Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

KUISMA MÄKI-JUSSILA

PowerProtect-Projekti

TIETOJENKÄSITTELYN TUTKINTO-OHJELMA
2024

TIIVISTELMÄ

Mäki-Jussila, Kuisma: PowerProtect-Projekti
Opinnäytetyö, AMK
Tietojenkäsittelyn tutkinto-ohjelma
Kesäkuu 2024
Sivumäärä: 48

Tämän opinnäytetyön toimeksiantajana toimi työpaikkani, joka on konesalipalveluita toimittava yritys. Työn tavoitteena oli tutkia ja vertailla kahden varmuuskopiointijärjestelmän, PowerProtect Data Managerin ja Dell Avamarin, ominaisuuksia ja soveltuvuutta. Halusimme selvittää, voiko PowerProtect-tuote käytännössä korvata vanhemman Avamar-tuotteen yritysten varmuuskopiointitarpeissa. Testasimme PowerProtectia kuvitteellisessa asiakasprojektissamme ja saimme tuloksia, jotka auttoivat vastaamaan tähän keskeiseen kysymykseen.

Kävimme myös läpi keskeisiä asioita liittyen näihin varmuuskopiointijärjestelmiin, kuten virtualisointia, VMware-yritystä ja myös itse varmuuskopiointiprosessia. Tämä sisälsi ymmärryksen virtualisoinnin roolista varmuuskopiointiympäristöissä, VMWare-yrityksen tarjoamista ratkaisuista ja niiden vaikutuksesta varmuuskopiointiin sekä varmuuskopiointiprosessin perusteista.

Avainsanat: varmuuskopiointi, virtualisointi, vmware, powerprotect, avamar

Abstract

Mäki-Jussila, Kuisma: PowerProtect-Projekti
Bachelor’s thesis
Business Information Systems
June 2024
Number of pages: 48

This thesis was commissioned by my workplace, a provider of data center services. The aim was to investigate and compare the features and suitability of two backup systems, PowerProtect Data Manager and Dell Avamar. We wanted to determine whether the PowerProtect solution could practically replace the older Avamar product for companies' backup needs. We conducted tests on PowerProtect in a hypothetical client project and obtained results that helped answer this key question.

Additionally, we delved into key aspects related to these backup systems, such as virtualization, the VMware company, and the backup process itself. This included understanding the role of virtualization in backup environments, VMware's offerings, and their impact on backup, as well as the fundamentals of the backup process.

Keywords: backup, virtualization, vmware, powerprotect, avamar

SISÄLLYS

LYHENTEET JA TERMIT

Pooli	Yhteiskäyttöisten resurssien varanto tietojenkäsittelyssä.
SaaS	Software as a Service - ohjelmiston hankinta palveluna.
Palautuspiste	Järjestelmän tilanne, jossa sen tiedot tallennetaan tietyllä hetkellä.
IP-osoite	Tunniste, joka määrittelee tietokoneen sijainnin ja tunnisteen verkossa.
Replikaatio	Prosessi, jossa tietoa kopioidaan yhdestä sijainnista toiseen.
CBT-tekniikka	Change Block Tracking-tekniikka, joka tallentaa tiedon muutoksista virtuaalikoneen levyllä sen sijaan, että koko levy kopioidaan joka varmuuskerralla.
Plug-in	Ohjelmistokomponentti, joka laajentaa tai lisää toiminnallisuutta olemassa olevaan ohjelmistoon.
Trunk-tila	Verkkoyhteyden asetus, joka mahdollistaa useiden verkkoväylien käytön yhden yhteyden kautta.
vRA	VMware vRealize Automation - automaatio- ja hallintaratkaisu, joka tarjoaa automatisoidun käyttöönotto-prosessin ja hallinnan virtuaali- ja pilvipalveluille.
vCD	vCloud Director - pilvipalvelujen hallintaratkaisu.

VCD Data Protection Extension	Lisäosa vCD:lle, joka mahdollistaa varmuuskopiointipalvelujen integroinnin suoraan vCD:hen.
Sivutustiedosto	Tietokoneen käyttöjärjestelmän käyttämä tiedosto, jota käytetään virtuaalimuistin laajentamiseen.
Vierasjärjestelmän tiedostojärjestelmän hiljennys	Prosessi, joka varmistaa että tiedostojärjestelmän eheys säilyy.
TSDM	Suojamekanismi PowerProtectissa.
BIOS UUID-tunniste	Yksilöllinen emolevyn tunniste.
Vikasietotila	Tila, johon tietokone tai käyttöjärjestelmä voidaan käynnistää, kun normaali käynnistysprosessi ei onnistu tai kun järjestelmässä on ongelmia.
Tenantti	Pilvipalvelun asiakas.
Klusteri	Useiden tietokoneiden tai palvelinten muodostamaa ryhmä.
Data Domain-järjestelmä	Dell EMC kehittämä tietojen varmuuskopiointi- ja tallennusratkaisujen tuoteperhe.

1 JOHDANTO

Opinnäytetyön tavoitteena oli tutkia ja vertailla kahta suosittua varmuuskopiointijärjestelmää, PowerProtect Data Manageria ja Avamaria, jotka ovat molemmat Dell EMC-yrityksen ratkaisuja. Asensin molempien järjestelmien tämänhetkiset versiot toimeksiantajani laboratorioympäristöön, konfiguroin ne toimimaan ja tutustuin niiden käyttöliittymiin ja ominaisuuksiin. Tämän jälkeen lähdin selvittämään kuvitteellisessa asiakasprojektissani voiko uudempi PowerProtect-varmuuskopiointijärjestelmä korvata vanhemman Avamar-varmuuskopiointijärjestelmän yrityskäytössä.

Tässä opinnäytetyössä tarkastelen aluksi virtualisointitekniikoiden ja komponenttien perusteita sekä VMware-ympäristön keskeisiä osia. Näiden asioiden ymmärtäminen on olennaista, koska ne liittyvät tiiviisti varmuuskopiointiin. Tästä siirrytään käymään läpi yleisesti mitä varmuuskopiointi on ja siihen liittyviä varmuuskopiointityyppejä. Sitten kerron, mitä ominaisuuksia tarkastelen tutkittavista varmuuskopiointijärjestelmistä. Tämän jälkeen kerron PowerProtectista ja Avamarista yleisesti ja tutkin minkälaiset tutkittavat ominaisuudet näillä järjestelmillä on. Lopuksi esittelen asiakasprojektin, jossa työn tarkoitus on käytännössä toteutettu, ja teen siitä loppupäätelmän.

2 VIRTUALISOINTI

Virtualisointi on prosessi, joka mahdollistaa useiden simuloitujen IT-ympäristöjen luomisen yhdestä fyysisistä järjestelmäresursseista koostuvasta poolista. Sitä käytetään usein ajamaan useita käyttöjärjestelmiä samassa laitteistojärjestelmässä samanaikaisesti. Virtualisointi muuntaa perinteisesti fyysisiä resursseja, kuten palvelimia, tallennuslaitteita ja työpöytäjärjestelmiä,

digitaaliseen muotoon. Teknologia erottaa fyysisen laitteiston ja sen päällä ajettavan ohjelmiston. Tämä mahdollistaa laitteistoresurssien tehokkaamman käytön jakamalla suurten järjestelmien resursseja pienemmiksi, tehokkaammiksi ja helpommin jaettaviksi osiksi. Näitä osia voidaan sitten jakaa useiden eri sovellusten ja käyttäjien kesken, joilla on erilaisia tarpeita, virtuaalikoneiden kautta. Yksi tämän teknologian yleisimmistä käyttötavoista on ajaa sovelluksia, jotka on tarkoitettu toisille käyttöjärjestelmille, ilman että niitä tarvitsee ajaa tietyssä laitteistojärjestelmässä. (HPE, n.d.)

2.1 Virtualisointitekniikat ja komponentit

2.1.1 Hypervisor

Virtualisoinnin mahdollistaa ohjelmistokerros, nimeltään hypervisor. Se erottaa isäntäjärjestelmän resurssit, kuten suorittimen, grafiikkasuorittimen, muistin, tallennustilan ja verkkokaistanleveyden, ja jakaa ne dynaamisesti järjestelmässä toimivien virtuaalikoneiden kesken niiden tarpeiden mukaisesti. (HPE, n.d.)

Type 1 (bare-metal) hypervisorit toimivat suoraan isäntälaitteiston päällä ilman erillistä käyttöjärjestelmää, kun taas Type 2 (hosted) hypervisorit vaativat käyttöjärjestelmän asentamisen ennen niiden käyttöä. Hypervisorit tarjoavat erilaisia ominaisuuksia, hallintamahdollisuuksia ja vaihtoehtoja eri toimittajilta, mikä antaa käyttäjille joustavuutta ja hallintaa virtualisoiduissa ympäristöissä.
(HPE, n.d.)

Suosituimmat hypervisorit ovat VMware ESXi ja Microsoft Hyper-V, ja muita saatavilla olevia hypervisoreita ovat muun muassa pilvipohjaiset virtuaalikoneet. (Commvault, n.d.)

2.1.2 Virtuaalikone

Virtuaalikoneet ovat ohjelmistoja, jotka jäljittelevät fyysisten tietokoneiden toimintaa ja pystyvät ajamaan käyttöjärjestelmiä ja sovelluksia. Virtualisointiohjelmistoilla voidaan luoda, hallita ja siirtää virtuaalikoneita, mikä tarjoaa joustavuutta, siirrettävyyttä ja tehokkaan resurssien käytön. (HPE,n.d.)

Koska yritykset luottavat yhä enemmän virtualisointiin, virtuaalikoneet ovat tulleet olennaiseksi osaksi yritysten IT-ympäristöjä. Liiketoimintasovellukset, tietokannat ja jopa konttityökuormat toimivat virtuaalikoneissa ja tuottavat valtavia tietomääriä, jotka on suojattava vahvalla tietojen suojausratkaisulla. (Commvault,n.d.)

2.1.3 Virtuaaliverkot

Virtuaaliset kytkimet, virtuaaliset LANit (VLANit) ja virtuaaliset reitittimet mahdollistavat verkon yhdistämisen ja jakamisen virtualisoiduissa ympäristöissä. Verkon asetuksia ja yhteyksiä hallitaan näiden virtuaalisten verkkokomponenttien avulla, mikä tarjoaa enemmän joustavuutta ja hallintaa verkon toimintaan. (HPE,n.d.)

2.1.4 Tallennusvirtualisointiteknologiat

Tallennusalueverkot (SANit) ja verkkoon liitetyt tallennusratkaisut (NASit) tarjoavat tallennuskapasiteettia virtualisoiduille ympäristöille. Tallennusvirtualisointialustat ja ohjelmistopohjaiset tallennusratkaisut hallinnoivat tallennusresursseja eriyttämällä fyysisen tallennuksen. Tämä mahdollistaa tehokkaan ja joustavan datan tallennuksen ja hallinnan. (HPE,n.d.)

2.2 Yleiset virtualisointityypit

2.2.1 Palvelimen virtualisointi

Palvelimen virtualisointi mahdollistaa useiden virtuaalipalvelimien ajamisen yhdellä fyysisellä palvelimella, mikä optimoi resurssien käytön tehokkuuden. Palvelimen virtualisointi on yleisin virtualisointiteknologian sovellus markkinoilla tällä hetkellä. Palvelimet on suunniteltu käsittelemään suuria määriä tehtäviä. Niiden resursseja voidaan jakaa virtuaalisiksi osiksi ja näitä virtuaalisia osia voidaan käyttää eri tehtävien suorittamiseen samassa järjestelmässä. Tämän avulla organisaatiot voivat käyttää palvelimia tehokkaammin. Hypervisorit, kuten Type 1 (bare-metal) ja Type 2 (hosted), hallinnoivat virtuaalikoneita ja helpottavat palvelimien virtualisointia. (HPE, n.d.)

2.2.2 Tallennustilan virtualisointi

Tallennusvirtualisointi tarkoittaa tallennusresurssien muuttamista virtuaalisiksi ja datan hallintaa niissä. Tallennusvirtualisointiarkkitehtuurit ja -teknologiat mahdollistavat tehokkaan tallennustilan tarjoamisen, datan siirron ja keskitetyn hallinnan. Tallennusvirtualisointi koostuu palvelimista, joita hallitaan virtuaalisella tallennusjärjestelmällä. Tämä järjestelmä hallitsee useista lähteistä peräisin olevaa tallennustilaa ja käsittelee sitä yhtenä tallennuspoolina, riippumatta isäntäjärjestelmien laitteistoeroista. Tämä virtualisointi helpottaa varmuuskopiointi-, arkistointi- ja palautustehtävien suorittamista. (HPE,n.d.)

2.2.3 Työpöydän virtualisointi

Työpöytävirtualisointi muuttaa työpöytäympäristöt ja käyttäjien työtilat virtuaalisiksi, mikä antaa mahdollisuuden käyttää niitä eri laitteilla. Virtuaalinen työpöytäinfrastruktuuri (VDI) ja sovellusvirtualisointiteknologiat mahdollistavat virtuaalisten työpöytien ja sovellusten tarjoamisen ja hallinnan. Tämä teknologia tarjoaa käyttäjille joustavuutta ja pääsyn työpöydilleen mistä tahansa.

