Alf Räsänen

Liiketoiminnan jatkuvuuden varmistaminen

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tieto- ja Viestintätekniikka

Opinnäytetyö

7.5.2022

Tiivistelmä

Tekijä(t):	Alf Räsänen
Otsikko:	Liiketoiminnan jatkuvuuden varmistaminen
Sivumäärä:	53 sivua + 1 liite
Aika:	7.5.2022
Tutkinto:	Insinööri (AMK)
Tutkinto-ohjelma:	Tieto- ja viestintätekniikka
Suuntautumisvaihtoehto:	Tietoverkot
Ohjaaja(t):	Osaamisaluepäällikkö Janne Salonen

Tämän opinnäytetyön tarkoitus on esitellä Zerto Virtual Replication tuotetta sekä sen vaatimaa ohjelmistopohjaista palvelinympäristöä. Opinnäytetyössä kuvataan liiketoiminnan jatkuvuuden varmistamisen tarve, käsitellään sitä, miten jatkuvuus on perinteisesti toteutettu sekä verrataan perinteistä toteutusta Zerton tarjoamiin mahdollisuuksiin. Opinnäytetyö esittelee osat ja vaatimukset, joista moderni palvelinsaliympäristö koostuu. Opinnäytetyön teorian pohjalta suoritetaan vastaavan ympäristön perustaminen ja käytännön testinä Zerto Virtual Replication tuotteen toiminnan esittely.

Opinnäytetyö rajattiin koskemaan vain yhtä ohjelmistopohjaisen palvelinympäristön ratkaisua. Ratkaisuksi valittiin VMwaren tuote, joka koostuu ESXi virtualisointialustasta ja VMware vSphere vCenter hallinta-alustasta. Valinta perustui arvioon tuotteen laajemmasta käytöstä, jolloin tulokset koskettavat useampaa yritystä. Valitun alustan esittelyn ja havainnoinnin lisäksi tavoitteena on lyhyesti esitellä lukijalle Zerton tuotteen taipuvuus useampaan palvelinkapasiteetin toteutustapaan. Opinnäytetyön päätavoite on osoittaa Zerton käyttöönoton ja toiminnallisuuden helppous unohtamatta toiminnan varmuutta. Käyttöönotto ja toiminnallisuus havainnoitiin käytännön testin kautta.

Opinnäytetyön testin tuloksena on näytetty Zerto Virtual Replicationin toimivuus tilanteessa, jossa yrityksen tuotantoympäristössä on ilmaantunut ongelma. Lopputuloksena on yrityksen palvelun siirtyminen varmistusympäristöön. Varmistusympäristön toimiessa yrityksen tuotantoa voidaan jatkaa varmistusympäristöstä käsin.

Avainsanat:	Palvelinkapasiteetti, Jatkuvuus, Varmistus, Liiketoiminta. Replikointi

Abstract

Author(s):	Alf Räsänen
Title:	Ensuring the continuity of business operations
Number of Pages:	53 pages + 1 appendice
Date:	7 May 2022
Degree:	Bachelor of Engineering
Degree Programme:	Information and Communication Technology
Specialisation option:	Information Networks
Instructor(s):	Janne Salonen, Head of the Department

The purpose of this thesis is to introduce the Zerto Virtual Replication product and the software defined datacentre it requires. The thesis describes the importance of ensuring the continuity of business operations, investigates how it has been traditionally done and compares the traditional way to the possibilities Zerto offers. The thesis introduces the building blocks and requirements a modern datacentre has. Based on the theory presented in the thesis a test environment is created and a practical test is conducted in which the function of Zerto Virtual Replication is presented.

The subject of the thesis was narrowed to consist of only the one software defined datacentre product. The product chosen was VMware ESXi virtualisation platform and VMware vSphere vCenter management platform. The choice was based on the evaluation that this product is more commonly used and as such the results fit a larger commercial audience. In addition to introducing the platform the aim of the thesis is to showcase the flexibility of Zertos product and how it can fit many other server capacity solutions. The main goal of the thesis is to show how effortless the set up of the product is and how easy it is to use without forgetting its reliability. A practical test was conducted to show the set up and functionality of the product.

The product of the tests conducted for the thesis demonstrates the utility of Zerto Virtual Replication product in a situation where a problem has occurred in the production environment. The end-product shows the replication of the business operations into the replication environment. When the replication environment operates as planned the production can continue from the replication environment.

Keywords: Server capacity, Continuity, Backup, Business operations, Replication

Sisällys

Lyhenteet ja sanasto

DR	Disaster Recovery, eli katastrofista palautuminen on prosessi missä yrityksen liiketoiminnan kannalta käytössä olevat palvelimet ja niissä toimivat palvelut palautetaan takaisin toimintaan.
Hypervisor	Vastaava nimike virtualisointialustalle, jonka päällä suoritetaan palvelimien virtualisointia.
VM	Virtuaalipalvelin, eli tavallinen palvelin joka on virtualisoitu.
Replikoida	Palvelimen datasta ylläpidetään kopiota reaaliaikaisesti toisessa järjestelmässä.
ESXi	VMwaren ohjelmistopohjainen virtualisoinnin käyttöjärjestelmä, joka toimii virtualisointialustana.
vCenter	ESXi kanssa käytettävä kyseisen virtualisointialustan sisälle asennettava virtualisointiympäristön hallinta-palvelin.
RPO	Recovery Point Objective. Palautuspiste, johon on mahdollista palautua. Zertossa seurataan palautuspisteen viivettä, sillä palautuspiste on aina etukäteen määrittelemättömän määrän sekunteja jäljessä.
Reverse Protection	Takaisin suojaus, virtuaalipalvelimen muutokset tallennetaan takaisin tuotantojärjestelmään.
Journal History	Päiväkirja, mihin tallennetaan kaikki virtuaalipalvelimelle tapahtuneet muutokset.
Bitmap	Taulukkoon kerätyt muutokset palvelimelle tapahtuneista muutoksista. Taulukkoon tallennetaan muuttuneet blokit tai blokkien alueet.
Blokki	Tallennusjärjestelmät käyttävät blokkeja tiedon tallentamiseen. Replikointituote seuraa muuttuneita blokkeja.

1 Johdanto

Yrityksen liiketoimintapalveluiden jatkuvuudelle ja turvaamiselle asetetaan jatkuvasti entistä enemmän vaatimuksia. Yrityksien liiketoiminnan kannalta oleelliset palvelut ovat modernissa konesaliympäristössä yleensä virtualisoituja palvelimia, jotka toimivat virtualisointialustan alla. Modernissa virtualisoidussa konesalissa kuormia, eli virtuaalipalvelimia, voidaan siirtää vapaasti alustapalvelimelta toiselle ja laajemmissa ympäristöissä jopa eri klusterien välillä. Tämänlainen kuorman liikuteltavuus sallii yrityksen tai palveluntarjoajan tuottaa korkeasti vikasietoista palvelua työkuormilleen. Palvelujen alustat rajoittuvat kuitenkin yleisesti samaan sijaintiin, eli tämänlaisessa tapauksessa konesaliin. Toiminnan keskittyminen tiettyyn sijaintiin johtuu yleensä sekä teknisistä, että kustannuksellisista rajoituksista. Palvelua halutaan tuottaa vikasietoisuuden lisäksi mahdollisimman tehokkaasti ja tehokkuutta mitataan tyypillisesti palvelun nopeuden sekä kustannuksen muodossa.

Perinteinen tapa varmistaa yrityksen liiketoimintapalveluiden jatkuvuus katastrofitilanteissa on suorittaa säännöllisiä varmuuskopioita tuotantoympäristöstä. Varmuuskopiot suoritetaan yleensä kerran päivässä ja tallennetaan isommissa ympäristöissä tyypillisesti deduplikoivaan tallennusratkaisuun joko paikallisesti samassa sijainnissa tai etänä olevaan sijaintiin. Deduplikoiva tallennusratkaisu voi sallia varmistuksien säilömiseen merkittäviä datansäästöjä sillä toistuvat dataketjut identifioidaan analysointiprosessissa, eikä niitä kirjoiteta uudelleen, vaan vastaavaan ketjuun osoitetaan pienellä viittauksella. Mikäli data viedään etänä olevaan tallennustilaan, toteutuksella voidaan saavuttaa parempi toiminnan varmuus katastrofitilanteessa, jossa tuotannon konesaliympäristö kärsii esimerkiksi tulipalosta. Varmuuskopiot voidaan silloin palauttaa sijainnista, jossa data pysyy turvassa tuotantoympäristön paikalliselta vikaantumiselta. Varmuuskopioista palautuminen vie kuitenkin erittäin paljon aikaa ja mikäli alkuperäinen konesaliympäristö on palanut käyttökelvottomaan kuntoon, tällöin todennäköisesti täytyy myös rakentaa uusi ympäristö, johon data voidaan palauttaa. Perin-

teiset varmuuskopioinnit on myös tyypillisesti ajoitettu tiettyyn vuorokaudenaikaan, jolloin palauttaminen saattaa olla mahdollista vain jopa päivän takaiseen dataan. Lyhyetkin katkoset saattavat aiheuttaa merkittäviä menetyksiä yrityksen liiketoiminnan kannalta. Tämä voi näkyä esimerkiksi menetettyinä mahdollisuuksina tai toiminnan luotettavuuden alenemana, jonka palvelun tavoittamattomuus aiheuttaa. Tyypillisten varmistusjärjestelmien lisäksi käytössä voi olla tallennusjärjestelmän omat näköiskuvat (storage snapshot). Näköiskuvien luominen ei aiheuta viivettä ja niitä voidaan siten tehdä useita peräkkäin esimerkiksi minuutin välein. Tällöin tallennustilassa kirjoituslukitaan alkuperäinen data ja siihen viitataan metadatalla, kun uusia kirjoituksia tulee järjestelmään. Näköiskuvien luomisessa on kuitenkin yhä olemassa perustavanlaatuinen ongelma, sillä tallennustilan näköiskuvat ovat luomisen jälkeen samassa järjestelmässä, missä varsinainen alkuperäinen data on. Dataa ei siis ole kopioitu talteen ulkopuoliseen sijaintiin, vaan tämän tyyppisillä näköiskuvilla voidaan ainoastaan palata johonkin tiettyyn kohtaa nopeasti alkuperäisen ympäristön sisällä. Tilanteissa, joissa alkuperäinen ympäristö tuhoutuu, ei näköiskuvien luonnilla siis ole palautuksen ja näin ollen turvallisuuden kannalta merkitystä.

Disaster Recovery -palvelu, eli katastrofipalautuminen palveluna, mahdollistaa asiakkaan virtuaalipalvelimien turvaamisen aktiivisesti käytössä olevan konesaliympäristön ulkopuolelle. Virtuaalipalvelimet ovat tällöin suojattu ympäristökohtaisilta tapahtumilta, missä kriittisiin palveluihin kohdistuu ei-toivottuja ulkoisia haittavaikutuksia kuten tulipalo, pitkä sähkökatko, vesivahinko tai järjestelmien vioittuminen, kuten esimerkiksi levyjärjestelmän tai palvelinkehikkojen viat. DR-palvelua voidaan käyttää myös suojana ohjelmistovikoja, haittaohjelmia tai epäonnistuneita päivityksiä vastaan. DR-palvelu tietyillä teknisillä toteutuksilla mahdollistaa myös liiketoiminnan kannalta merkittävien järjestelmien osittaisen palauttamisen viimeiseen toimivaan tilaan esimerkiksi yllättävässä korruptoitumistilanteessa.

Usein katastrofisuojautumisjärjestelmät koetaan kalliiksi ja raskaiksi ympäristöiksi, joiden pelkkä käyttöönotto edellyttää merkittäviä investointeja resurssei-

hin ja laitteistoihin. Laitevalmistajan toteutuksessa se voidaan esimerkiksi tarjota levyjärjestelmän lisensoinnin kautta, mutta yrityksen täytyy tällöin hankkia täysin samanlainen laitteisto kuin mikä on käytössä tuotannossa Disaster Recovery toteutusta varten. Tämänlaisen laiteriippuvuuden takia jo pelkästään palvelun perustaminen voi luoda merkittävät kustannukset yritykselle, mikä voi estää tai vähintään vaarantaa katastrofisuojautumisjärjestelmän käyttöönoton.

Tässä opinnäytetyössä esiteltävä Zerto Virtual Replication tarjoaa tuotteena yrityksille DR-palveluratkaisun, joka ei ole riippuvainen alustan toteutuksesta, sillä Zerton ohjelmisto on yhteensopiva usean eri virtualisointialustan kanssa. Zerton kanssa yritys ostaa lisensoinnin esimerkiksi sadalle virtuaalikoneelle vuodeksi ja voi täten suojata sata virtuaalikonetta toiseen klusteriin. [11.] Tässä opinnäytetyössä keskitytään Zerton Virtual Replication tuotteen tarjoamaan Disaster Recovery ratkaisuun, kun käytössä on VMwaren ohjelmistopohjainen virtualisointialusta.

2 Moderni konesali

Tässä luvussa perehdytään tarkemmin modernin konesalin ominaisuuksiin ja erilaisiin rakennusmahdollisuuksiin sekä virtuaalipalvelimen rakenteeseen. Luvussa käydään läpi kahta yleistä virtualisointialustan toteutusta, mutta keskitytään tarkemmin VMwaren ratkaisuun, joka liittyy opinnäytetyön toteutukseen. Modernissa konesalissa laitteistoalusta rakennetaan käyttäen perinteisiä laitevalmistajien palvelimia, keskitettyjä ja laajennettavia modulaarisia yksiköitä laajennuspaikoilla tai hyperkonvergenttisiä palvelimia.

Perinteiset fyysiset palvelimet ovat sellaisia, missä tilaaja pystyy itse mukauttamaan laajalla otannalla laitteiston kokoonpanoa ja vastaa käytännössä itse siitä, että se toimii tarkoitettuun käyttötarkoitukseen. Perinteisessä mallissa voidaan tehdä tiettyjä kustannussäästöjä komponenttien osalta ja valita useamman eri valmistajan ratkaisu.

Keskitetyt ja laajennettavat modulaariset yksiköt taas ovat laitevalmistajien valmiita kehikoita, mihin yritys voi ostaa oman tarpeensa mukaan tarvittavan määrän asennettavia moduuleja. Kehikossa on aina rajallinen määrä laajennuspaikkoja ja kokoonpanon kannalta valinnanvara on huomattavasti rajatumpi. Positiivisena asiana kokoonpanossa voidaan nähdä palvelimien yhteensopivuus ja samanlaisuus, mikä voi pienentää ylläpidollisia kustannuksia.

Uusimpana tarjontana palvelinsalin alustaksi on eri valmistajien hyperkonvergentit ratkaisut. Näissä yhdistyy laitevalmistajan valmis kokoonpano ja palvelimen mukana tulevat omat kiintolevyt, joista levyjärjestelmä koostuu. Avainasemassa kyseisessä ratkaisussa on kuitenkin laitevalmistajan tarjoama hallintarajapinta, virtualisointialustan kanssa verifioitu yhteensopivuus sekä laaja tuki vikatilanteissa. Hyperkonvergentti ratkaisu on kuitenkin yleensä hieman hintavampi, sillä sen tarkoituksena on tarjota asiakkaalle niin sanotusti avaimet käteen -ratkaisu, mihin sisältyy myös laitevalmistajan tekninen tuki. Asiakkaan kannalta ylläpito jää täten minimaaliseksi. [1.][4.]

2.1 Ohjelmistopohjainen konesali

Yhteisenä kaikilla näillä fyysisillä palvelimilla on kuitenkin modernin konesalin perusajatus; ohjelmistolla toteutettu konesalin virtualisointiympäristö ja kattava kuormien liikuteltavuus reaaliajassa ilman käyttökatkoja. [2.] Ohjelmistopohjaisia virtualisointialustoja tarjoavat esimerkiksi Microsoft ja VMware. Microsoftin virtualisointialusta on Hyper-V ja sen hallinta-alustana toimii System Center with Virtual Machine Manager (VMM). VMwaren virtualisointialusta taas on ESXi ja sen hallinta-alustana toimii vSphere vCenter.

Microsoftin tuotteissa Hyper-V toimii virtualisointialustana sekä rajattuna hallinnointialustana, jonka päällä virtuaalipalvelimien kuormia ajetaan. System Center Configuration Manager with VMM taas tarjoaa laajemmat hallittavuudet, sekä merkittävämmän muokattavuuden ohjelmistopohjaisen virtualisointialustan toiminnallisuuksiin. VMwarella vastaavasti ESXi on virtualisointialusta sekä rajattu

hallinnointialusta, missä virtuaalipalvelimet toimivat ja vSphere vCenter tuo mukanaan kehittyneet ohjelmistopohjaisen virtualisointialustan toiminnallisuudet, sekä laajan reaaliajassa toimivan kuorman liikuteltavuuden.

Käytännössä molempiin ratkaisuihin tuodaan palvelimen kautta prosessointikyvykkyys ja toteutuksen mukaan tallennustila voi olla joko alustan sisäistä tai tuotu ulkoisesta levyjärjestelmästä. Fyysiset palvelimet voivat koostua erilaisista tai samanlaisista komponenteista, mutta tulevaisuutta ajatellen voidaan laittaa prosessorien käskykannan yhteensopivuustila päälle. Mikäli olemassa olevaa klusteria myöhemmin laajennetaan, niin yhteensopivuustilan myötä virtuaalipalvelimia on kuitenkin mahdollista siirtää vanhemmalta alustalta uudemmalle alustalle sekä takaisin. Prosessorin käskykannan yhteensopivuustila maskeeraa raudan prosessorin ominaisuudet samanlaisiksi kuin mitä on saatavilla kaikilla alustapalvelimilla ja näyttää tämän virtuaalipalvelimelle. Virtuaalipalvelin ei tällöin tiedä toisen alustapalvelimen prosessorin uudemmista ominaisuuksista eikä pysty käyttämään niitä hyödyksi, mutta voi silti toimia kyseisellä alustalla. Microsoftilla ominaisuus otetaan käyttöön jokaisen erillisen virtuaalipalvelimen ominaisuuksista, kun taas VMwarella vastaava ominaisuus on mahdollista asettaa koko klusterille tai pelkästään tietylle virtuaalipalvelimelle. [3.]

Kuorman liikuteltavuuden mahdollistamiseksi tarvitaan alustojen ja hallinnointipalvelimien väliset verkkoyhteydet. Tämänlaisessa ratkaisussa, kun kuorma voi olla useammalla alustalla sekä samanaikaisesti sen tallennustila toisessa järjestelmässä, verkkoyhteydet täytyy toteuttaa mahdollisimman virtaviivaisesti saman konesalin sisällä. Käytännössä tämä tarkoittaa sitä, että alustapalvelimilla ja mahdollisilla muilla järjestelmillä (levyjärjestelmä) tulee olla suorin mahdollinen yhteys konesalin runkoverkkoon, jotta hyppyjen määrä jää minimiin. Tällä tavalla maksimoidaan käytettävissä oleva kaistanleveys ja minimoidaan yhteyksien viive. Huomioitava on myös se, että alustapalvelimien verkkoyhteydet tulisi kytkeä vikasietoisesti vähintään kahdella liitännällä kahteen eri kytkimeen. Näin kahdentamalla yhteydet, voidaan tarvittavat tietoliikenneyhteydet tuottaa yhä, vaikka toinen kytkimistä olisi poissa käytöstä huoltoa varten. Kuormia siirrettä-

essä, virtualisointialustan ohjelmiston mukaan, voi olla käytössä älykäs tunnistus ja kuorma siirtyy suorinta reittiä toiselle alustapalvelimelle. Tällöin minimoidaan hyppyjen määrä sekä siirrosta aiheutuva rasitus runkoverkkoon.

Ilman älykästä lyhimmän polun tunnistusta kuorma ei siirry toiselle alustapalvelimelle lyhintä reittiä pitkin, vaan siirtyy palvelimelle jotakin tunnettua reittiä pitkin, joka ei välttämättä ole lyhyin. Perusajatus molemmissa verkkopolun käyttömetodeissa kuitenkin säilyy, eli kuorma on mahdollista siirtää verkkoyhteyttä pitkin toiselle alustapalvelimelle.

