Toipumissuunnitelmat AWS-pilvipalvelussa

Riku Mannonen

Haaga-Helia ammattikorkeakoulu
Tradenomin tutkinto
Opinnäytetyö
2023

Tiivistelmä

Tekijä(t)
Riku Mannonen

Tutkinto
Tradenomi

Raportin/Opinnäytetyön nimi
Toipumissuunnitelmat AWS-pilvipalvelussa

Sivu- ja liitesivumäärä
31 + 24

Tämän toiminnallisen opinnäytetyön tavoitteena oli tuottaa opas, jossa AWS (Amazon Web Services) -pilvipalvelutarjoajan toipumissuunnitelma vaihtoehdoille, kaikki oleellisin käytännön ja teorian tieto, ovat saatavilla samassa paikassa. Opas on suunnattu ICT-alan opiskelijoille ja valmistuneille, joiden työnkuvaan ja opintoihin aihe liittyy.

Työn tietoperustassa käsiteltiin työhön liittyvät teemat ja käsitteet: pilvipalvelu, pilvipalvelun eri palvelumallit ja käyttöönoton mallit, AWS ja sen tähän työhön liittyvät keskeiset palvelut ja parhaat käytännöt. Lisäksi käsiteltiin toipumissuunnitelma ja siihen vaikuttavat seikat. Lopuksi käytiin läpi eri AWS:n tarjoamat suunnitelmavaihtoehdot.

Empiirisessä osassa suunniteltiin opas, jossa on kaksi osaa. Siinä kuvattiin oppaan tuottamiseen liittyvät asiat, siihen liittyvät vaiheet ja rajoittavat seikat. Oppaan 1. osa tuotettiin tekemällä AWS Well-Architected Labs -sivustolta löytyvät aiheeseen liittyvät harjoitukset. 2. osa tuotettiin itse tekemällä vastaavanlainen harjoitus. Lopullinen opas lisättiin liitteeksi tähän työhön.

Opas onnistui kohtalaisesti, siinä havaittiin, että se ei täysin noudata alan parhaita käytäntöjä. Valittu harjoittelusivusto osoittautui kuitenkin käteväksi ja edulliseksi harjoitusalustaksi. Opasta voi jatkokehittää lisäämällä automaatiota sekä lisäämällä manuaalisesti tehtävät vaiheet osaksi mallinteita.

Asiasanat
Cloud Computing, Public Cloud, Amazon Web Services, Disaster Recovery

Sisällys

1 Johdanto ... 1
1.1 Työn tavoitteet ja rajaus ... 2
1.2 Käsitteet ... 2
2 Pilvipalvelu ... 5
2.1 Pilvipalvelujen olennaiset ominaisuudet ... 5
2.2 Palvelumallit ... 6
2.3 Käyttöönoton mallit ... 7
3 Amazon Web Services ... 9
3.1 AWS palvelut ... 9
3.2 Jaetun vastuun malli ... 11
3.3 AWS ja parhaat käytännöt ... 12
4 Toipumissuunnitelma ... 15
4.1 Palautusaika ... 16
4.2 Palautuspiste ... 17
5 Toipumissuunnitelmavaihtoehdot AWS-pilvipalvelussa ... 18
5.1 Backup and restore ... 19
5.2 Pilot light ... 20
5.3 Warm standby ... 21
5.4 Hot standby / Multi-site active/active ... 23
5.5 AWS Elastic Disaster Recovery ... 24
6 Oppaan suunnittelu ja toteutus ... 26
6.1 Lähtötilanteen kuvaus ja suunnittelun esittely ... 26
6.2 Oppaan tuottamisen kuvaus ... 26
7 Pohdinta ... 28
Lähteet ... 29
Liitteet ... 32
Liite 1. Toipumissuunnitelmavaihtoehtojen toteuttaminen harjoitusympäristössä ... 32

1 Johdanto

Pilvipalvelu on tarvittaessa saatavissa olevien laskentapalvelujen, kuten palvelimien, tallennustilan, tietokantojen, ohjelmistojen, analytiikan ja tekoälyn, toimittamista Internetin kautta. Pilvipalvelu poistaa yrityksiltä tarpeen omistaa fyysisiä palvelimia tai infrastruktuuria tiloissa, jolloin ne voivat käyttää laskentaresursseja ja skaalata toimintaansa ylös tai alas tarpeen mukaan. (Mell & Grance 2011, 2)

Amazon Web Services (AWS) on pilvilaskenta-alusta, joka tarjoaa laajan valikoiman palveluita, kuten tietojenkäsittelyä, tallennusta ja tietokantoja, analytiikkaa, koneoppimista, tietoturvaa ja paljon muuta. AWS on Amazonin tytäryhtiö, ja se lanseerattiin vuonna 2006. (Amazon Web Services s.a. a.)

AWS on tärkeä, koska sen avulla kaikenkokoiset yritykset voivat käyttää tehokkaita laskentaresursseja, jotka olivat aiemmin vain suurten IT-budjetin omaavien suurten yritysten käytettävissä. AWS:n avulla yritykset voivat vähentää laitteisto- ja infrastruktuuri-investointejaan sekä juoksevia toimintakulujaan. AWS tarjoaa hinnoittelumallin, jonka avulla yritykset voivat maksaa vain käyttämistään resursseista, mikä tekee siitä edullisen vaihtoehdon startupeille ja pienyrityksille. (Amazon Web Services s.a. a.)

AWS tarjoaa myös korkean skaalautuvuuden, jonka avulla yritykset voivat nopeasti skaalata tai vähentää toimintaansa kysynnän mukaan. Tämä tekee siitä ihanteellisen ratkaisun yrityksille, jotka kokevat vaihtelevaa kysyntää tai jotka tarvitsevat nopeaa skaalausta toimintaansa. (Amazon Web Services s.a. a.)

Lisäksi AWS tarjoaa korkeatasoista luotettavuutta, turvallisuutta ja vaatimustenmukaisuutta. AWS:llä on useita datakeskuksia eri puolilla maailmaa, mikä varmistaa, että tiedot ovat aina saatavilla ja suojattu katkoksilta tai katastrofeilta. AWS noudattaa myös eri teollisuuden ja valtion säädöksiä, mikä tekee siitä sopivan hyvin säänneltyjen alojen, kuten terveydenhuollon ja rahoituksen, yrityksille. (Amazon Web Services s.a. a.)

Liiketoiminnan jatkuvuuden suunnittelu (BCP business continuity plan) ja toipumissuunnitelma (disaster recovery) ovat kaksi toisiinsa liittyvää mutta erillistä prosessia, jotka auttavat organisaatioita varautumaan odottamattomiin tapahtumiin, jotka voivat häiritä niiden normaalia toimintaa, ja reagoida niihin. (VMware s.a. a.)

Liiketoiminnan jatkuvuuden suunnitteluun kuuluu strategioiden ja menettelytapojen kehittäminen sen varmistamiseksi, että keskeiset liiketoiminnan toiminnot voivat jatkua häiriön tai katastrofin, kuten luonnonkatastrofin, kyberhyökkäyksen tai laitevian sattuessa. BCP sisältää toimenpiteitä, joilla

minimoidaan häiriön vaikutus liiketoimintaan, kuten vaihtoehtoisten työpaikkojen perustaminen, etätyöominaisuuksien käyttöönotto ja varatoimittajien ja -toimittajien tunnistaminen. (VMware s.a. a.)

Toipumissuunnitelma puolestaan keskittyy erityisesti kriittisten IT-järjestelmien ja infrastruktuurin palauttamiseen häiriön tai katastrofin jälkeen. Toipumissuunnitelma sisältää tietojen ja sovellusten varmuuskopioinnin, palautusprosessin testaamisen ja toimenpiteiden toteuttamisen sen varmistamiseksi, että järjestelmät voidaan palauttaa nopeasti ja tehokkaasti. (VMware s.a. a.)

1.1 Työn tavoitteet ja rajaus

Työn aiheena on toipumissuunnitelmat AWS-pilvipalvelussa. Halusin valita aiheen, joka liittyy pilvipalveluihin, koska se on olennaisen osa opiskeluani ja aion työskennellä niiden parissa tulevaisuudessa. Tästä aiheesta en löytänyt opinnäytetöitä, vaikka aihe on mielestäni tärkeä ja ajankohtainen, joten uskon sillä olevan tarvetta.

Valitsin pilvipalveluntarjoajan AWS:n ja Azuren väliltä. AWS valikoitui koska olen opiskellut sitä hieman enemmän ja koen osaavani sen peruspalvelut paremmin kuin Azuren. AWS:ltä löytyi myös laadukkaita artikkeleita tästä aiheesta.

Tässä työssä keskitytään ainoastaan AWS:n pilven sisällä tapahtuvaan palauttamiseen eli yhdeltä alueelta toiselle alueelle tapahtuvaan. Työn ulkopuolelle jää toipumissuunnitelmat toiseen julkipilveen tai yksityiseen pilveen sekä yrityksen omiin toimitiloihin (on-premises).

Työn tavoitteena on tuottaa opas, jossa oleellisin käytännön ja teorian tieto AWS:n toipumissuunnitelmavaihtoehdoista on pyritty sisällyttämään yhteen ja samaan paikkaan.

Työn tietoperustassa (luvut 2–5) käsitellään työhön liittyvät teemat ja käsitteet: pilvipalvelu, pilvipalvelun eri palvelumallit ja käyttöönoton mallit, Amazon Web Services ja sen tähän työhön liittyvät keskeiset palvelut, parhaat käytännöt ja toipumissuunnitelma ja AWS:n suunnitelmavaihtoehdot.

Empiirinen osa on luvussa 6. se sisältää lähtötilanteen kuvauksen ja suunnittelun esittelyn sekä oppaan tuottamisen kuvauksen. Lopullinen opas löytyy liitteenä.

1.2 Käsitteet

Toipumissuunnitelma (Disaster Recovery Plan) Tarkoittaa suunnitelmaa sovelluksien, resurssien ja datan varmuuskopioinnille, kun pilvipalveluntarjoajan käyttämä alue (region), jossa edellä mainitut asiat ovat, ei esimerkiksi luonnonkatastrofin takia ole saavutettavissa.

Luotettavuus Pilvessä tapahtuvassa katastrofipalautuksessa luotettavuudella tarkoitetaan pilvipalvelun tai -infrastruktuurin kykyä tarjota jatkuvasti ja ennustettavasti tarvittavaa palvelutasoa myös katastrofin tai käyttökatkon sattuessa.

Joustavuus Pilven katastrofipalautuksen yhteydessä joustavuus viittaa järjestelmän tai infrastruktuurin kykyyn ottaa vastaan häiriöt tai häiriöt ja mukautua niihin sekä jatkaa olennaisten palveluiden tarjoamista keskeytyksettä tai tietoja menettämättä**.**

Vikasiirto (Failover) Viittaa prosessiin, jossa sovellus tai työkuorma siirretään automaattisesti tai manuaalisesti ensisijaisesta järjestelmästä toissijaiseen järjestelmään vian tai käyttökatkon sattuessa. Vikasiirron tavoitteena on minimoida seisokit ja varmistaa, että sovellus tai työkuorma pysyy käytettävissä ja toimivana.