Työpöydän virtualisointi luo ohjelmistopohjaisen version käyttäjän työpöydästä, johon voi kirjautua etänä internetin välityksellä. Tämä tarkoittaa, että käyttäjän työpöytäympäristö on tallennettu palvelimelle ja se on käytettävissä millä tahansa laitteella, kunhan internetyhteys on saatavilla. (HPE,n.d.)

2.2.4 Verkon virtualisointi

Verkkovirtualisointi tarkoittaa verkkotoimintojen ja -resurssien virtualisointia, mikä mahdollistaa joustavamman ja tehokkaamman verkkoympäristön luomisen. Ohjelmistomääritteinen verkkorakenne (SDN) ja verkkovirtualisointikerrokset mahdollistavat virtuaalisten verkkojen luomisen ja keskitetyn verkonhallinnan. (HPE,n.d.)

2.2.5 Sovelluksen virtualisointi

Sovellusvirtualisointi irrottaa sovelluksen käyttöjärjestelmästä ja laitteistosta, joilla se toimii. Loppukäyttäjä yleensä käyttää virtualisoituja sovelluksia ohuella asiakasohjelmalla, kun taas sovellus itsessään toimii datakeskuksen palvelimella, joka on yhteydessä Internetin välityksellä. Tämä voi helpottaa vanhempien käyttöjärjestelmäversioiden vaativien sovellusten suorittamista tai muita järjestelmäresursseja uhkaavien sovellusten käyttöä. (HPE,n.d.)

3 VMWARE

VMwaren pääkonttori sijaitsee Palo Altossa, Kaliforniassa, ja se perustettiin vuonna 1998. EMC Corporation osti sen vuonna 2004 ja Dell Technologies puolestaan vuonna 2016. Se tarjoaa virtualisointiteknologiaa, joka perustuu x86-arkkitehtuuriin tarkoitettuun ESX/ESXi-bare-metal-hypervisoriin. VMware auttaa käyttäjiä luomaan virtuaalikoneen tietokoneelleen helposti. VMware

toimii saumattomasti tarjoamalla pilviteknologian parhaat hyödyt käyttäjien virtualisointiominaisuuksien toteuttamiseksi. VMware on Dell Technologiesin johtava virtualisointi- ja pilvitietojenkäsittelyohjelmisto. (Daisy, 2024)

3.1 vSphere

VMware vSphere on kattava virtualisointialusta, jonka avulla yritykset voivat luoda ja hallita virtuaalisia ympäristöjä. Se sisältää sekä ESXi-hypervisoriohjelmiston että vCenter Server -hallintalaitteiston, jolla hallitaan useita hypervisoriohjelmistoja. VSphere on saatavilla kolmessa eri versiossa: Standard, Enterprise Class ja Platinum. Jokainen näistä tukee politiikkapohjaista virtuaalikoneiden tallennusta, elävää työkuormien siirtoa ja sisäänrakennettuja tietoturvatoimintoja. Korkeamman tason vaihtoehdot sisältävät virtuaalikoneiden tason salauksen, integroidun konttien hallinnan, kuormien tasapainotuksen ja keskitetyn verkonhallinnan. Platinum-versio tukee yksinomaan automaattisia vastatoimia tietoturvariskeihin ja integroitumista kolmannen osapuolen tietoturvatoimintojen työkaluihin. (IBM, n.d.)

3.2 vCenter

Yksi tärkeimmistä komponenteista vSphere-alustalla on vCenter Server, joka toimii vSphere-alustan hallintakomponenttina. Sen avulla mahdollistetaan virtuaalikoneiden käyttöönotto ja hallinta laajassa valikoimassa isäntäpalvelimia. Vcenterillä voi myös määritellä virtuaalikoneiden sijoittumisen isäntäpalvelimille, varata resursseja niille, seurata suorituskykyä ja automatisoida työnkulkuja. Sitä voidaan käyttää työkaluna käyttäjäoikeuksien hallintaan käyttäjän omien politiikkojen perusteella. (IBM, n.d.)

3.3 ESXi

VMware virtualisoi fyysisiä tietokoneita käyttämällä ydinteknologiaansa, ESXi hypervisoria. VMwaren ESXi-datakeskuskäyttöön suunnattu hypervisor on ns. Type 1 eli "bare metal" -hypervisor, joka korvaa tietokoneen fyysisiin

komponentteihin vuorovaikutuksessa olleen ensisijaisen käyttöjärjestelmän. ESXi on seuraaja ESX:lle, joka oli suurempi hypervisor ja käytti enemmän isäntäkoneen resursseja. VMware on lopettanut ESX:n käytön. (IBM, n.d.)

4 VARMUUSKOPIOINTI

Varmuuskopiointi on prosessi, jossa kopioidaan dataa IT-järjestelmän tiedoista toiseen sijaintiin, jotta ne voidaan palauttaa, jos tiedot menetetään. Varmuuskopioinnin tavoitteena on varmistaa, että tiedot säilyvät turvassa jos vaikka laitteet vikaantuisi tai tapahtuisi joku muu tietojen menetykseen liittyvä tilanne. Tietojen varmuuskopiointi on siis tärkeä osa yrityksen tietojen suojausstrategiaa, johon yleensä kuuluu myös liiketoiminnan jatkuvuuden ja katastrofien varalta suunnitellun palautumisen suunnitelma. (Moore, n.d.)

4.1 Varmuuskopiotyypit

4.1.1 Täysvarmuuskopio

Täysvarmuuskopio on kattavin varmuuskopion muoto, jossa kloonataan kaikki valitut tiedot. Tämä kattaa esimerkiksi tiedostot, kansiot, SaaS-sovellukset ja kiintolevyt. Täysvarmuuskopion suurin etu on, että tietojen palauttaminen on nopeaa. Kuitenkin, koska kaikki tiedot varmuuskopioidaan kerralla, itse varmuuskopiointiprosessi kestää kauemmin kuin muissa varmuuskopiointimenetelmissä. Täysvarmuuskopioiden toinen haaste on tallennustilan suuri tarve. Tämän vuoksi useimmat yritykset tekevät ensin täysvarmuuskopion ja käyttävät sen jälkeen ajoittain differentiaali- tai inkrementaalivarmuuskopiointia. Tämä helpottaa tallennustilan hallintaa ja nopeuttaa varmuuskopiointiprosessia. (Wallen, n.d.)

4.1.2 Inkrementaalinen varmuuskopio

Inkrementaalivarmuuskopion ensimmäinen varmuuskopio on täysvarmuuskopio. Seuraavat varmuuskopiot tallentavat vain muutokset, jotka on tehty edellisen varmuuskopion jälkeen. Yrityksillä on enemmän joustavuutta tehdä tämän tyyppisiä varmuuskopioita niin usein kuin haluavat, sillä vain uusimmat muutokset tallennetaan. Inkrementaalivarmuuskopiointi vaatii tilaa vain muutosten eli inkrementtien tallentamiseen, mikä mahdollistaa nopeat varmuuskopiot. (Wallen, n.d.)

4.1.3 Differentiaalinen varmuuskopio

Differentiaalinen varmuuskopio sijoittuu täys- ja inkrementaalisten varmuuskopioiden väliin. Tämä varmuuskopiointityyppi sisältää tiedot, jotka on luotu tai muutettu edellisen täysvarmuuskopion jälkeen. Yksinkertaisesti sanottuna, aluksi tehdään täysvarmuuskopio, ja sen jälkeen varmuuskopioidaan kaikki muutokset tiedostoihin ja kansioihin. Differentiaalivarmuuskopioiden avulla tiedot voidaan palauttaa nopeammin kuin täysvarmuuskopiolla, koska tarvitaan vain kaksi varmuuskopiokomponenttia: alkuperäinen täysvarmuuskopio ja uusin differentiaalivarmuuskopio. (Wallen, n.d.)

4.1.4 Synteettinen täysvarmuuskopio

Tämä menetelmä yhdistää alkuperäisen täydellisen varmuuskopion ja inkrementaalikopioiden tiedot. Synteettinen täysi varmuuskopio vaatii lyhyemmän varmuuskopiointiajan kuin perinteinen täysi varmuuskopio, koska vain muuttunut data kopioidaan. (Moore, n.d.)

4.1.5 Inkrementaalinen ikuisuusvarmuuskopio

Tämä variaatio inkrementaalisista varmuuskopioista pyrkii minimoimaan varmuuskopiointiajan tarjoten samalla nopeamman datan palautuksen.

Inkrementaalinen ikuisuusvarmuuskopio tallentaa koko datan ensin ja täydentää sitä sitten eteenpäin täydentävillä varmuuskopioilla. (Moore, n.d.)

4.1.6 Käänteisinkrementaalinen varmuuskopio

Tämä menetelmä alkaa perinteisellä täydellisellä varmuuskopioinnilla ja luo sitten sarjan synteettisiä täysiä varmuuskopioita, joista jokainen sisältää inkrementaalivarmuuskopion. Kun seuraava täysi varmuuskopio luodaan, käänteisinkrementaaliset varmuuskopiot tarjoavat useita datan palautuspisteitä, joihin organisaatio voi tarvittaessa palata. (Moore, n.d.)

5 VARMISTUSJÄRJESTELMIEN TUTKITTAVAT OMINAISUUDET

Mietin opinnäytetyömentorini ja projektipäälliköni kanssa, mitä keskeisiä varmuuskopiointijärjestelmän ominaisuuksia tulisi minun tutkia opinnäytetyössäni. Alun perin tutkittavia ominaisuuksia oli enemmän, mutta jouduimme karsimaan osan pois, koska opinnäytetyö olisi paisunut silloin liian pitkäksi ja myös projektin aikataulu olisi tullut liian tiukaksi. Kokosimme lopulta tutkittavaksi seuraavat ominaisuudet.

5.1 Virtuaalikoneen ja tiedostotason varmuuskopiointi ja palautus

Virtuaalikoneiden varmuuskopiointi on prosessi, jossa varmuuskopioidaan yritysympäristössä toimivat virtuaalikoneet. Näitä virtuaalikoneita yleensä ajetaan vieraina hypervisoreilla, jotka emuloivat tietokonejärjestelmää ja sallivat useiden virtuaalikoneiden jakamisen yhden fyysisen isäntälaitteen kanssa. (Commvault, n.d.)

Jos virtuaalikone sattuu vikaantumaan, voit palauttaa sen varmuuskopiotiedostosta. Voit palauttaa yhden tai useita virtuaalikoneita alkuperäiseen tai

uuteen sijaintiin. Jotta virtuaalikone voidaan palauttaa, tarvitsee se ainakin yhden palautuspisteen. (Veeam, n.d.). Yleensä ensimmäinen palautuspiste luodaan ensimmäisessä täysinäisessä varmuuskopiossa.

Tiedostotason varmuuskopiointi keskittyy yksittäisiin tiedostoihin, kansioihin ja sovellusdatan suojaamiseen. Tämä on yleisin varmuuskopiointimenetelmä ja yleensä nopeampi toteuttaa. Se antaa käyttäjälle mahdollisuuden valita tiedostot ja kansiot sekä aikatauluttaa niiden varmuuskopioinnin säännöllisesti. Tiedostotason varmuuskopiot sopivat paremmin pienempien tietomäärien palauttamiseen. Kuitenkin koko järjestelmän palauttaminen on mahdotonta esimerkiksi palvelinongelman tai muun katastrofin sattuessa. (IDrive, n.d.)

Tietojen palautus on yksinkertaisesti prosessi, jossa menetettyjä tietoja tuodaan takaisin käyttöön varmuuskopion avulla. Näin ollen nämä kaksi käytäntöä ovat toisistaan riippuvaisia; toisin sanoen, jotta tietoja voidaan palauttaa, täytyy olla olemassa varmuuskopio. (Ciesielski, 2023)

5.2 Tietojen säilytyskäytäntö

Varmuuskopioiden säilytyskäytäntö on sääntö tai sääntöryhmä, jonka yritys asettaa määritelläkseen, mitä tietoja täytyy tallentaa, minne ne tulisi tallentaa ja kuinka kauan, jotta noudatetaan sekä laillisia että liiketoiminnallisia vaatimuksia. Tämän lisäksi sen tulisi asettaa ohjeet arkistoinnista, tallennusmuodoista sekä siitä, miten tietoja käytetään ja salataan niiden elinkaaren aikana. Eri toimialoilla on hyvin erilaisia lakisääteisiä ohjeita, ja joillakin aloilla edellytetään myös, että tiedot on poistettava tietyn ajanjakson jälkeen. Vahva tietojen säilytyskäytäntö ei ainoastaan varmistaa, että yritys noudattaa lakisääteisiä vaatimuksia, vaan myös mahdollistaa sen, että yritys voi tasapainottaa tietojen säilyttämistarpeensa niiden aiheuttamien lisätallennuskustannusten kanssa. (Reber, 2023)

5.3 Varmuuskopiointitilat

Yrityksen kriittisten tietojen suojaaminen voi olla haastavaa – olipa kyseessä sitten suuri tietomäärä tai tietojen uhkakuvat. Mutta oikeilla varmuuskopiointimenetelmillä varmistat, että pystyt palautumaan katastrofitilanteista ja että IT-infrastruktuurisi pysyy vakaana. (Moir, 2024)

Katsotaan siis minkälaisia varmuuskopiointimenetelmiä varmuuskopiointijärjestelmä sisältää ja miten ne toimivat.