2.2 Virtuaalipalvelimen rakenne

Alustalla oleva virtuaalipalvelin koostuu yleensä useasta objektista. Virtualisointiratkaisuissa tyypillisesti virtuaalipalvelimella on konfiguraatiotiedosto, levytiedosto, boottitiedosto, näköiskuvatiedosto (snapshot) ja lokitiedosto. Konfiguraatiotiedosto pitää tallessa sen, miten virtuaalipalvelin on koostettu ja mitä resursseja sekä komponentteja sille on annettu. Käytännössä tämä tiedosto sisältää tiedon virtuaalipalvelimen käyttämien prosessorien määrästä, keskusmuistin määrän, tiedot levyohjaimesta ja siitä, mistä palvelimen kiintolevytiedosto löytyy. Sen lisäksi konfiguraatiotiedostossa on tieto verkkokortista ja siitä, mihin se on yhdistetty, cd/dvd-asemasta ja USB-ohjaimesta sekä sen mitä USB-laitteita palvelimella on. [5.]

Levytiedosto on kohde, johon asennetaan käyttöjärjestelmä ja se toimii siis käyttöjärjestelmän kiintolevynä. Käynnistystiedostosta taas luetaan virtuaalipalvelimen käynnistämiseen tarvittavat BIOS tai EFI asetukset. Näköiskuvatiedostoa (snapshot) käytetään, kun halutaan esimerkiksi suorittaa varmistuksia palvelimesta ja alkuperäinen levytiedosto halutaan suojata muutoksilta tietystä ajankohdasta eteenpäin. Lokitiedostoon kerätään virtuaalikoneen ja alustapalvelimen välillä tehtyjä muutoksia sekä virtualisointialustan kautta tehtyjä palvelimen tapahtumia. Tiedostojen muodot ovat erilaisia virtualisointialustan mukaan, mutta niiden käyttötarkoitus säilyy samana.

Virtuaalipalvelimen siirtäminen reaaliajassa alustalta toiselle tapahtuu käyttäjien näkökulmasta ilman katkoja. Prosessia kutsutaan Microsoftin alustalla Live Migrationiksi ja VMwarella vastaavasti vMotioniksi. Ominaisuutta hyväksikäyttäen on alustalla mahdollista toteuttaa käyttökatkoja tai siirtää intensiivisempiä kuormia toiselle, enemmän vapaita resursseja sisältävälle alustalle, ilman ympäristön alasajoa. Virtuaalipalvelimen osalta voidaan siirtää sen käyttöjärjestelmän prosessointikuorma (prosessori, keskusmuisti, liitännäiset laitteet) toiselle virtualisointialustalle tai vastaavasti mahdollista on myös siirtää pelkästään virtuaalipalvelimen kiintolevy(t) toiseen tallennustilaan. VMwaren vMotion ominaisuus käyttää kolmea rakenneosaa hyödyksi toimenpidettä varten. [6, s.1.]

Ensimmäinen näistä rakenneosista on jaettu tallennustila, jossa virtuaalipalvelimen tiedostot sijaitsevat. Jaettu tallennustila voi olla teknologialtaan toteutettu FC tai iSCSI SAN, NAS tai vSAN tallennustila. Kun tallennustila on jaettu, eli se on kaikille alustapalvelimille nähtävillä, voivat VMwaren ESXi palvelimet samanaikaisesti käsitellä tiedostoja, joista virtuaalipalvelin koostuu. [6, s.1.]

Toinen rakenneosa on virtuaalipalvelimen aktiivinen keskusmuisti ja sen tarkka käskyjen tila, jotka siirretään verkon yli alkuperäiseltä ESXi palvelimelta kohdepalvelimeen. Tähän VMware käyttää hyödyksi bitmap taulukkoa, johon kerätään talteen kaikki aktiiviset ja meneillään olevat keskusmuistin muutokset. VMwaren vMotion jäädyttää alkuperäisen virtuaalipalvelimen, kopioi bitmapin kohteena olevaan ESXi palvelimeen ja jatkaa virtuaalipalvelimen toimintaa kohteessa. Uusimpien VMwaren optimointien myötä koko vMotion toimenpide aiheuttaa vain alle sekunnin katkoksen (stun time) virtuaalipalvelimen omaan toimintaan eikä siitä aiheudu suorituskyvyn kannalta hidastelua. Käyttäjän ja käyttöjärjestelmän kannalta kyseinen katkos ei ole havaittavissa mitenkään tyypillisessä järjestelmässä. [6, s.1.]

Virtuaalipalvelimen toiminnallisuus ei yleensä koostu ainoastaan palvelimen sisällä tapahtuvista toimenpiteistä, vaan yhteyksiä tulee myös ulkopuolelta. Virtuaalipalvelimen verkot, jotka ovat myös virtualisoituja VMwaren ESXi palveli-

mella, ovat kuormansiirron kolmas rakenneosa. Virtuaalipalvelimen verkon identiteetti ja yhteydet säilytetään, kun palvelin siirretään alustapalvelimelta toiselle. VMotion toimenpiteen aikana kohdealustalle siirretyn virtuaalipalvelimen MAC-osoitetta hallitaan siten, että vMotion lähettää ping käskyn verkon reitittimelle, jotta se tietää missä palvelimen fyysinen sijainti jatkossa on. Verkon pakettien osalta menetetään vain yksi paketti, kun palvelin siirtyy alustapalvelimelta toiselle. Koska palvelimen tarkka käskyjen tila keskusmuistissa, verkon identiteetti ja aktiiviset verkkoyhteydet siirretään reaaliajassa hallitusti ESXi:ltä toiselle, toimenpiteestä ei aiheudu käyttökatkoja tai työn keskeytystä käyttäjille. [6, s.1.]

2.3 Modernin konesalin hyödyt

VMwaren virtualisointiympäristössä on mahdollista ottaa käyttöön saman klusterin sisällä High Availability (HA) ominaisuus. VMware vSphere HA sallii virtuaalipalvelimen automaattisen uudelleen käynnistämisen toisella ESXi palvelimella, mikäli virtuaalipalvelimen alkuperäisellä alustalla on ilmaantunut jokin ongelma. VMwaren HA on virtuaalipalvelimen käyttöjärjestelmästä riippumaton ratkaisu ja se toimii kaikilla klusterin ESXi palvelimilla sen jälkeen, kun ominaisuus otetaan käyttöön.

Microsoftin Hyper-V alustalla vastaava ominaisuus on nimeltään Failover Clustering. Failover Clustering vaatii huomattavasti enemmän konfiguraatiota virtuaalipalvelimen osalta, mutta sen on mahdollista tarjota käytännössä käyttökatkoton siirtyminen toimivalle alustapalvelimelle, mikäli virtuaalipalvelimen oma käyttöjärjestelmä tukee kyseistä ominaisuutta. Nämä ominaisuudet toteuttavat toiminnallisuudet käytännössä seuraamalla virtualisointialustalla eri komponentteja. Jos toiselle alustapalvelimelle siirtyminen on mahdollista toteuttaa virtuaalipalvelimen sovelluksia varten, kyseessä on huomattavasti monimutkaisempi toteutus verrattuna VMwaren HA ratkaisuun. [7.] Opinnäytetyön toteutukseen valittiin käsiteltäväksi VMwaren ratkaisu, joten Microsoftin ratkaisu rajautuu käytännön vuoksi opinnäytetyön ulkopuolelle eikä Microsoftin ratkaisuja käsitellä tästä syystä syvemmin.

VMwarella HA jakaa Master ja Subordinate roolit ESXi palvelimille. Master palvelin seuraa ja vastaanottaa raportointia Subordinate alustoilta, seuraa virtuaalipalvelimien sisäistä toimintaa Heartbeat ja VMware Tools raportoimien tietojen mukaisesti, sekä tarkistaa jaetun tallennustilan tapauksessa levyillä tapahtuvia muutoksia ja juttelevatko muut alustapalvelimet sinne. Master ja Subordinate palvelimet vaihtavat keskenään verkossa Heartbeat tunnisteita joka sekunti. Mikäli Heartbeat on epäonnistunut, suorittaa Master alustapalvelimen elossaolon tarkistuksen (host liveness check). Kyseinen tarkistus määrittelee, jutteleeko kadonnut ESXi yhä jaetun tallennustilan kanssa, ja lähettää sen jälkeen sen hallintaosoitteeseen ICMP ping paketteja. Jos suorat yhteydet Subordinate alustan HA agenttiin ja ICMP ping pakettien lähetys sen hallintaosoitteeseen epäonnistuvat, alustapalvelimen katsotaan olevan epäonnistuneessa (failed) tilassa ja sen virtuaalipalvelimet käynnistetään uudelleen toisella alustalla. Mikäli Subordinate alustapalvelin jakaa Heartbeat paketteja jaetun tallennustilan kanssa, sen oletetaan olevan erkaantunut verkosta (network isolated) ja Master palvelin monitoroi alustapalvelinta sekä sen virtuaalipalvelimia. Mikäli virtuaalipalvelimet sammuvat verkosta erkaantuneella alustapalvelimella, Master käynnistää kyseiset virtuaalipalvelimet toisella alustapalvelimella. [8.]

Tallennustilan Heartbeat ominaisuudella HA luo jaetun tallennustilan juureen hakemiston (.vSphere-HA), jota käytetään tallennustilan Heartbeat ominaisuuden tarkistamiseen sekä suojattujen virtuaalipalvelimien listaamiseen. Minimissään HA tarvitsee tähän kaksi tallennustilajärjestelmästä alustalle näytettyä loogista levy-yksikköä voidakseen toteuttaa luotettavasti seurantaa tallennustilan kautta. [8.]

3 Zerto

Zerto tarjoaa useita eri ohjelmistopohjaisia ratkaisuja modernin konesaliympäristön suojaamiseen ja yrityksen liiketoiminnan jatkuvuuden varmistamiseen. Zerton perusajatuksena on toimittaa ratkaisuja, jotka ovat alustasta riippumattomia, jotta tuotteita on mahdollista käyttää laajasti erilaisissa ympäristöissä.

Tässä luvussa tarkastellaan Zerton pääasiallista tuotetta, Zerto Virtual Replication ratkaisua ja sen eri ominaisuuksia. Opinnäytetyön myöhemmin kuvattava käytännön simulaatio toteutettiin Zerto Virtual Replicationilla. Tuote on julkaistu ensimmäistä kertaa vuonna 2011. [9.]

3.1 Zerto Virtual Replication

Zerton Virtual Replication on Zerton tarjoama Disaster Recovery -toteutus. Tuotteen perusajatuksena on automatisoida DR-toteutusta, testausta sekä sen hallintaa. Zerton tuotteella on mahdollista toteuttaa virtuaalipalvelimien reaaliaikaista synkronointia toiseen virtualisointiympäristöön vain muutaman sekunnin viiveellä, mikä mahdollistaa sen, että käyttäjälle voidaan tarjota palautuspisteitä sekuntien tarkkuudella [10, s. 7]. Replikointi tapahtuu alustapalvelimen käyttöjärjestelmän tasolla.

Zerto ei tarvitse pääsyä varsinaiseen virtuaaliseen palvelimeen, jota tuotteella on tarkoitus suojata. Kun suojaus tehdään alustapalvelimen tasolla, Zerton käyttö tarjoaa kustannustehokkuutta ja ketteryyttä verrattaessa perinteisiin tallennusjärjestelmien replikointiratkaisuihin. Zerton ohjelmiston käyttäminen ei sisällä erityisiä vaatimuksia laitteistolle, jonka kanssa replikointia aiotaan käyttää. Näin ollen asiakas voi vapaasti käyttää mitä tahansa valitsemaansa laitteistoa. [10, s. 2.][10, s. 4.]

Zerto Virtual Replication on saatavilla tyypillisempiin VMware vSphere ja Microsoft Hyper-V ympäristöihin. Public ja hybrid cloud puolella tuote on saatavilla myös Disaster Recovery as a Service (DRaaS) palveluna Microsoftin Azure, Amazonin AWS, IBM Public Cloud ja Zerton oman CSP ympäristön kanssa. Toimintoina Zerto tarjoaa virtuaalipalvelimen replikoinnin yhdestä sijainnista useampaan eri sijaintiin, automaattisen palautuksen, palautumisen takaisin tuotantoon sekä yliheiton suojattuun sijaintiin. Zerton Virtual Replication tuote sallii myös virtuaalipalvelimen automaattisen konvertoinnin VMwaren virtualisointialustalta Hyper-V alustalle sekä toisin päin. Zertolla on myös mahdollista suo-

rittaa replikointia muiden tuettujen ympäristöjen välillä, eli ylläpitäjän ei ole tarvetta sitoutua käyttämään tietyn tarjoajan tuotteita. Ylläpitäjän tulee toki varmistaa, että virtuaalipalvelimet lähtevät toimimaan erilaisessa ympäristössä ja huomioida mahdolliset tarvittavat muutokset replikoitavan palvelimen yliheittoa tehdessä. Replikoitaessa esimerkiksi Hyper-V:ltä VMwarelle tulee ylläpitäjän etukäteen asentaa virtuaalipalvelimelle VMware Tools komponentit yhteensopivuuden takaamiseksi. [10, s. 5.]

Tänä päivänä Zertolla on jo useampia vastaavia tuotteita tarjoavia kilpailijoita. Suurin osa kilpailijoista keskittyy omaan tuotteeseensa pohjautuvaan ratkaisuun. Tunnetuimpia kilpailijoita ovat Veeam Backup & Replication, VMware SRM, Rubrik, Azure Site Recovery, Commvault, Dell EMC RecoverPoint for Virtual Machines, Cohesity DataProtect sekä Oracle Data Guard [20]. Läheisimpänä näistä, tarjoten DR ratkaisua useampaan eri alustaan, on Veeam Backup & Replication.

3.1.1 Replikoinnin toimintakuvaus

Yrityksen liiketoiminnan jatkuvuuden takaamisen kannalta tarvitaan nykypäivänä toimintaa tukevia ratkaisuja, mikä modernin konesalin kohdalla tarkoittaa yhden tai tyypillisesti useamman palveluun liittyvän virtuaalipalvelimen varmistamista. Tämän päivän konesalissa ja moderneilla ratkaisuilla tarvitaan kuitenkin jatkuva suojaus palveluille ilman, että se vaikuttaa tuotannon suorituskykyyn. Toiminnan jatkuvuus tulisi toteuttaa jatkuvalla varmistuksella perinteisen ajastettujen varmistuksien sijaan. Jatkuvalla datan replikoinnilla pystytään tarjoamaan palautuspisteitä sekuntien tarkkuudella (Recovery Point Objectives = RPOs), koska kaikki muutokset replikoidaan reaaliajassa suojattuun sijaintiin. [10, s. 3.]

Replikoidut muutokset tallennetaan päiväkirjaan (Journal History), mikä sallii palautumisen viimeisimpään replikoituun ajankohtaan sekä mahdollistaa sen, että käyttäjä voi sekuntien tarkkuudella valita halutun ajankohdan palauttamispisteeksi. Päiväkirjaa ylläpitää kohdesijainnissa Virtual Replication Appliance ja jokainen replikoitu virtuaalipalvelin saa oman päiväkirjansa. Muutaman sekunnin

välein luodaan palautuspiste (Checkpoint), millä varmistetaan kirjoituksien oikea järjestys sekä johdonmukainen palvelimien tila kirjoituksien ollessa samasta ajankohdasta.

Päiväkirjalle on mahdollista asettaa tallennustilan osalta pehmeitä ja kiinteitä rajoituksia. Pehmeä rajoitus pyrkii pitämään päiväkirjan tietyn koon rajoissa, mutta sen on myös mahdollista mennä tämän rajan yli. Kiinteän rajan tullessa vastaan alkaa Zerto poistamaan vanhimpia palautuspisteitä päiväkirjasta, kunnes päiväkirjaan mahdutaan kirjoittamaan uusimmat replikoitavalla palvelimella tapahtuneet muutokset. Tämä tarkoittaa sitä, että päiväkirjan määritetty pituus, kuten esimerkiksi viiden päivän aikana tapahtuneet muutokset, voi poiketa alun perin asetetusta pituudesta. Päiväkirjassa on päällä kompressointi, minkä voi nähdä päiväkirjan tiedoista prosentteina. Mikäli päiväkirjan datan tallennuksen kiinteä raja-arvo on 20 Gt, niin esimerkiksi 50 % kompressiolla voidaan kirjoittaa 40 Gt dataa. Päiväkirjaa voidaan ylläpitää kohdesijainnin tallennustilan rajoitteissa jopa 30 päivään asti, jolloin ylläpitäjälle jää kattavat vaihtoehdot palautuspisteen valintaan. Useamman päivän päiväkirjaan on syytä huomioida päiväkirjaan kirjoitettava datan muutosmäärä, joka on noin 10 % palvelimen alkuperäisestä koosta päivää kohden [19, s. 4]. Mikäli tallennustila kohteessa on täynnä (30 Gt tai vähemmän vapaata tilaa), päiväkirjan kirjoitus pysähtyy ja RPO kasvaa, koska Zerto ei kirjaa viimeisimpiä tapahtuneita muutoksia. Päiväkirjan historiaa ei kuitenkaan menetetä. Zerto jatkaa päiväkirjaan kirjoitusta vasta, kun tallennustilan ongelma kohteessa on korjattu. [19, s.1-3.]

Tarkkoja palautuspisteitä sekuntien tarkkuudella on tarve säilyttää vain muutamia päiviä ja niitä tarvitaan tyypillisesti tietokantojen korruptoitumisen, ransomwaren tai tiedostojen poiston takia. Mikäli tarve myöhemmältä ajankohdalta haettavaan dataan syntyy, sitä varten ei enää tarvita palautuspisteitä sekuntien tarkkuudella. Palautuspisteiden tarkkuutta on mahdollista vähentää, sillä tämänlaiselta aikaväliltä haettavaa dataa ei välttämättä tarvitse palauttaa nopeasti ja suurella tarkkuudella. Sekuntien tarkkuudella olevien palautuspisteiden syntyminen sallii kuitenkin sen, että jatkuva replikointi ja tarkat palautuspisteet voidaan

yhdistää jatkuvaan datan suojaukseen. Tämä mahdollistaa siirtymisen kokonaan pois tiettyyn ajankohtaan sidotusta kopioinnista, jota käytetään perinteisessä varmistusteknologiassa. [10, s. 3.]

Koska perinteinen varmuuskopiointi on sidottu tiettyyn ajankohtaan rajoittaa se palautuksen tarkkuutta, jolloin kaikki varmuuskopioinnin jälkeen kirjoitettu data menetetään varmistuksen näkökulmasta. Jatkuvalla datan suojauksella mahdollistetaan siis palaaminen mahdollisimman lähelle hetkeä ennen datan menetystä. Perinteinen ajastettu varmistus ei välttämättä edes tiedä menetetystä datasta mitään, mikäli se on luotu ja poistettu yhden varmistusikkunan välissä. [10, s. 3.]

Sovelluksia koskevissa tapauksissa sovellus on voitu erottaa useampaan eri komponenttiin eli virtuaalipalvelimeen, jolloin syntyy tarve suojata kaikki komponentit yhtenäisessä kokonaisuudessa. Sovelluksen kaikki virtuaalipalvelimet tulisi saada varmistettua samasta ajankohdasta ja palautettua samasta palautuspisteestä, minkä Zerto sallii palvelimien osalta yhdistämällä ne loogisiin kokonaisuuksiin. Palvelimien kannalta ei ole väliä missä ne sijaitsevat virtualisointiympäristössä, kun ne suojataan Zerton loogiseen kokonaisuuteen. Tällöin niiden tallennettujen kirjoituksien ajankohdat ovat samoja saman kokonaisuuden sisällä. [10, s. 6.]

3.2 Zerton komponentit

Zerto replikointia varten täytyy ohjelmiston pystyä liikennöimään replikoinnissa mukana olevien komponenttien kanssa. Virtualisointialustan tasolla Zerton täytyy päästä käsittelemään virtuaalipalvelimen omia komponentteja, mikä tapahtuu Virtual Replication Appliance (VRA):n ja ESXi alustapalvelimelle asennetun Zerton kernel moduulin (vib) avulla. VRA käskyttää kaikki tarvittavat toimenpiteet virtuaalipalvelimen komponenteille sekä alustalle, mikäli alustalla tapahtuu muutoksia. VRA:ailla on yleensä isommissa replikointiympäristöissä myös VRA Helper (VRAH) virtuaalipalvelimia, joihin liitetään vain levyjä. VRA lähettää tie-

dot tapahtuneista muutoksista eteenpäin Zerto Virtual Manager (ZVM) palvelimelle, joka replikoi lähde tai kohdepäässä tapahtuvia toimenpiteitä ja välittää myös tietoja muutoksista toiseen päähän. [13, s. 8-9.]