Työkuorma (Workload) Viittaa joukkoon ohjelmistosovelluksia ja infrastruktuurikomponentteja, jotka on otettu käyttöön yhdessä tietyn liiketoimintatoiminnon tai prosessin suorittamiseksi. Työkuorma voi sisältää laajan valikoiman komponentteja, kuten palvelimia, tietokantoja, tallennustilaa, verkkoa ja sovelluksia.

Alue (Region) AWS:ssä alue on maantieteellinen sijainti, jossa AWS on läsnä. Jokainen alue on erillinen maantieteellinen alue, jolla on useita palvelinkeskuksia, jotka on yhdistetty nopeisiin ja pienen viiveen verkkoihin. AWS-alueet on suunniteltu täysin eristetyiksi toisistaan ja tarjoavat itsenäisiä infrastruktuuria, palveluita ja hallintaliittymiä. (Amazon Web Services s.a. b.)

Saatavuusvyöhyke (Availability Zone) AWS:ssä saatavuusvyöhyke on eristetty datakeskus alueella, joka on suunniteltu erittäin käytettäviksi ja vikasietoiseksi. Jokainen vyöhyke koostuu yhdestä tai useammasta datakeskuksesta, jotka ovat fyysisesti erillään toisistaan ja jotka on yhdistetty nopeisiin, pienen latenssin verkkoihin. Saatavuusvyöhykkeiden ensisijainen tarkoitus on tarjota asiakkaille mahdollisuus ottaa käyttöön sovelluksia ja palveluita erittäin joustavalla tavalla. Jakamalla resursseja useille vyöhykkeille asiakkaat voivat varmistaa, että heidän sovelluksensa pysyvät saatavilla ja reagoivat myös vian tai katkoksen sattuessa yhden vyöhykkeen sisällä. Jokainen vyöhyke on suunniteltu olemaan riippumaton muista. (Amazon Web Services s.a. c.)

VPC (Virtual Private Cloud) AWS:ssä VPC on virtuaalinen verkko, jonka avulla voi käynnistää AWS-resursseja, kuten EC2-instansseja, RDS-tietokantoja ja Lambda-toimintoja, loogisesti eristetyssä AWS-pilven osassa. Kun luodaan VPC, voidaan määrittää sen IP-osoitealue, aliverkot ja reititystaulukot. Voidaan myös määrittää erilaisia sääntöjä ohjaamaan resursseihin tulevaa ja sieltä lähtevää liikennettä. (Amazon Web Services s.a. d.)

Instanssi Pilvipalveluissa instanssi on virtuaalinen laskentaympäristö, joka on luotu pilvipalveluntarjoajan infrastruktuuriin. Sitä voidaan pitää yhtenä yksikkönä laskentaresursseja, mukaan lukien CPU, muisti, tallennus ja verkko, jota voidaan käyttää sovelluksen tai palvelun suorittamiseen.

Infrastructure as Code (IaC) Infrastruktuuri koodina on koodin avulla määritellyn infrastruktuurin provisiointi- ja hallintaprosessi manuaalisen prosessin sijaan. Koska infrastruktuuri määritellään koodiksi, sen avulla käyttäjät voivat helposti muokata ja jakaa määrityksiä varmistaen samalla infrastruktuurin halutun tilan. (Merron & Wickramasinghe 2021)

Mallinne (Template) Infrastruktuuri koodina (IaC) yhteydessä mallinne viittaa deklaratiiviseen konfiguraatiotiedostoon tai komentosarjaan, joka määrittää järjestelmän tai infrastruktuurin halutun tilan. Sitä voidaan pitää suunnitelmana infrastruktuuriresurssien, kuten palvelimien, tallennustilan ja turvallisuuden, luomiseen ja hallintaan.

Replikointi Tietojen replikointi tarkoittaa prosessia, jossa luodaan ja ylläpidetään useita kopioita tiedoista eri paikoissa tai järjestelmissä. Tietojen replikoinnin ensisijainen tavoite on parantaa tietojen saatavuutta, luotettavuutta, vikasietoisuutta ja suorituskykyä.

Replika Viittaa tietojen kopioon, joka luodaan ja jota ylläpidetään eri paikassa tai tallennusjärjestelmässä kuin alkuperäiset tiedot.

Tietokatastrofi tarkoittaa tässä katastrofaalista tapahtumaa tai tilannetta, joka johtaa varmuuskopioiden korruptoitumiseen tai tuhoutumiseen.

2 Pilvipalvelu

Pilvilaskennalla tarkoitetaan mallia, joka mahdollistaa tarvittaessa ja helposti saatavilla olevan verkkoyhteyden jaettuun verkkoon, joka tarjoaa joukon konfiguroitavia laskentaresursseja (esim. verkot, palvelimet, tallennustila, sovellukset ja palvelut), jotka voidaan valmistaa ja julkaista nopeasti minimaalisella hallintatyöllä tai palveluntarjoajan vuorovaikutuksella. (Mell & Grance 2011, 2)

2.1 Pilvipalvelujen olennaiset ominaisuudet

Olennaisimmat pilvipalveluiden ominaisuudet ja hyödyt NIST:in (National Institute of Standard and Technology) mukaan ovat:

- **Vain tarvittaessa (on-demand)**: Kuluttaja voi yksipuolisesti tuottaa pilvilaskentaa hyödyntäviä palveluja kuten palvelimia ja tallennustilaa oman tarpeensa mukaan automaattisesti ja ilman vuorovaikutusta ihmisten ja palveluntarjoajan välillä.
- **Laaja verkkoyhteys**: Ominaisuudet ovat saatavilla verkon yli ja niihin pääsee standardimekanismeilla, jotka edistävät eri asiakasalustojen käyttöä (esim. matkapuhelimet, tabletit, kannettavat tietokoneet ja työasemat).
- **Resurssien jakaminen:** Palveluntarjoajan laskentaresurssit yhdistetään palvelemaan useita kuluttajia usean vuokralaisen mallin avulla, ja erilaisia fyysisiä ja virtuaalisia resursseja kohdistetaan dynaamisesti ja jaetaan uudelleen kuluttajien kysynnän mukaan. Sijainnista riippumattomuus tarkoittaa sitä, että asiakkaalla ei yleensä ole hallintaa tai tietoa toimitettujen resurssien tarkasta sijainnista, mutta hän saattaa pystyä määrittämään sijainnin korkeammalla abstraktiotasolla (esim. maa, osavaltio tai tietokeskus). Esimerkkejä resursseista ovat tallennus, käsittely, muisti ja verkon kaistanleveys.
- **Joustavuus:** Ominaisuudet voidaan joustavasti varata ja vapauttaa, joissain tapauksissa automaattisesti, skaalautuakseen nopeasti ulospäin ja sisäänpäin kysynnän mukaan. Kuluttajalle tarjontaan käytettävissä olevat ominaisuudet näyttävät usein olevan rajattomat ja niitä voidaan ottaa käyttöön missä tahansa määrässä milloin tahansa.
- **Monitorointi ja mittaaminen:** Pilvijärjestelmät ohjaavat ja optimoivat resurssien käyttöä automaattisesti hyödyntämällä mittauskykyä jollakin palvelutyyppiin sopivalla abstraktiotasolla (esim. tallennus, käsittely, kaistanleveys ja aktiiviset käyttäjätilit). Resurssien käyttöä voidaan seurata, hallita ja raportoida, mikä tuo läpinäkyvyyttä sekä käytetyn palvelun tarjoajalle että kuluttajalle.

(Mell & Grance 2011, 2)

2.2 Palvelumallit

Infrastructure as a service (IaaS): Kuluttajalle tarjotaan prosessointia, tallennusta, verkkoja ja muita perustavanlaatuisia laskentaresursseja, joissa kuluttaja voi ottaa käyttöön ja käyttää mielivaltaisia ohjelmistoja, jotka voivat sisältää käyttöjärjestelmiä ja sovelluksia. Kuluttaja ei hallitse tai ohjaa taustalla olevaa pilvi-infrastruktuuria, mutta hänellä on hallinnan käyttöjärjestelmät, tallennustila ja käyttöönotetut sovellukset ja mahdollisesti rajoitettu tiettyjen verkkokomponenttien hallinta (esim. isäntäpalomuurit). (Mell & Grance 2011, 2)

IaaS tarkoittaa siis sitä, että palveluntarjoaja vastaa palvelimista, tiedon varastoinnista, virtualisoinnista ja verkosta. Käyttäjä vastaa lopusta. Mallissa käyttäjälle siis tarjotaan ulkoistettua laskentatehoa ja tallennustilaa jättäen käyttäjälle kuitenkin paljon pelivaraa. (Berg 2021)

Toipumiseen liittyen asiakkaat voivat käyttää IaaS-palveluita tietojen ja sovellusten varmuuskopiointi- ja palautusprosessien luomiseen ja hallintaan. He voivat myös hyödyntää AWS-palveluita, kuten Amazon S3, Amazon Glacier ja Amazon EBS tietojen varmuuskopiointiin ja palauttamiseen. (Amazon Web Services s.a. e.)

Platform as a service (PaaS): mallissa voi ottaa käyttöön pilvi-infrastruktuuriin kuluttajien luomia tai hankkimia sovelluksia, jotka on luotu palveluntarjoajan tukemilla ohjelmointikielillä, kirjastoilla, palveluilla ja työkaluilla. Kuluttaja ei hallitse tai ohjaa taustalla olevaa pilvi-infrastruktuuria, mukaan lukien verkkoa, palvelimia, käyttöjärjestelmiä tai tallennustilaa, mutta hänellä on hallinnassa käytössä olevat sovellukset ja mahdollisesti sovellusisännöintiympäristön asetukset. (Mell & Grance 2011, 2)

PaaS tarkoittaa siis palvelualustan ulkoistamista. PaaS malli toimii IaaS-mallin ”päällä” eli se tarjoaa kaiken minkä IaaS. PaaS on suunnattu kehittäjille. (Butler 2013)

Toipumiseen liittyen asiakkaat voivat automatisoida sovellusten käyttöönotto- ja palautusprosesseja PaaS palveluiden avulla. AWS-palveluilla, kuten AWS CloudFormationilla, voidaan luoda infrastruktuurimallinteita, jotka voidaan ottaa nopeasti käyttöön toisella alueella katastrofin sattuessa. (Amazon Web Services s.a. e.)