5.4 Verkkoadapterien ja VLAN-yhteensopivuus

Verkkosovitin on laitteisto-osa tai laite, joka yhdistää tietokoneen tai muun sähköisen laitteen verkkoon, mahdollistaen kommunikoinnin muiden verkossa olevien laitteiden kanssa. Nämä sovittimet ovat olennaisia yhteyksien luomisessa paikallisverkkoihin (LAN), laajakaistaverkkoihin (WAN) ja internetiin. (NordVPN, n.d)

Verkkoadapterit ovat siis olennaisia varmuuskopiointijärjestelmissä, koska ne mahdollistavat varmuuskopioidun datan siirtämisen verkkoon nopeasti ja tehokkaasti.

VLANit luovat tietokoneiden, palvelinten ja muiden verkkolaitteiden loogisen yhteyden virtuaaliseen LANiin niiden fyysisestä sijainnista riippumatta. Lisäksi niiden toimiminen tietoturvavälineenä, VLANit helpottavat yritysten ja organisaatioiden verkkoresurssien hallintaa ja työnkulun optimointiprosesseja. (Einorytė, 2023).

VLAN-yhteensopivuus varmuuskopiointijärjestelmässä siis kiteytettynä parantaa sen tietoturvaa ja hallittavuutta. Varmuuskopioliikenteen hallinta selkeytyy ja vähentää verkon ruuhkautumista.

5.5 Moniasiakaskäyttö (Multi-tenancy)

Ohjelmisto, joka mahdollistaa moniasiakaskäytön, on ohjelmistoratkaisu, jota useiden asiakkaiden (esim. yksittäisten organisaatioiden, osastojen, ryhmien jne.) käyttäjät voivat käyttää ja hyödyntää yhdellä ohjelmiston asennuksella. Asiakkaat on erotettu toisistaan, vaikka ne jakavatkin saman ohjelmiston ja mahdollisesti sen alustan. Jokaisen asiakkaan käyttäjät voivat käyttää vain kyseiselle asiakkaalle kuuluvia tietoja, raportteja ja mahdollisia ominaisuuksia, eikä heillä ole pääsyä muihin tietoihin tässä ympäristössä. Tietojärjestelmän päivitysnäkökulmasta yhden palvelun ylläpitäminen ja päivittäminen yhden instanssin kautta on helpompaa kuin useiden ohjelmistojen päivittäminen, joita on asennettu jokaiselle asiakkaalle erikseen. Lisäksi, kun useat käyttäjäryhmät hyödyntävät samaa ohjelmistoa ja jakavat sen taustalla olevan infrastruktuurin, kokonaisomistuksen ja hallinnan kustannukset vähenevät. Tämä tekee palveluntarjoajan liiketoiminnasta kannattavampaa. (Auwau.com, n.d.)

Moniasiakaskäyttö on siis tärkeää, koska se mahdollistaa useiden asiakkaiden samanaikaisen käytön yhden ohjelmiston asennuksen kautta. Tämä merkitsee sitä, että jokainen asiakas voi säilyttää ja hallita omia tietojaan erillään muista asiakkaista, mikä lisää tietoturvaa ja yksityisyyttä.

5.6 Välityspalvelin-mahdollisuus (Proxy)

Jos etsit luotettavaa tapaa suojata tietojasi, välityspalvelinten käyttäminen varmuuskopiointiin ja palautukseen on erinomainen vaihtoehto. Välityspalvelimet toimivat välikäsinä tietokoneesi ja internetin välillä, jolloin voit käyttää verkkoa paljastamatta IP-osoitettasi tai sijaintiasi. Ne voivat myös tarjota lisäturvaa, mikä tekee kyberrikollisten vaikeammaksi siepata tietojasi. Välityspalvelimet voidaan asettaa salaamaan tietosi ennen niiden tallentamista, mikä tekee käytännössä mahdottomaksi kenellekään päästä käsiksi tietoihin ilman asianmukaisia tunnistetietoja. Lisäksi välityspalvelimet voidaan konfiguroida varmuuskopioimaan tietosi automaattisesti säännöllisesti, varmistaen, että sinulla on aina käytettävissäsi uusin versio. (Bunal, 2023)

Välityspalvelin-mahdollisuus varmuuskopiointijärjestelmässä on siis tärkeä, koska se tarjoaa lisäkerroksen tietoturvaa ja yksityisyydensuojaa. Se mahdollistaa myös automaattisen varmuuskopioinnin, mikä varmistaa, että sinulla on aina käytettävissäsi ajantasaiset tiedot.

5.7 Asiakastuki

Jokainen hyökkäys, koodirivi tai integraation yhdistäminen voi aiheuttaa sen, että menetät pääsyn SaaS-tietoihisi. Kun olet paineen alla, tarvitset täyden luottamuksen palveluntarjoajaasi, jotta voit palata normaaliin liiketoimintaan mahdollisimman nopeasti. Tästä syystä asiakastuki on yksi tärkeimmistä tekijöistä, jotka on otettava huomioon arvioitaessa mahdollisia varmuuskopiointi- ja palautusratkaisuja. (Own Company, 2022)

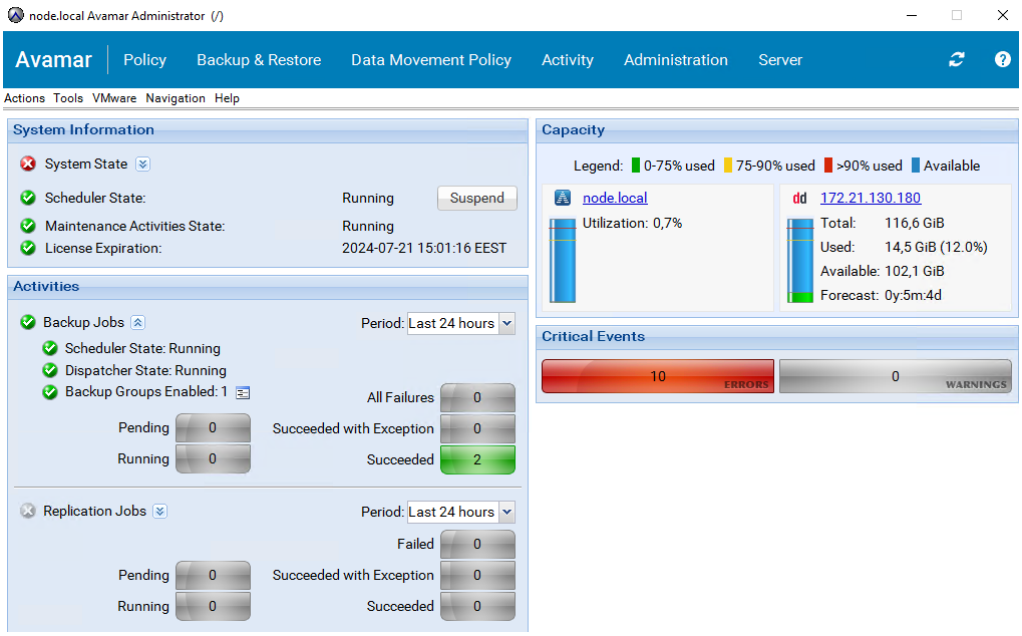
6 DELL AVAMAR

Avamar-ohjelmisto tarjoaa joustavia ja tehokkaita varmuuskopiointi- ja palautustoimintoja käyttäjälleen. Toiminnot voivat skaalautua päivittäisestä varmuuskopiointisuojasta päätelaitteille aina suurten yritysten monipuolisten sovellusten ja työmäärien tehokkaaseen suojaukseen. Jos siirrät osan tai kaiken varmuuskopiointiympäristöstäsi pilveen, Avamar mahdollistaa investointisi täyden hyödyntämisen mahdollistaen replikaation, katastrofin palautuksen ja pitkäaikaisen säilytyksen asiakkaille, jotka käyttävät AWS:ää, Microsoft Azurea tai Google Cloudia. Avamar tarjoaa sovelluskohtaisen palautuksen auttaakseen sinua täyttämään palvelutasosopimuksesi ja optimoimaan varmuuskopiointi- ja palautusprosessejasi. Avamar ja Avamar Virtual Edition (AVE) ovat saatavilla osana Dell Data Protection Suite -kokonaisuutta, joka tarjoaa kattavia tietojen suojan ohjelmistoja ja työkaluja, tai tietovarastolaitteena Avamar Data Store Gen5A. (DellTechnologies, n.d.-a)

Latasin Avamarin version 19.10.0-135 palveluntarjoajan verkkosivuilta ja asensin sen toimeksiantajani laboratorioympäristöön. Tämän jälkeen määritin asennuksen toimimaan ja tutustuin ohjelmiston käyttöliittymiin ja työssä tutkittaviin ominaisuuksiin.

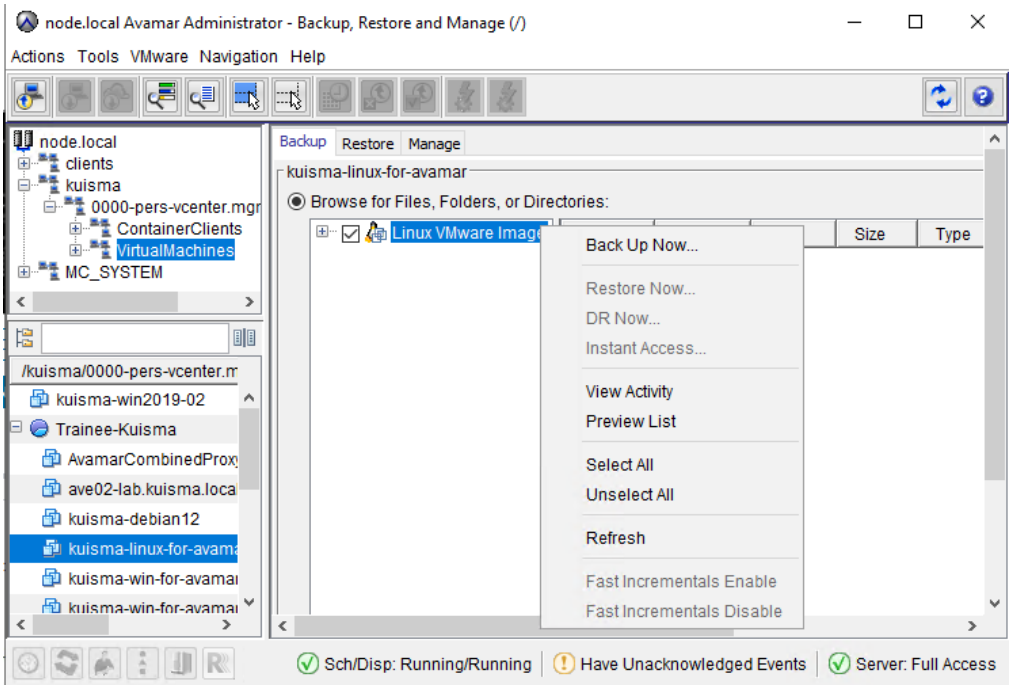
6.1 Virtuaalikoneen varmuuskopiointi Avamarilla

Avamar Administratorin käyttöliittymästä painoin vasemmasta yläkulmasta ”Backup & Restore”-valintaa, joka käynnisti varmuuskopiointiohjelman (Kuva 1).



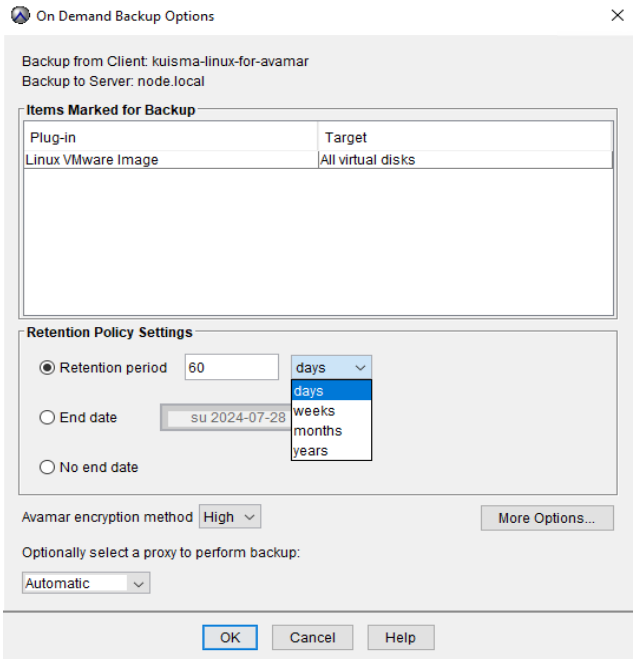
Kuva 1. Avamarin käyttöliittymä

Plugin-paneelista vasemmalta etsin haluamani virtuaalikoneen, josta tein varmuuskopion, ruksasin valintaruudun tietokoneen kuvasta ja painoin ”Back up now” (Kuva 2).