Laajemmassa palveluntarjoajan tai yrityksen omassa ympäristössä on käytössä keskitetty palvelualusta. Tämänlaisessa isossa ympäristössä tulee tällöin myös olla käytössä Zerto Cloud Manager (ZCM), joka on varsinainen palveluntarjoajan hallinta-alusta. [13, s. 8.] Täällä tehdään kaikki replikoinnin määritykset. Tällöin väliin tulee Zerto Cloud Connector, joka yhdistää yhden ympäristön johonkin toiseen keskitettyyn tai keskitettyihin replikointiympäristöihin. Zerto Cloud Connector (ZCC) toimii siis esimerkiksi asiakkaan ja palveluntarjoajan välillä. Kohdeympäristössä on vastaanottavan pään ZVM palvelin sekä VRA että VRAH komponentit tekemässä samoja toimenpiteitä replikoinnin toteuttamiseksi.

3.2.1 Zerto Cloud Manager

Zerto Cloud Manager (ZCM) on käytössä isoissa replikointiympäristöissä, missä on yksi tai useampi keskitetty replikointikohde. [13, s. 19.] ZCM:ään yhdistetään kaikki kohdeympäristöt sijainteina (Site), mikä onnistuu kyseiseen sijaintiin asennetun Zerto Virtual Managerin kautta. ZCM alusta toimii keskitettynä hallintaportaalina esimerkiksi palveluntarjoajalle, mistä ylläpitäjä voi määrittää vain tietyt kohteet asiakkaan käyttöön ja nähtäväksi palveluntarjoajan replikointialustalta. Tämän toiminnon avulla voidaan käytännössä tarjota useammalle asiakkaalle Disaster Recovery as a Service (DRaaS) palveluna ilman, että asiakkaat näkevät toisten asiakkaiden palvelimia tai tietoja.

Asiakkaille voidaan tarjota oma pääsy ZCM:n asiakasportaaliin (Self-service portal), jotta he voivat ylläpitäjästä riippumatta siirtää virtualisointialustan vikatilanteen sattuessa virtuaalipalvelimien kuormat kohdesijaintiin käyttöön. Ylläpitäjä näkee helposti yhdestä sijainnista kaikkien replikointien ajankohtaisen tilanteen ja voi tarvittaessa tehdä muutoksia asiakkaiden replikointien asetuksiin. ZCM hallinnassa voidaan tietyn asiakkaan (Organization) kohdalla määritellä

mihin sijaintiin tai sijainteihin replikointia on mahdollista toteuttaa [13, s. 40]. [13, s. 14.]

Tyypillisesti asiakkaalle näytetään replikointisijaintiin tuodut asiakkaan omat Distributed Port Group verkot, mikäli käytössä on vSphere Distributed Switch, tai perinteisen Port Groupin verkot. Näissä verkoissa liikenne erotellaan käyttämällä Virtual Local Area Networks (VLAN) tunnisteita, mikä tarkoittaa sitä, että verkkoteknisesti 12-bittinen VLAN ID (VID) merkitsee VLANin, johon kyseinen Ethernet -kehys kuuluu. Lisäksi näytetään resurssipooli (Resource Pool), joka määrittää mihin vCenter klusteriin replikoitavat virtuaalipalvelimet menevät sekä kuinka paljon prosessointi (CPU) sekä keskusmuisti (RAM) resursseja ne saavat käyttää, mikäli palvelimet nostetaan DR tilanteessa pystyyn (Failover) replikointisijainnissa. Replikointia varten tulee myös näyttää yksi tai useampi soveltuva Zerton tukema tallennusjärjestelmän looginen levy-yksikkö (Datastore).

ZCM asennetaan ainoastaan palveluntarjoajan päähän ja tyypillisesti näitä on vain yksi. ZCM asennus tapahtuu Windows käyttöjärjestelmälle ja sille annetaan resursseiksi minimivaatimuksina 1 prosessoriydin, 2 Gt keskusmuistia sekä 2 Gt vapaata kiintolevytilaa Zerton ohjelmistolle. Verkkoyhteyksien kannalta ZCM:n tulee voida liikennöidä palveluntarjoajan ZVM palvelimille portin 9080 kautta. Selaimen kautta käyttöliittymään pääsy tapahtuu käyttäjille portin 9989 kautta. [14.]

3.2.2 Zerto Cloud Connector

Zerto Cloud Connectoria (ZCC) käytetään ZCM kanssa hallituissa laajemmissa replikointiympäristöissä, joihin on tarkoitus tuoda sisään useammasta eri lähteestä replikoitavia virtuaalipalvelimia. Lähdepään sijainneissa on tyypillisesti käytössä erilaisia verkkoja, jotka täytyy saada reititettyä erikseen kohdepäähän ilman risteävyyttä muiden replikointilähteiden kanssa. ZCC käytännössä yhdistää kohdepäähän asiakkaan lähdepään replikointiverkon ja se säilyy erillään muista kohdepään replikointiverkoista. Palveluntarjoajan tapauksessa heidän omat verkkonsa kohdepäässä eivät ole suoraan yhteydessä asiakkaan omiin

verkkoihin ja ZCC reitittää replikointiin liittyvät oleelliset yhteydet sijaintien välillä. [13, s. 16]

Zerto Cloud Connector asennetaan palveluntarjoajan replikointikohteeseen palveluntarjoajan toimesta ja sille määritetään kaksi Ethernet -liitäntää, joista toinen saa IP-osoitteen asiakkaan omaan verkkoon ja toinen palveluntarjoajan Zerto verkkoon. [12.] Kun palveluntarjoajan ja asiakkaan Zerto Virtual Manager (ZVM) komponentit yhdistetään, ZCC:lle luodaan automaattisesti reititystä varten staattiset reitit tietyille porteille. Nämä portit ovat käytössä Zertoa varten. ZCC osalta yhteyksien tulee toimia porttien 9071 ja 9081 kautta kummankin pään ZVM järjestelmiin sekä porttien 4007 ja 4008 kautta kummankin ympäristön VRA komponenteille [14]. Käytännössä ZCC toimii välissä pelkästään yhteyksien välittäjänä (Proxy). Asiakkaan näkökulmasta katsottuna, asiakkaan ZVM yhdistetään ZCC:n Ethernet-liitäntään, joka on asiakkaan omassa verkossa. Näin ollen asiakas ei koskaan saa tietoonsa palveluntarjoajan käytössä olevaa Zerto verkkoa. Mikäli replikoinnissa tapahtuu virheitä, viitteet voivat viitata kohteen VRA:han, mutta tämä voi todellisuudessa myös olla välissä oleva ZCC komponentti. [13, s. 16.]

3.2.3 Zerto Virtual Manager

Zerto Virtual Manager (ZVM) komponentti käsittää sisällään Zerton kaikki replikoinnin hallintaan liittyvät toimenpiteet ja toimii keskipisteenä replikoinnissa ympäristöjen välillä. Jokainen virtualisointialustan ympäristö tarvitsee oman ZVM palvelimen, koska sen kautta määritetään yhteydet virtualisointialustaan ja saatavilla oleviin komponentteihin. ZVM noutaa vCenterin kautta tiedot virtuaalipalvelimista, kiintolevyistä, verkkokorteista, alustapalvelimista sekä muista tarvittavista virtuaalipalvelimien komponenteista. ZVM palvelin ilmoittaa myös kaikki virheet mitä replikoinnissa tai replikointiin liittyvissä komponenteissa ilmenee. Tämän kautta suoritetaan myös ympäristön replikointiin liittyvien komponenttien päivitykset. [10, s. 5.]

ZVM asennetaan Windows Server palvelimelle, mikä vaatii minimissään 2 prosessoriydintä sekä 4 Gt keskusmuistia ja 20 Gt kiintolevytilaa. ZVM toimii Windows käyttöjärjestelmässä tavallisena Windows palveluna (service). ZVM:n Ethernet-liitännän yhteydet tulee toimia replikoinnissa mukana olevan sijainnin vCenter hallintaan sekä ESXi alustapalvelimien hallintaan porttien 443, 80 ja 22 kautta [14]. ZVM asennuksessa on mahdollista käyttää ulkopuolista SQL.tietokantaa, kuten Microsoft SQL, tai sisäänrakennettua SQL-tietokantaa. Palveluntarjoajan päässä ZVM yhdistetään lisensointia varten ZCM palvelimelle ja asiakkaiden päässä yhteydet kulkeutuvat palveluntarjoajalle asennetun ZCC komponentin kautta.

Jokaiselle mukana olevalle alustapalvelimelle asennetaan ZVM:n kautta Virtual Replication Appliance (VRA) komponentti. Zerto Virtual Managerin kautta määritetään lähdepäässä, mitkä alustapalvelimet otetaan mukaan replikointiin. Käytännössä mukaan otetuilta alustapalvelimilta sallitaan virtuaalipalvelimien replikoinnit. Virtualisointialustan liikutettavuuden hyötyjä ei myöskään menetetä replikoinnissa, kun jokaiselle tarvittavalle alustapalvelimelle on asennettu VRA komponentti. ZVM valvoo virtualisointialustassa tapahtuvia muutoksia ja pystyy myös reagoimaan niihin. Virtuaalipalvelimen alustapalvelimen sekä tallennustilan voi vaihtaa joko ZVM:n hallinnan kautta tai perinteisen vCenterin vMotion toimenpiteen kautta. Mikäli muutos tehdään vMotionin kautta, niin Zerto tunnistaa replikoitavan virtuaalipalvelimen vaihtaneen alustapalvelinta tai tallennustilaa [10, s. 6]. Tällöin virtuaalipalvelimen kanssa samalla alustapalvelimella oleva VRA johon virtuaalipalvelin on siirtymässä jatkaa replikointia ilman katkoja.

On myös mahdollista, että alustapalvelimella suoritetaan huoltotoimenpiteitä, jolloin ylläpitäjä voi asettaa jonkin alustapalvelimen huoltotilaan (Maintenance Mode). Ylläpitäjä tyhjentää huoltotilaa varten alustapalvelimen kaikista virtuaalipalvelimista ja Zerto tunnistaa vCenterin sekä alustapalvelimen yhteytensä kautta tapahtuvan toimenpiteen. Tällöin tapahtuva vMotion toimenpide siirtää kaikki tuotannossa olevat palvelimet toiselle alustalle eikä replikoinnissa tapahdu katkoksia. Zerto on asettanut omalle VRA komponentilleen tiettyjä ehtoja

eivätkä ne saa siirtyä alustapalvelimelta toiselle. Jos näin tapahtuu Zerto sammuttaa älykkäästi VRA komponentin, kunhan kaikkien palvelimien replikointi jatkuu toisilla VRA komponenteilla. Ylläpitäjä pystyy jatkamaan alustapalvelimen huoltotoimenpiteitä, kun Zerton VRA komponentti on sammunut automatiikan avulla, ja alustapalvelin on tyhjä päällä olevista virtuaalipalvelimista.

Replikointiin lisättävät virtuaalipalvelimet konfiguroidaan ZVM selainhallinnan kautta mukaan virtuaaliseen suojausryhmään (Virtual Protection Group = VPG). VPG:hen voi lisätä mukaan yhden tai useamman virtuaalipalvelimen samanaikaisesti. Kun halutaan esimerkiksi suojella jonkin tietyn applikaation palvelimia, niin on järkevää laittaa ne samaan ryhmään replikoitumaan. Mikäli VPG:ssä on useampi palvelin, siihen voi määrittää palvelimien käynnistysjärjestyksen, millä pyritään huomioimaan mitä palveluita tulee olla ensin käynnissä muiden palveluiden toimintaan saamiseksi katastrofista palautumisen yhteydessä. Katastrofitilanteessa kaikki sovellukseen liittyvät palvelimet käynnistyvät tällöin samasta palautuspisteestä. [10, s. 6.]

Replikointiin lisätyt palvelimet on syytä myös testata etukäteen ja tätä varten VPG:tä luotaessa määritetään myös erillinen testausverkko virtuaalipalvelimelle. Kun palvelin nostetaan ylös kohdeympäristössä testin aikana, niin voidaan varmistaa palvelimen käynnistyvän normaalisti ilman ongelmia ja se on tällöin liitettynä testiverkkoon, mistä ei aiheudu häiriötä tuotantoon. Tyypillisesti testiverkkoa ei esimerkiksi viedä edes lähiverkossa oleville kytkimille, eli se on vain kohdeympäristön virtualisointialustan sisäinen verkko ja muut siihen liitetyt palvelimet pystyvät yhä juttelemaan toisilleen samassa aliverkossa.

3.2.4 Virtual Replication Appliance

Virtual Replication Appliance (VRA) on ZVM:n asentama virtuaalipalvelin, joka on alustapalvelinkohtainen. VRA:ta käytetään suojaamaan alustalla olevia virtuaalipalvelimia, kun ne on lisätty mukaan replikointiin. Kun VRA asennetaan alustapalvelimelle, Zerto asentaa oman kernel-moduulinsa käyttöön alustapal-

velimen käyttöjärjestelmän sisälle. Tällä Zerton ajurilla VRA pystyy älykkäästi lukemaan virtuaalipalvelimeen tehdyt muutokset reaaliajassa, ottamaan niistä kopion ja välittämään samat muutokset replikointiin. Alkuperäinen virtuaalipalvelimen muutos menee yhä sen omalle kiintolevylle levyjärjestelmään. Zerton oman ajurin avulla pystytään siis kopioimaan talteen virtuaalipalvelimelle tapahtuvia muutoksia reaaliajassa ja replikoimaan ne eteenpäin ilman, että käytön kannalta tarvitsee tyytyä hitaampiin virtualisointiympäristön näköistiedostoihin (snapshot). Näköistiedostojen käytön ongelmana on, että talteen saadaan tietty kohta palvelimen tilanteesta, mutta sen varmistamisen aikana kaikki muut kyseisestä ajankohdasta eteenpäin tapahtuneet muutokset eivät tallennu varmistukseen. Vasta seuraavassa varmistuksessa tallennetaan palvelimen seuraava tilanne. Zerto VRA:n jatkuvalla replikoinnilla meillä on kaikki muutokset koko ajan tallessa sen päiväkirjassa.

VMware ympäristössä on rajoitettu SCSI kontrollerien lukumäärä, joka on neljä virtuaalipalvelinta kohden. Tämän lisäksi jokaiselle kontrollerille voi määritellä maksimissaan 15 kohdetta, mikä tarkoittaa tässä tapauksessa kiintolevytiedostoja (.vmdk). Tämä rajoittaa yhdelle virtuaalipalvelimelle maksimissaan 60 kiintolevyä. Sama rajoitus koskettaa kaikkia virtuaalipalvelimia, myös VRA:ta, ja tätä varten Zerto käyttää Virtual Replication Application Helpers (VRA-H) virtuaalipalvelimia. VRA-H komponentit toimivat pelkästään kiintolevyjen liitosjärjestelmänä eikä niillä ole käyttöjärjestelmää, IP-osoitteita tai juurikaan mitään resursseja. Zerto hoitaa itse VRA-H palvelimien ylläpitämisen ja luo sellaisen tarvittaessa, mikäli lähestytään 60 levyn raja-arvoa. [10, s. 6.]

4 Disaster Recovery toteutus ja testaus

Tässä luvussa käydään läpi opinnäytetyötä varten suoritettu Disaster Recoveryn toteutus ja testaus sekä sen tulokset. Disaster Recovery toteutuksessa käytettiin hyödyksi VMwaren vSphere ohjelmistopohjaista virtualisointiympäristöä. Toteutuksessa on kaksi erillään olevaa virtualisointiympäristöä, jotka sijaitsevat sekä verkon että fyysisen sijaintinsa kannalta eri paikoissa, eivätkä pysty suo-

raan juttelemaan keskenään. Toinen sijainti on tuotantoympäristö, missä pääasialliset virtuaalipalvelimet sijaitsevat ja toimivat. Toinen sijainti on tätä toteutusta varten luotu DR-ympäristö. DR-ympäristöön replikoidaan tärkeät virtuaalipalvelimet, jotka ovat tuotannolle kriittisiä. Jos tuotantoympäristössä tapahtuu ongelmatilanne, on replikoidut palvelimet tarve saada takaisin toimintaan nopeasti. Testissä on käytetty yksittäistä Windows Server palvelinta, DC01-Test, jolla on yhteys ulkoverkkoon.

4.1 Testauksen virtualisointiympäristöt

Virtualisointiympäristön toteutusta varten käytössä on kaksi Dell T620 tornipalvelinta. Raudan päälle asennetaan VMware ESXi 7.0u3c käyttöjärjestelmä, joka toimii virtualisointialustana. Virtualisointialustan rinnalla on ympäristöjen Juniper vSRX palomuurit, jotka tarjoavat palomuurisuojauksen ja yhteydet virtualisointiympäristöön. Palomuurien välille luodaan IPsec tunneli. Palomuurien välistä siirtyy IPsec tunnelia pitkin Zerto Virtual Replication liikenne eli näiden kahden eri järjestelmän verkot yhdistetään tämän avulla toisiinsa. Verkoilla on silti erilliset yhteydet julkiverkkoon oman sijaintinsa palomuurin kautta. Zerto Virtual Replication toiminnallisuutta varten asennetaan VMware vSphere vCenter virtualisointympäristön hallintapalvelin kumpaankiin virtualisointialustaan.

Taulukko 1. Virtualisointiympäristön komponentit sekä niiden verkot, IP-osoitteet ja aliverkon peite.

Laite / Tuote	**IP-osoite tai Verkko / verkon peite**
Site-A aliverkko	**10.10.10.0/24**
Site-A-ESXi1	10.10.10.5/24
vSRX-Site-A sisäinen	10.10.10.1/24
vSRX-Site-A ulkoinen	193.164.25.91/32
vSRX-Site-A IPsec liitäntä	10.0.250.10/24

Site-A-VCSA7	10.10.10.10/24
Site-A-NFS/DNS	10.10.10.2/24
Site-A-ZVM	10.10.10.20/24
Site-A-ZVRA	10.10.10.21/24
DC01-Test	10.10.10.50 -> 10.10.20.50
Site-B aliverkko	**10.10.20.0/24**
Site-B-ESXi1	10.10.20.5/24
vSRX-Site-B sisäinen	10.10.20.1/24
vSRX-Site-B ulkoinen	185.188.34.26/32
vSRX-Site-B IPsec liitäntä	10.0.250.20/24
Site-B-DNS	10.10.20.2/24
Site-B-VCSA7	10.10.20.10/24
Site-B-ZVM	10.10.20.20/24
Site-B-ZVRA	10.10.20.21/24

Toteutuksessa on Site-A sekä Site-B ympäristöt, joilla on niiden virtualisointialustaan liitetyillä komponenteilla omat aliverkot. Palomuurit (Juniper vSRX) toimivat omissa aliverkoissa yhdyskäytävänä (Site-A = 10.10.10.1 ja Site-B = 10.10.20.1) sekä jakavat liikenteet ulospäin ulkoisen verkon liitäntöjen kautta (Site-A = 193.164.25.91 ja Site-B = 185.188.34.26). Virtuaalipalvelimet toimivat samassa aliverkossa kuin ympäristöjen muut järjestelmät (Site-A = 10.10.10.0/24 ja Site-B = 10.10.20.0/24).