Software as a service (SaaS): mallissa voi käyttää palveluntarjoajan pilvi-infrastruktuurissa toimivia sovelluksia. Sovellukset ovat käytettävissä eri asiakaslaitteilta joko ohuen asiakasrajapinnan, kuten verkkoselaimen (esim. web-pohjainen sähköposti), tai ohjelmaliittymän kautta. Kuluttaja ei hallitse taustalla olevaa pilvi-infrastruktuuria, mukaan lukien verkkoa, palvelimia, käyttöjärjestelmiä, tallennustilaa tai edes yksittäisiä sovellusominaisuuksia, lukuun ottamatta mahdollisesti rajoitettuja käyttäjäkohtaisia sovelluskokoonpanoasetuksia. (Mell & Grance 2011, 2)

SaaS tarkoittaa siis IaaS ja PaaS mallien päälle rakennettua valmista palvelua, jossa käyttäjän tarvitsee vain konfiguroida palvelun asetukset ja pitää huolta käyttämästään datasta. (Turner 2020).

Toipumiseen liittyen AWS huolehtii kaikesta, mukaan lukien tietojen varmuuskopiointi, replikointi ja palautus. Asiakkaat voivat luottaa siihen, että AWS tarjoaa SaaS-sovelluksilleen korkean käytettävyyden ja vikasietoisuuden. (Amazon Web Services s.a. e.)

Kuvassa 1 kiteytetään näiden kolmen palvelumallin vastuut ja miten ne vertautuvat perinteiseen IT-ympäristöön.

Kuva 1 Mikä on palveluntarjoajan vastuulla (IBM 2021)

Disaster Recovery as a service (DRaaS) on pilvilaskentapalvelumalli, jonka avulla organisaatio voi varmuuskopioida tietonsa ja IT-infrastruktuurinsa kolmannen osapuolen pilvilaskentaympäristöön ja tarjota kaiken orkestroinnin toipumissuunnitelmalle, kaikki SaaS-ratkaisun kautta, jotta se voi saada takaisin pääsyn ja toiminnallisuuden IT-infrastruktuuriin katastrofin jälkeen. Palvelumalli tarkoittaa, että organisaation ei itse tarvitse omistaa kaikkia resursseja tai hoitaa kaikkea hallintaa katastrofipalautuksessa, vaan luottaa palveluntarjoajaan. (VMware s.a. b.)

2.3 Käyttöönoton mallit

Pilvipalvelun käyttöönottamiseen on valittavissa neljä erilaista pilvityyppiä.

Yksityinen pilvi on tarkoitettu yksinomaiseen käyttöön yhdelle organisaatiolle, joka koostuu useista kuluttajista (esim. liiketoimintayksiköistä). Sen voi omistaa, hallinnoida ja ylläpitää organisaatio, kolmas osapuoli tai jokin näiden yhdistelmä, ja se voi olla toimitiloissa tai sen ulkopuolella. (Mell & Grance 2011, 2)

Yhteisö pilvi on tarkoitettu yksinomaiseen käyttöön tietylle kuluttajayhteisölle organisaatioista, joilla on samat huolenaiheet (esim. tehtävä, turvallisuusvaatimukset, käytännöt ja vaatimustenmukaisuusnäkökohdat). Se voi olla yhden tai useamman yhteisön organisaation, kolmannen osapuolen tai niiden yhdistelmän omistuksessa, hallinnoinnissa ja toiminnassa, ja se voi esiintyä tiloissa tai sen ulkopuolella. (Mell & Grance 2011, 2)

Julkinen pilvi on tarkoitettu suuren yleisön avoimeen käyttöön. Sen voi omistaa, hallinnoida ja ylläpitää yritys, akateeminen tai valtion organisaatio tai jokin näiden yhdistelmä. Se on olemassa pilvipalvelun tarjoajan tiloissa. (Mell & Grance 2011, 2)

Hybridi pilvi on yhdistelmä kahdesta tai useammasta erillisestä pilvi-infrastruktuurista (yksityinen, yhteisöllinen tai julkinen), jotka pysyvät ainutlaatuisina kokonaisuuksina, mutta joita yhdistää standardoitu tai patentoitu teknologia, joka mahdollistaa tietojen ja sovellusten siirrettävyyden (esim. kuormituksen tasaamisen). (Mell & Grance 2011, 2)

3 Amazon Web Services

Amazon Web Services (AWS) on maailman kattavin ja laajimmin käytetty pilvipalvelu, joka tarjoaa yli 200 täysin varusteltua palvelua datakeskuksistaan maailmanlaajuisesti. (Amazon Web Services s.a. a.)

Amazon on ollut jo pitkään hallitseva pilvimarkkinoiden markkinajohtaja, AWS omaa kolmanneksen maailman kokonaispilvimarkkinoista vuoden 2022 viimeisellä neljänneksellä. (Haranas 2023)

3.1 AWS palvelut

AWS tarjoaa lukemattoman määrän erilaisia palveluja. Tässä esitellään niitä, jotka ovat tässä työssä olennaisimpia.

Amazon Elastic Compute Cloud (Amazon EC2) tarjoaa skaalautuvaa laskentakapasiteettia Amazon Web Services (AWS) -pilvessä. Amazon EC2:n käyttäminen eliminoi tarpeen investoida laitteistoon etukäteen, joten voidaan kehittää ja ottaa sovelluksia käyttöön nopeammin. Amazon EC2:ta voidaan käyttää käynnistämään niin monta virtuaalipalvelinta kuin tarvitaan. Amazon EC2:n avulla palvelinten määrää voidaan skaalata ylös tai alas vaatimuksen tai kysynnän mukaan, mikä vähentää tarvetta ennustaa liikennettä. (Amazon Web Services s.a. f.)

Amazon Simple Storage Service (Amazon S3) on tallennuspalvelu, joka tarjoaa skaalautuvuutta, saatavuutta, turvallisuutta ja suorituskykyä. Kaikenkokoiset ja eri toimialojen asiakkaat voivat käyttää Amazon S3:a tallentaakseen ja suojatakseen minkä tahansa datamäärän erilaisiin käyttötarkoituksiin, kuten datajärviin, verkkosivustoihin, mobiilisovelluksiin, varmuuskopiointiin ja palautukseen, arkistointiin, yrityssovelluksiin, IoT-laitteisiin ja suuraineiston analytiikkaan. Amazon S3 tarjoaa hallintaominaisuuksia, joiden avulla voidaan optimoida, järjestää ja määrittää pääsy tietoihin vastaamaan erityisiä liiketoiminta-, organisaatio- ja vaatimustenmukaisuusvaatimuksia. (Amazon Web Services s.a. g.)

Amazon Relational Database Service (Amazon RDS) on verkkopalvelu, joka helpottaa relaatiotietokannan määrittämistä, käyttöä ja skaalaamista AWS-pilvessä. Se tarjoaa kustannustehokasta, kokoa muutettavaa kapasiteettia alan standardinmukaiselle relaatiotietokannalle ja hallitsee yleisiä tietokannan hallintatehtäviä. (Amazon Web Services s.a. h.)

AWS Backup on täysin hallittu (fully-managed) palvelu, jonka avulla on helppo keskittää ja automatisoida tiedon suojaaminen AWS-palveluissa, pilvessä ja omissa konesaleissa (on-prem). Tämän palvelun avulla voidaan määrittää varmuuskopiointikäytännöt ja seurata AWS-resurssien

toimintaa yhdessä paikassa. Sen avulla voidaan automatisoida varmuuskopiointitehtävät. (Amazon Web Services s.a. i.)

Amazon Aurora (Aurora) on täysin hallittu relaatiotietokanta, joka on yhteensopiva MySQL:n ja PostgreSQL:n kanssa. Koodia, työkaluja ja sovelluksia, joita käytetään nykyisin olemassa olevien MySQL- ja PostgreSQL-tietokantojen kanssa, voidaan käyttää Auroran kanssa. Joillakin työkuormilla Aurora pystyy toimittamaan jopa viisinkertaisen suorituskyvyn kuin MySQL ja jopa kolme kertaa suuremman kuin PostgreSQL ilman, että useimpiin olemassa oleviin sovelluksiin tarvitsee tehdä muutoksia. (Amazon Web Services s.a. j.)

Aurora sisältää tehokkaan tallennusalijärjestelmän. Sen MySQL- ja PostgreSQL-yhteensopivat tietokantamoottorit on räätälöity hyödyntämään tätä nopeaa hajautettua tallennustilaa. Taustalla oleva tallennustila kasvaa automaattisesti tarpeen mukaan. Aurora myös automatisoi ja standardoi tietokantojen klusteroinnin ja replikoinnin, jotka ovat tyypillisesti tietokannan konfiguroinnin ja hallinnan haastavimpia puolia. (Amazon Web Services s.a. j.)

Elastic Load Balancing jakaa saapuvan liikenteen automaattisesti useille kohteille, kuten EC2-instansseille, konteille ja IP-osoitteille, yhdelle tai useammalle saatavuusalueelle. Se tarkkailee rekisteröityjen kohteidensa tilaa ja reitittää liikenteen vain terveisiin kohteisiin. Elastic Load Balancing skaalaa kuormantasaajan kapasiteetin automaattisesti vastauksena saapuvan liikenteen muutoksiin. (Amazon Web Services s.a. k.)

Amazon EC2 Auto Scaling auttaa varmistamaan, että on käytettävissä oikea määrä Amazon EC2 -instansseja sovelluksen kuormituksen käsittelemiseen. Tämän avulla luodaan EC2-instanssien kokoelmia, joita kutsutaan automaattisiksi skaalausryhmiksi (auto scaling groups). Instanssien vähimmäismäärä voidaan määrittää kussakin Auto Scaling -ryhmässä, ja Amazon EC2 Auto Scaling varmistaa, että ryhmä ei koskaan alita tätä kokoa. Instanssien enimmäismäärä voidaan määrittää kussakin Auto Scaling -ryhmässä, ja Amazon EC2 Auto Scaling varmistaa, että ryhmä ei koskaan ylitä tätä kokoa. Kun haluttu kapasiteetin määrä asetetaan joko ryhmän luomisen yhteydessä tai milloin tahansa sen jälkeen, Amazon EC2 Auto Scaling varmistaa, että ryhmässä on niin monta instanssia. Jos skaalauskäytännöt on määritelty, Amazon EC2 Auto Scaling voi käynnistää tai lopettaa instansseja, kun sovelluksen kysyntä kasvaa tai vähenee. (Amazon Web Services s.a. l.)

AWS CloudFormation on palvelu, jonka avulla voit mallintaa ja määrittää AWS-resursseja, jotta voi käyttää vähemmän aikaa resurssien hallintaan. Ideana on luoda mallinne, joka kuvaa kaikki haluttavat AWS-resurssit (kuten Amazon EC2 -instanssit tai Amazon RDS DB -tietokanta), ja CloudFormation huolehtii näiden resurssien luomisesta ja määrittämisestä käyttäjän puolesta. Näin ei tarvitse erikseen luoda ja määrittää AWS-resursseja ja selvittää, mikä riippuu mistä;

CloudFormation hoitaa sen. CloudFormationia voi käyttää, kun halutaan yksinkertaistaa infrastruktuurin hallintaa, monistaa infrastruktuuri nopeasti (esim. toiselle alueelle), tai hallita ja seurata infrastruktuurin muutoksia helposti. (Amazon Web Services s.a. m.)