Kuva 2. Virtuaalikoneen varmuuskopiointiohjelma Avamarilla

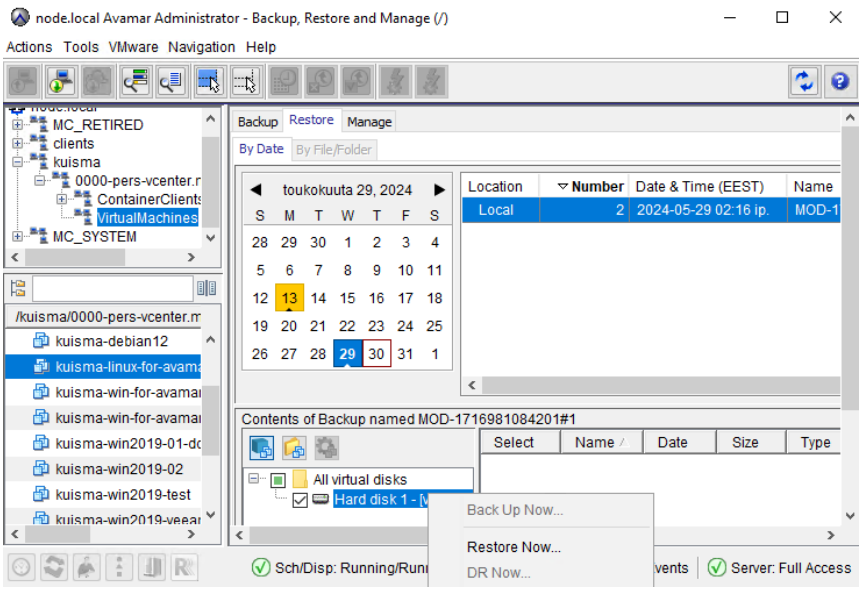
Tämän jälkeen ruudulle ilmestyi konfiguraatioikkuna (Kuva 3). Tästä ikkunasta pystyi asettamaan säilytyskäytäntöasetuksia, salausmenetelmää ja valitsemaan työlle välityspalvelimen. Lisäksi pääsi määrittelemään lisäasetuksia. Lisäasetuksissa pystyit laittamaan päälle tai pois CBT-ominaisuuden, antaa luvan Avamar-palvelimelle raportoida tietoja vSpherelle viimeisimmästä varmuuskopiosta ja viimeisimmästä onnistuneesta varmuuskopiosta. Lisäksi pystyit valita mihin tietotallennusjärjestelmään varmuuskopio tallennetaan ja mitä salausmenetelmää tietotallennusjärjestelmässä käytetään. Konfiguraatioikkunasta painoin OK-nappulaa ja järjestelmä alkoi tekemään varmuuskopiota.



Kuva 3. Avamarin varmuuskopiointiohjelman konfiguraatioikkuna

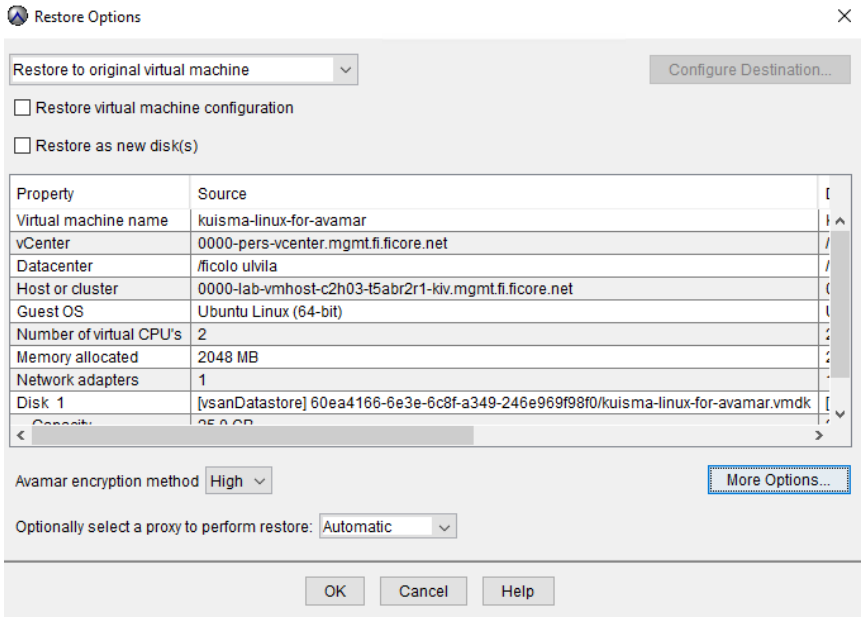
6.2 Virtuaalikoneen palautus Avamarilla

Virtuaalikoneen palauttaminen varmuuskopiosta tapahtui ensin navigoimalla valmis varmuuskopio käyttöliittymän kalenterista. Löydettyäni varmuuskopion sisällön, aloitin sen palauttamisen painamalla ”Restore Now”. (Kuva 4).



Kuva 4. Virtuaalikoneen palautus Avamarilla

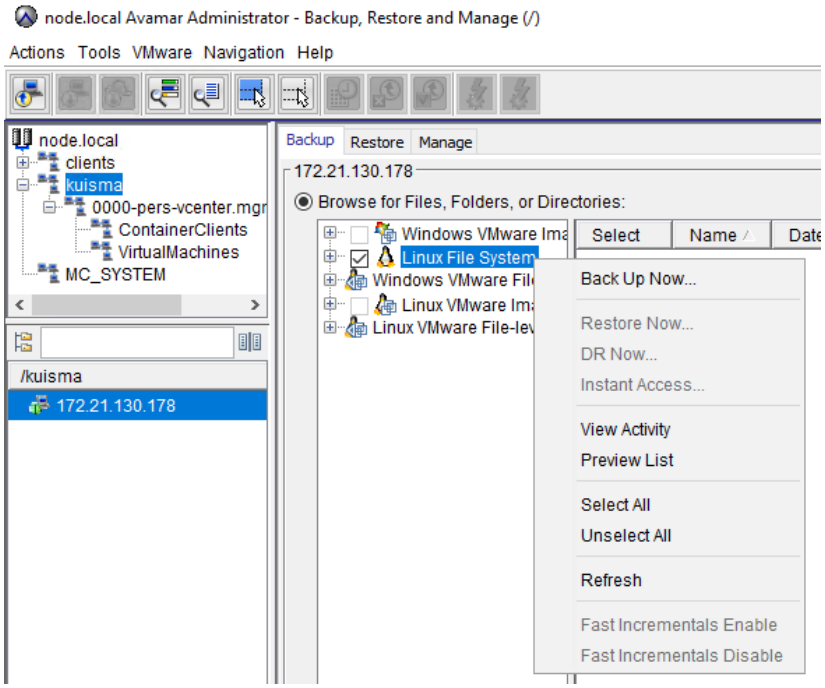
Seuraavaksi pääsin määrittelemään palautuksen asetuksia (Kuva 5). Palautuksen pystyi tallentamaan alkuperäiseen, toiseen olemassaolevalle tai uuteen virtuaalikoneeseen. Virtuaalikoneen määritykset voitiin myös palauttaa, ja virtuaalikone voitiin palauttaa uusina levyinä. Salausmenetelmän tasoa pystyi määrittämään ja pystyit valita haluamasi välityspalvelimen. Lisäasetuksissa pystyit valita liitännäistyypin, ottaa päälle tai pois CBT- menetelmän, määrittää palauttamisen jälkeisiä asetuksia ja valita salausmenetelmän tietojärjestelmälle. Lopuksi täytyi nimetä palautus ja valita palautuksen sijainti.



Kuva 5. Palauttamisen asetukset Avamarilla

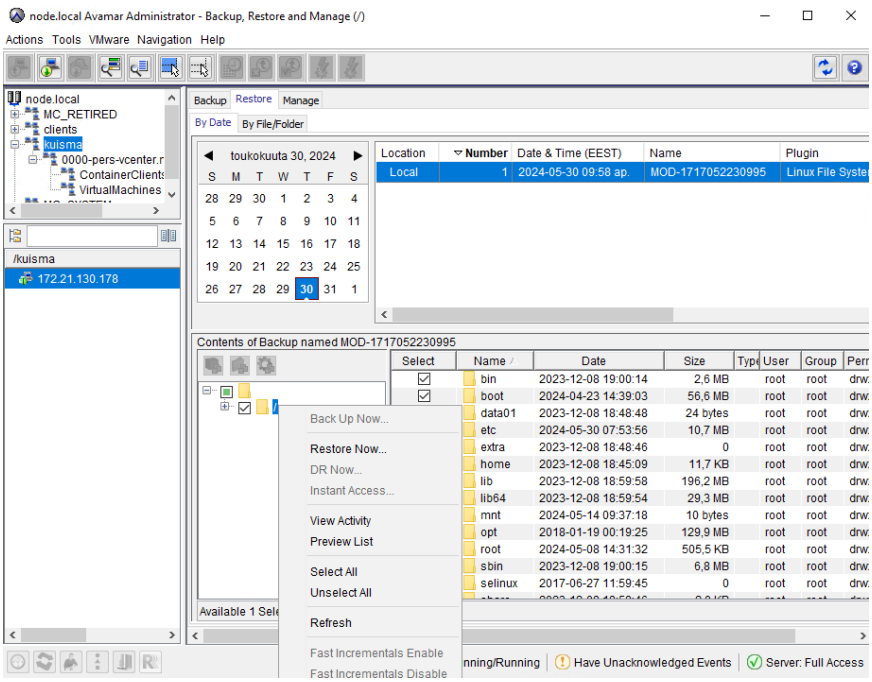
6.3 Tiedostotason varmuuskopiointi ja palautus Avamarilla

Tiedostotason varmuuskopiointi toimi valitsemalla varmuuskopioitava kohde, jonka jälkeen valittiin tiedostotason varmuuskopiointimenetelmä ja painettiin ”Back up now”-valintaa aloittaaksemme varmuuskopioinnin (Kuva 6). Seuraavaksi pääsi määrittelemään asetuksia tiedostotason varmuuskopioinnille. Asetuksista pystyi määrittelemään samoja asioita kuin virtuaalikoneen varmuuskopioinnissa. Eroavia asioita oli, että pystyi antamaan varmuuskopiolle kuvaavan etiketin, määrittelemään kirjausasetuksia, raportoimaan edistyneitä tilastoja ja muokkaamaan tiedostojärjestelmän läpikäynnin asetuksia.



Kuva 6. Tiedostotason varmuuskopiointi Avamarilla

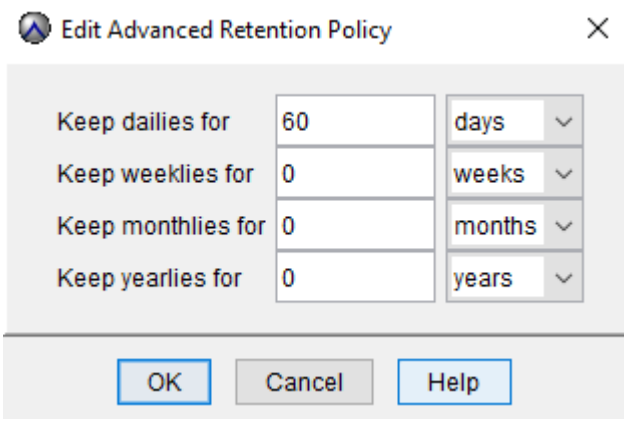
Tiedostotason palautus toimi navigoimalla tekemämme varmuuskopio käyttöliittymän kalenterista. Sitten valitsin palautettavat tiedostot, tässä tapauksessa valitsin kaikki mahdolliset tiedostot. Painoin ”Restore now”-valintaa aloittaakseni palautuksen (Kuva 7). Tämän jälkeen pääsi määrittelemään palautuksen asetuksia. Asetuksissa pääsi tuttuun tapaan määrittelemään, mihin palautus tallennetaan ja että minkälaista salausmenetelmää käytetään. Lisäasetuksissa pääsi määrittelemään korvataanko olemassa olevat tiedostot, salausmenetelmää tallennusjärjestelmään ja lokitusvaihtoehtoja.



Kuva 7. Tiedostotason palautus Avamarilla

6.4 Tietojen säilytyskäytäntö Avamarilla

Kuten kuvasta 3 näkee, Avamarin voi määritellä poistamaan automaattisesti varmuuskopiot tietyn määränpäivien, viikkojen, kuukausien tai vuosien jälkeen. Voit myös määritellä sen poistamaan varmuuskopiot tiettynä kalenteripäivänä. Vaihtoehtona on myös säilyttää varmuuskopiot niin kauan kuin asiakas on aktiivinen (kuva 3). Tietojen säilytyskäytännön lisäasetuksissa (kuva 8) voit määrittää neljä erilaista säilytysjaksoa yhdelle varmuuskopiolle säilytystunnisteen arvon perusteella.