4.1.1 Juniper vSRX

Virtualisointiympäristön verkotuksia varten käytettiin Juniper vSRX 3.0 palomuureja. Kummallakin ympäristöllä on oma vSRX palomuuri. Palomuurit saavat Julkiverkoista omat IP-osoitteensa (Site-A = 193.164.25.91 ja Site-B

185.188.34.26) ja palomuureille lisätään toinen liitäntä, joka yhdistetään virtualisointialustojen sisäverkkoihin (Site-A = 10.10.10.1/24 ja Site-B = 10.10.20.1/24). Ympäristöjen verkkoyhteyksien yhdistämiseen luodaan IPsec tunneli, ettei virtualisointialustojen liikenne kulkisi salaamattomana julkiverkon yli [15]. Zerto Virtual Replication komponenttien paketit eri ympäristöistä kulkevat tällöin salattuna tunnelia pitkin.

vSRX-Site-A

Konfiguroidaan IPsec tunnelia varten oma st0.1 liitin ja määritetään sille IP-osoite sekä sallitaan IKE-protokollat.

set interfaces st0 unit 1 family inet address 10.0.250.10/24
set security zones security-zone untrust host-inbound-traffic system-services ike
set security zones security-zone untrust interfaces st0.1

Määritetään IKE kättelyn asetukset ja politiikat. Tärkeää huomioida mihin osoitteeseen yhteys muodostetaan ja minkä liittimen kautta.

set security ike proposal ike-phase1-proposalA authentication-method pre-shared-keys
set security ike proposal ike-phase1-proposalA dh-group group2
set security ike proposal ike-phase1-proposalA authentication-algorithm sha-256
set security ike proposal ike-phase1-proposalA encryption-algorithm aes-256-cbc
set security ike proposal ike-phase1-proposalA lifetime-seconds 1800
set security ike policy ike-phase1-policyA mode aggressive
set security ike policy ike-phase1-policyA proposals ike-phase1-proposalA
set security ike policy ike-phase1-policyA pre-shared-key ascii-text SecuredVPN-Tunnel
set security ike gateway gw-siteB ike-policy ike-phase1-policyA
set security ike gateway gw-siteB address 185.188.34.26
set security ike gateway gw-siteB external-interface ge-0/0/0.0

Määritetään IPsec tunnelin muodostamisen määritykset ja käyttämään aikaisemmin luotuja IKE määrityksiä.

set security IPsec proposal IPsec-proposalA protocol esp
set security IPsec proposal IPsec-proposalA authentication-algorithm hmac-sha1-96
set security IPsec proposal IPsec-proposalA encryption-algorithm aes-256-cbc
set security IPsec proposal IPsec-proposalA lifetime-seconds 7200
set security IPsec proposal IPsec-proposalA lifetime-kilobytes 102400000
set security IPsec policy IPsec-policy-siteB proposals IPsec-proposalA
set security IPsec vpn ike-vpn-siteB bind-interface st0.1
set security IPsec vpn ike-vpn-siteB ike gateway gw-siteB
set security IPsec vpn ike-vpn-siteB ike IPsec-policy IPsec-policy-siteB
set security IPsec vpn ike-vpn-siteB establish-tunnels immediately

Määritetään reititys toimimaan vSRX-Site-B takana olevaan verkkoon tämän IPsec tunnelin liitintä pitkin.
set routing-options static route 10.10.20.0/24 next-hop st0.1

vSRX-Site-B
Konfiguroidaan IPsec tunnelia varten oma st0.1 liitin ja määritetään sille IP-osoite sekä sallitaan IKE-protokollat.
set interfaces st0 unit 1 family inet address 10.0.250.20/24
set security zones security-zone untrust host-inbound-traffic system-services ike
set security zones security-zone untrust interfaces st0.1

Määritetään IKE kättelyn asetukset ja politiikat. Tärkeää huomioida mihin osoitteeseen yhteys muodostetaan ja minkä liittimen kautta.
set security ike proposal ike-phase1-proposalA authentication-method pre-shared-keys
set security ike proposal ike-phase1-proposalA dh-group group2
set security ike proposal ike-phase1-proposalA authentication-algorithm sha-256
set security ike proposal ike-phase1-proposalA encryption-algorithm aes-256-cbc
set security ike proposal ike-phase1-proposalA lifetime-seconds 1800
set security ike policy ike-phase1-policyA mode aggressive

set security ike policy ike-phase1-policyA proposals ike-phase1-proposalA
set security ike policy ike-phase1-policyA pre-shared-key ascii-text SecuredVPN-Tunnel
set security ike gateway gw-siteA ike-policy ike-phase1-policyA
set security ike gateway gw-siteA address 193.164.25.91
set security ike gateway gw-siteA external-interface ge-0/0/0.0

Määritetään IPsec tunnelin muodostamisen määritykset ja käyttämään aikaisemmin luotuja IKE määrityksiä.
set security IPsec proposal IPsec-proposalA protocol esp
set security IPsec proposal IPsec-proposalA authentication-algorithm hmac-sha1-96
set security IPsec proposal IPsec-proposalA encryption-algorithm aes-256-cbc
set security IPsec policy IPsec-policy-siteB proposals IPsec-proposalA
set security IPsec vpn ike-vpn-siteB bind-interface st0.1
set security IPsec vpn ike-vpn-siteB ike gateway gw-siteB
set security IPsec vpn ike-vpn-siteB ike IPsec-policy IPsec-policy-siteB
set security IPsec vpn ike-vpn-siteB establish-tunnels immediately

Määritetään reititys toimimaan vSRX-Site-A takana olevaan verkkoon tämän IPsec tunnelin liitintä pitkin.
set routing-options static route 10.10.10.0/24 next-hop st0.1

Konfiguraatioiden jälkeen tarkistetaan, että palomuurien välinen IPsec tunneli on noussut pystyyn.
zmanager> show security ike security-associations
Index State Initiator cookie Responder cookie Mode Remote Address
2154952 UP 32b58715e0be2682 698e441ae863b39f Aggressive 193.164.25.91

zmanager> show security IPsec security-associations
Total active tunnels: 1 Total IPsec sas: 1
ID Algorithm SPI Life:sec/kb Mon lsys Port Gateway

<131073 ESP:aes-cbc-256/sha1 94adf824 3560/ 102400000 - root 500 193.164.25.91
>131073 ESP:aes-cbc-256/sha1 5a0086d2 3560/ 102400000 - root 500 193.164.25.91

4.1.2 VMware ESXi 7.0u3c

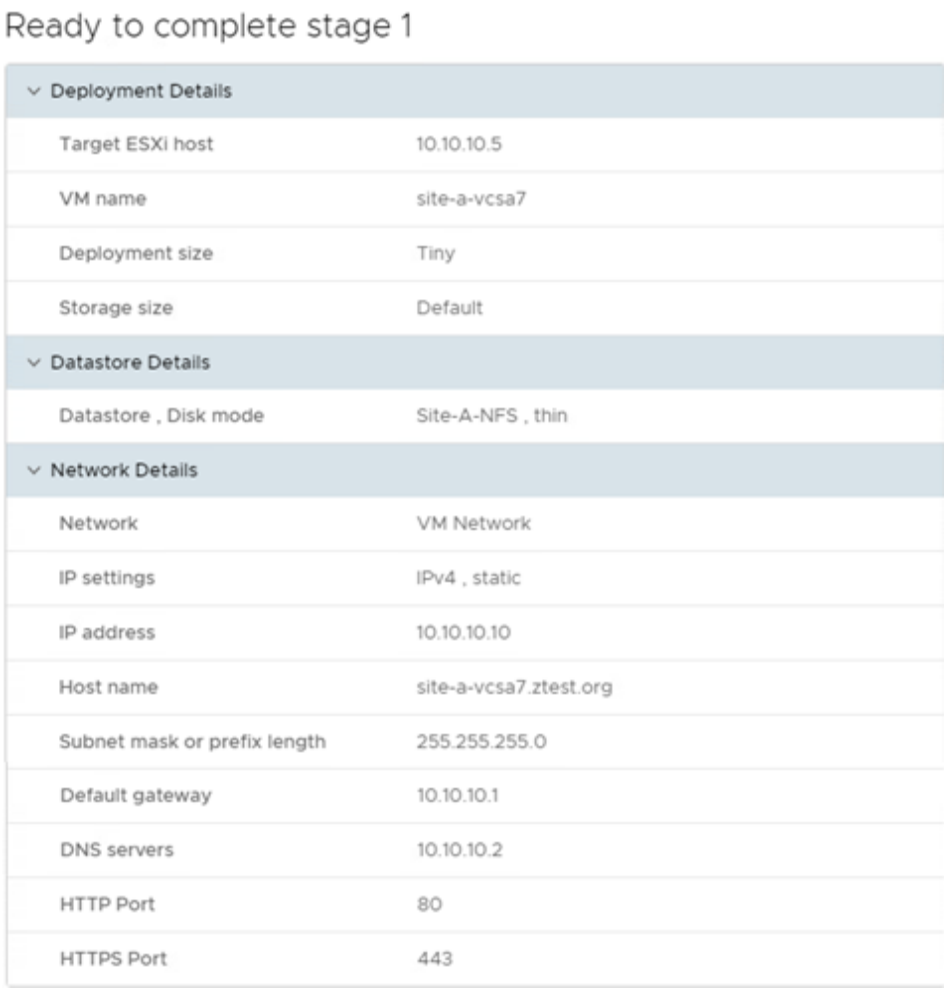
VMwaren ESXi käyttöjärjestelmä asennettiin 16 Gt USB-muistikorteille. Asennusvaiheessa ohjelma varoitti, ettei tämänlaista tallennusmediaa suositella jatkossa käytettävän vaan VMwaren suositus on asentaa ESXi käyttöjärjestelmä kiinteälle tallennusmedialle, joka kestää enemmän luku- sekä kirjoitusoperaatioita. Virtualisointialustan palvelin asennettiin IP-osoitteilla 10.10.10.5 Site-A-ESXi1 osalta ja 10.10.20.5 Site-B-ESXi1 osalta.

Virtualisointialustan virtuaalipalvelimia varten Site-A:lla on erillinen Windows –palvelin jakamassa Site-A-NFS, IP-osoite 10.10.10.2, tallennustilaa NFS protokollan kautta. Tällä samalla palvelimella toimivat kyseisen ympäristön DNS-palvelut, jotka vCenter vaatii toimiakseen. DNS:ään lisätään merkinnät Forward Lookup Zone alla olevaan “zorg.test” DNS-zoneen, missä on kerrottu Host A-tietueella “site-a-vcsa7.ztest.org” löytyvän IP-osoitteesta 10.10.10.10, sekä että Reverse Lookup Zonessa on alue 10.10.10.in-addr.arpa ja vastaavasti vCenterin PTR-tietue. Site-B osalta käytössä on paikallinen 1 Tt kiintolevy, jota käytetään tarjoamaan tallennustilaa ympäristölle. Site-B:llä luotiin oma DNS-palvelin, mihin toteutettiin vastaavat DNS tietueet kuin Site-A:lla, mutta käytössä on eri aliverkko (10.10.20.0/24) vaikkakin sama DNS-suffix.

4.1.3 VMware vSphere vCenter 7.0u3c

VMwaren vCenter palvelin asennettiin Site-A/B-ESXi1 virtualisointialustapalvelimen sisälle. Asennus suoritetaan käynnistämällä .ISO mediassa oleva Installer.exe ja määritetään ympäristöjen omat vastaavat konfiguraatiot. Asennus tapahtuu kahdessa vaiheessa; Stage 1 määritetään vCenterin yleiset virtualisointiympäristöön tuontiin liittyvät asetukset sekä Stage 2 määrityksissä pystyssä on

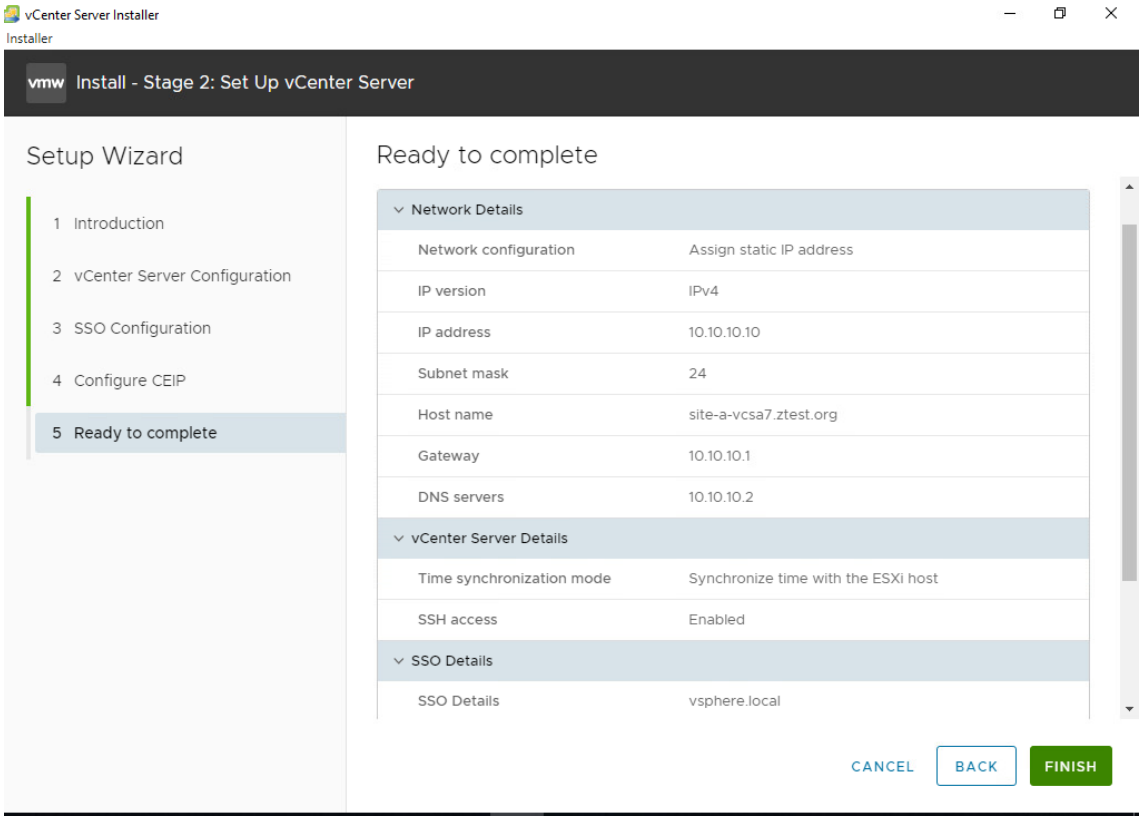
virtuaalipalvelin, mihin määritetään vCenterin loput määritykset, kuten Network Time Policy –palvelin (NTP) ja hallinnan Single Sign-On (SSO) toimialue ja hallintatunnus. Tärkeää on siis huomioida, että vCenterin asennuksessa tyypillisesti tarvitaan vCenterin Fully Qualified Domain Name (FQDN) tietue DNS-palvelimella ja toimiva NTP määritys. Asennus epäonnistuu, mikäli edellä mainitut asetukset eivät ole kunnossa ennen asennusta. VMwaren vCenter ja ESXi välisien komponenttien tulee olla samassa ajassa, jotta ne tietävät järjestelmässä tapahtuvien muutoksien tapahtuvan samaan aikaan [22]. VMwaren vCenter varoittaa myöhemmin NTP määrityksistä, mikäli sen ja alustapalvelimien välillä on merkittäviä kellonajan eroja.



Kuva 1. Tätä testausta varten määritettiin vCenterin kooksi Tiny, jonka vaatimuksina on 2 CPU, 12 GB RAM ja 580 GB vapaana olevaa tallennustilaa levyjärjestelmässä. Asennuksessa valittiin Site-A-ESXi1 osalta tallennustilaksi Site-A-NFS tallennustila, verkoksi VM Network, määritettiin vCenterin oma IP-osoite, verkon

oletusyhdyskäytävä sekä DNS-palvelimen osoite. Lopussa näkyvät portit, joista vCenterin hallintaan voidaan jutella.

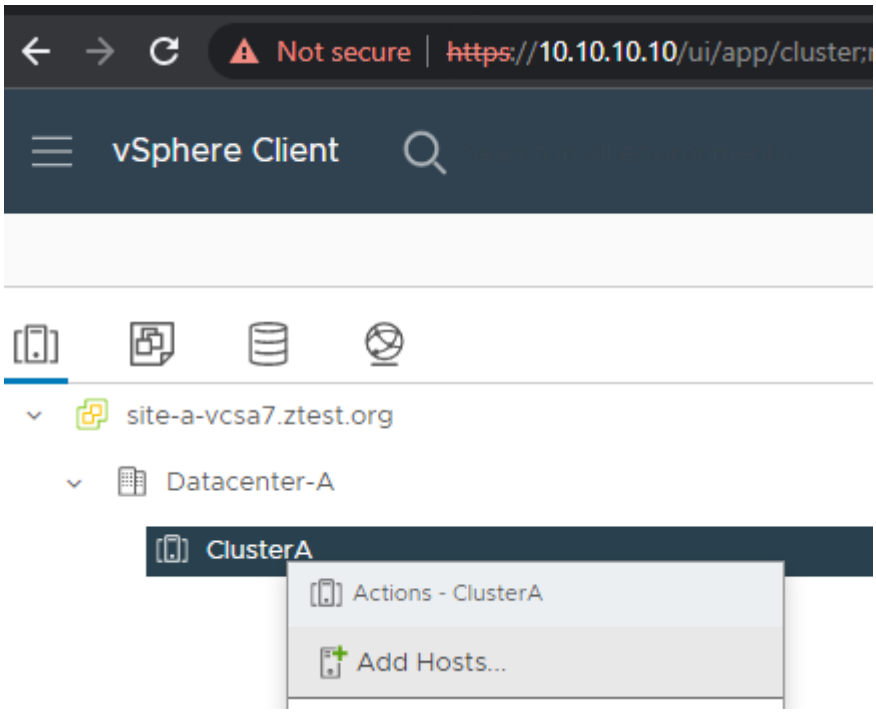
Stage 2 määrityksissä määritettiin ajan synkronointi ESXi hostilta, mutta vaihtoehtona on myös määrittää mikä tahansa julkinen NTP-palvelu, mikäli yhteydet toimivat ulkoverkkoon virtualisointiympäristöstä. Useamman alustapalvelimen ympäristössä on tärkeää, että käytetään keskitettyä ajan lähdettä NTP:n kautta. Hallinnan osalta sisäänkirjautumiseen määritettiin oletusasetukset, eli käytännössä toimialueeksi vCenterin sisäinen vsphere.local ja hallintatunnukseksi Administrator.



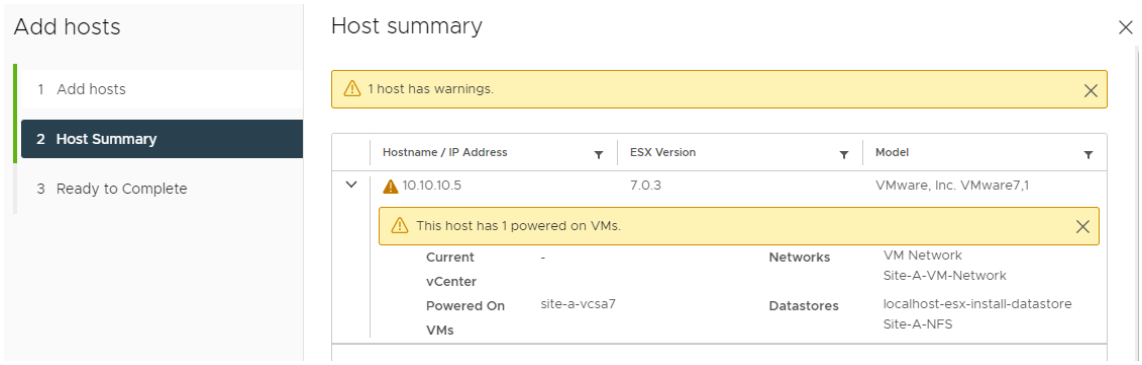
Kuva 2. vCenterin asennuksen loput määritykset koostettuna.

Asennuksen päätteeksi kirjauduttiin varsinaiseen vCenterin selainhallintaan osoitteessa https://10.10.10.10 tai vastaavasti Site-B:llä https://10.10.20.10. Täällä lisättiin vCenterin Hosts and Clusters valikossa uusi Datacenter sekä sen alla Cluster, johon liitettiin Site-A/B-ESXi1 alustapalvelin. Tämä käytännössä li-

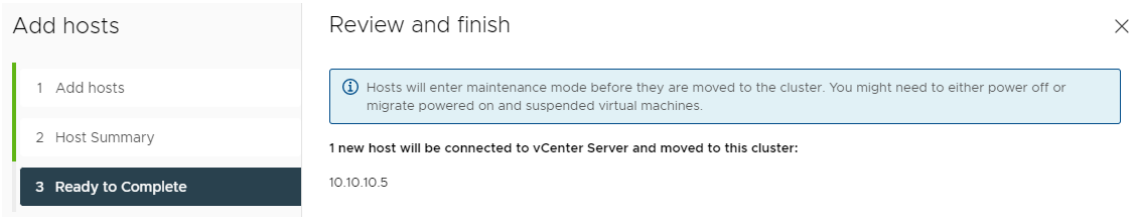
sää virtualisointialustan hallittavaksi vCenterin alle ja mahdollistaa Zerton määrittelemistä käyttöön. Zerton vaatimuksena replikointiin on VMware vCenter hallintapalvelin, minkä alle se luo replikointiin tarvittavat oikeudet.



Kuva 3. Site-A vCenterin alle on lisätty Datacenter, Cluster ja liitetään ESXi valinnasta Add Host.