Amazon CloudFront on verkkopalvelu, joka nopeuttaa staattisen ja dynaamisen verkkosisällön, kuten html-, css-, js- ja kuvatiedostojen, jakelua käyttäjille. CloudFront toimittaa sisällön maailmanlaajuisen datakeskusten verkoston kautta, jota kutsutaan reunapaikoiksi (edge locations). Kun käyttäjä pyytää sisältöä, jota tarjotaan CloudFrontilla, pyyntö reititetään reunasijaintiin, joka tarjoaa pienimmän viiveen, jotta sisältö toimitetaan parhaalla mahdollisella suorituskyvyllä. (Amazon Web Services s.a. n.)

3.2 Jaetun vastuun malli

Turvallisuuden ja vaatimustenmukaisuuden noudattaminen on pilvipalveluntuottajan ja asiakkaan yhteisellä vastuulla. Shared Responsibility Model määrittää sen mitkä ovat pilvipalveluntuottajan vastuulla ja mitkä ovat asiakkaan vastuulla. (Alvarenga 2022)

Resilienssi on AWS:n ja asiakkaan, yhteinen vastuu (kuva 2). On tärkeää, että ymmärretään, kuinka toipumissuunnitelma ja korkea käytettävyys ovat osana kestävyyttä ja miten ne toimivat tässä jaetussa mallissa. (Amazon Web Services 2021)

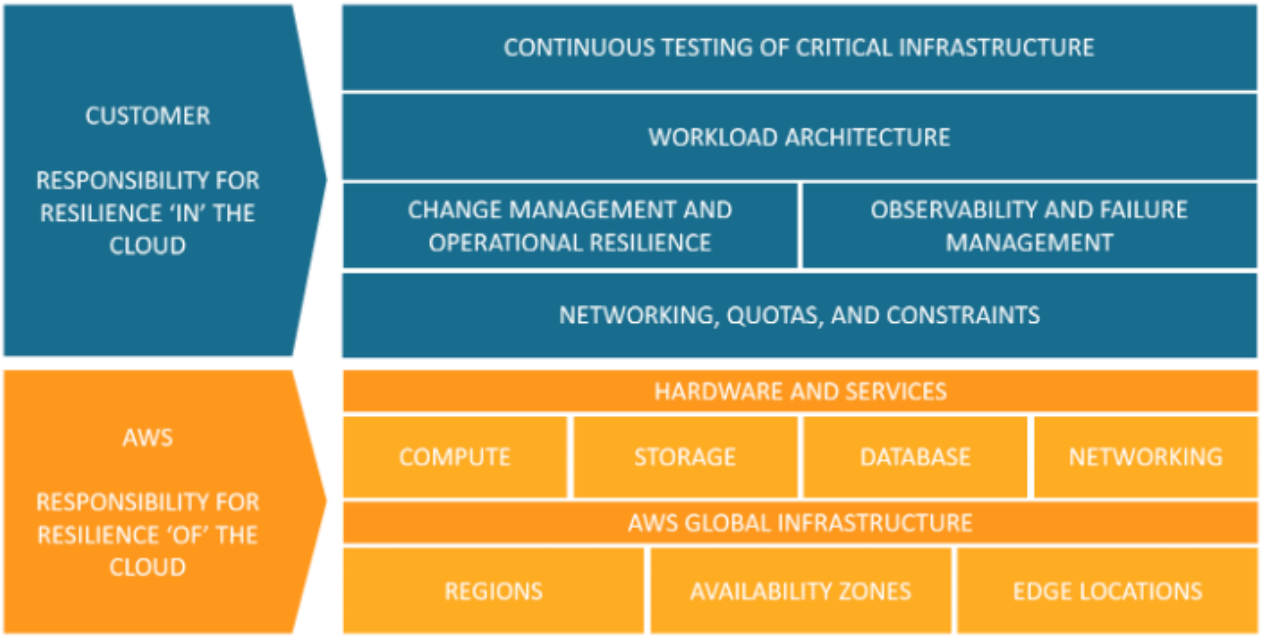
AWS vastaa infrastruktuurin kestävyydestä, joka ylläpitää kaikkia AWS-pilven palveluita. Tämä infrastruktuuri sisältää laitteistot, ohjelmistot, verkot ja tilat, jotka käyttävät AWS-pilvipalveluita (kuva 2). AWS käyttää kaupallisesti kohtuullisia toimia saattaakseen nämä AWS-pilvipalvelut saataville ja varmistaa, että palvelun saatavuus täyttää tai ylittää AWS-palvelutason sopimukset (SLA). (Amazon Web Services 2021)

SLA (service level agreement) eli palvelutasosopimus on palvelun tarjoajan ja käyttäjän välinen sopimus, jossa määritellään käyttäjälle hyväksyttävän vähimmäispalvelun määrä. (Hiles 2002, 6). AWS tarjoaa 99,99 %:n käytettävyyden palvelutasosopimuksen resursseille, jotka on otettu käyttöön useilla saatavuusvyöhykkeillä yhdellä alueella. (Amazon Web Services 2023)

Asiakkaan vastuu määräytyy valittujen AWS-pilvipalveluiden mukaan. Tämä määrittää konfigurointityön määrän, joka on asiakkaan vastuulla (kuva 2). Esimerkiksi Amazon Elastic Compute Cloud (Amazon EC2) -palvelu vaatii asiakkaan suorittamaan kaikki tarvittavat resilienssiin vaikuttavat määritys- ja hallintatehtävät. Asiakkaat, jotka ottavat käyttöön Amazon EC2 -instansseja, ovat vastuussa EC2-instanssien käyttöönotosta useissa saatavuusvyöhykkeissä, tarvittavien korvauksien toteuttamisesta AWS Auto Scaling -palvelun kaltaisten palveluiden avulla sekä joustavan työkuorma-arkkitehtuurin parhaiden käytäntöjen käyttämisestä instansseille asennetuille sovelluksille.

Hallittujen palveluiden, kuten Amazon S3:n ja Amazon DynamoDB:n, osalta AWS käyttää infrastruktuurikerrosta, käyttöjärjestelmää ja alustoja, ja asiakkaat pääsevät päätepisteisiin tallentaakseen ja hakeakseen tietoja. Asiakas on vastuussa tietojen resilienssin hallinnasta, mukaan lukien varmuuskopiointi-, versiointi- ja replikointistrategiat. (Amazon Web Services 2021)

Työkuorman sijoittaminen useille saatavuusvyöhykkeille AWS-alueella on osa korkean käytettävyyden strategiaa, joka on suunniteltu suojaamaan työkuormia eristämällä ongelmat yhteen saatavuusvyöhykkeeseen ja käyttää muiden saatavuusvyöhykkeiden redundanssia jatkaakseen pyyntöjen käsittelyä. Useiden saatavuusvyöhykkeiden käyttäminen on myös osa toipumissuunnitelmaa, joka on suunniteltu eristämään työmäärät paremmin ja suojaamaan niitä ongelmilta, kuten sähkökatkoilta, salamaniskuilta, tornadoilta, maanjäristyksiltä ja muilta. Toipumissuunnitelmissa voidaan myös käyttää useita AWS-alueita. Esimerkiksi aktiivisessa/passiivisessa tavassa työkuorman palvelu siirtyy aktiiviselta alueelta passiiviselle alueelle, joka toimii ”toipumisalueena”, jos aktiivinen alue ei voi enää palvella pyyntöjä. (Amazon Web Services 2021)



Kuva 2 Jaetun vastuun malli resilienssille (Amazon Web Services 2021)

3.3 AWS ja parhaat käytännöt

AWS Well-Architected Framework auttaa pilviarkkitehtejä rakentamaan turvallista, tehokasta, joustavaa ja tehokasta infrastruktuuria erilaisille sovelluksille ja työkuormille. Se kuvaa keskeisiä käsitteitä, suunnitteluperiaatteita ja arkkitehtonisia parhaita käytäntöjä työkuormien suunnittelussa ja

suorittamisessa pilvessä. Framework koostuu kuudesta pilarista – toiminnallinen erinomaisuus, tietoturva, luotettavuus, suoritustehokkuus, kustannusten optimointi ja kestävyys – AWS Well-Architected Framework tarjoaa asiakkaille ja kumppaneille johdonmukaisen lähestymistavan arkkitehtuurien arvioimiseen ja skaalautuvien suunnitelmien toteuttamiseen. (Amazon Web Services s.a. o.)

Reliability – luotettavuus kattaa työmäärän kyvyn suorittaa aiottu toiminto oikein ja johdonmukaisesti, kun sen odotetaan toimivan. Tämä sisältää kyvyn käyttää ja testata työtaakkaa sen koko elinkaaren ajan. (Eliot & Valverde 2018) Suunnittelun periaatteet ja parhaat käytännöt Eliotin ja Valverden mukaan ovat.

Suunnittelun periaatteet

- Epäonnistumisesta palautuminen automaattisesti
- Palautusmenettelyjen testaaminen
- Skaalaa horisontaalisesti kokonaistyökuorman saatavuuden lisäämiseksi
- Kapasiteetin arvailun lopettaminen
- Muutosten hallitseminen automaation avulla

Parhaat käytännöt

- Luotettavuuteen vaikuttavat perustavanlaatuiset vaatimukset pitäisi olla olemassa
- Täytetään riittävät verkko- ja laskentakapasiteetin vaatimukset, jolloin voidaan vapaasti muuttaa resurssin kokoa ja varauksia tarpeen mukaan
- Luotettavuuden vuoksi on noudatettava tiettyjä malleja, kuten löyhästi kytketyt riippuvuudet, graceful degradation ja yritysten rajoittaminen (limiting retries)
- Työkuormaan tai sen ympäristöön tehtävät muutokset on ennakoitava ja niihin on mukauduttava, jotta työkuorma toimisi luotettavasti. Muutokset sisältävät työmäärää koskevia muutoksia, kuten kysynnän piikit, sekä sisäisiä muutoksia, kuten ominaisuuksien käyttöönotot ja tietoturvakorjaukset
- Tarvittavat toimenpiteet työkuorman joustavuuden toteuttamiseksi, kuten vikojen eristäminen, automaattinen vikasiirto terveisiin resursseihin ja toipumissuunnitelmastrategia katastrofia varten

(Eliot & Valverde 2018)

AWS Well-Architected Labs on ohjelma, joka tarjoaa joukon käytännön työpajoja, opetusohjelmia ja harjoituksia, joiden avulla asiakkaat oppivat suunnittelemaan ja käyttämään työkuormaa AWS:ssä parhaiden käytäntöjen avulla. Nämä laboratoriot on suunniteltu auttamaan asiakkaita ymmärtämään AWS Well-Architected Frameworkia, joka tarjoaa joukon parhaita käytäntöjä ja ohjeita

luotettavien, turvallisten, tehokkaiden ja kustannustehokkaiden pilvijärjestelmien suunnitteluun ja käyttöön. (Amazon Web Services s.a. p.)