Kuva 8. Tietojen säilytyskäytännön lisäasetukset Avamarilla

6.5 Varmuuskopiointitilat Avamarilla

Avamarin varmuuskopiointivaihtoehdot riippuvat käytettävästä plug-inistä. AIX file system / HP-UX file system / Linux file system / Macintosh file system plug-init tarjoavat varmuuskopiointivaihtoehtoja näiden käyttöjärjestelmien tiedostojärjestelmille. Ne voivat sisältää koko tiedostojärjestelmän varmuuskopioinnin tai tietyt osiot. Avamar Plug-in for Microsoft Windows vaihtoehdossa on varmuuskopiointitiloja, jotka ovat erityisesti Windows-ympäristölle. VMware Plug-in mahdollistaa VMWare-virtuaalikoneiden kuvan varmuuskopioinnin. Sovelluspluginit, kuten SQL Server ja SharePoint VSS tarjoavat varmuuskopiointivaihtoehtoja kyseisille sovelluksille. Vaihtoehdot voivat sisältää tietokantatason varmuuskopioinnin, sovellustason varmuuskopioinnin ja integroidun VSS-varmuuskopioinnin. (Dell, n.d.-a)

6.6 Verkkoadapterien ja VLAN-yhteensopivuus Avamarilla

Kaikki verkkoadapterit, jotka ovat yhteydessä Avamariin, on oltava trunk-tilassa, jotta tarvittavat VLAN-verkot voidaan määrittää Avamarissa. (dell.com,nd). ESXi/ESX-palvelimissa VLAN-tunnisteet voi määrittää ulkoisella kytkintunnustuksella, virtuaalikytkintunnistuksella tai virtuaalivierastunnistuksella. (Broadcom, 2024)

6.7 Moniasiakaskäyttö Avamarilla

Avamarin tiivis integrointi VMware-ympäristöön mahdollistaa itsepalveluperusteisen tietojen suojaamisen. VRealize Automation (vRA) ja vCloud Director (vCD) tarjoaa tietosuojapalveluja julkisiin pilviin, yksityisiin pilviin, hybridipilviin ja syntymäpilviin. VCD Data Protection Extension upottaa varmuuskopiointipalvelut suoraan vCloud Directoriin jonka myötä niitä voidaan jakaa moniasiakaskäyttöisessä mallissa. (DellTechnologies, n.d.-b)

6.8 Välityspalvelin-mahdollisuus Avamarilla

Jotta Avamarissa voi tehdä kuvan tason varmuuskopiointi- ja palautustoimintoja, tarvitsee se välityspalvelimena toimivan virtuaalikoneasiakkaan. Asiakkaan rekisteröinti on prosessi, jossa määritetään välityspalvelin-virtuaalikoneasiakkaiden tunnistetiedot Avamar-palvelimen kanssa. Kun Avamar "tuntee" asiakkaan, se määrittää sille ainutlaatuisen asiakastunnuksen, jonka se välittää takaisin asiakkaalle aktivoinnin aikana. (Dell, n.d.-b)

6.9 Asiakastuki Avamarilla

Avamarin omaa dokumentaatiota selaamalla voi huomata, että se tarjoaa monenlaista tukea asiakkailleen. ”Top Solutions”- osio sisältää yleisimmin kysytyt kysymykset ja niiden ratkaisut. Asiakkaat voivat löytää nopeita vastauksia ja ratkaisuja yleisiin ongelmiin ilman, että heidän tarvitsee ottaa yhteyttä tukeen.”Knowledge Base Articles”-osio sisältää tietopankkiartikkeleita, joissa on yksityiskohtaisia ohjeita, vianmääritysoppaita ja teknistä tietoa. Nämä artikkelit auttavat asiakkaita ratkaisemaan ongelmia itsenäisesti ja saamaan syvällistä tietoa Avamarin tuotteista ja niiden käytöstä.”Manual and Documents”-osio sisältää käyttöohjeet, asennusoppaat ja muut tekniset dokumentit. Nämä dokumentit tarjoavat kattavat ohjeet Avamarin tuotteiden asentamiseen, konfigurointiin ja käyttöön.”Regulatory Information”-osio sisältää sääntelyyn liittyvät tiedot ja dokumentit, jotka auttavat asiakkaita varmistamaan, että Avamarin tuotteiden käyttö täyttää kaikki tarvittavat sääntelyvaatimukset ja standardit.”Videos”-osio sisältää opastus- ja koulutusvideot, jotka tarjoavat visuaalisia ohjeita tuotteiden käyttöön. (Dell, n.d.-c)

7 POWERPROTECT DATA MANAGER

PowerProtect Data Manager (PPDM) tarjoaa tehokkaita tietojen suojaustoimintoja hyödyntäen Dellin luotettavaa suojavarastoratkaisun arkkitehtuuria.

Toiminnallisen yksinkertaisuuden, ketteryyden ja joustavuuden ollessa sen ytimessä, PowerProtect Data Manager mahdollistaa tietojesi suojaamisen, hallinnan ja palautuksen, antaen sinulle mahdollisuuden nopeasti mukautua tuleviin IT-vaatimuksiin. Voit myös suojata pilvessä syntyneitä työmääriä useissa julkisissa pilvissä integroidun SaaS-pohjaisen PowerProtect Cloud Snapshot Managerin avulla. (Dell,n.d.-d)

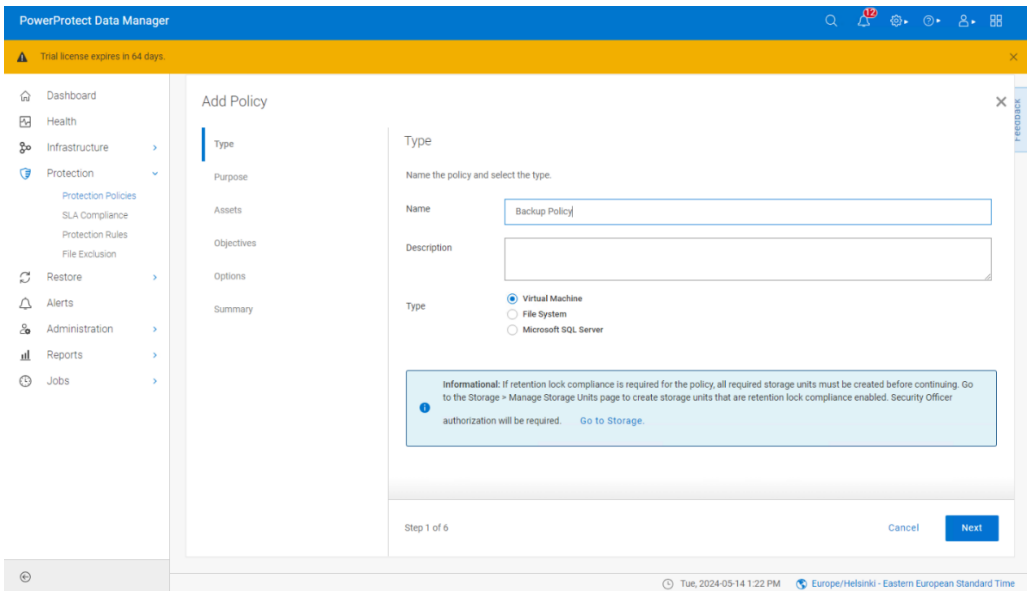
Latasin PowerProtect Data Managerista version 19.15.0-25 palveluntarjoajan verkkosivuilta ja asensin sen toimeksiantajani laboratorioympäristöön. Tämän jälkeen määritin asennuksen toimimaan ja tutustuin ohjelmiston käyttöliittymään ja työssä tutkittaviin ominaisuuksiin.

7.1 Virtuaalikoneen varmuuskopiointi PPDM:llä

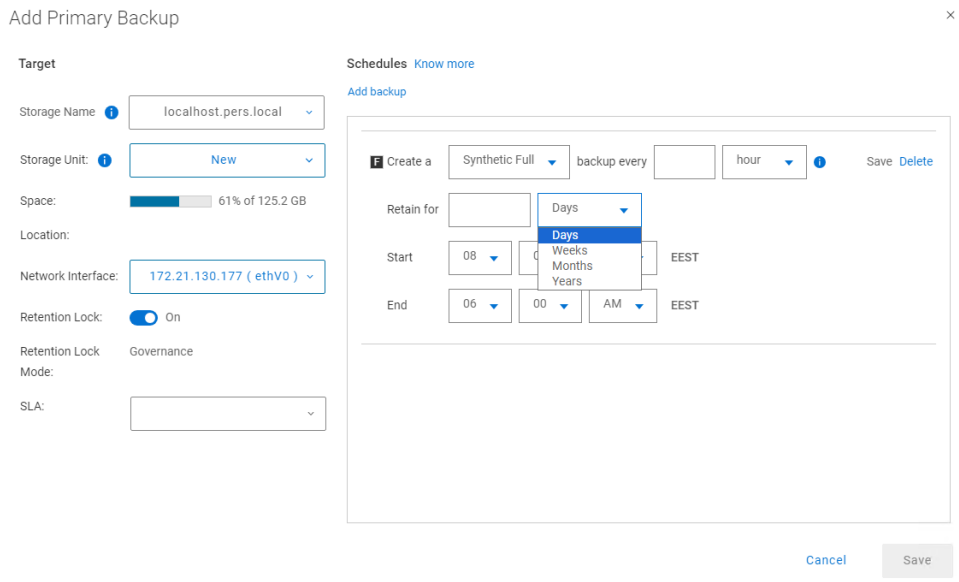
Ennen kuin voit varmuuskopioida mitään PPDM:llä, sinun on ensin luotava suojelupolitiikka kullekin kohteelle. Suojelupolitiikat määrittelevät joukon tavoitteita, jotka koskevat tiettyjä ajanjaksoja. Nämä tavoitteet ohjaavat asetusten määrittämistä, aktiivista suojelua ja kopiodatan hallintatoimenpiteitä, jotka täyttävät määritetyn datan liiketoimintavaatimukset. Jokaisella suojelupolitiikan tyypillä on omat käyttäjätavoitteensa. (Dell, n.d.-e)

Aloitin suojelupolitiikan tekemisen vasemmasta navigointiruudusta painamalla ”Protection”, ja sen jälkeen ”Protection Policies”. Sitten minun piti nimetä suojelupolitiikka, antaa kuvaus sille ja valita sen tyyppi, joka oli tässä tapauksessa virtuaalikone. Seuraavassa kohdassa piti ilmoittaa suojelupolitiikan tarkoitus. Vaihtoehtoina oli ”Crash Consistent”, joka on tehty virtuaalikoneiden ajankohtaiseen varmuuskopiointiin, ”Application Aware”, joka on tehty virtuaalikoneille, joihin on asennettu SQL-sovellus ja ”Exclusion”, joka valitaan, jos suojauskäytännössä on virtuaalikoneen resursseja, joita aikoo jättää tietosuojatoimien ulkopuolelle. Seuraavaksi ”Assets”- sivulla valittiin varmuuskopioitavat kohteet. ”Objectives”-sivulla pääsi valitsemaan suojauskäytännölle palvelutasosopimuksen ja määrittelemään varmuuskopion asetuksia (Kuva 9). Varmuuskopion asetuksissa pääsi valitsemaan mihin varmuuskopio tallennetaan ja

tehdäänkö suojelupolitiikalle uusi säilytysyksikkö vai käytetäänkö olemassa olevaa. Lisäksi pääsi valitsemaan verkkoliitännän ja muokkaamaan säilytyskäytäntöasetuksia (Kuva 10). ”Options”- sivulla pääsi määrittelemään varmuuskopion optioimointitilaa valitsemalla joko ”Performance” tai ”Capacity”-tilan. Ensimmäinen tila optimoi varmuuskopioinnin- ja replikointinopeutta. Jälkimmäinen tila optimoi varmuuskopion kokoa. Lisäksi tällä sivulla pääsi valitsemaan vaihtoehdon, missä varmuuskopiosta jätetään pois sivutustiedostot ja myös vaihtoehdon missä otetaan käyttöön vierasjärjestelmän tiedostojärjestelmän hiljennys. Viimeisenä vaihtoehtona pystyi valitsemaan, käytetäänkö datan siirtämiseen ”TSDM”-tilaa, jota käytetään yleensä kaatumisyhteensopivissa politiikoissa tai ”VADP”-tilaa, jota käytetään sovellustietoisissa politiikoissa ja kaatumisyhteensopivissa politiikoissa, jotka eivät täytä TSDM:n vaatimuksia.