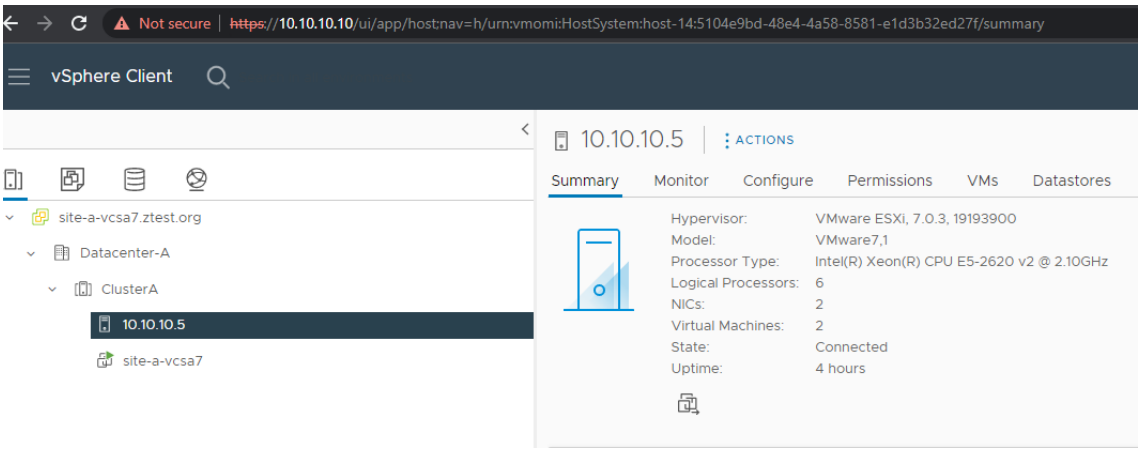


Kuva 4. Lisäyksessä huomautetaan päällä olevista virtuaalipalvelimista. Mikäli ainoa palvelin on vCenter itse, huomautuksesta ei tarvitse välittää.



Kuva 5. Mikäli virtualisointialustassa on päällä muita kuin vCenter Appliance -palvelin, ne sammutetaan. Tämä on hyvä huomioida lisäystä tehdessä.

Tämän jälkeen virtualisointiympäristö on asennettuna ja sen sisällä on VMware ESXi 7.0u3c versiolla oleva virtualisointialusta sekä hallinta-alusta VMware vCenter 7.0u3c versiolla.



Kuva 6. Virtualisointialusta Site-A on valmis virtuaalipalvelimille sekä Zerton komponenteille.

4.2 Zerto Virtual Replication toteutus ja testaus

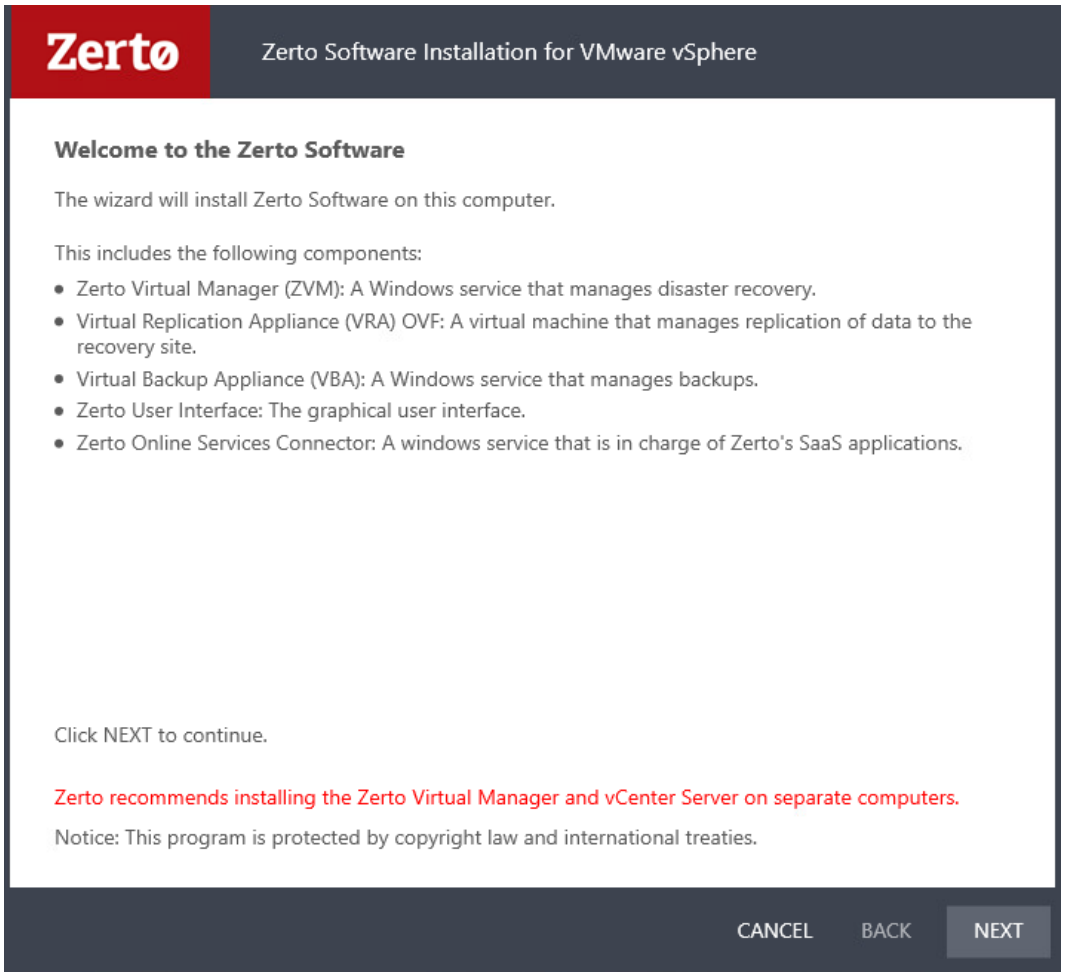
Zerto Virtual Replication komponentit asennettiin Site-A ja Site-B virtualisointialustojen sisälle. Tätä ennen täytyy käytössä olla ympäristöjen verkot ja näiden väliset verkkoyhteydet tulee olla toiminnassa. Myös varsinainen virtualisointiympäristö tulee olla valmiiksi luotuna.

Molempiin ympäristöihin asennettiin tavallinen Windows Server 2019 virtuaalipalvelin, jonka sisälle asennetaan Zerto Virtual Manager komponentit sekä sen Windows palvelut. [12.] Isommassa palveluntarjoajan ympäristössä, mikäli käytössä on keskitetty replikointikohde, asennettuna tulisi olla myös Zerto Cloud

Manager sekä Zerto Cloud Connector, mutta tämänlaisessa pienessä testiympäristössä niitä ei tarvita. Vastaavasti mikäli tarkoitus on replikoida vain kahden ympäristön välillä, eikä tämä koskaan laajene muihin ympäristöihin, replikoinnissa pärjätään vain kahdella Zerto Virtual Manager palvelimella, jotka juttelevat suoraan toisilleen.

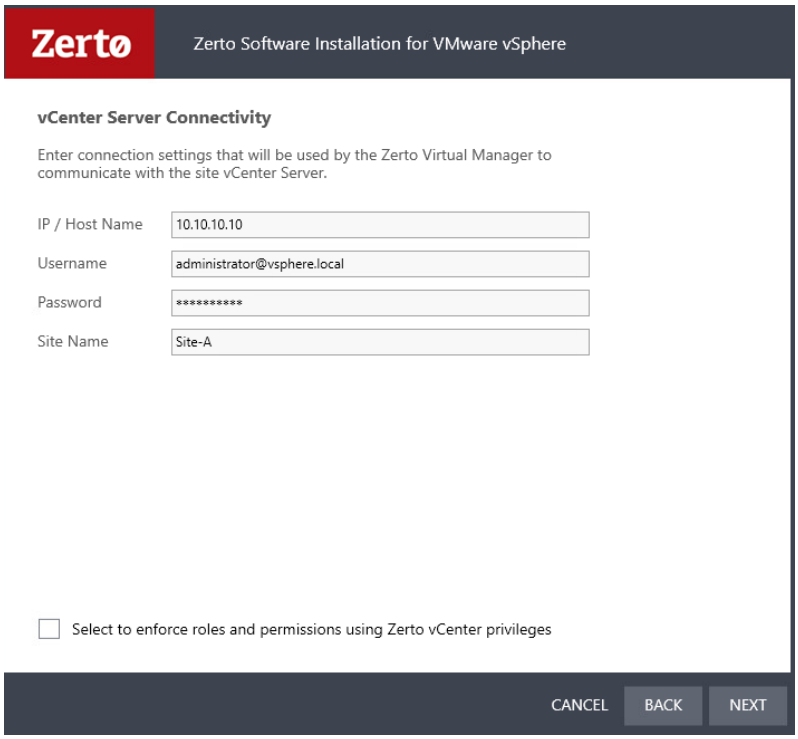
4.2.1 Zerto Virtual Manager ja Virtual Replication Appliance

ZVM asennus tehtiin Site-A\B-ZVM palvelimelle, jossa on käyttöjärjestelmänä Windows Server 2019.

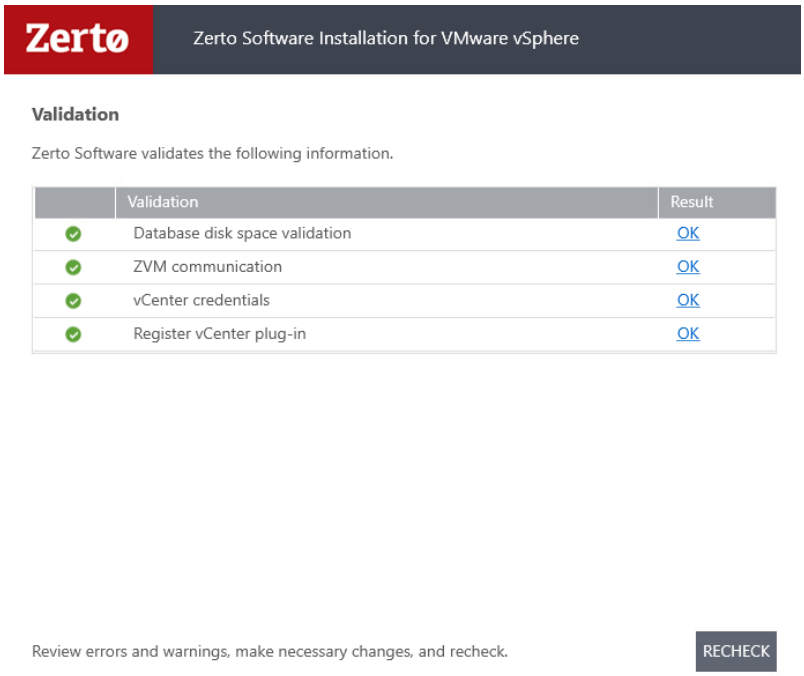


Kuva 7. Zerto Virtual Manager asennus käynnissä ja lueteltuna mitä komponentteja ja toiminnallisuuksia ZVM tarjoaa.

Asennuksen aikana ZVM komponenttien asennus vaatii kyseiseltä virtuaalipalvelimelta 4 Gt tallennustilaa. ZVM asennus tehtiin testin tapauksessa Express Installation vaihtoehdolla, mutta toisena vaihtoehtona on mahdollisuus käyttää Custom Installation vaihtoehtoa. Mukautetun asennuksen kautta on mahdollista määritellä esimerkiksi jokin ulkoinen SQL palvelin, kuten Microsoftin SQL palvelin, johon Zerton tietokanta asennetaan [21].

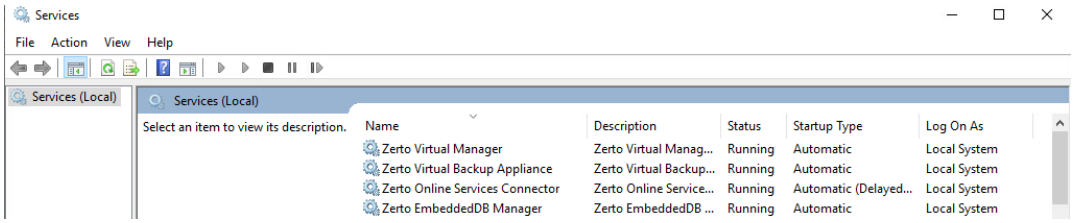


Kuva 8. ZVM asennuksessa määritetään vCenterin IP-osoite sekä tunnukset vCenter järjestelmään. Lisäksi määritellään millä nimellä tämä ympäristö näkyy Zerton hallinnassa.



Kuva 9. ZVM asennus validoi asennukselle olevan tarpeeksi levytilaa, yhteyden toimivan vCenteriin ja vCenter liitännäisen asennuksen onnistuvan määritetyillä tunnuksilla.

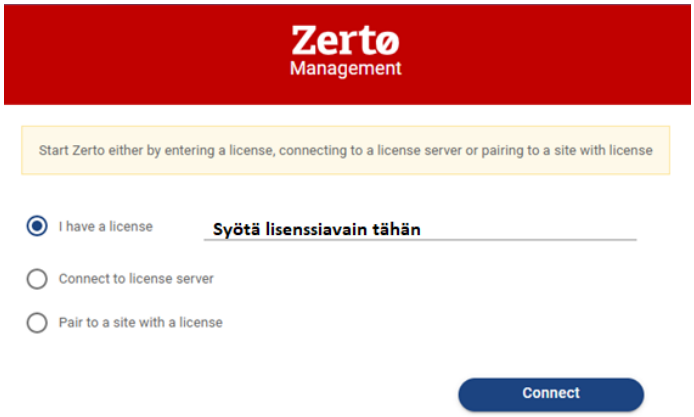
Asennuksen aikana Express -valinnalla Zerto asentaa paikallisesti kyseiselle palvelimelle Microsoft SQL Server 2016 Express tietokannan käyttöön. Tietokanta asentuu kummankin pään ZVM palvelimelle. Asennuksen lopuksi Windowsin Services -työkalusta voidaan tarkistaa Zerton palveluiden olevan päällä.



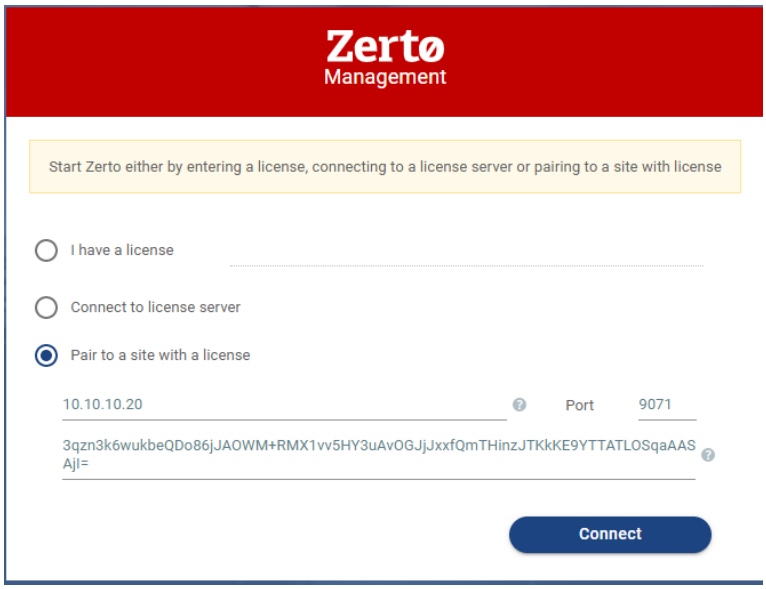
Kuva 10. ZVM palvelut (services) palvelimella asennuksen jälkeen.

Tämän jälkeen Zerton ZVM hallinta vastaa selaimella osoitteessa https://10.10.10.20:9669 tai vastaavasti Site-B:llä https://10.10.20.20:9669. Asennuksen lopuksi on syytä huomioida HTTPS yhteyden lisäksi portti, jonka kautta hallintasivusto vastaa. Zerto hallintaan kirjaudutaan sisään VMware vSphere vCenterin SSO -toimialueen tunnuksilla, jotka oli testin tapauksessa

määritetty vsphere.local toimialueelle, ja koko tunnus on muodossa administrator@vsphere.local.



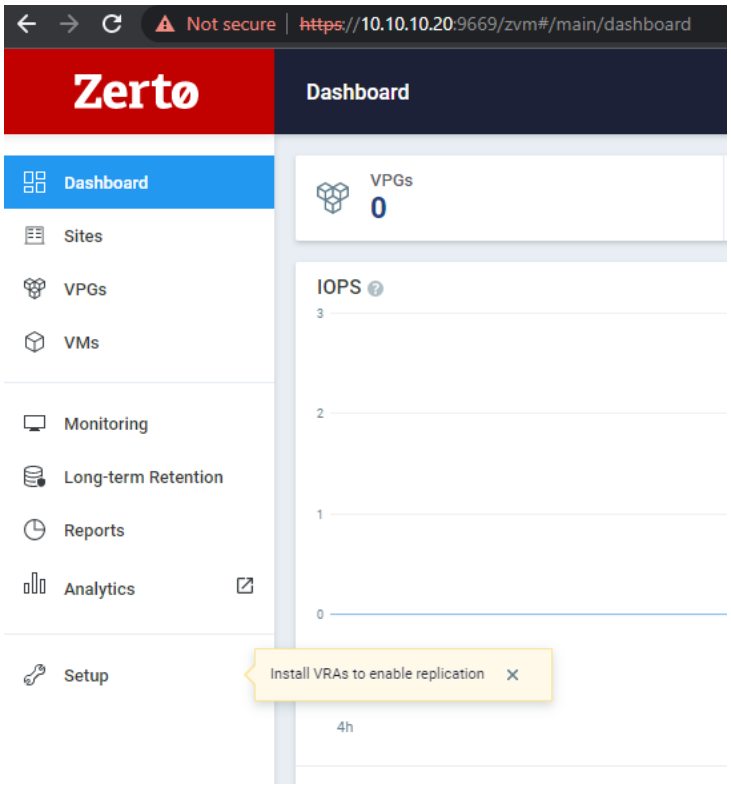
Kuva 11. Sisään kirjautumisen jälkeen ZVM tulee aktivoida voimassa olevalla lisenssillä. Vaihtoehtoisesti on mahdollista yhdistää sijaintiin, joka on lisensoitu valmiiksi. Tämä voi olla toinen ZVM palvelin tai palveluntarjoajan lisenssiä käytettäessä yhdistäminen tapahtuu heidän ZCC palvelimelle, joka maskeeraa yhteyden heidän omaan ZVM palvelimeensa.



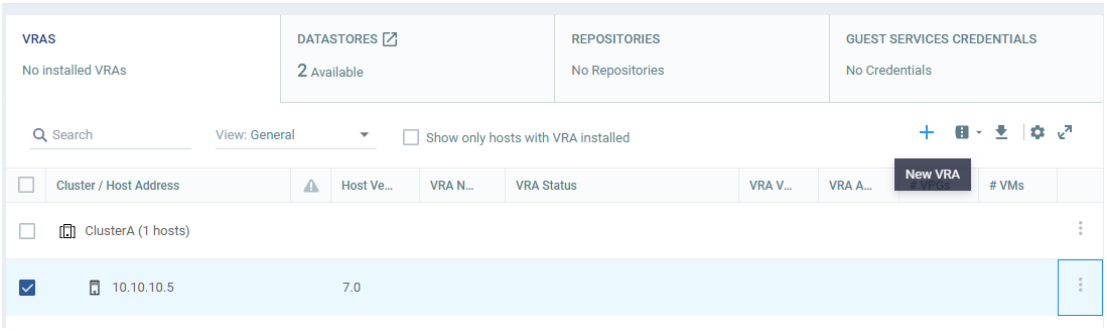
Kuva 12. Site-B-ZVM osalta tehdään liitos Site-A-ZVM kanssa. Ympäristöjen välillä sisäverkot pystyvät yhdistämään toisiinsa IPsec tunnelin ja sen kautta tehdyn reitityksen avulla. Site-A-ZVM Zerto hallinnassa käydään luomassa yhdistämisen avain (Generate Pairing Token), joka syötetään Site-B-ZVM:ssä. Yhdistäminen tapahtuu portin 9071 kautta.

Mikäli asennuksen vaiheessa toinen ZVM palvelin yhdistetään toiseen lisensoinnin osalta, yhdistää tämä myös (Pair) ympäristöt keskenään. Muutoin ympäristöt on erikseen yhdistettävä ZVM hallinnan kautta.