AWS Well-Architected Labs tarjoaa vaiheittaiset ohjeet AWS-työkuormien suunnitteluun, rakentamiseen ja optimointiin käyttämällä Well-Architected Frameworkia. Laboratoriot kattavat useita aiheita, kuten turvallisuutta, luotettavuutta, suorituskykyä, kustannusten optimointia ja toiminnan erinomaisuutta. Jokainen laboratorio toimii omatoimisesti ja sisältää yksityiskohtaiset ohjeet ja resurssit, mukaan lukien esimerkkikoodin, dokumentaation ja video-opetusohjelmat. (Amazon Web Services s.a. p.)

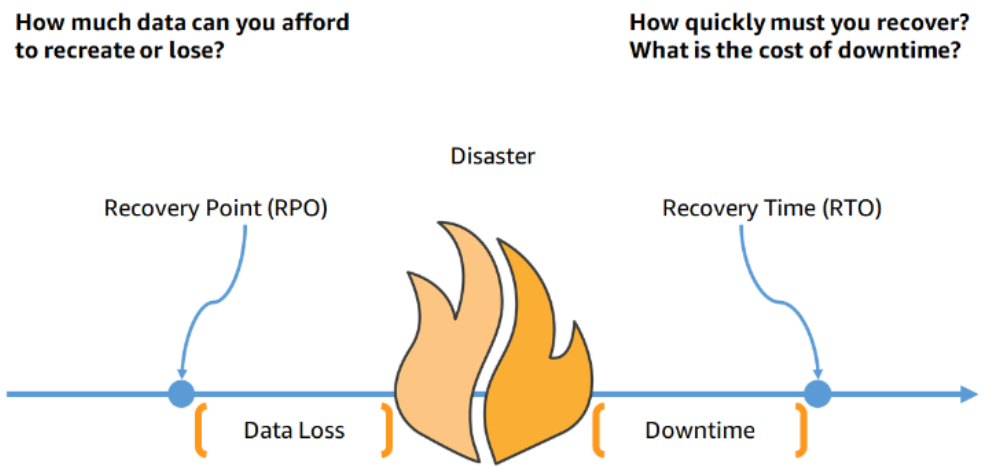
4 Toipumissuunnitelma

Jatkuvuuden hallinnassa on kyse siitä, että järjestelmien kyky kestää katkoja ja niihin liittyvät tukijärjestelyt pyritään mitoittamaan organisaation tarpeiden mukaiseksi. Tähän liittyy mm. sen arvioiminen, millaisia katkoja organisaatio hyväksyy. Lisäksi voidaan arvioida, miten hyvin järjestelmät sietävät erilaisia häiriöitä ja mitä häiriöistä seuraisi. Usein tällaiset pohdinnat liittyvät Disaster Recovery -suunnitelmien tekemiseen tai ainakin Disaster Recovery -valmiuksien arvioimiseen. (Wallenius 2022)

Toipumissuunnitelma on organisaation tapa saada takaisin pääsy ja toiminnallisuus IT-infrastruktuuriinsa tapahtumien, kuten luonnonkatastrofin tai kyberhyökkäyksen liittyvien liiketoimintahäiriöiden jälkeen. (VMware s.a. a.)

Toipumissuunnitelma perustuu tietojen ja tietokoneen käsittelyn replikointiin muualla kuin toimitiloissa, joihin katastrofi ei vaikuttanut. Kun palvelimet kaatuvat luonnonkatastrofin, laitevian tai kyberhyökkäyksen vuoksi, yrityksen on palautettava kadonneet tiedot toisesta paikasta, johon tiedot varmuuskopioidaan. Ihannetapauksessa organisaatio voi siirtää tietokoneen käsittelyn myös kyseiseen etäsijaintiin toiminnan jatkamiseksi. (VMware s.a. a.)

Luodessaan toipumissuunnitelmaa organisaatiot suunnittelevat useimmiten palautusaikatavoitteen (RTO) ja palautuspistetavoitteen (RPO) (kuva 3).

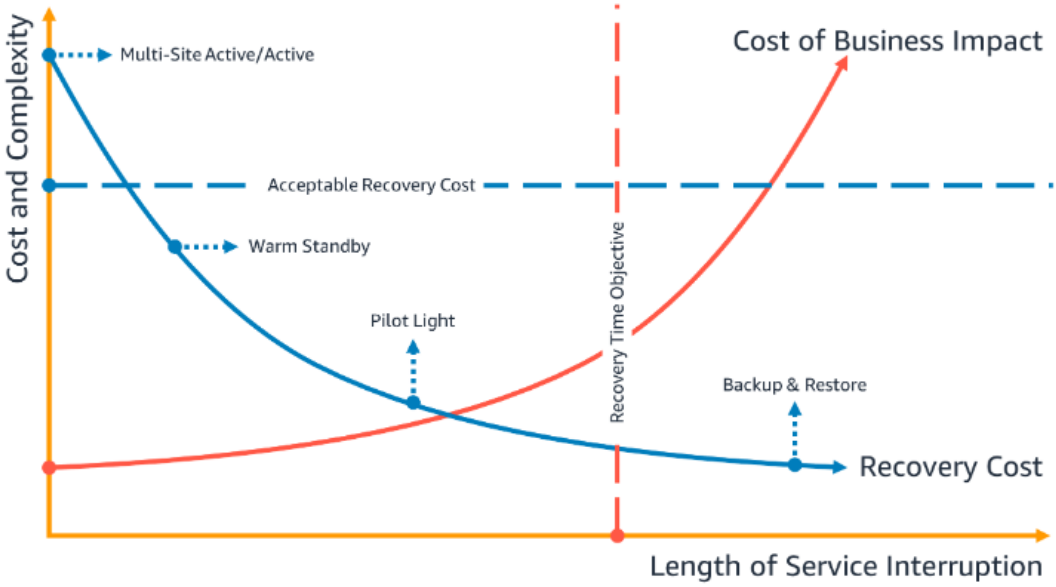


Kuva 3 Palautusaika ja palautuspiste (Amazon Web Services 2021)

4.1 Palautusaika

Palautusaika on suurin hyväksyttävä viive palvelun keskeytyksen ja palvelun palauttamisen välillä. Tämä tavoite määrittää, mitä pidetään hyväksyttävänä ajanjaksona, kun palvelu ei ole saatavilla, ja sen määrittelee organisaatio. (Amazon Web Services 2021)

Palautusaika määrittelee siis ajan, jonka kuluessa kyseessä oleva asia tai toiminto tulee saada palautettua ennalleen. Aika voidaan ilmoittaa sekunteina, minuutteina, tunteina tai vuorokausina. Palautusaika kertoo siis ajan, jonka sisällä järjestelmän pitäisi toipua ongelmasta. Palautusaika ei kuitenkaan ole ehdoton takaraja toipumiselle vaan ennemminkin tavoite. Palautusaikaa voidaan käyttää apuna esimerkiksi SLA-vaatimusten määrittelyssä. (Wallenius 2022)



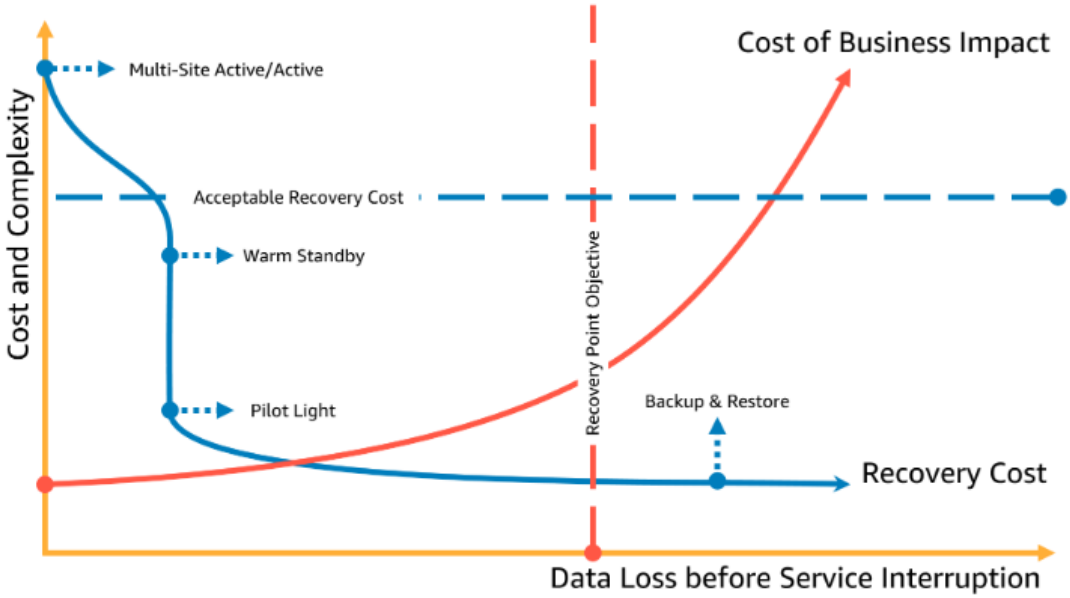
Kuva 4 Palautusaika ja toipumisvaihtoehdot (Amazon Web Services 2021)

Kuvassa 4 havainnoidaan suunnitelman valintaperustetta, kun tekijöinä on palauttamiseen vaadittava aika ja kustannukset. Sininen ja punainen suoraviiva kuvaa suurinta hyväksyttävää aikaa ja kustannuksia. Tässä hyväksyttyjä vaihtoehtoja ovat Warm Standby ja Pilot Light, joista Warm Standby omaa lyhyemmän palautusajan, mutta suuremmat kustannukset ja Pilot Light kohdalla toisinpäin.