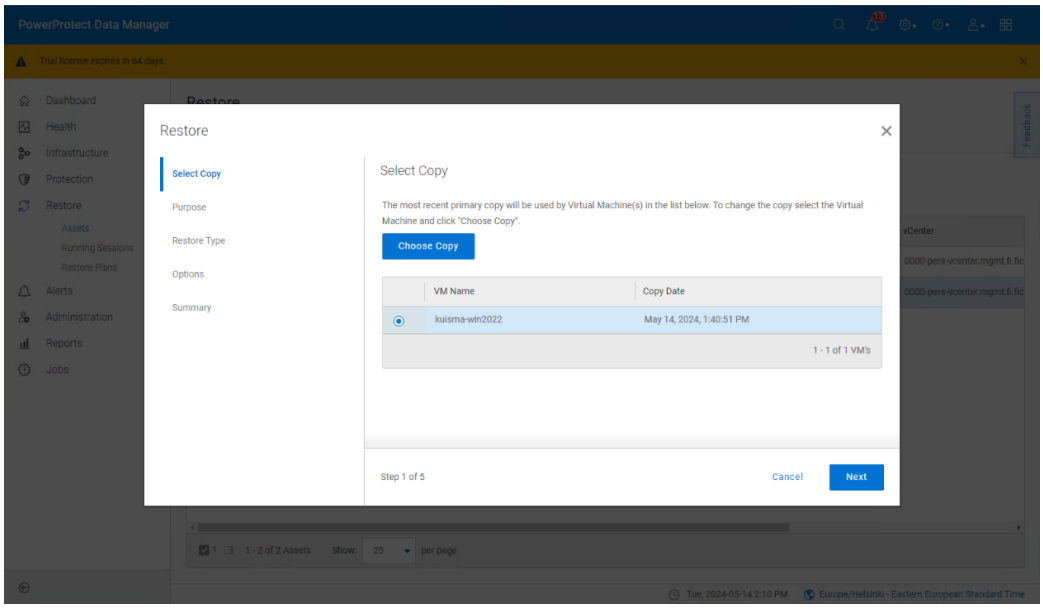
Kuva 9. Virtuaalikoneen suojelupolitiikan asetukset PPDM:llä



Kuva 10. Varmuuskopion- ja säilytyskäytännön asetukset PPDM:llä

7.2 Virtuaalikoneen palautus PPDM:llä

Virtuaalikoneen palauttaminen tapahtui valitsemalla vasemmasta navigointiruudusta ”Restore”-kohta, josta valitsin virtuaalikoneen, jolla on olemassaoleva suojelupolitiikka.”Purpose”-kohdassa, pystyi palauttamaan joko kokonaisen virtuaalikoneen tai virtuaalikoneen yksittäisiä virtuaalilevyjä. ”Restore type”-kohdassa pääsi valitsemaan palautuksen tyypin. Vaihtoehtoina oli palautus alkuperäiseen virtuaalikoneeseen, luoda uusi virtuaalikone ja palautus siihen tai välitön pääsy virtuaalikoneen varmuuskopioon selausta ja palautusta varten. ”VM Information” ,”Restore Location”,”ESX” ja ”Datastore”- kohdissa pääsi valitsemaan mihin virtuaalikone palautetaan.”Options”-kohdassa pääsi valitsemaan haluaako palautukseen välittömän pääsyn. Lisäksi pääsi valitsemaan palautetaanko palautuksessa virtuaalikoneen metatietoja ja tallennusasetuksia. Vaihtoehtoina oli myös laittaa päälle DDBoost-tekniikka, joka tehostaa varmuuskopiointi- ja palautusprosesseja, sekä mahdollisuus palauttaa alkuperäinen BIOS UUID-tunniste. Viimeisenä vaihtoehtona pystyi asettamaan palautukselle vianmääritystilan. ”Networks”-kohdassa näkyi ne verkkosovittimet ja niihin liittyvät verkot, jota virtuaalikone oli käyttänyt siinä hetkessä, kun se varmuuskopioitiin (Kuva 11).

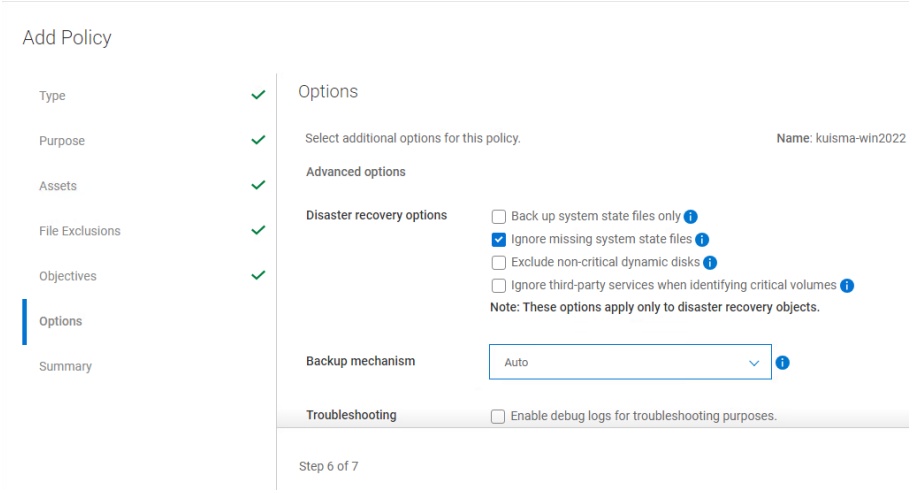


Kuva 11. Virtuaalikoneen palautusasetukset PPDM:llä

7.3 Tiedostotason varmuuskopiointi ja palautus PPDM:llä

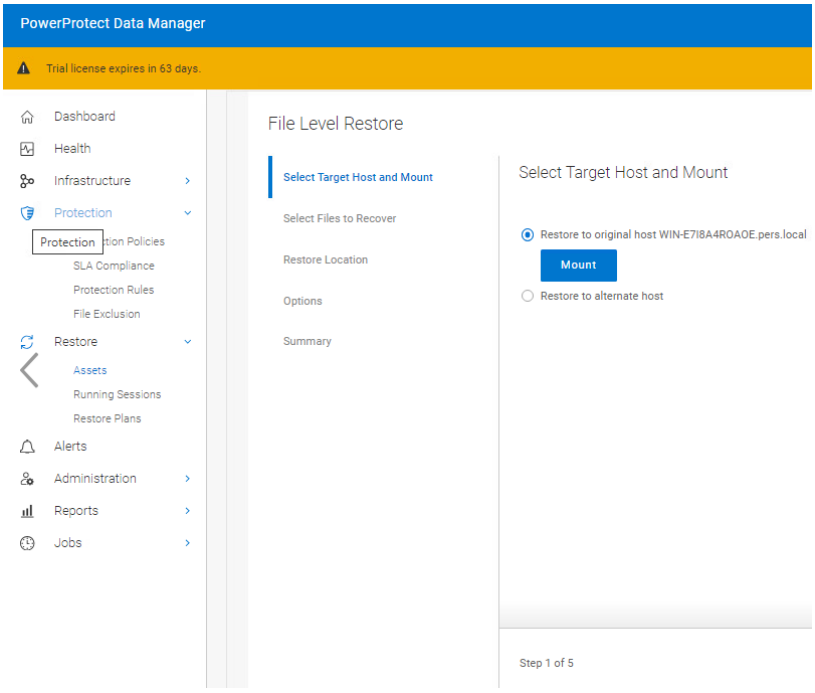
PPDM:ssä täytyy ensiksi ladata File System Agent-ohjelmisto, ennen kun voi tehdä tiedostotason varmuuskopiointeja. Tämä ohjelmisto antaa sovellusylläpitäjälle mahdollisuuden suojata ja palauttaa tiedostoja isäntäkoneella, jossa tiedostojärjestelmä sijaitsee. Latasin ohjelmiston PPDM:stä ”Downloads”-sivulta. Tämän jälkeen asensin ja konfiguroin sen yhteensopivaksi kohteen isäntäkoneen kanssa.

Agentin asentamisen jälkeen loin tuttuun tapaan suojelupolitiikan varmuuskopiolle. Tyypiksi valitsin tiedostojärjestelmän, jonka jälkeen valitsin halutut varmuuskopioitavat tiedostot. Muut asetukset olivat identtiset mitä oli, kun varmuuskopioitiin virtuaalikonetta. Ainoa ero oli ”Options”-kohdassa, missä pystyi määrittelemään katastrofipalautusasetuksia. Näistä asetuksista pystyin valita, tekeekö järjestelmä varmuuskopion pelkästään järjestelmän tilatiedostoista, ohitanko puuttuvat järjestelmän tilatiedostot ja kolmannen osapuolen palvelut määriteltäessä kriittisiä taltioita ja, että jätänkö varmuuskopioista pois ei-kriittiset dynaamiset levyt. Pystyin myös valitsemaan, onko varmuuskopio mekanismi automaattinen vai tiedostotasoinen ja, että laitetaanko päälle vikasietotila (Kuva 12).



Kuva 12. Tiedostotason suojelupolitiikan asetukset PPDM:llä

Tiedostotason palautuksen tein samalla periaatteella kuin virtuaalikoneen palautuksen, paitsi että tyypiksi valitsin tiedostotason palautuksen. Tämän jälkeen valitsin tiedostotason kohteen, jolla oli olemassa suojelupolitiikka ja tämän jälkeen valitsin tiedostotason palautuksen. Seuraavaksi valitsin isäntäkohteen ja sen jälkeen liitin siihen tiedostojärjestelmän. Sen jälkeen valitsin tiedostot, mitkä halusin palauttaa, jonka jälkeen sain valita, palautetaanko nämä tiedostot alkuperäiseen vai johonkin toiseen kohteeseen. Ennen palauttamista sain myös valita, tehdäänkö palautus vianmääritystilassa (Kuva 13).



Kuva 13. Tiedostotason palautusasetukset PPDM:llä

7.4 Tietojen säilytyskäytäntö PPDM:llä

Kuvasta 10 näkee kiteytettynä PPDM:än säilytyskäytännön asetukset varmuuskopioille. Voit valita kalenterin päivämäärän varmuuskopioiden vanhentumispäiväksi tai sitten määrittää kiinteän säilytysajan päivinä, viikkoina, kuukausina tai vuosina.

PowerProtect Data Domainilla on oma lisensoitu ominaisuus, ”Retention Lock”, joka voidaan laittaa päälle varmuuskopion asetuksista (Kuva 10). Se tarjoaa muuttumattomien tiedostojen lukituksen ja turvatun tiedon säilytyksen asiakkaan tarpeisiin noudattaa sekä yrityksen hallintovaatimuksia että säänte-lynmukaisuutta. Retention Lock soveltaa säilytysaikaa yksittäisiin tiedostoihin ja mahdollistaa säilytysaikojen hienovaraisen hallinnan tiedostoittain (DellTechnologies ,n.d.-c).

7.5 Varmuuskopiointitilat PPDM:llä

PPDM:llä on omat suojelupolitiikat, jotka voivat sisältää erilaisia käyttäjän määrittelemiä tavoitteita, jotka ohjaavat varmuuskopiointi-, aktiivisen suojauksen ja kopiodatanhallinnan toimintoja. Varmuuskopiointitiloja ja suojelupolitiikkoja ovat VMware-virtuaalikoneet, Microsoft Exchange Server -tietokannat, Microsoft SQL Server -tietokannat, Oracle-tietokannat, SAP HANA -tietokannat, tiedostojärjestelmät, Kubernetes-klusterit, tallennusryhmät ja verkkoon liitetty tallennustila (NAS). (Dell, n.d.-e). PPDM:llä voi siis palauttaa virtuaalikoneita, tietokantoja ja tiedostojärjestelmiä.

7.6 Verkkoadapterien ja VLAN-yhteensopivuus PPDM:llä

PowerProtect Data Manager voi erottaa hallinta- ja varmuuskopioliikenteen eri virtuaalisiin verkkoihin (VLAN). Virtuaaliset verkot auttavat parantamaan dataliikenteen reititystä, tietoturvaa ja organisointia. (Delltechnologies, 2022)

Data Managerin 19.13 versiosta alkaen NAS tukee useita VLANEja. Tämä tarjoaa joustavuutta erottaa NAS-tietojen suojaus verkko- liikenteestä hyödyntämällä VLANeja. Koska erilliset VLANit on määritetty ympäristöön, varmistetaan, että tiedot suojataan VLANeissa, jotka on määritetty suojatehtävää varten. Se mahdollistaa myös Datansuojan käytön useissa VLANeissa. Esimerkiksi, jos sinulla on kolme VLANia (hallinta, varmuuskopio ja tuotanto), PowerProtect Data Manager sallii ohjaus- ja datapolun toimintojen erottamisen jokaiselle VLANille, jonka olet määrittänyt PowerProtect Data Managerissa. (Dell, n.d.-f)

7.7 Moniasiakaskäyttö PPDM:llä

PowerProtect Data Manager ei luonnostaan tue moniasiakastukea VMware-tietojen suojaamiseen. Jotta moniasiakastuki voidaan ottaa käyttöön vRA:ssa niin suositellaan, että jokaiselle vRA:n tenantille tulisi olla omistettu PowerProtect Data Manager -esiintymä. Tenantin PowerProtect Data Managerin esiintymän tietojen suojeluohjelmat koskevat sitten vain kyseistä tenanttia. Tapauksissa, joissa varmuuskopioiden ylläpitäjälle sallitaan näkymä kaikkiin virtuaalikoneisiin useissa tenantteissa, saattaa olla mahdollista jakaa PowerProtect Data Managerin esiintymä useille vRA-tenantteille. (Dell, n.d.-g)

7.8 Välityspalvelin PPDM:llä

PowerProtect Data Manager sisältää valmiiksi sisäänrakennetun VM Direct Engine -moottorin. Tämä moottori toimii automaattisesti varmuuskopiointi- ja palautustoimintojen varavälityspalvelimena, kun lisätyt ulkoiset välityspalvelimet epäonnistuvat tai ne on poistettu käytöstä. VM Direct Engine helpottaa datan siirtoa sekä virtuaalikoneiden suojauskäytännöille että Kubernetes-klustereiden suojauskäytännöille. Dell Technologies suosittelee aina ulkoisen suojamoottorin, joka tunnetaan myös nimellä VM-proxy, käyttöönottoa, koska sisäänrakennetun välityspalvelimen kapasiteetti rinnakkaisten varmuuskopioiden suorittamiseen on rajoitettu. (DellTechnologies, 2022)

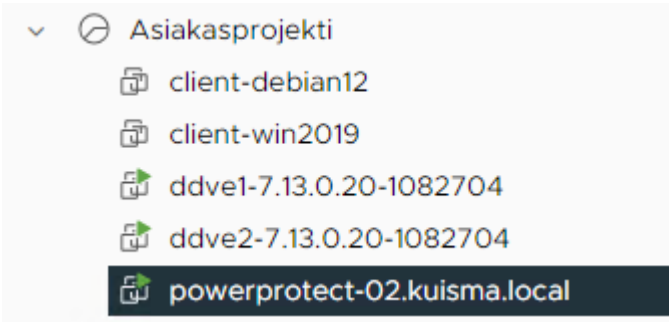
7.9 Asiakastuki PPDM:llä

Kuten Avamarkin, PPDM on myös Dellin omistama tuote. Täten asiakastuki tarjoaa samat tukimahdollisuudet, mitä Avamarilla (Top Solutions, Knowledge Base Articles, Manuals and Documents, Regulatory Information, Videos).