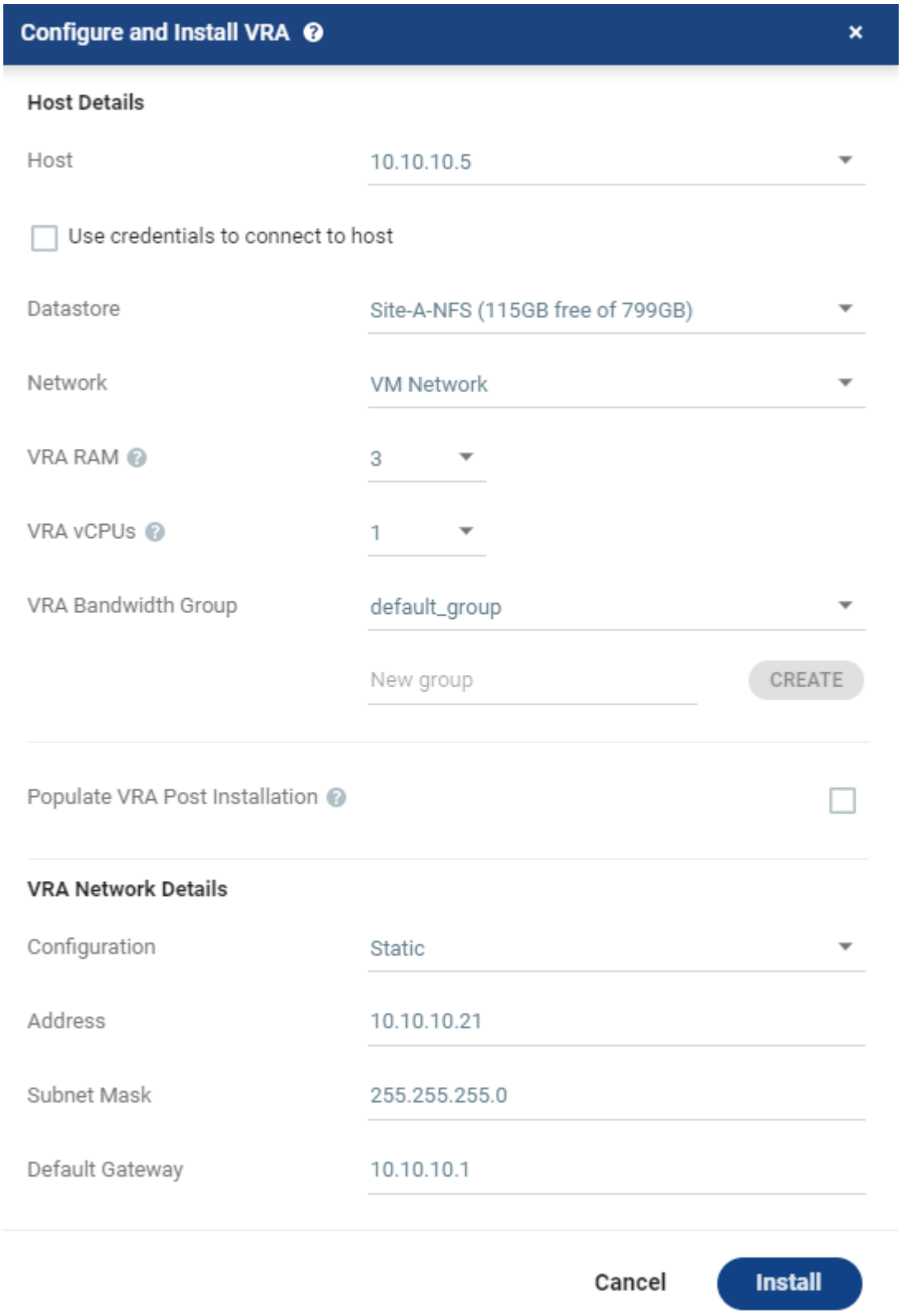
ZVM asennuksen jälkeen on mahdollista määritellä varsinainen VRA komponentti, joka suorittaa virtualisointialustalle Zerton kernel moduulin asennuksen, ja tämän kautta replikoitavien palvelimien muutoksien replikoinnin. VRA asennus tapahtuu ZVM hallinnan Setup-valikon kautta. Vaihtoehtoina on asentaa yksittäiselle alustapalvelimelle kerrallaan VRA komponentti tai asentaa koko klusterin kaikille alustoille kerralla VRA komponentit. Jälkimmäisessä vaihtoehdossa Zerto tiedustelee IP-osoitealueen, josta voidaan määritellä VRA komponenttien omat IP-osoitteet.



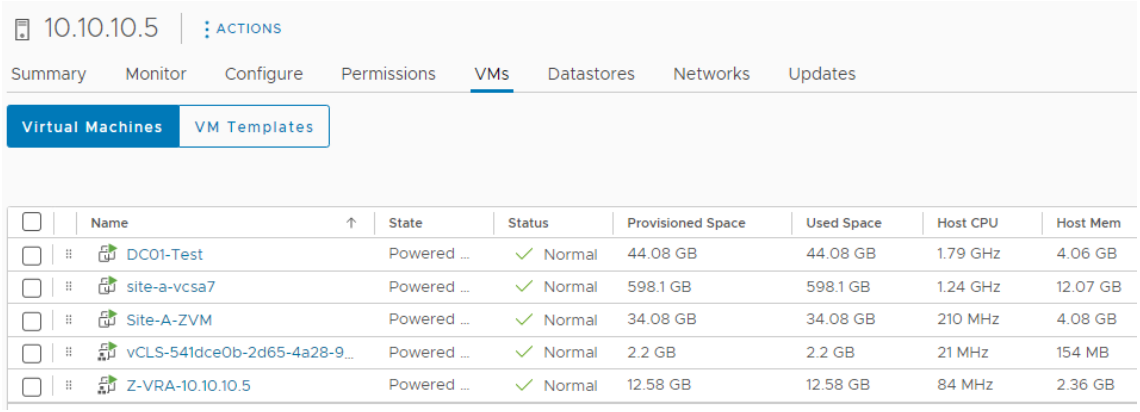
Kuva 13. ZVM hallinta on käyttökunnossa, mutta ennen kuin replikointeja voidaan määritellä, tarvitaan Virtual Replication Appliance (VRA) asennus ESXi alustalle. Valitaan Setup -valikko, kuten käyttöliittymä ehdottaa.



Kuva 14. Setup -valikossa näkyy klusterin ja sen alaiset virtualisointialustat. Uusi VRA asennetaan valitsemalla + -valikon kautta vaihtoehto New VRA.



Kuva 15. Täytetään VRA:n asennustiedot ja tarvittaessa käytetään optiota syöttämään ESXi palvelimen root -tunnukset asennusta varten. Root -tunnusta voi tarvita silloin, jos käytössä olevalla vCenter alustan toimialueen tunnuksella ei ole riittäviä oikeuksia suorittaa Zerton kernel moduulin asennusta alustapalvelimelle.



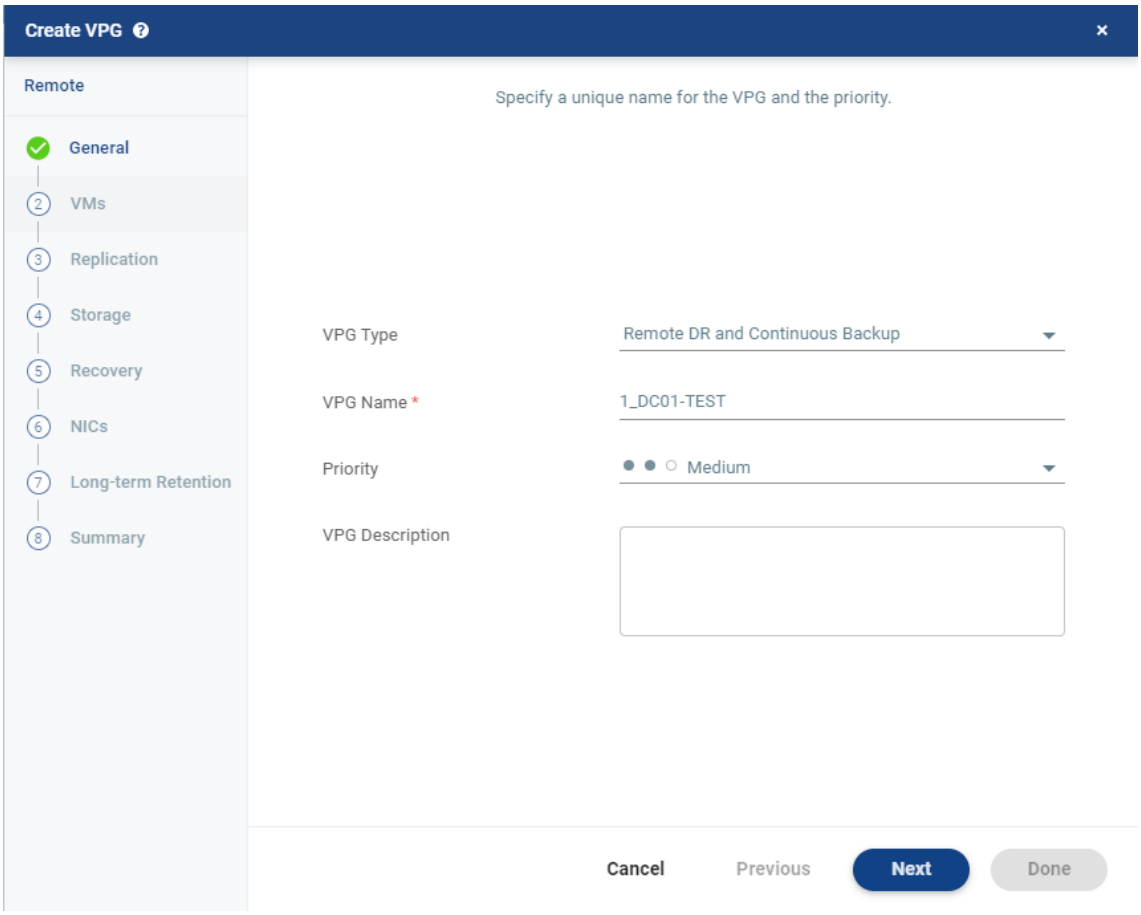
Kuva 16. Asennuksen jälkeen virtualisointialustan sisällä on Z-VRA-komponentti asennettuna.

ZVM ja VRA asennuksien jälkeen on mahdollista käyttää hyödyksi replikointia.

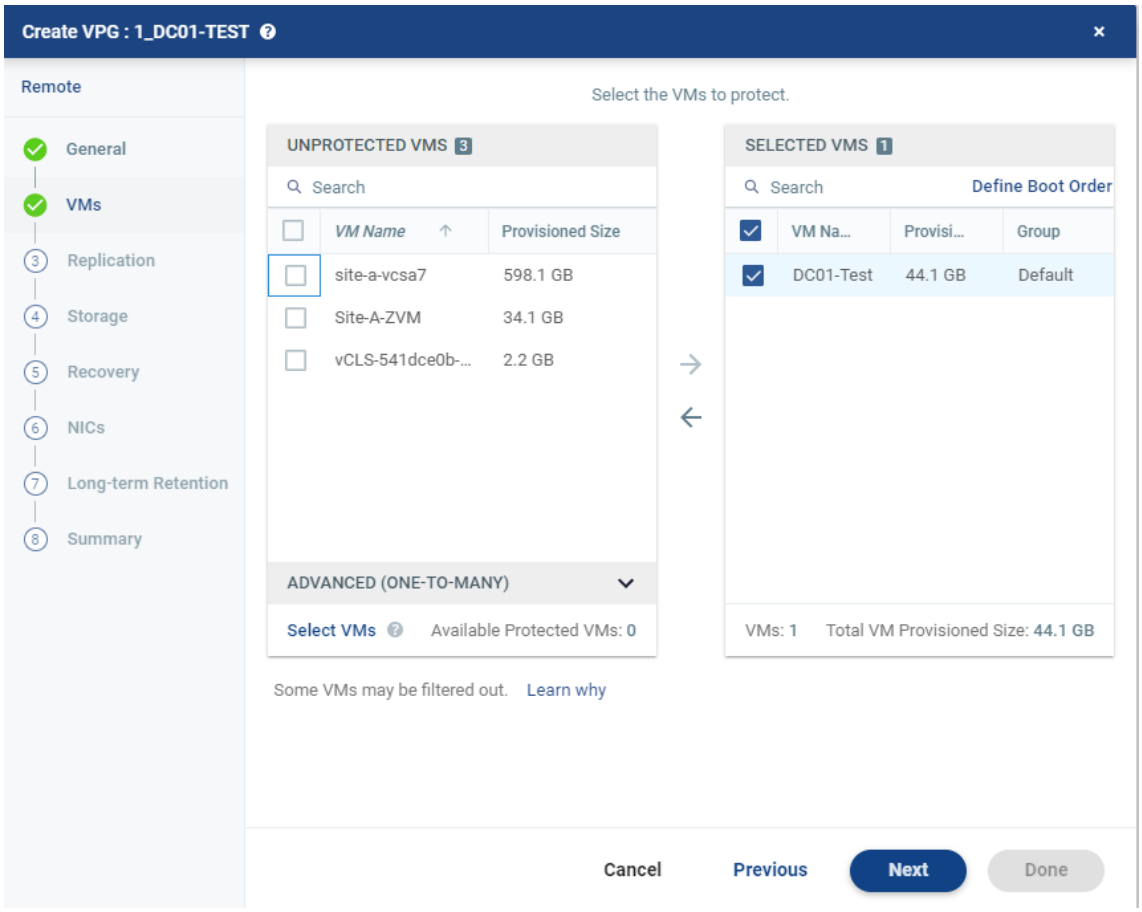
4.2.2 Replikoinnin määritys

Virtuaalipalvelimia on mahdollista replikoida virtualisointiympäristöstä toiseen, kunhan molemmissa on asennettuna Zerton ZVM sekä VRA komponentit. Tämän jälkeen ZVM hallinnassa sijainnit täytyy yhdistää toisiinsa. Tämän testin tapauksessa ympäristöt on jo yhdistetty Site-B-ZVM lisenssin aktivoinnin yhteydessä.

Palvelin lisätään replikointiin ZVM selainhallinnan VPGs näkymän kautta luomalla uusi virtuaalinen suojausryhmä (Virtual Protection Group = VPG). Luonti tehdään sen ympäristön ZVM kautta, jolta halutaan saada virtuaalipalvelin replikoinnin suojauksen piiriin, eli tässä tapauksessa Site-A-ZVM kautta. VPGs valikossa valitaan vaihtoehto + New VPG.

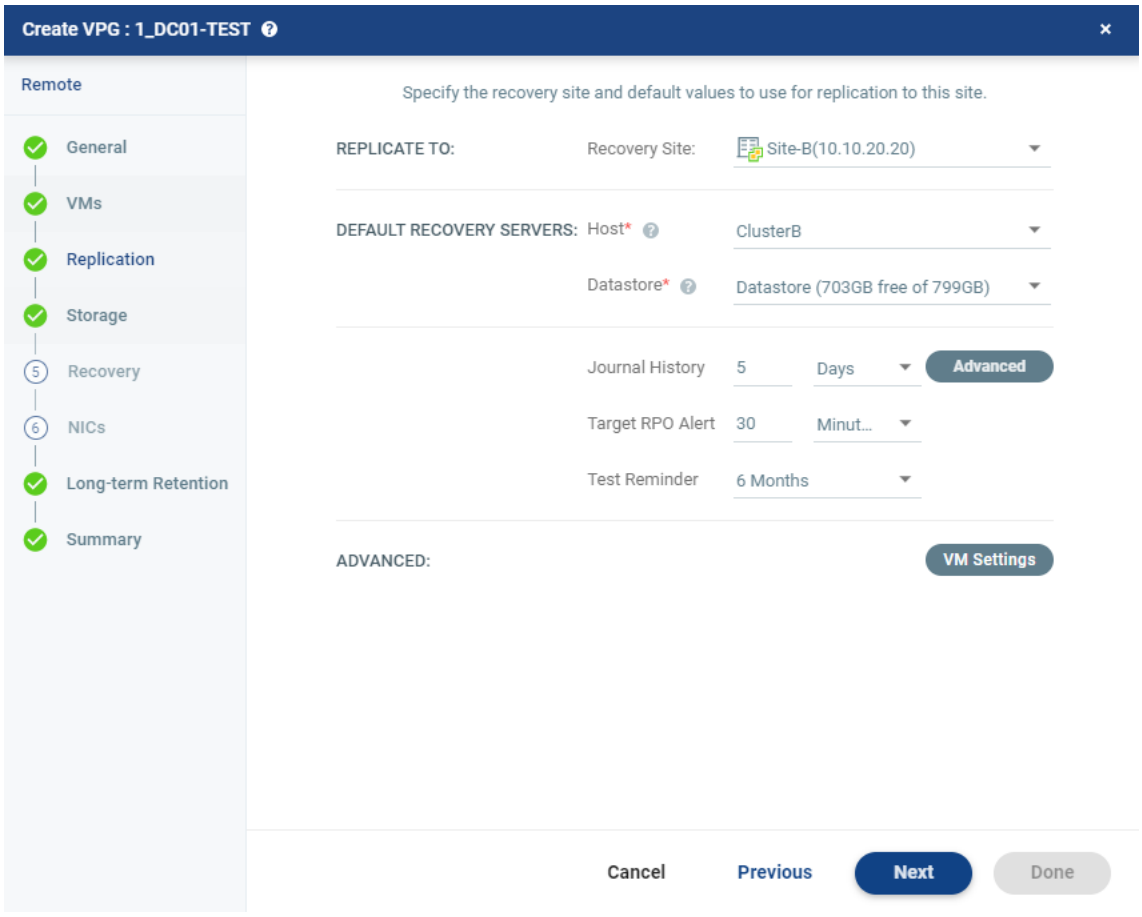


Kuva 17. Määritetään jokin soveltuva VPG nimi. Tässä vaiheessa on mahdollista muokata prioriteettia ja VPG muotoa. Korkeampi prioriteetti antaa tämän replikoida ennen muita. VPG menetelmän vaihtamisella voidaan määrittää tämän olevan paikallinen varmistus, replikointi etäkohteeseen (DR suoja) tai virtuaalikoneen siirto toiseen kohteeseen. Testin tapauksessa valittiin oletusvaihtoehdot.

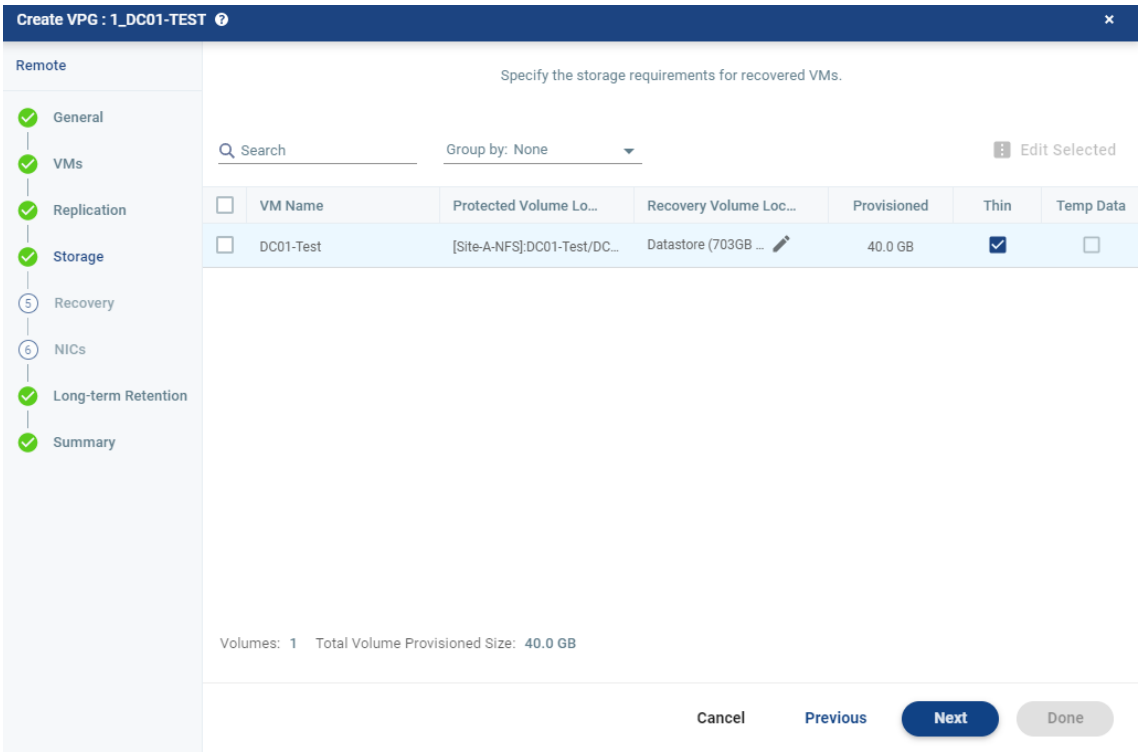


Kuva 18. Seuraavaksi valitaan DR replikointiin lisättävä VM. Näet palvelimen nykyisen koon, huomioitava on palvelimen nykyinen koko sekä suojaukseen arvioitava Journal History koko.