4.2 Palautuspiste

Palautuspiste on suurin sallittu aika viimeisestä tietojen palautuspisteestä. Tämä tavoite määrittää, mikä katsotaan hyväksyttäväksi tietojen katoamiseksi viimeisen palautuspisteen ja palvelun keskeytyksen välillä, ja organisaatio määrittelee sen. (Amazon Web Services 2021)

Palautuspiste kertoo sen pisteen, johon järjestelmä pitäisi pystyä palauttamaan, jos sitä kohtaa häiriö. Palautuspiste ilmoitetaan yleensä sekunteina, minuutteina tai tunteina. Palautuspiste kertoo, miten paljon dataa saa hävitä, jos häiriö ilmenee juuri ennen seuraavan varmuuskopion ottamista. Käytännössä palautuspiste siis kertoo sen, miten usein järjestelmän tila halutaan varmistaa esimerkiksi varmuuskopioimalla. Palautuspiste on käyttökelpoinen termi, kun suunnitellaan esimerkiksi varmuuskopioinnin käytäntöjä. Miten usein järjestelmästä pitää ottaa varmuuskopioita? Jos järjestelmän palautuspiste on tiedossa, varmuuskopiointikäytäntöjen suunnittelu on helpompaa. (Wallenius 2022)



Kuva 5 Palautuspiste ja toipumisvaihtoehdot (Amazon Web Services 2021)

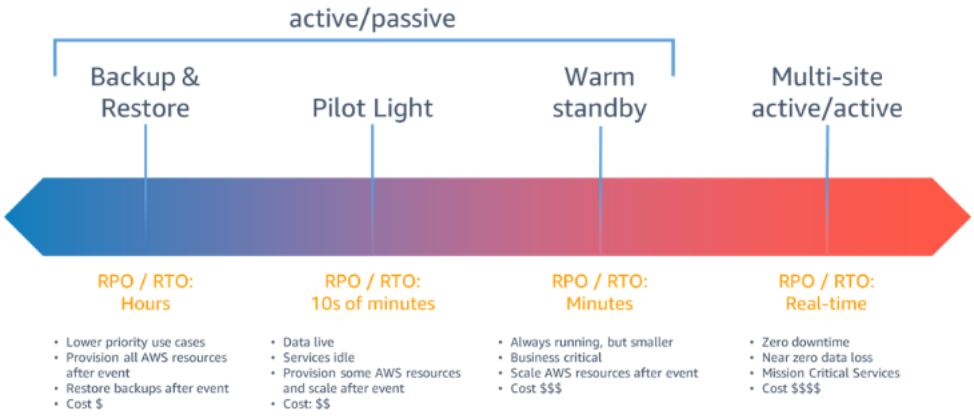
Kuvassa 5 havainnoidaan suunnitelman valintaperustetta, kun tekijöinä on menetettävän tiedon määrä ja kustannukset. Sininen ja punainen suoraviiva kuvaa suurinta hyväksyttävää tiedon määrän menettämistä ja kustannuksia. Tässäkin hyväksyttyjä vaihtoehtoja ovat Warm Standby ja Pilot Light, joissa molemmissa palautuspiste on sama ja menetettävää tietoa yhtä paljon. Erona on, että Warm Standby on kalliimpi kuin Pilot Light.

5 Toipumissuunnitelmavaihtoehdot AWS-pilvipalvelussa

AWS:ssä käytettävissä olevat toipumissuunnitelmavaihtoehdot voidaan luokitella neljään lähestymistapaan (kuva 6), jotka vaihtelevat varmuuskopioiden ottamisesta monimutkaisempiin strategioihin, joissa käytetään useita aktiivisia alueita. Aktiiviset/passiiviset strategiat käyttävät aktiivista sivustoa (tietty AWS-alue) isännöimään työkuormaa ja palvelemaan liikennettä. Passiivista sivustoa (eri AWS-alue) käytetään palautukseen. Passiivinen sivusto ei palvele liikennettä aktiivisesti ennen kuin vikasiirtotapahtuma käynnistetään. (Amazon Web Services 2021)

Katastrofitapahtumassa, joka perustuu yhden fyysisen tietokeskuksen häiriintymiseen tai menettämiseen, saatetaan vaatia vain varmuuskopiointi- ja palautusmenetelmä katastrofipalautukseen. Jos määritelmä katastrofista menee pidemmälle kuin fyysisen datakeskuksen häiriintyminen tai menettäminen alueen vastaavaan tai jos sitä edellyttävien lakisääteisten vaatimusten alainen, tulee harkita vaihtoehtoja Pilot Light, Warm Standby tai Multi-Site Active / Active. (Amazon Web Services 2021)

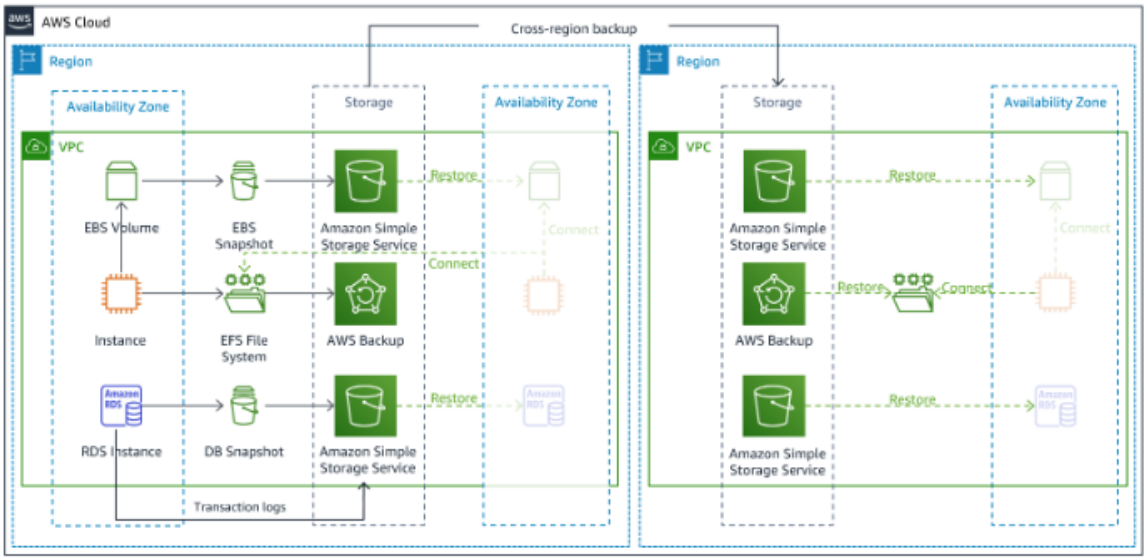
Kun strategiaa ja sen toteuttamiseen tarvittavia AWS-resursseja valitaan, pitää muistaa, että AWS jakaa palvelut yleisesti tietotasoon (data plane) ja ohjaustasoon (control plane). Tietotaso vastaa reaaliaikaisen palvelun toimittamisesta, kun taas ohjaustasoja käytetään ympäristön konfigurointiin. Parhaan joustavuuden saavuttamiseksi tulee käyttää vain datatason operaatioita osana vikasiirtotoimintoa. Tämä johtuu siitä, että datatasoilla on tyypillisesti korkeammat käytettävyyden suunnittelutavoitteet kuin ohjaustasoilla. (Amazon Web Services 2021)



Kuva 6 Toipumissuunnitelmavaihtoehdot ja niiden olennaisimmat ominaisuudet (Amazon Web Services 2021)

5.1 Backup and restore

Backup and restore eli varmuuskopiointi ja palautus (esimerkki arkkitehtuuri kuvassa 7) on sopiva tapa suojautua tietojen katoamiselta tai korruptiolta. Tätä lähestymistapaa voidaan käyttää myös lieventämään alueellista katastrofia replikoimalla tietoja muille AWS-alueille tai vähentämään redundanssin puutetta työkuormituksille, jotka on otettu käyttöön yhdelle käytettävyysalueelle. Tietojen lisäksi on otettava uudelleen käyttöön infrastruktuuri, kokoonpano ja sovelluskoodi palautusalueella. Jotta infrastruktuuri voidaan ottaa uudelleen käyttöön nopeasti ilman virheitä, se tulee aina ottaa käyttöön käyttämällä infrastruktuuri koodina tapaa. (Amazon Web Services 2021)



Kuva 7 Backup and restore arkkitehtuuri (Amazon Web Services 2021)

Tässä suunnitelmassa palautusaika ja palautuspiste ovat korkeampia. Tämä johtaa pidempiin seisokkeihin ja suurempaan tietojen menetykseen katastrofitapahtuman ja toipumisen välillä. Varmuuskopiointi ja palautus voivat kuitenkin olla oikea strategia työmäärälle, koska se on helpoin ja halvin strategia toteuttaa. Lisäksi kaikki työkuormat eivät vaadi palautusaikaa ja palautuspistettä minuuteissa tai vähemmän. (Eliot 2021a)

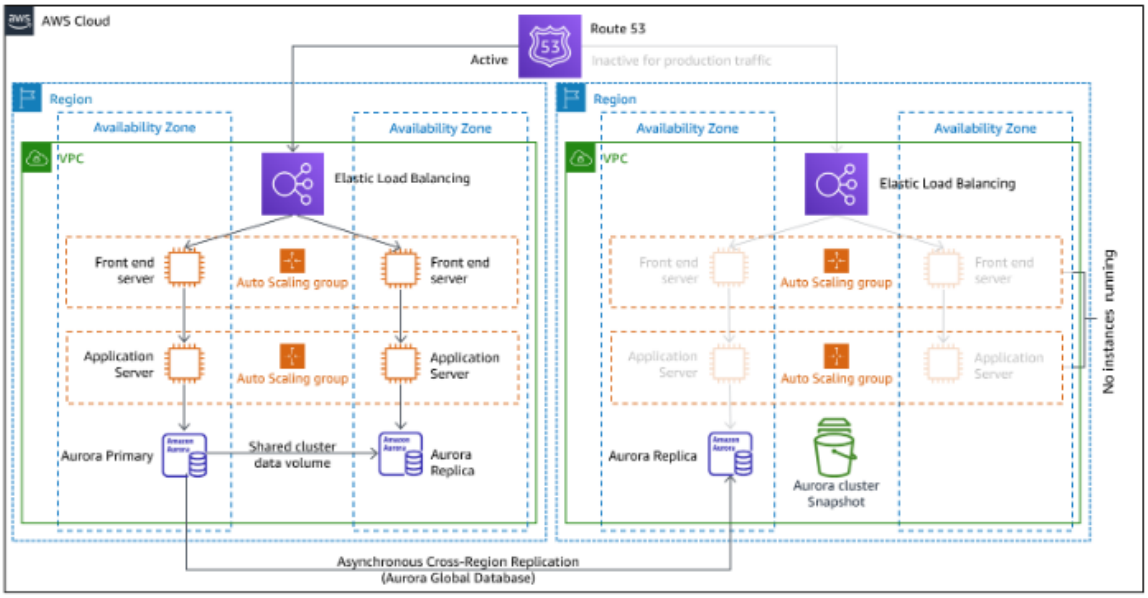
AWS Backup tarjoaa keskitetyn näkymän, jossa voit määrittää, ajoittaa ja valvoa näiden resurssien varmuuskopioita. Palautuspiste määräytyy sen mukaan, kuinka usein varmuuskopiot suoritetaan. Varmuuskopioiden keskitetyn hallinnan lisäksi AWS Backupin avulla voi kopioida varmuuskopioita alueiden ja AWS-tilien välillä, kuten kuvassa 7. Kopioimalla tiedot toiselle alueelle, voi käsitellä suurimmat katastrofit. (Eliot 2021b)