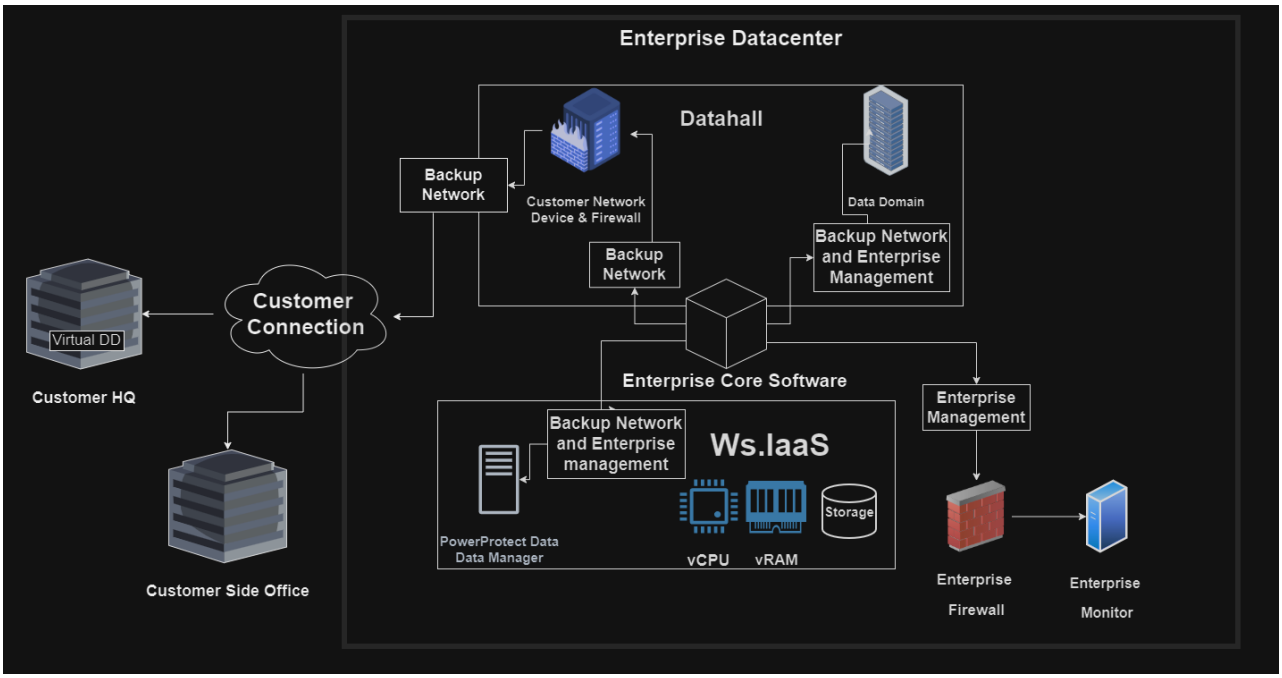
8 ASIAKASPROJEKTI

Kuvitteellisessa asiakasprojektissa tavoitteenani oli vastata kysymykseen, voiko Dell PowerProtect Data Manager-tuote korvata vanhemman Avamar-ratkaisun toimeksiantajani tarpeissa.

Aloitin projektin tekemällä samanlaisen myyntiskenaarion, mitä toimeksiantajallani tehdään usein asiakastapauksissa. Kuvasta 15 saa hyvän kuvan, minkälaista myyntiskenaariota haemme tässä projektissa. Kuvassa on toimeksiantajani jaettu virtuaaliasiakasympäristö, joka sisältää VMWare- ja muita virtualisointiympäristöjä, jotka ovat toimeksiantajani hallinnassa, ylläpidossa ja omistuksessa. Tämän alustan päällä pyörii eri asiakkaiden virtuaalipalvelimia ja omia ympäristöjä omissa dedikoiduissa verkoissaan. Asiakkaat hallinnoivat yleisesti palvelimiaan toimeksiantajani Morpheus Multi-Cloud -hallintatuotteen avulla (Kuva 15). Loin asiakkaalle vCenterissä oman resurssipoolin, johon asensin PowerProtect Data Managerin, Data Domain-järjestelmän ja Data Domain-järjestelmälle replikan. Lisäksi asensin muutaman testikoneen, joita varmuuskopioin PPDM:llä. Kuvassa 14 on asiakkaalle luotu resurssiallas (Kuva 14).



Kuva 14. Asiakaspooli



Kuva 15. Toimeksiantajan ratkaisukuva

Tämän jälkeen tutkin, miten projekti käytännössä toimisi ja onnistuisiko PPDM olemaan tässä projektissa käytettävä varmuuskopiointijärjestelmä. Vertailin kappaleissa 6 ja 7 tutkittuja järjestelmien ominaisuuksia ja soveltuvuutta ja arvioin kumpi ratkaisuista sopisi paremmin toimeksiantajani tarpeisiin tulevissa tämänkaltaisissa projekteissa. Koska kappaleissa 6 ja 7 kävin siis jo läpi tutkittavia ominaisuuksia, niin tämän vuoksi tässä osiossa keskityn enemmän tulosten vertailuun ja analysointiin, eikä perusominaisuuksien yksityiskohtainen käsittely ole tarpeen uudelleen. Kertauksena vielä, tutkittavat ominaisuudet olivat virtuaalikoneen varmuuskopiointi ja palautus, tiedostotason varmuuskopiointi ja palautus, tietojen säilytyskäytäntö, varmuuskopiointitilat,

verkkoadapterien ja VLAN-yhteensopivuus, välityspalvelin-mahdollisuus, asiakastuki sekä moniasiakaskäyttö.

8.1 Järjestelmien ominaisuuksien vertailu

Käyttöliittymä eroaa näillä kahdella alustalla siten, että Avamarin käyttöliittymässä varmuuskopiointi ja palautus tapahtuvat erillisten ikkunoiden kautta, kun taas PowerProtectissa prosessi on integroituna yhteen käyttöliittymään.

Virtuaalikoneen varmuuskopioinnissa sekä Avamar että PowerProtect tarjoavat käyttöliittymän kautta mahdollisuuden suorittaa virtuaalikoneiden varmuuskopioita. Molemmissa käyttäjä voi valita haluamansa virtuaalikoneen varmuuskopioitavaksi ja määrittää varmuuskopiointiasetukset. Avamarissa käyttäjä voi asettaa varmuuskopiointiprosessin konfiguraatioasetuksia, kuten säilytyskäytäntöjä ja salausmenetelmää. PowerProtectissa vastaavasti käyttäjä voi määrittää suojelupolitiikan asetuksia, tallennuspaikkaa ja muita varmuuskopiointiasetuksia. Molemmat ratkaisut tarjoavat myös varmuuskopioinnin lisäasetuksia, kuten CBT-menetelmän käytön ja salaustason määrittämisen.

Virtuaalikoneen palauttamisessa sekä Avamar että PowerProtect tarjoavat käyttöliittymän kautta mahdollisuuden palauttaa virtuaalikoneita varmuuskopioista. Käyttäjä voi valita palautettavan kohteen, määrittää palautuksen asetukset ja valita palautuksen sijainnin.

Avamarilla tiedostotason varmuuskopiointi voidaan suorittaa suoraan valitsemalla varmuuskopioitava kohde ja käyttämällä tiedostotason varmuuskopiointimenetelmää. PowerProtectissa tiedostotason varmuuskopiointia varten on ensin ladattava ja asennettava File System Agent -ohjelmisto, joka mahdollistaa tiedostojen suojaamisen ja palauttamisen isäntäkoneella. Huomasin myös, että PowerProtect tarjoaa enemmän vaihtoehtoja ja lisäasetuksia tiedostotason varmuuskopioinnissa, kuten katastrofipalautusasetukset, kun taas Avamarin asetukset saattavat olla hieman rajatummat.

Tiedostotason palautus tehdään samalla periaatteella kuin Avamarissa, mutta valitsemalla tiedostotason kohde ja liittämällä siihen tiedostojärjestelmä. Palautuksen asetuksissa käyttäjä voi määrittää palautuksen sijainnin ja muut lisäasetukset.

Tietojen säilytyskäytännöissä PowerProtect tarjoaa tarkempaa hallintaa tiedostojen säilytykseen ja turvallisuuteen liittyen Retention Lock-ominaisuudella, kun taas Avamarin säilytyskäytännöt tarjoavat mahdollisuuden hienovaraisempaan säilytysajan hallintaan varmuuskopioille eri perusteiden perusteella.

Varmuuskopiointitiloja PPDM:llä ohjaa sen suojelupolitiikat, jotka tarjoavat laajan valikoiman varmuuskopiointitiloja erilaisille järjestelmille ja ympäristöille, kun taas Avamarin varmuuskopiointivaihtoehdot vaihtelevat plug-inin mukaan ja ovat usein kohdistettuja tiettyihin käyttöjärjestelmiin ja sovelluksiin.

PPDM voi erottaa hallinta- ja varmuuskopioliikenteen eri VLANeihin. PPDM mahdollistaa useiden paikallisverkkojen käytön NAS-tietojen suojaamisessa ja tarjoaa laajemman tukivalikoiman VLANeille ja niiden hallinnalle. Avamarilla verkkoadaptereiden on oltava trunk-tilassa, jotta VLAN-verkot voidaan määrittää, ja VLAN-tunnisteet voi määrittää eri tavoin ESXi/ESX-palvelimissa.

Molemmat PowerProtect ja Avamar ovat Dellin omistamia tuotteita, joten ne tarjoavat samanlaista monipuolista asiakastukea, joka sisältää "Top Solutions" -osion yleisimpien ongelmien ratkaisemiseen, "Knowledge Base Articles" -osion yksityiskohtaisine ohjeineen ja vianmääritysoppaineen, sekä "Manuals and Documents" -osion asennus- ja käyttöohjeineen. Lisäksi se tarjoaa "Regulatory Information" -osion sääntelyyn liittyvään tietoon sekä "Videos" -osion opetusvideoineen.

Välityspalvelin-asioissa PPDM:llä on sisäänrakennettu moottori, joka toimii automaattisesti varavälityspalvelimena, kun taas Avamarissa välityspalvelinominaisuus vaatii erillisen virtuaalikoneasiakkaan käyttöönoton. Lisäksi Dell suosittelee ulkoisen suojamoottorin käyttöä PPDM:llä, kun taas Avamar ei tarjoa vastaavaa sisäänrakennettua vaihtoehtoa.

Moniasiakaskäyttö toimii loistavasti Avamarilla, sillä se tarjoaa tiiviin integroinnin VMware-ympäristöön mahdollistaen itsepalveluperusteisen tietojen suojaamisen. Lisäksi Avamarin VCD Data Protection Extension mahdollistaa varmuuskopiointipalvelujen integroinnin suoraan vCloud Directoriin, jolloin niitä voidaan jakaa moniasiakaskäyttöisessä mallissa. PPDM:ssä moniasiakaskäyttömahdollisuudet ovat kuitenkin erilaiset. Kuten kappaleessa 7.7 todetaan, niin PPDM ei tue natiivisti moniasiakaskäyttöä VMware-datan suojauksessa. Tämä tarkoittaa, että PPDM:llä ei ole sisäänrakennettuja ominaisuuksia eristää dataa ja käytäntöjä eri asiakkaiden välillä samassa PPDM-instanssissa. Yksittäisen PPDM-instanssin jakaminen useille vuokralaisille mainitaan vain mahdollisuutena, jos varmuuskopioinnin ylläpitäjän on nähtävä kaikki virtuaalikoneet. Tämä viittaa siihen, että jakaminen on epäsuositeltavaa tyypillisissä moniasiakaskäyttö-ympäristöissä, joissa datan eristäminen ja erilliset käytännöt ovat ratkaisevan tärkeitä. PPDM keskittyy pääasiassa yhden vCenter-ympäristön (asiakkaan) tehokkaaseen hallintaan. Vaikka se voidaan konfiguroida näkemään useita vCenter-ympäristöjä, sillä ei ole vahvoja eristysominaisuuksia datan suojauksessa näissä vCenter-ympäristöissä. Tämä tekee PPDM:stä vähemmän sopivan todellisille moniasiakaskäytön-ympäristöille, joissa tarvitaan itsenäisiä datan suojauskäytäntöjä ja eristystä. Tämä on isoin eroavaisuus ja epäkohta PPDM:ssä, kun vertaa Avamariin. PPDM puutteet moniasiakaskäytössä luovat suuren esteen sen soveltuvuudelle monimutkaisissa ympäristöissä, joissa on useita asiakkaita tai vuokralaisia.