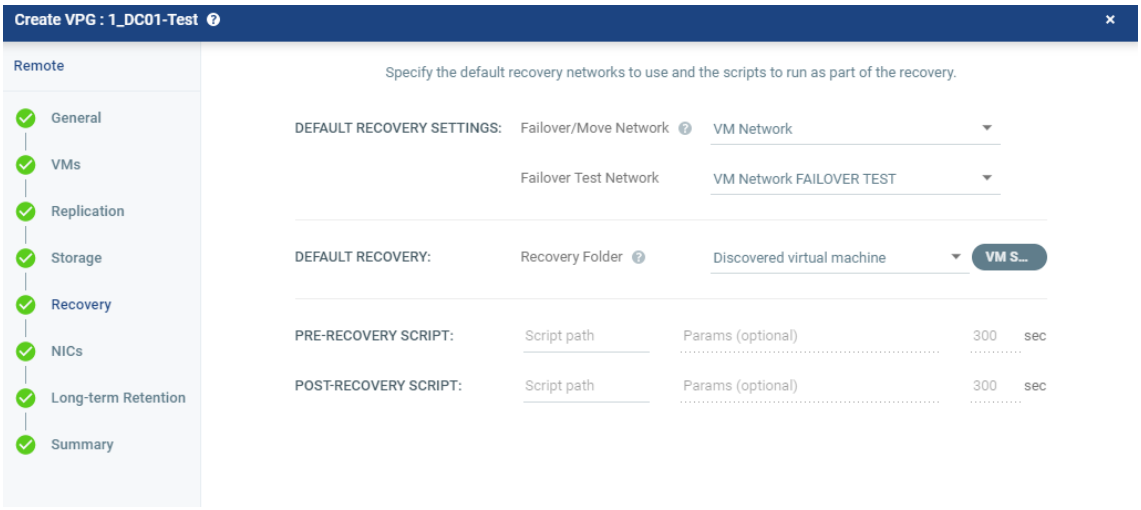
Kun virtuaalipalvelimia lisätään mukaan replikointiin, tulee huomioida kohdesijainnissa olevan riittävästi vapaata tilaa replikoitaville palvelimille, sekä niiden päiväkirjalle. Jokainen palvelin saa oman päiväkirjan ja sen koon karkean arvion voi laskea replikoitavien päivien määrällä, kun yhden päivän aikana tapahtuvat muutokset ovat arviolta 10 % virtuaalipalvelimen käytetystä tallennustilasta [19, s. 4].



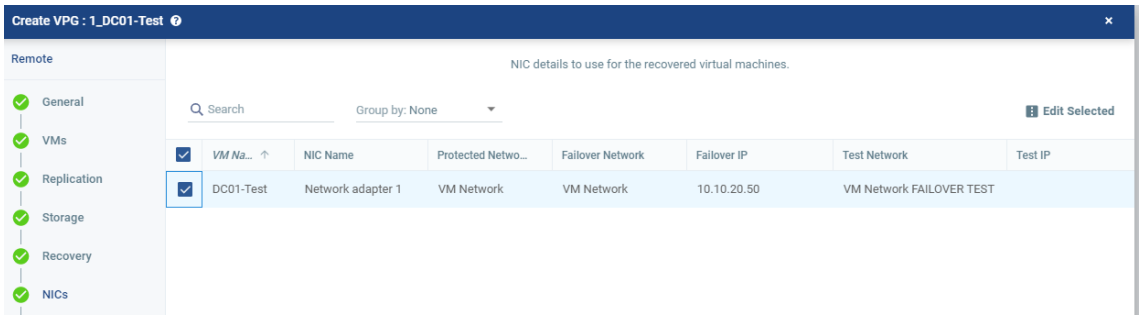
Kuva 19. Määritetään varsinaiset replikoinnin asetukset. Kohteeksi valitaan Site-B ja sen alla olevat resurssit. Journal History määritykseksi valittiin viisi (5) päivää, eli palvelin on mahdollista palauttaa maksimissaan viisi (5) päivää vanhaan versioon. Syynä viiden (5) päivän päiväkirjalle on sen mahdollistaminen, että mahdollinen viikonlopun aikana tapahtunut virhe voidaan huomata ja korjata viikonlopun jälkeen [10, s. 9]. RPO Alert määritetään 30 minuuttia eli ZVM Monitoring näkymään tulee varoitus, jos palvelimen osalta ei ole tullut uutta dataa 30 minuuttiin. Tässä vaiheessa on mahdollista määrittää myös DR testauksen muistutus.



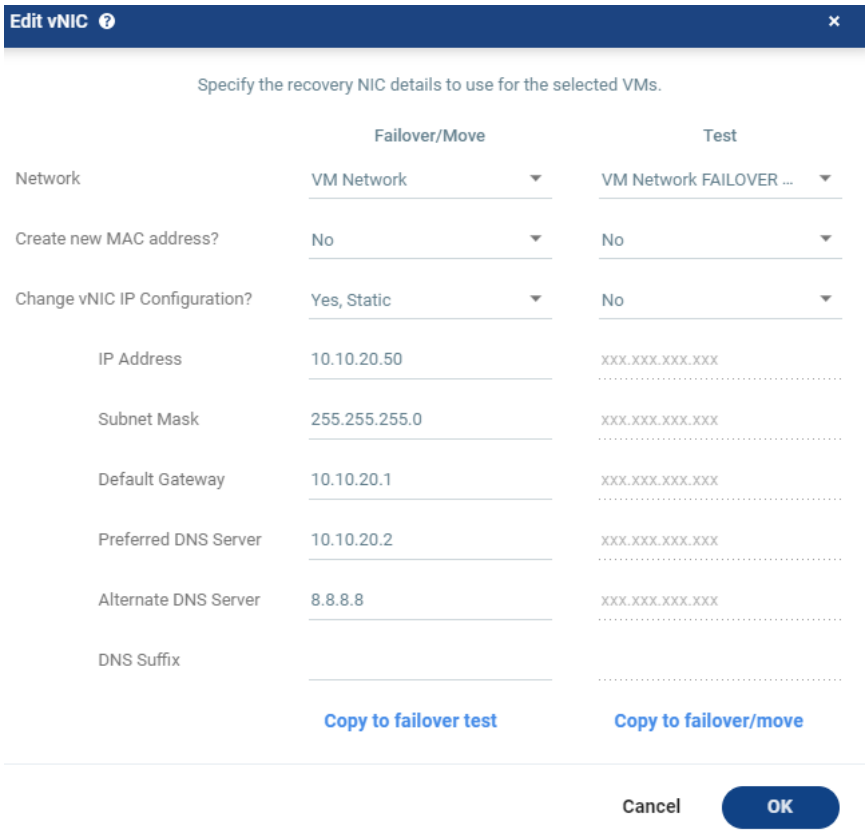
Kuva 20. Storage -valikossa voidaan vielä tehdä muutoksia replikoitavan VM:n tallennustilan määrityksiin. Esimerkiksi mahdollista on muuttaa levy Thin-muotoon kohteessa.



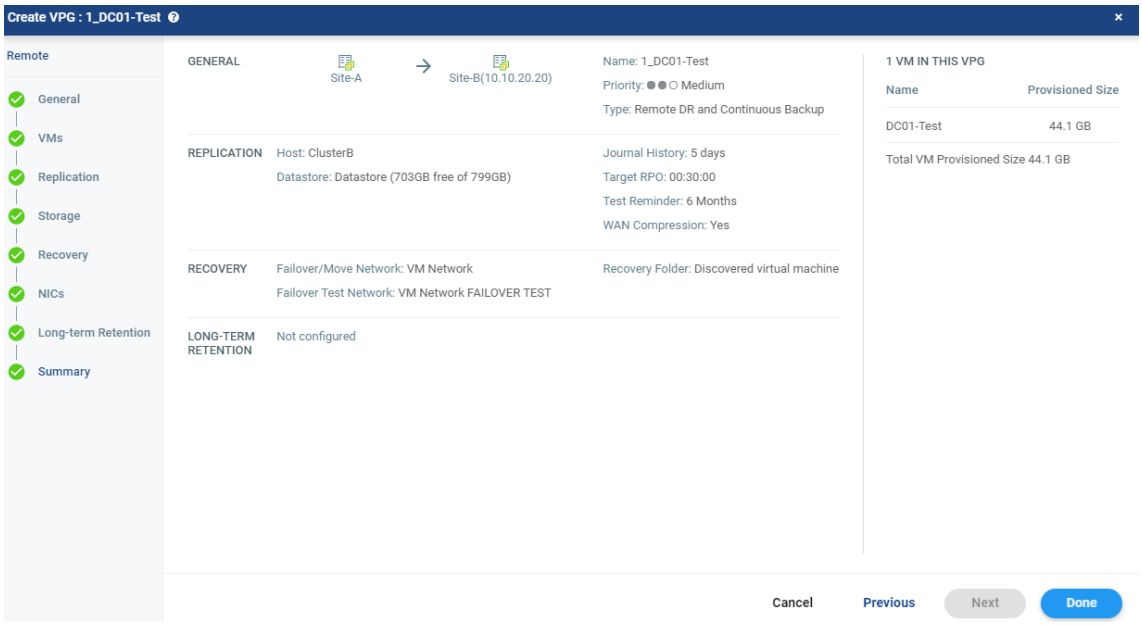
Kuva 21. Recovery -näkymässä määritetään mihin Port Group -verkkoon palvelin kohteessa yhdistetään. Kohteen verkossa virtuaalikoneen verkkoyhteys tulisi toimia normaalisti Failover/Move Network vaihtoehdossa. Testiverkon osalta kyseisen verkon ei tulisi reitittyä mihinkään ympäristöstä ulospäin. Mahdollista on myös valita mihin vCenter kansioon palvelin laitetaan sekä määrittää joitain hyödyllisiä skriptejä.



Kuva 22. NICs -valikossa on mahdollista määrittää palvelimelle uudet IP-osoitteet. IP-osoitteen vaihdos ei ole välttämättä tarpeen riippuen ympäristöjen välisen verkkoyhteyden toteutustavasta. Testin tapauksessa on määritetty uusi IP-osoite eri aliverkkoon, joka on käytössä kohteessa. Zerto vaihtaa Failoveria tehdessään palvelimelle uudet verkkokortin asetukset. Määritys tapahtuu hyödyntäen VMware Toolsin ominaisuuksia.



Kuva 23. IP-osoite määritykset. Failover toimenpiteen jälkeen voi olla tarve varmistaa kaiken toimivan sekä tehdä tarvittavat muutokset DNS tietueisiin, mikäli palvelimen IP-osoite vaihdetaan. Toteutustavan mukaan kohteessa voi olla tarve muutoksille.



Kuva 24. Koostetusti lopulliset määritykset. Replikointi alkaa painamalla Done -nappia.

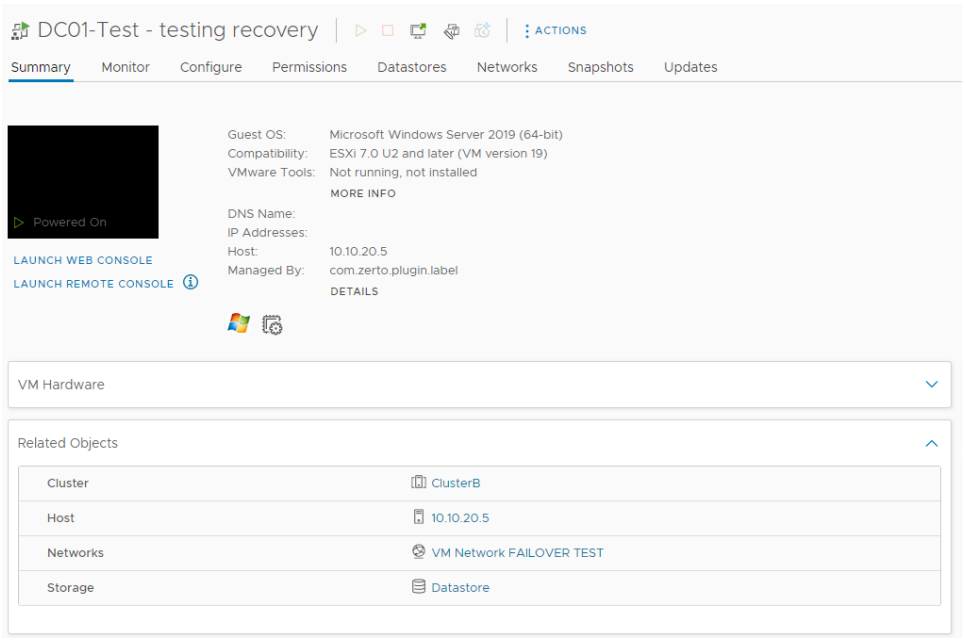
Kun palvelimen VPG on määritetty, Zerto luo vCenterissä Protection Group määrityksen, lisää palvelimen suojauksen piiriin ja alkaa replikoimaan (Initial sync) virtuaalipalvelimen tiedostoja kohdesijaintiin. Tämän jälkeen tehdään Bitmap synkronointi, missä Zerto tallentaa lähdesijainnin VRA:lle virtuaalipalvelimeen tapahtuvat muutokset reaaliajassa ja alkaa sen jälkeen replikoimaan tapahtuneet muutokset kohdesijaintiin. Bitmap synkronointi tapahtuu silloin, kun yhteyden nopeus ei riitä synkronoimaan reaaliajassa kaikkia muutoksia kohteeseen. Replikointi ottaa kiinni palvelimen tilannetta nykytilanteeseen nähden, kun välimuistiin tallennettu data siirretään kohteeseen. Lopuksi palvelimesta on replikoituna muutaman sekunnin viiveellä palautuspisteitä ja Recovery Point Objective näyttää palautuspisteiden välin.

Bitmap synkronointi ei tarkoita sitä, etteikö palvelimen tiedot replikoituisi kohteeseen. Syinä bitmap synkronoinnin aktivoitumiseen voi olla riittämätön verkon nopeus kaikkien palvelimella tapahtuvien muutosten synkronointiin tai palvelimella tapahtuu niin paljon muutoksia, ettei VRA:n kapasiteetti riitä synkronoimaan niitä kaikkia. Virtuaalipalvelimen muutoksista Zerton kernel-moduuli lähettää datan oikealle VRA:lle käsiteltäväksi. VRA kirjoittaa muutokset omaan keskusmuistiinsa ja lähettää ne sen jälkeen eteenpäin kohdepään VRA:lle. Mikäli

lähdepään VRA on niin kuormittunut, että sen keskusmuisti loppuu, seurattavien muuttuvien tallennusjärjestelmän blokkien seurannan tarkkuus vähenee. Ensin Zerto tarkkailee tarkalleen mitkä tallennusjärjestelmän blokit muuttuvat, mutta mikäli VRA keskusmuisti loppuu, Zerto alkaa vähentämään tarkkuutta. Tällöin VRA lähettää kohdepäähän muuttuneen alueen blokeista, jotka ovat saattaneet muuttua palvelimella. VRA hallinnoi älykkäästi tarkkuutta ja varmistaa sen, että muutokset replikoituvat aina kohteeseen. Tämänlaisessa tilanteessa data on replikoitavana enemmän, koska tarkkuus on vähentynyt. Zerton ei myöskään tarvitse ylläpitää erillistä päiväkirjaa lähteessä olevassa tallennustilassa, kun se käyttää omaa keskusmuistiaan älykkäänä bufferina. [16.]

4.2.3 Replikoinnin testaus

Replikoitua virtuaalipalvelinta voi testata ZVM selainhallinnan kautta valitsemalla VPGs valikosta testattava VPG ja sen jälkeen alhaalta vasemmalta optio Failover ja Test. Päiväkirjasta on mahdollista valita palautuspiste, jota halutaan testata.



Kuva 25. Testauksen DC01-Test palvelin lähtee käyntiin, niillä asetuksilla mitä oli määritetty VPG:n asetuksissa. Mikäli palvelimella on erillinen Failover Test verkko, niin palvelimen virtualisoitu verkkokortti on tällöin siinä kiinni. Tässä huomataan mahdolliset ongelmat esimerkiksi käyttöjärjestelmän osalta.

Replikoitaessa palvelinta kaikki sen data on jo kohteessa olemassa. Sen kiintolevy on tallessa ja sen päiväkirjassa on palautuspisteinä tallessa kaikki palvelimelle tapahtuneet muutokset. Replikoinnin aikana palvelinta ei ole vielä rekisteröity kohdesijainnin virtualisointialustalle. Käytännössä tällöin replikoitava kohde kuluttaa vain tallennustilaa.

Kun virtuaalipalvelimen Failover tai Failover Test toimenpide käynnistetään, Zerto rekisteröi palvelimen kohdesijainnin virtualisointialustalle. Failover Test toimenpiteen aikana Zerto lukee replikoidun palvelimen alkuperäisen levyn sekä päiväkirjan tiedoista kyseisen ajankohdan tilanteen ja käynnistyy kyseisen ajankohdan tilanteesta. Kaikki mahdolliset Failover Test toimenpiteen aikana tehdyt muutokset kirjoitetaan väliaikaiseen tallennustilaan, jonka rajoituksena on päiväkirjan maksimikoko. Mikäli päiväkirjan maksimikoko tulee vastaan, uusia muutoksia ei voi testin aikana tehdä. Tuotannossa olevan palvelimen muutokset kirjoitetaan testin aikana normaalisti päiväkirjaan. [17.]

Suoritetun testauksen aikana ei törmätty ongelmiin. Palvelin lähti käyntiin täysin normaalisti ja se oli lisättynä VMware verkkoon, mikä ei reitity mihinkään. Tällöin testipalvelin ei pysty millään tavalla aiheuttamaan häiriötä tuotannossa oleviin palveluihin, vaikka sen IP-osoite olisi sama kuin tuotannossa.

Huomioitavaa on myös, että tuotannossa oleva palvelin on Failover Test toimenpiteen aikaan täysin normaalisti päällä tuotantoympäristössä, eli testistä ei aiheudu millään tavalla häiriötä tuotantoon.

Kun testi on valmis, Zerton hallinnasta VPGs näkymästä voi kyseisen VPG:n kohdalla lopettaa testauksen valinnasta Stop Failover Test. Zerto siivoaa kohdesijainnista testipalvelimen. Koska kaikki testipalvelimen muutokset kirjoitetaan väliaikaiseen tallennustilaan, sen siivoaminen on todella helppoa.

4.2.4 Disaster Recovery -tilanne

Katastrofista palautumisen tilanteeseen tulee valmistautua Zerton sekä muun ympäristön osalta. Kun virtuaalipalvelin on lisätty replikointiin, ensimmäisenä on

syytä suorittaa Failover Test toimenpide ja varmistaa palvelimen käynnistyvän normaalisti.

Varsinaista katastrofitilannetta varten tulisi myös suunnitella replikointiympäristön verkot toimintakuntoon sekä miettiä miten palvelut toimivat kohdeympäristöstä. Mikäli käytössä ei ole Layer 2 Metro-Ethernet yhteyttä, jossa paikallinen tuotantoverkko on venytetty myös DR-ympäristöön, on todennäköistä, että palvelimen IP-osoitteen täytyy muuttua.

Tämän testiympäristön kanssa käytössä oli IPsec tunneli kahden eri sijainnin välillä. Sijainneilla oli eri aliverkot. Tällöin virtuaalipalvelimen IP-osoite tulee muuttua, jotta se voi toimia uudessa aliverkossa. Zertossa on kuitenkin sisäänrakennettuna ominaisuus, jolla ylläpitäjä voi valmiiksi määritellä DR-tilanteessa käytettävän IP-osoitteen. Tämän jälkeen jää vielä muun verkon valmistelu kyseistä tilannetta varten sekä suunnitelma siitä, miten mahdolliset muut palvelut yhdistävät DR-ympäristössä oleviin palvelimiin, jos niiden paikalliset IP-osoitteet sekä mahdollisesti julkinen IP-osoite on muuttunut. DR-tilanteessa voi siis vielä jäädä konfiguroitavaa palveluiden toiminnallisuuden varmistamiseksi.

Vaihtoehtoisena tapana olisi tehdä sama aliverkko sekä tuotannon että DR:n sijainteihin ja sen sijaan konfiguroida palomuurissa staattinen Network Address Translation asetukset molempiin päihin. Kummassakaan päässä ei voi kuitenkaan suoraan viitata kohdesijainnin aliverkkoon, kun se on sama, vaan tällöin täytyy viitata johonkin toiseen osoitteeseen, mikä käännetään palomuurin toiminnallisuuden kautta oikeaan kohteeseen.