5.2 Pilot light

Pilot light (esimerkki arkkitehtuuri kuvassa 8) vaihtoehdolla kopioidaan tiedot alueelta toiselle ja lisäksi kopio ydintyökuormitusinfrastruktuurista. Tietojen replikoinnin ja varmuuskopioinnin tukemiseen tarvittavat resurssit, kuten tietokannat ja objektien tallennus, ovat aina käytössä. Muut elementit, kuten sovelluspalvelimet, ladataan sovelluskoodilla ja määrityksillä, mutta ne "sammutetaan" ja niitä käytetään vain testauksen aikana tai kun hätäpalautuksen vikasiirtoa kutsutaan. Pilvessä voidaan joustavasti poistaa resurssien hallintaa, kun niitä ei tarvita, ja tarjota niitä vain silloin, kun niitä tarvitaan. Paras käytäntö on olla ottamatta käyttöön resurssia ja luoda sitten kokoonpano ja ominaisuudet sen käyttöönottamiseksi tarvittaessa. Toisin kuin varmuuskopiointi- ja palautusmenetelmässä, ydininfrastruktuuri on aina käytettävissä ja on aina mahdollisuus luoda nopeasti täyden mittakaavan tuotantoympäristö kytkemällä päälle ja skaalaamalla sovelluspalvelimet. (Amazon Web Services 2021)

Pilot light minimoi katastrofipalautuksen jatkuvat kustannukset minimoimalla aktiiviset resurssit ja yksinkertaistaa palauttamista katastrofihetkellä, koska kaikki perusinfrastruktuurivaatimukset ovat kunnossa. Tämä palautusvaihtoehto edellyttää, että muutetaan käyttöönottotapa. On tehtävä perusinfrastruktuurin muutokset jokaiselle alueelle ja otettava käyttöön työkuorman (kokoonpanon, koodin) muutokset samanaikaisesti jokaiselle alueelle. Tätä vaihetta voidaan yksinkertaistaa automatisoimalla käyttöönotot ja käyttämällä infrastruktuuria koodina infrastruktuurin käyttöönottamiseksi useiden tilien ja alueiden kesken (täysi infrastruktuurin käyttöönotto ensisijaiselle alueelle ja skaalattu/pois päältä infrastruktuurin käyttöönotto palautusalueille). AWS suosittelee, että käytetään eri tiliä alueittain, jotta resurssien ja turvallisuuden eristys on mahdollisimman korkea (jos vaarantuneet kirjautumistiedot ovat myös osa katastrofipalautussuunnitelmia). (Amazon Web Services 2021)

Tällä lähestymistavalla on myös vältettävä tietokatastrofi. Jatkuva tietojen replikointi suojaa tietyntyyppisiltä katastrofeilta, mutta se ei välttämättä suojaa tietojen vioittumiselta tai tuhoutumiselta, ellei strategiaan sisälly myös tallennettujen tietojen versiointia tai palautuspisteen palautusvaihtoehtoja. Replikoiduista tiedoista tulee tehdä varmuuskopiot palautusalueelle. (Amazon Web Services 2021)

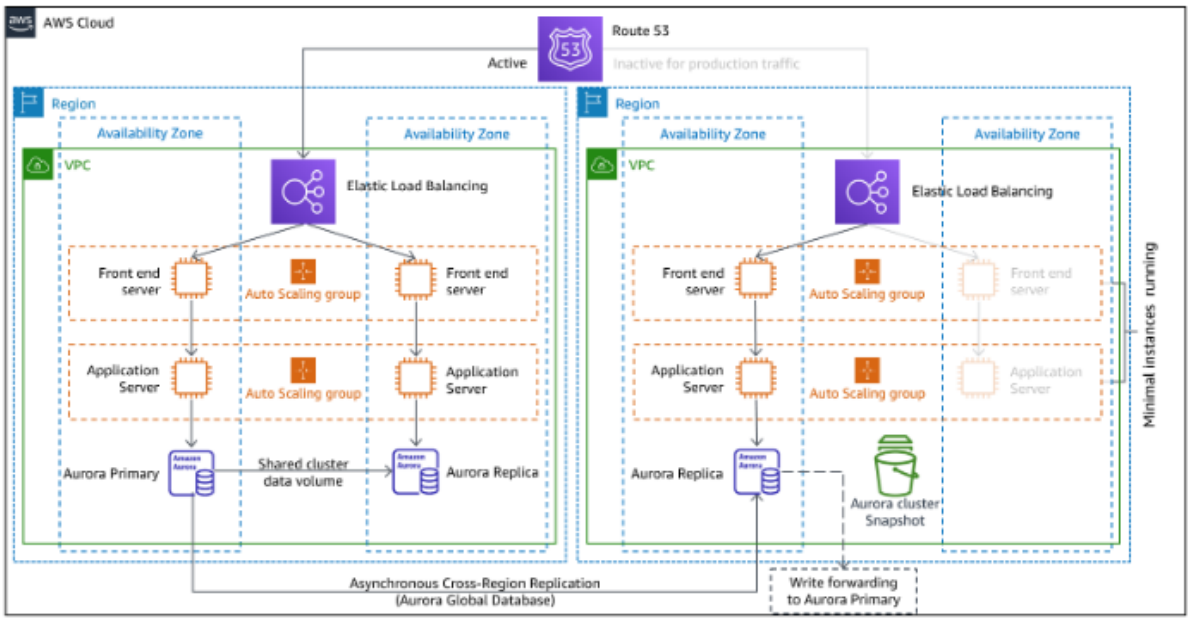


Kuva 8 Pilot light arkkitehtuuri (Amazon Web Services 2021)

5.3 Warm standby

Warm standby (esimerkki arkkitehtuuri kuvassa 9) lähestymistapaan kuuluu sen varmistaminen, että tuotantoympäristöstä on pienennetty, mutta täysin toimiva kopio toisella alueella. Tämä lähestymistapa laajentaa Pilot light tapaa ja lyhentää palautumisaikaa, koska työkuorma pyörii aina toisella alueella. Tämän lähestymistavan avulla voi myös helpommin suorittaa testauksia tai ottaa käyttöön jatkuvan testauksen. (Amazon Web Services 2021)

Pilot light ja Warm standbyn eroa voi joskus olla vaikea ymmärtää. Molemmat sisältävät ympäristön valitulla palautusalueella, jossa on kopiot ensisijaisen alueen resursseista. Erona on, että Pilot light ei pysty käsittelemään pyyntöjä ilman lisätoimenpiteitä, kun taas Warm standby voi käsitellä liikennettä (alennetulla kapasiteettitasolla) välittömästi. Pilot light lähestymistapa edellyttää, että palvelimet käynnistetään, mahdollisesti lisää (ei-ydininfrastruktuuria) otetaan käyttöön ja skaalautuu, kun taas Warm standby vaatii vain laajentamista (kaikki on jo otettu käyttöön ja käynnissä). (Amazon Web Services 2021)



Kuva 9 Warm standby arkkitehtuuri (Amazon Web Services 2021)

Pilot Light ja Warm Standby tavoissa on paljon samaa. Molemmat strategiat replikoivat tiedot ensisijaiselta alueelta palautusalueen tietoresursseihin, kuten Amazon Relational Database Service (Amazon RDS) tietokantaan tai Amazon DynamoDB -taulukoihin. Nämä tietoresurssit ovat valmiita palvelemaan pyyntöjä. Replikoinnin lisäksi molemmat strategiat edellyttävät jatkuvan varmuuskopion luomista palautusalueelle. Tämä johtuu siitä, että kun tapahtuu ihmisen toiminnasta johtuvia katastrofeja, tiedot voidaan poistaa tai ne voivat vioittua, ja replikointi replikoi huonot tiedot. Varmuuskopiot ovat välttämättömiä, jotta voidaan palata viimeiseen tunnettuun hyvään tilaan. Työkuormitusinfrastruktuuriin käytetyt resurssit otetaan käyttöön palautusalueella molemmissa strategioissa. Tämä sisältää tuki-infrastruktuurin, kuten Amazon Virtual Private Cloudin (Amazon VPC), jossa aliverkot ja reititys on määritetty, Elastic Load Balancing ja Amazon EC2 Auto Scaling -ryhmät. Molemmissa strategioissa käyttöön otettu infrastruktuuri vaatii lisätoimenpiteitä, jotta se on valmis tuotantoon. Työkuorman infrastruktuurin valmiusaste vaihtelee kuitenkin näiden kahden strategian välillä. Näiden strategioiden palautuspiste on samanlainen, koska niillä on yhteinen tietostrategia. (Eliot 2021c)

Pilot Light ja Warm Standby tavoilla on myös eroja. Ensisijainen ero näiden kahden strategian välillä on infrastruktuurin käyttöönotto ja valmius. Warm Standby käyttää toimivaa pinoa, mutta pienemmällä kapasiteetilla. DR-päätepiste voi käsitellä pyyntöjä, mutta ei voi käsitellä liikenteen tuotantotasoja. Tämä näkyy yhtenä Amazon Elastic Compute Cloud (Amazon EC2) -instanssina tasoa kohti kuvassa 9. Se voi olla enemmän, mutta on aina pienempi kuin koko tuotantokäyttö

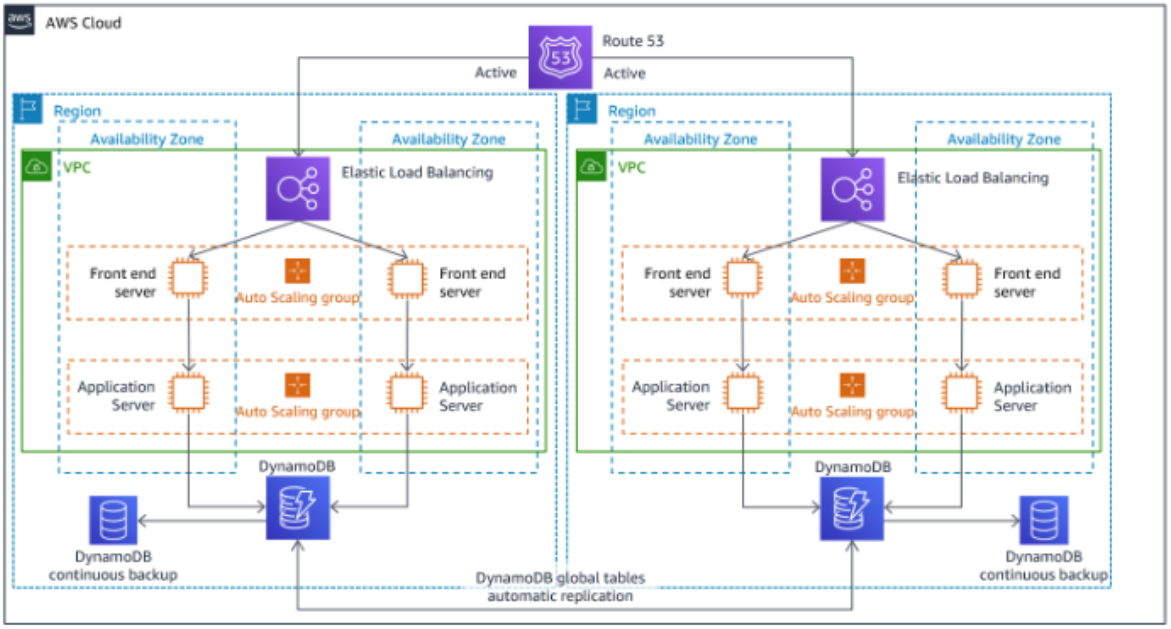
kustannussäästöjen vuoksi. Jos passiivinen pino kuitenkin otetaan käyttöön palautusalueella täydellä kapasiteetilla, tämä strategia tunnetaan nimellä "Hot Standby". Koska Warm Standby ottaa käyttöön toiminnallisen pinon palautusalueelle, tämä helpottaa alueen valmiuden testaamista synteettisten tapahtumien avulla. Pilot Light (toisin kuin Warm Standby) ei voi palvella pyyntöjä ennen kuin lisätoimenpiteitä on suoritettu. Kuvassa 8 näkyy EC2 Auto Scaling -ryhmä, joka on määritetty, mutta siinä ei ole käytössä EC2-instanssia. Näiden strategioiden palautusaika on erilainen. Warm Standby pystyy käsittelemään liikennettä vähäisellä tasolla välittömästi. Tämän jälkeen on skaalattava tämä olemassa oleva tuotanto, mikä antaa sille lyhyemmän palautusajan kuin Pilot Light. Tämä johtuu siitä, että Pilot Light edellyttää, että on ensin otettava käyttöön infrastruktuuri ja sitten skaalattava resursseja, ennen kuin työkuorma voi käsitellä pyyntöjä. (Eliot 2021c)