Laadin vertailun selkeyttämiseksi taulukon, jossa on esitetty Avamarin ja PowerProtectin keskeiset ominaisuudet. Tämä auttaa tekemään lopullisen päätöksen varmuuskopiointijärjestelmän valinnasta (Taulukko 1).

Taulukko 1. Varmuuskopiojärjestelmien ominaisuuksien vertailu tiivistettynä

Vertailtava ominaisuus	PowerProtect	Avamar
Virtuaalikoneen varmuuskopiointi ja palautus	Suojelupolitiikan luominen ennen varmuuskopiointia. Politiikat määrittelevät varmuuskopion asetukset. Käyttöliittymän kautta mahdollisuus palauttaa virtuaalikone varmuuskopiosta. Voidaan valita palautettava kohde, määrittää palautuksen asetukset ja valita palautuksen sijainti.	"Backup & Restore" -osion kautta valitaan varmuuskopioitavat virtuaalikoneet. Konfiguraatioikkunassa asetetaan säilytyskäytännöt, salausmenetelmä ja valitaan välityspalvelin Käyttöliittymän kautta mahdollisuus palauttaa virtuaalikone varmuuskopiosta. Voidaan valita palautettava kohde, määrittää palautuksen asetukset ja valita palautuksen sijainti.
Tiedostotason varmuuskopiointi ja palautus	Ladataan ja asennetaan File System Agent -ohjelmisto. Tiedostojärjestelmän suojelupolitiikka. Enemmän vaihtoehtoja ja lisäasetuksia. Palautuksessa valitaan tiedostotason kohde ja liitetään siihen tiedostojärjestelmä.	Valitaan varmuuskopioitava kohde ja tiedostotason varmuuskopiointimenetelmä. Asetukset rajatummat. Simppeli palautus "Restore Now"-toiminnalla.
Tietojen säilytyskäytäntö	Kalenteripäivämäärä tai kiinteä säilytysaika.	Poistaminen tietyn määrän päivien, viikkojen,

Vertailtava ominaisuus	PowerProtect	Avamar
	"Retention Lock" tarjoaa muuttumattoman tiedostojen lukituksen ja turvatun säilytyksen.	kuukausien tai vuosien jälkeen. Neljä erilaista säilytysjakoa yhdelle varmuuskopiolle.
Varmuuskopiointitilat	VMware-virtuaalikoneet, Microsoft Exchange Server -tietokannat, Microsoft SQL Server -tietokannat, Oracle-tietokannat, SAP HANA -tietokannat, tiedostojärjestelmät, Kubernetes-klusterit, tallennusryhmät, NAS.	Tiedostojärjestelmät (AIX, HP-UX, Linux, Macintosh, Windows), VMWare Image, SQL Server ja SharePoint VSS -sovellukset, Tietokanta- ja sovellustason varmuuskopiointi sekä integroitu VSS-varmuuskopiointi.
Verkkoadapterien ja VLAN-yhteensopivuus	Erottaa hallinta- ja varmuuskopioliikenteen eri VLANeihin. Tukee useita VLANeja NAS-tietojen suojaamisessa. Ohjaus- ja datapolun toimintojen erottaminen VLANien välillä.	Verkkoadapterit trunk-tilassa VLAN-verkkojen määrittämiseksi. VLAN-tunnisteet määritetään ulkoisella kytkintunnustuksella, virtuaalikytkintunnistuksella tai virtuaalivierastunnistuksella.
Moniasiakaskäytäntö	Ei tue natiivisti moniasiakaskäyttöä VMware-datan suojauksessa. Jokaiselle vRA-tenantille oma PPDM-esiintymä.	Integroituu VMware-ympäristöön itsepalvelupe-rusteiseen tietojen suojaamiseen. Tukee tietosuojapalveluja julkisissa, yksityisissä ja

Vertailtava ominaisuus	PowerProtect	Avamar
		hybridipilvissä.
Välityspalvelimet	Sisäänrakennettu VM Direct Engine -moottori toimii automaattisesti varmuuskopiointi- ja palautustoimintojen varavälityspalvelimena. VM Direct Engine helpottaa datan siirtoa virtuaalikoneiden ja Kubernetes-klustereiden suojauskäytännöille	Vaatii välityspalvelimena toimivan virtuaalikoneasiakkaan, jotta voi tehdä varmuuskopiointi- ja palautustoimintoja. Asiakkaan rekisteröinti varmistaa tunnistetiedot Avamar-palvelimen kanssa.
Asiakastuki	"Top Solutions", "Knowledge Base Articles", "Manuals and Documents", "Regulatory Information", "Videos"-osiot palveluntarjoajan sivuilla.	"Top Solutions", "Knowledge Base Articles", "Manuals and Documents", "Regulatory Information", "Videos"-osiot palveluntarjoajan sivuilla.

9 LOPPUPÄÄTELMÄ

Vertailtuani PowerProtectin ja Avamarin ominaisuuksia ja soveltuvuutta toimeksiantajani tarpeisiin, olen tullut siihen tulokseen, että PowerProtect ei voi korvata Avamaria. Vaikka PowerProtect tarjoaa useita edistyneitä

ominaisuuksia, kuten laajan tietojen suojausstrategian ja hyvän suojelupolitiikkojen hallinnan, niin silti sen puutteet moniasiakaskäytössä tekevät siitä vähemmän sopivamman vaihtoehdon toimeksiantajani tarpeisiin. PowerProtect voi hyvin toimia Avamarin sijaan, jos se myydään asiakkaalle, jolla on oma IT-ympäristö. Tällaisessa kontekstissa PowerProtectin ominaisuudet voivat täyttää kaikki tarvittavat vaatimukset, ja sen integroitu käyttöliittymä voi tarjota selkeän ja hallitun varmuuskopiointikokemuksen. Kuitenkin, jos asiakas käyttää jaettua VMware-ympäristöä, kuten toimeksiantajani tarjoamaa, PowerProtectin käyttö ei ole suositeltavaa. Tällaisessa tilanteessa PowerProtect ei kykene tarjoamaan tarvittavaa eristystä ja itsenäisyyttä eri asiakkaiden välillä. Avamarin kyky tarjota vahvempi ja skaalautuvampi moniasiakaskäytön tuki tekee siitä yksinkertaisesti paremman vaihtoehdon toimeksiantajani kaltaisten organisaatioiden varmuuskopiointitarpeisiin.

LÄHTEET:

Auwau. (n.d.). Multi-tenancy for backup-as-a-service. Haettu 24.05.2024 osoitteesta https://auwau.com/articles/multi-tenancy-for-backup-as-a-service

Broadcom. (21.03.2024). VLAN configuration on virtual switches, physical switches and virtual machines. https://knowledge.broadcom.com/external/article?legacyId=1003806

Bunal, M. (01.06.2023). How To Use Proxies For Data Backup And Recovery. https://geonode.com/blog/how-to-use-proxy-for-data-backup-and-recovery

Ciesielski, J. (16.01.2023). Data restore vs. Backups: What is the difference? https://rewind.com/blog/data-restore-vs-backup/

Commvault. (n.d.). VM Backup. Haettu 27.05.2024 osoitteesta https://metallic.io/knowledge-center/glossary/vm-backup

Daisy. (11.01.2024). [Beginner Guide] What Is VMware? What Is It Used for? https://www.easeus.com/knowledge-center/vmware.html

Dell. (n.d.-a). Plug-in Options. Haettu 16.5.2024 osoitteesta https://www.dell.com/support/manuals/en-us/avamar-server/av_p_admin_guide/plug-in-options?guid=guid-0f05a8cf-6ae9-4898-91b0-8c40e9292c51&lang=en-us

Dell. (n.d.-b). Register or add a proxy client. Haettu 05.06.2024 osoitteesta https://www.dell.com/support/manuals/en-us/avamar-server/av_p_vmware_user_guide/register-or-add-a-proxy-client?guid=guid-582050c2-4091-4f38-b603-39ff329676ce&lang=en-us

Dell. (n.d.-c). Documentation. Haettu 20.05.2024 osoitteesta https://www.dell.com/support/home/en-us/product-support/product/avamar/docs

Dell. (n.d.-d). PowerProtect Data Manager. Haettu 07.06.2024 osoitteesta https://www.dell.com/en-in/dt/data-protection/powerprotect-data-manager.htm

Dell. (n.d.-e). Protection policies. Haettu 30.05.2024 osoitteesta https://www.dell.com/support/manuals/en-us/enterprise-copy-data-management/pp-dm_ag/protection-policies?guid=guid-cbfb0a3a-493f-409f-bbd1-3b3862803125&lang=en-usa

Dell. (n.d.-f). PowerProtect Data Manager 19.16 Network-Attached Storage User Guide. Haettu 31.05.2024 osoitteesta https://www.dell.com/support/manuals/en-in/enterprise-copy-data-management/pp-dm_19.16_nas_ug/multiple-vlan-support-for-nas?guid=guid-2d706ca5-5941-42aa-b18c-9cb137ed4521&lang=en-us

Dell. (n.d.-g) vRealize 7.x Data Protection Extension for PowerProtect Data Manager Installation and Administration Guide. Haettu 14.05.2024 osoitteesta https://www.dell.com/support/manuals/en-in/enterprise-copy-data-management/vrealize_7x_ppdm_iag/multi-tenancy-support-with-powerprotect-data-manager?guid=guid-b4ac048f-981b-4fa0-858b-8364d73b9285&lang=en-us

DellTechnologies. (n.d.-a). Dell Avamar. Haettu 07.06.2024 osoitteesta https://www.delltechnologies.com/asset/en-ie/products/data-protection/technical-support/h2568-dellemc-avamar-ds.pdf

DellTechnologies. (n.d.-b). Dell Emc Avamar Deduplication Backup Software and System. Haettu 20.05.2024 osoitteesta https://www.delltechnologies.com/asset/en-in/products/data-protection/technical-support/h2568-emc-avamar-ds.pdf

DellTechnologies. (n.d.-c). PowerProtect DD Retention Lock overview. Haettu 14.05.2024 osoitteesta https://infohub.delltechnologies.com/en-us/l/immutability-in-dell-data-protection-software-and-appliances/powerprotect-dd-retention-lock-overview/

DellTechnologies. (12.2022). Dell PowerProtect Data Manager: Deployment Best Practices. https://www.delltechnologies.com/asset/en-lt/products/storage/industry-market/h18564-powerprotect-data-manager-deployment-best-practice-wp.pdf

Einorytė, A. (01.10.2023). What is a VLAN? Virtual LANs explained. https://nordvpn.com/fi/blog/what-is-vlan/

Hewlett Packard Enterprise. (n.d.). What is virtualization? Haettu 21.05.2024 osoitteesta https://www.hpe.com/fi/en/what-is/virtualization.html

IBM. (n.d.). What is VMware? Haettu 22.05.2024 osoitteesta https://www.ibm.com/topics/vmware

IDrive. (n.d.). File-level Backup vs Disk Image Backup. Haettu 27.05.2024 osoitteesta https://www.idrive.com/file-backup-vs-image-backup

Moir, A. (2023). 9 data backup methods every business should know. https://blog.quest.com/9-data-backup-methods-every-business-should-know/

Moore, J. (04.2024). What is data backup? An in-depth guide. https://www.techtarget.com/searchdatabackup/definition/backup

NordVPN. (n.d.). Network adapter. Haettu 24.05.2024 osoitteesta https://nordvpn.com/fi/cybersecurity/glossary/network-adapter/

Own Company. (18.02.2022). Why Customer Support Is So Important In Backup And Recovery. https://www.owndata.com/blog/why-customer-support-is-so-important-in-backup-and-recovery

Reber, C. (21.02.2023). A Guide to Backup Retention Policy Best Practices. https://www.n-able.com/blog/backup-retention-policy-best-practices

Veeam. (22.11.2023). Restoring Entire VM. https://helpcenter.veeam.com/docs/backup/qsg_vsphere/vm_restore.html?ver=120

Wallen, D. (n.d.). Types of Backup: Understanding Full, Differential, and Incremental Backup. Haettu 27.05.2024 osoitteesta https://spanning.com/blog/types-of-backup-understanding-full-differential-incremental-backup/