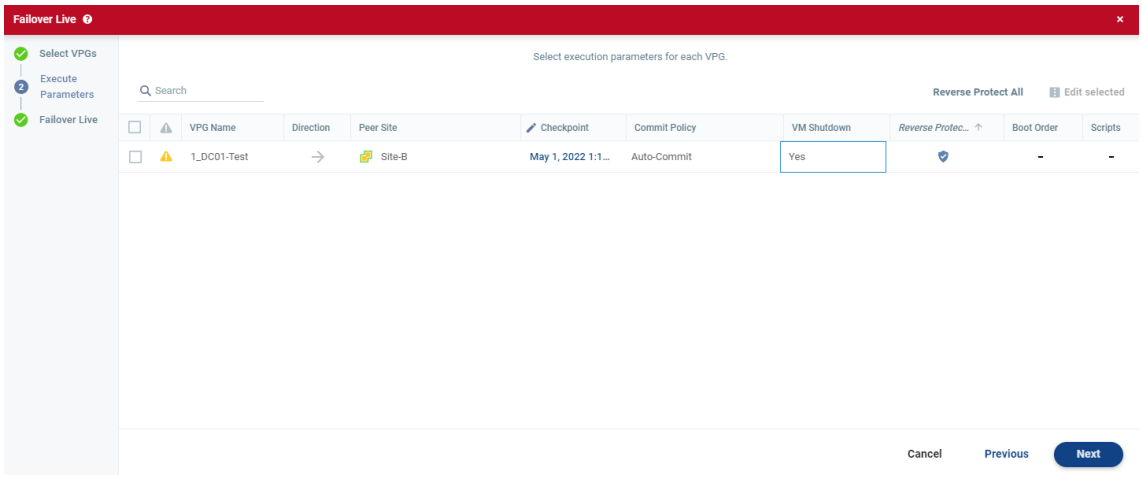
Kun suoritetaan varsinainen Failover Live toimenpide, Zertolla ollessaan yhä yhteys lähdesijaintiin käy se sammuttamassa lähteessä olevan replikoinnin piirissä olevan virtuaalipalvelimen [18]. Tuotantoympäristössä aiheutuu tällöin katkos kyseisen palvelimen toimintaan. Mikäli lähdesijainti on jo tavoittamattomissa, katkos tuotantoon on jo tapahtunut.

Failover Live toimenpiteessä valitaan mistä päiväkirjan palautuspisteestä palvelin tai palvelimet halutaan käynnistää. Replikoitavalle virtuaalipalvelimelle on

mahdollista määritellä takaisin suojaus (Reverse protection) tuotantoon, minkä myötä Zerto replikoi kaikki muutokset DR ympäristöstä takaisin tuotantoon, kun tuotantoympäristö palaa takaisin toimintaan. Tuotannossa olevan virtuaalipalvelimen voi myös sammuttaa valinnalla, mikäli alkuperäinen replikoitava palvelin on yhä päällä. Mikäli lähdesijainnin replikoitavalla palvelimella ei ole VMware Toolseja asennettuna ja yhteys lähteeseen toimii, toimenpide epäonnistuu, koska se ei saa virtuaalipalvelimen sammutuksen käskytystä tehtyä hallitusti. Vaihtoehtona on myös pakottaa virtuaalipalvelimen sammutus, jolloin Zerto pystyy jatkamaan toimenpidettä. Vaihtoehtoisesti ylläpitäjä voi käydä itse sammuttamassa virtuaalipalvelimen hallitusti lähdesijainnissa. [18.]

Commit Policy määrityksessä on mahdollista määrittää, viimeistelläänkö DR ympäristöön palautettu palvelin heti tai tietyn ajan jälkeen. Takaisin suojaus (Reverse protection) ei käynnisty uudelleen ennen siirron viimeistelyä ja sen jälkeen ei ole mahdollista palautua muihin replikoinnin palautuspisteisiin. Palvelimen palautettu tilanne kyseisestä ajankohdasta on mahdollista tarkistaa, mikäli muutoksia ei viimeistellä heti. Tällöin on mahdollista peruuttaa toimenpide ja valita toinen palautuspiste. Viimeistelyn myötä replikointiympäristön päiväkirja yhdistetään tähän uuteen siirrettyyn palvelimeen ja loput päiväkirjan palautuspisteet tuhotaan. Palvelimen replikoituun levytiedostoon kirjoitetaan päiväkirjan mukaiset replikoidut muutokset, minkä jälkeen jäljellä on vain kyseisen ajankohdan levytiedosto. Palvelin käynnistyy kyseisen ajankohdan levytiedostosta, kun kaikki muutokset on siihen yhdistetty. [18.]

Failover Live toimenpiteen aikana Zerto ei salli vCenterin siirtää palvelinta toiselle alustapalvelimelle vMotion toimenpiteen avulla. Palvelin voi myös jäädä sammutettuun tilaan, mikäli palvelimen verkkokortilla on samat asetukset jonkin toisen palvelimen kanssa. [18.]

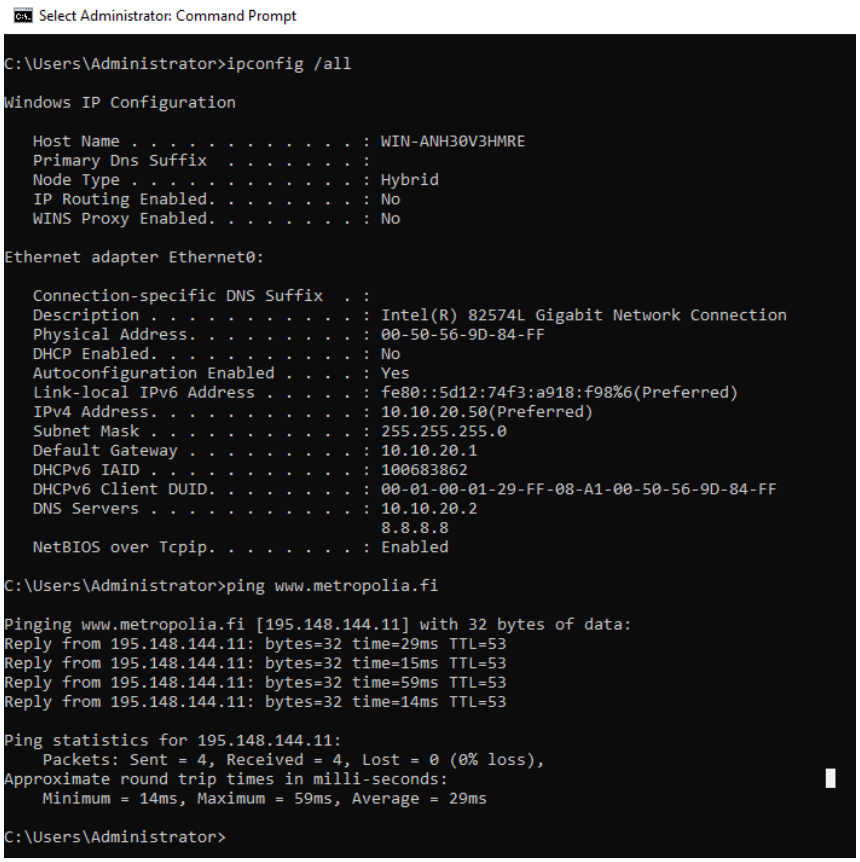


Kuva 26. Failover Live toimenpiteen vaihtoehdot.

Kuvassa 26 näkyvillä [Kuva 26] vaihtoehdoilla Zerto sammuttaa lähdepään virtuaalipalvelimen, mikäli se on päällä ja sinne on toimiva verkkoyhteys. Tämän jälkeen palvelimen kopio käynnistetään DR ympäristössä ja Auto-Commit 0 minuuttia asetuksella tulee tästä palvelimesta tuotantopalvelin. Takaisin suojaus käynnistyy heti ja Zerto alkaa replikoimaan DR sijainnista muutoksia takaisin tuotantosijaintiin, mikäli tuotantoympäristö on toiminnassa. [18.]

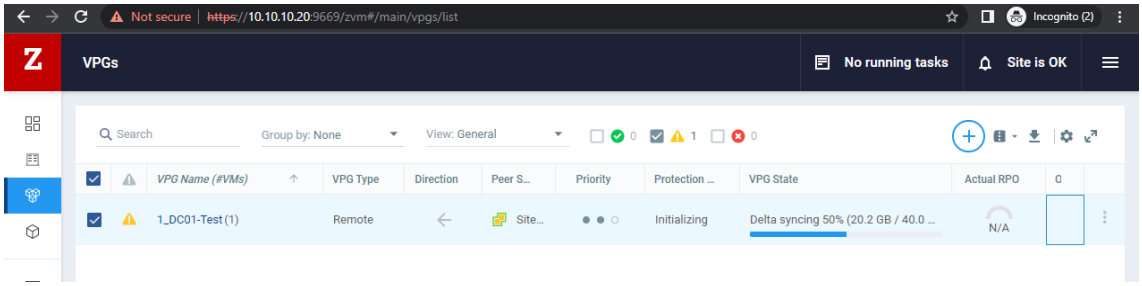
Tuotantoympäristössä alkuperäisen palvelimen aliverkko oli 10.10.10.0/24 ja IP-osoite 10.10.10.50. Zerto määrityksien myötä IP-osoite ja aliverkko ovat vaihtuneet. Palvelin lähtee käyntiin ja tarkistaa käyttäjältä onko tämä uusi verkko luotettava toimialueverkko tai yksityinen verkko sekä pyytää syyn miksi palvelin on omasta näkökulmastaan kaatunut.

Takaisin suojauksen myötä, kun Zertolla on yhteys tuotantoympäristöön, se sammuttaa tuotantoympäristössä olevan palvelimen sekä poistaa sen rekisteröinnin virtualisointiympäristöstä. Kyseisen palvelimen alkuperäiset levytiedostot kuitenkin säilyvät tallennustilassa. Zerto suorittaa delta synkronoinnin alkuperäisestä kohdeympäristöstä tuotantoympäristöön, millä varmistetaan molempien ympäristöjen levytiedostojen olevan ristiriidattomia. [18.]



Kuva 27. Zerton tekemät verkkoadapterin muutokset ovat menneet läpi. Yhteys ulkoverkkoon toimii normaalisti, koska DR-sijainnin verkotukset ovat kunnossa.

Failover tilanteen jälkeen, mikäli VPG:n tietoja tarkistetaan, voidaan huomata muutokset.



Kuva 28. Tarkisteltaessa Site-A-ZVM hallinnasta, josta voidaan nähdä, että VPG 1_DC01-Test on nyt Remote, eli ei paikallinen ja replikoinnin suunta on takaisin kohti tuotantoympäristöä. Delta synkronointi on parasta aikaa käynnissä eli muutoksia ollaan synkronoimassa takaisin tuotantoon, mutta päiväkirja ei ole vielä ajan tasalla.

Kun palvelin halutaan palauttaa takaisin tuotantoon, tehdään Failover toimenpide tuotantoa kohden ja asetetaan takaisin suojauksen asetus päälle. Zerto säilyttää tässä tapauksessa tuotannossa olleen verkkokortin IP-asetukset ja tallentaa ne VPG:n määrityksiin. Palvelimen IP-osoite palautuu samaksi kuin mitä se oli tuotannossa. Palvelimen palauttaminen tuotantoympäristöön on siis myös mahdollista vain muutamalla napin painalluksella Zerton hallinnan kautta ja katkokset palvelimen toimintaan minimoituvat, kun sen tiedot on jo replikoitu valmiiksi takaisin tuotantoympäristöön.

Ilman takaisin suojausta palvelimen replikointi takaisin tuotantoympäristöön on silti mahdollista. Tällöin luodaan uusi virtuaalinen suojausryhmä, missä replikoidaan replikointiympäristöstä virtuaalipalvelin takaisin tuotantoympäristöön. Mikäli alkuperäistä tuotantoympäristöä ei ole tai se on vaihtunut, niin Zerton komponenttit asennetaan uudelleen toiseen ympäristöön ja lopuksi määritetään replikointi. Jos tuotantoympäristö on asennettu uudelleen, niin vanhan tuotantoympäristön yhteyden voi poistaa replikointiympäristön ZVM hallinnasta Sites välilehdeltä tekemällä Unpair toimenpiteen ja sen jälkeen suorittaa paritus uuteen tuotantoympäristöön. Replikoinnin määrityksien jälkeen Zerto suorittaa aluksi palvelimen datan siirron tuotantoon ja alkaa tämän jälkeen synkronoimaan palvelimelle tapahtuneita muutoksia. Lopuksi päiväkirja tavoittaa palvelimen nykyisen tilanteen niin lähelle kuin replikoinnin nopeus tämän sallii.

Palvelimen siirtämisen takaisin tuotantoympäristöön voi tehdä Zerton Failover Live toimenpiteellä tai Move toimenpiteellä. Move toimenpide tekee samat vaiheet kuin Failover Live toimenpide, mutta se tarjoaa lopuksi vaihdoehdon tuhota tai jättää alkuperäisen replikoitavan palvelimen datat replikointiympäristöön.

5 Yhteenveto

Opinnäytetyötä varten suoritetun testauksen tuloksena rakennettiin toimiva tuontato- ja DR-ympäristö ja yhdistettiin näiden väliset verkot IPsec tunnelin avulla (Liite 1). Kyseistä tunnelia hyödyntäen määritettiin Zerto Virtual Replication onnistuneesti toimintaan ja tämän kautta määritettiin virtuaalipalvelimen replikointi tuotantoympäristöstä DR-ympäristöön. Replikoitavan palvelimen ja ympäristöjen eri verkkoasetukset huomioitiin DR-tilannetta varten ja Zerton asetuksiin määritettiin se, että replikoitavan palvelimen IP-osoite ja aliverkko muutetaan sellaisenaan, joka toimi kohdeympäristössä.

Varsinaisen replikoitavan palvelimen osalta suoritettiin ensin Failover Test toimenpide, jossa palvelin käynnistettiin ilman toimivaa verkkoyhteyttä ja todettiin palvelimen käynnistyvän onnistuneesti DR-ympäristössä.

Tämän jälkeen testattiin varsinaista DR-tilannetta, missä replikoitava virtuaalipalvelin siirrettiin DR-ympäristöön ja sen verkkoasetusten havainnoitiin muuttuneen. Näin ollen varmistettiin, että verkkoyhteydet toimivat myös DR-ympäristössä ja todettiin palvelimen toimivan normaalisti. DR-tilanteesta palautumista ajatellen takaisin suojaus asetettiin päälle, jolloin Zerto automaattisesti replikoi muutokset takaisin tuotantoympäristöön, minkä vuoksi voitiin todeta, että palautuminen tuotantoon olisi myöhemmin mahdollista.

Suoritetun testin lopputuloksena voidaan nähdä toimiva tuotanto ja DR-ympäristö, joiden välinen replikointi toimii. Tämän lisäksi varsinaisen Zerto Virtual Replication tuotteen testaus on onnistuneesti todettu toimivan kuten sen kuuluukin. Jatkon kannalta Zerto Virtual Replication ominaisuuksista voisi tutkia Zerton Application Consistent Protection tuotteen tarjoamaa suojausta, joka mahdollistaa palvelimen sisällä olevan palvelun suojaamisen ristiriidattomassa tilassa. Tämä mahdollistaisi teoriassa vieläkin paremman suojauksen palvelimen datalle sekä sen alla toimiville palveluille.

Lähteet

1 Palvelinalustan eri vaihtoehdot. 2021. Verkkoaineisto. TechTarget – Robert Sheldon. https://www.techtarget.com/searchdatacenter/feature/Learn-the-major-types-of-server-hardware-and-their-pros-and-cons Luettu 2.4.2022

2 VMwaren ohjelmistopohjainen palvelinsali. 2020. Verkkoaineisto. Parallels - Nicolette Carklin https://www.parallels.com/blogs/ras/vmware-sddc/ Luettu 2.4.2022.

3 VMware CPU maskeeraus. 2019. Verkkoaineisto. VMware – Niels Hagoort. https://blogs.vmware.com/vsphere/2019/06/enhanced-vmotion-compatibility-evc-explained.html Luettu 2.4.2022.

4 Palvelinsali ja virtualisointi. 2022. Verkkoaineisto. VMware. https://www.vmware.com/topics/glossary/content/data-center.html Luettu 3.4.2022.

5 VMware virtuaalipalvelimen komponentit. 2019. Verkkoaineisto. VMware. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.vm_admin.doc/GUID-F559CE9C-2D8F-4F69-A846-56A1F4FC8529.html Luettu 2.4.2022.

6 VMware vMotion oletustoiminto. 2007. Verkkoaineisto. VMware. https://www.vmware.com/pdf/vmotion_datasheet.pdf Luettu 3.4.2022.

7 Hyper-V Failover Clustering. 2019. Verkkoaineisto. Nakivo – Jessie Reed. https://www.nakivo.com/blog/hyper-v-high-availability-works/ Luettu 8.4.2022.

8 VMware HA explained. 2021. Verkkoaineisto. Nakivo – Michael Bose. https://www.nakivo.com/blog/vmware-vsphere-ha-and-drs-compared-and-explained/ Luettu 9.4.2022.

9 Zerto Virtual Replication tuotteen julkaisu. 2022. Verkkoaineisto. Zerto. https://www.zerto.com/zerto-platform/core-elements/continuous-data-protection/always-on-replication/ Luettu 9.4.2022.

10 Zerto Virtual Replication arkkitehtuurin kuvaus ja suunnitteluohje. 2019. Verkkoaineisto. Zerto. https://www.zerto.com/wp-content/uploads/2019/04/architecture-guide-for-the-it-resilience-platform-whitepaper.pdf Luettu 9.4.2022.

11 Zerto Virtual Replication lisensointi. 2021. Verkkoaineisto. HPE. https://www.zerto.com/wp-content/uploads/2021/05/Zerto-Solutions-with-HPE.pdf Luettu 9.4.2022.

12 Zerton vaatimukset palveluntarjoajille. 2022. Verkkoaineisto. Zerto. https://help.zerto.com/bundle/Prereq.MSP.HTML.90/page/Content/Cloud_SP_Guide/For_Managed_Service_Provider_Sites.htm Luettu 9.4.2022.

13 Zerto Cloud Manager hallintaohje. 2021. Verkkoaineisto. Zerto. http://s3.amazonaws.com/zertodownload_docs/Latest/Zerto%20Cloud%20Manager%20Administration%20Guide.pdf?cb=1578909518 Luettu 9.4.2022.

14 Zerton käyttämät portit. 2022. Verkkoaineisto. Zerto. https://help.zerto.com/bundle/Prereq.MSP.HTML.90/page/Content/Cloud_SP_Guide/DRaaS_Architecture_Diagram_Showing_Ports.htm Luettu 9.4.2022.

15 vSRX IPsec tunnelin pystytys. 2020. Verkkoaineisto. Juniper Networks. https://www.juniper.net/documentation/us/en/software/vsrx/vsrx-consolidated-deployment-guide/vsrx-azure/topics/example/security-vsrx-example-azure-VPN.html Luettu 17.4.2022.

16 Zerton Bitmap synkronointi. 2022. Verkkoaineisto. Protos Techonologies. https://protostechnologies.com/blog/high-availability/is-your-vpg-bitmap-syncing-lots-of-data/ Luettu 1.5.2022.

17 Zerto Failover test toimenpide. 2022. Verkkoaineisto. Zerto https://help.zerto.com/bundle/Admin.VC.HTML.90/page/Content/AdminVC/The_Failover_Test_Operation.htm Luettu 5.5.2022.

18 Zerto Failover Live toimenpide. 2022. Verkkoaineisto. Zerto. https://help.zerto.com/bundle/Admin.VC.HTML.90/page/Content/AdminAzure/The_Failover_Live_Process.htm#failover_ma_3874202203_1026024 Luettu 5.5.2022.

19 Zerto Journal yleiskuva. 2016. Verkkoaineisto. Zerto. https://www.zerto.com/wp-content/uploads/2018/02/ZVR-Journal-Overview.pdf Luettu 5.5.2022.

20 Zerto kilpailijat. 2022. Verkkoaineisto. Zerto https://www.zerto.com/zerto-platform/how-zerto-compares/competitive-comparison/ Luettu 5.5.2022.

21 Zerto SQL vaatimukset. 2022. Verkkoaineisto. Zerto. https://help.zerto.com/bundle/Install.VC.HTML.90/page/Content/Install_ZVM-Hyper-V/Database_Requirements.htm Luettu 5.5.2022.

22 VMware NTP määrityksestä. 2021. Verkkoaineisto. VMware. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.vcenterhost.doc/GUID-8756D419-A878-4AE0-9183-C6D5A91A8FB1.html Luettu 5.5.2022.

Liitteet

Luotu testausympäristö

Liitteestä näkyy testausympäristön Site-A ja Site-B rakenne.