	Yritys B	1
Teppo Testi	Specialist	Yritys B	1

Dokumentin versiointi

Versio	Päivämäärä	Päivittäjä	Muutos
1	28.4.2021	Mikko Mallikas	Ensimmäinen versio

1. Yleiset tiedot

Analyysin kohde
Täytetään organisaatio

Kohteen sijainti
Täytetään kohteen sijainti. Esim: Palveluntarjoajan konesali, oma konesali

Palveluntarjoaja
Täytetään palveluntarjoaja. Palveluntarjoajia voi olla useampia kentässä.

Arvoinnissa mukana olleet henkilöt
Täytetään henkilöt jotka ovat olleet mukana täyttämässä analyysiä.

Dokumentin versiointi
Täytetään dokumentin versio, muokkauspäivämäärä, päivittäjä sekä täytetään muutos kenttään tehdyt muutokset.

2. Palvelutason määrittely

Palvelutaso (SLA)	Palveluaika	Käytettävyys	Palveluvaste	Ratkaisuaika
5	24/7	99,9 %	30min	2h
4	24/7	99,5 %	60min	4h
3	työpäivinä 6-24	99 %	90min	12h
2	työpäivinä 6-24	99 %	4h	24h
1	työpäivinä 6-24	99 %	8h	48h

Eheystasot	Kriittisyys
3	Erittäin tärkeä
2	merkityksellinen
1	Vähäinen merkitys

Saatavuustasot	Kriittisyys
3	Erittäin tärkeä
2	merkityksellinen
1	Vähäinen merkitys

Palvelu	RTO (h)	RPO (h)	SLA	Eheys	Saatavuus
Palvelu 1	5	24	5	2	3
Palvelu 2	1	0,25	4	3	3
Palvelu 3	1	0,25	4	3	3
Palvelu 4	1	24	5	3	2
Integraatiopalvelu 1	2	24	2	2	1
Integraatiopalvelu 2	3	24	4	2	2
Integraatiopalvelu 3	4	24	2	2	1
Integraatiopalvelu 4	4	24	2	2	1
Integraatiopalvelu 5	4	24	4	2	2
Integraatiopalvelu 6	4	24	5	3	3
Integraatiopalvelu 7	4	24	5	3	3

2. Palvelutason määrittely

Eheystaso:
Arvioinnissa määritellään miten kriittinen datan eheys on sekä kuinka datan oikeellisuuteen voidaan luottamaan.

Saatavuustaso:
Määritellään aikakriittisyyden ja palvelutason tavoitteiden perusteella miten kriittinen palvelun saatavuus on.
Huomioonotettavaa on myös palveluntasotavoitteiden mukaisesti korkeamman palvelutasosta johtuvat kustannusvaikutukset.

Matriisin täyttöohjeet
Täytä palvelu- / palvelinkenttään palvelun kuvaus.

RTO
Täytä RTO, missä ajassa palvelu täytyy olla käytettävissä häiriötilanteen jälkeen
RPO
Täytä RPO, miten lähelle vikatilannetta pitää päästä. Tämä vaikuttaa kuinka monta kertaa

3. Odottamattoman katkon vaikutukset

Arviointikriteerit	
3	Sietämätön
2	Kohtuuton
1	Merkittävä

Odottamattoman katkon vaikutukset	Oma organisaatio	Asiakkaat
Lakisääteiset tehtävät	2	1
Taloudelliset vahingot	2	2
Mainevaikutukset	2	2

Häiriön kesto					
Kesto		Kesto, pieni vaikutus		Kesto, suuri vaikutus	
tunteina		Kesto	Vaikutus	Kesto	Vaikutus
Palvelun toiminnan täysin keskeyttävä odottamaton ja suunnittelematon häiriö					
	Palveluaika	1h	1	2h	2
	palveluajan ulkopuolella	4h	1	24h	2

Tiedon menetys					
Kesto		Kesto, pieni vaikutus		Kesto, suuri vaikutus	
minuutteina		Kesto	Vaikutus	Kesto	Vaikutus
Aika ja vaikutukset sen mukaan, miten pitkältä ajalta tiedot voidaan menettää					
	Palveluaika	1h	2	2h	2
	palveluajan ulkopuolella	4h	1	24h	1
Aika ja vaikutukset sen mukaan, miten pitkään voidaan toimia ilman tietojen päivittymistä:					
	Palveluaika	1h	1	4h	2
	palveluajan ulkopuolella	12h	1	24h	2

3. Odottamattoman katkon vaikutukset

Lakisääteiset tehtävät
Arvioidaan arviointikriteerien perusteella odottamatton katkon vaikutuksista koskien lakisääteisten tehtävien suorittamiseen oman organisaation ja asiakkaan näkökulmasta.

Taloudelliset vahingot
Arvioidaan suoria taloudellisia vahinkoja oman organisaation ja asiakkaan näkökulmasta.

Mainevaikutukset
Arvioidaan mainevaikutuksia oman organisaation ja asiakkaan näkökulmasta.
Mainevaikutukseen voidaan huomioida myös epäsuoria taloudellisia vahinkoja.

Häiriön kesto

Määritellään ja arvioidaan häiriön keston vaikutuksia eri aikoina. Arviointi on jaettu kahteen eri kategoriaan, kesto jolla pieni vaikutus sekä kesto jolla suuri vaikutus.

Palvelun toiminnan täysin keskeyttävä odottamaton ja suunnittelematon häiriö

Määritellään kesto ja arvioidaan odottamattoman häiriön tai suunnittelematon häiriön vaikutuksia.

Aika ja vaikutukset sen mukaan, miten pitkältä ajalta tiedot voidaan menettää
Määritellään aika miltä ajalta tieto häviää ja arvioidaan tiedon häviämisen vaikutuksia.

4. Keskeiset riippuvuudet

Arviointikriteerit	
3	Kriittinen
2	Erittäin tärkeä
1	tärkeä

Keskeiset riippuvuudet						
	Riippuvuuden tärkeys	palvelu/järjestelmä	Organisaatio	Riippuvuus	Lisätietoja	SLA
1	Tärkeä	O365	Yritys B	Riippuvainen kommunikointiin		
3	Kriittinen	Integraatiopalvelu 1	Yritys C	Riippuvainen maksuliikenteestä		
3	Kriittinen					
2	Erittäin tärkeä					
1	Tärkeä					
1	Tärkeä					
2	Erittäin tärkeä					
1	Tärkeä					
1	Tärkeä					
3	Kriittinen					

4. Keskeiset riippuvuudet

Arviointikriteerit
Määritellään arviointikriteerit joilla palveluiden arvioidaan riippuvuuksien kriittisyys

Riippuvuuden tärkeys

Arvioidaan arviointiasteikolla

Palvelu/Järjestelmä
Määritellään palvelu tai järjestelmä josta liiketoiminta on riippuvainen

Organisaatio
Määritellään organisaatio joka on vastuussa ensisijaisesti palvelusta tai järjestelmästä
Palvelun toimittava organisaatio, joka ensisijaisesti vastaa palvelun hallinnasta.

Riippuvuus
Voidaan tarkentaa mihin palvelu tai järjestelmä on riippuvainen

Lisätietoja
Kirjataan mahdollisia lisätietoja tai huomioita palvelusta

SLA
Määritellään palvelutaso palvelulle. Voidaan käyttää samaa arviointitaulukkoa kuin kohdassa 2. Voidaan jättää myös tyhjäksi mikäli palvelu/järjestelmä on käsitelty aiemmin kohdassa 2.