5.4 Hot standby / Multi-site active/active

Työkuorma voidaan suorittaa samanaikaisesti useilla alueilla osana Multi-Site Active/Active tai Hot Standby aktiivista/passiivista strategiaa (esimerkki arkkitehtuuri kuvassa 10). Multi-Site Active/Active palvelee liikennettä kaikilta alueilta, joille se on otettu käyttöön, kun taas Hot Standby palvelee liikennettä vain yhdeltä alueelta, ja muita alueita käytetään vain katastrofipalautukseen. Multi-Site Active/Active lähestymistavan avulla käyttäjät voivat käyttää työkuormaa millä tahansa alueilla, joilla se on käytössä. Tämä lähestymistapa on monimutkaisin ja kallein toipumissuunnitelma, mutta se voi lyhentää palautusaikaa lähes nollaan useimmissa katastrofeissa oikeilla teknologiavalinnoilla ja -toteutuksella (tosin tietojen korruption takia on luotava varmuuskopioita, mikä yleensä johtaa korkeampaan palautumispisteeseen). Hot Standby käyttää aktiivista/passiivista kokoonpanoa, jossa käyttäjät ohjataan vain yhdelle alueelle ja passiiviset alueet eivät ota liikennettä vastaan. Useimmat asiakkaat huomaavat, että jos he aikovat siirtyä täyteen tuotantoympäristöön toisella alueella, on järkevää käyttää molempia alueita aktiivisena. Vaihtoehtoisesti, jos ei haluta käyttää molempia alueita käyttäjäliikenteen käsittelemiseen, Warm Standby tarjoaa taloudellisemman ja toiminnallisesti vähemmän monimutkaisen lähestymistavan. (Amazon Web Services 2021)

Multi-Site Active/Active tapauksessa, koska työkuorma on käynnissä useammalla kuin yhdellä alueella, ei ole vikasiirtoa. Toipumissuunnitelman testaus keskittyisi tässä tapauksessa siihen, miten työmäärä reagoi alueen menettämiseen: Onko liikenne reititetty pois katastrofin kohdanneelta alueelta? Voivatko muut alueet hoitaa kaiken liikenteen? Myös tietokatastrofin testaus vaaditaan. Varmuuskopiointi ja palautus ovat edelleen tarpeen, ja ne tulee testata säännöllisesti. On myös huomattava, että palautumisajat datakatastrofin yhteydessä, johon liittyy tietojen vioittuminen, poistaminen tai hämärtyminen, ovat aina suurempia kuin nolla ja palautuspiste on aina jossain vaiheessa ennen katastrofin havaitsemista. Jos Multi-Site Active/Active (tai Warm Standby) lähestymistavan monimutkaisuus ja lisäkustannukset ovat välttämättömiä lähes nollan palautumisaikojen

säilyttämiseksi, on ryhdyttävä lisätoimiin turvallisuuden ylläpitämiseksi ja inhimillisten virheiden estämiseksi inhimillisten katastrofien lieventämiseksi. (Amazon Web Services 2021)

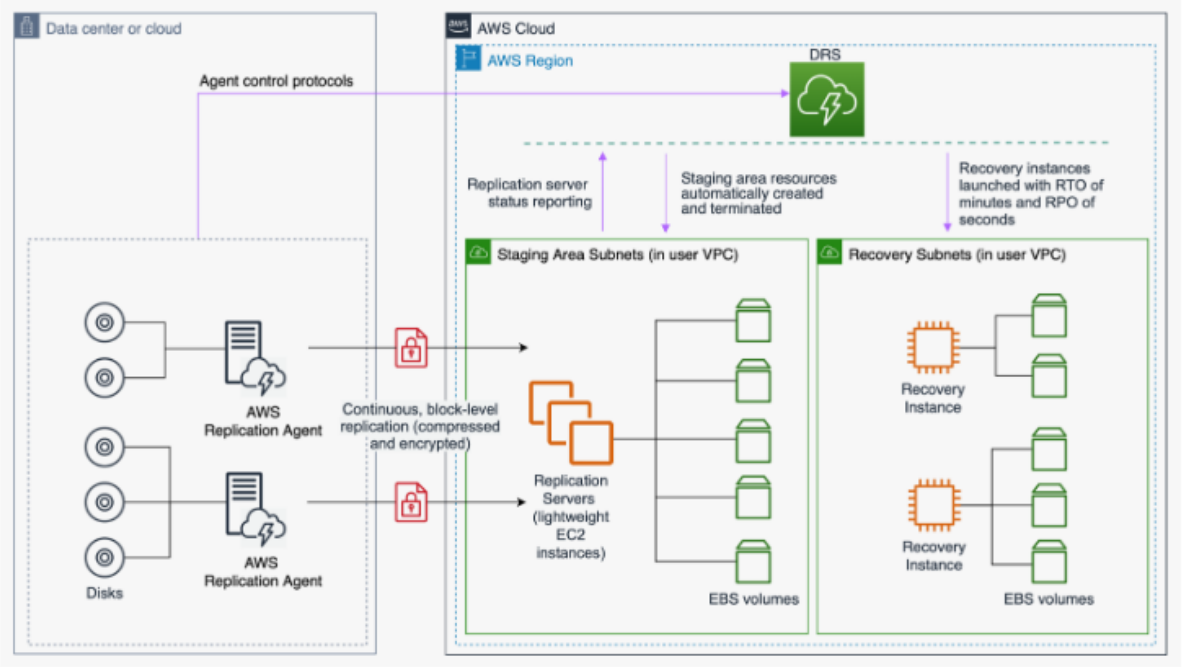


Kuva 10 Multi-site arkkitehtuuri (Amazon Web Services 2021)

Multi-Site Active/Active on hyvä suunnitelma työkuormitukselle, jos tarvitaan toipumissuunnitelmaa, jolla on nopein palautusaika ja pienin tiedonhäviö eli palautuspiste. Sen käyttöönotto eri alueilla on hyvä vaihtoehto, jos tarvitaan sivustojen tai sovellusten mahdollisimman suurta eristäytymistä ja täydellistä riippumattomuutta tai jos halutaan tarjota alhainen viive käyttäjille maailmanlaajuisesti eri paikoissa. Tämän strategian toteuttaminen ja käyttäminen, varsinkin usean alueen käytössä, voi olla monimutkaisempaa ja kalliimpaa kuin muut toipumissuunnitelmat. (Eliot 2021d)

5.5 AWS Elastic Disaster Recovery

AWS Elastic Disaster Recovery -palvelua voidaan käyttää tuetuissa käyttöjärjestelmissä toimivien paikallisten tai pilvipohjaisten sovellusten replikointiin. AWS-hallintakonsolin avulla voidaan määrittää replikointi- ja käynnistysasetukset, seurata tietojen replikointia ja käynnistää instansseja palautusharjoituksia tai oikeaa palautusta varten. (Amazon Web Service s.a. q.)



Kuva 11 Elastic Disaster Recovery arkkitehtuuri

AWS Elastic Disaster Recovery (DRS) replikoi jatkuvasti palvelimella olevia sovelluksia ja tietokantoja mistä tahansa lähteestä AWS:ään käyttämällä taustalla olevan palvelimen lohkotason replikointia (kuva 11). Sitä voidaan käyttää myös AWS-isännöityjen työkuormien katastrofipalautukseen, jos ne koostuvat vain EC2:ssa (eli ei RDS:ssä) isännöidyistä sovelluksista ja tietokannoista. Elastic Disaster Recovery käyttää Pilot Light -strategiaa, joka ylläpitää kopiota tiedoista ja "sammutettuja" resursseja palautusalueella. Kun vikasiirtotapahtuma laukeaa, vaiheittaisten resurssien avulla luodaan automaattisesti täyden kapasiteetin käyttöönotto palautusalueelle. (Amazon Web Service s.a. q.)

6 Oppaan suunnittelu ja toteutus

Oppaassa on kaksi erilaista osaa. Ensimmäisessä osassa tehdään neljä erilaista labraharjoitusta AWS Well-Architected Labs ympäristössä liittyen toipumissuunnitelmavaihtoehtoihin. Tavoitteena on havainnollistaa sitä, mitkä seikat vaikuttavat suunnitelman valintaan, mitä eri AWS:n tarjoamia palveluja eri vaihtoehdot käyttävät ja miten suunnitelmat käytännössä toteutetaan. Tavoitteena on myös arvioida AWS Well-Architected Labs Frameworkia oppimisympäristönä.

Toisessa osassa esitellään AWS Elastic Disaster Recovery -palvelun käyttöä. Tälle ei ole olemassa harjoitusta, vaan laadin sellaisen itse. Harjoituksen tavoitteena on kuvata palvelun käyttöä. Harjoituksessa siirrettävänä palveluna käytetään AWS Lightsail -palvelulla tehtyä wordpress sovellusta.

6.1 Lähtötilanteen kuvaus ja suunnittelun esittely

Oppaan suunnittelussa huomioon otettavia asioita ovat budjetti, helppokäyttöisyys ja toistettavuus. Budjettia varten, hyödynnetään AWS:n tarjoamaa free tier -tilausta eli joukkoon erilaisia resursseja on saatavissa ilmaista käyttöaikaa. Tiedonsiirrosta, varmuuskopioista ja replikoinnista tulee kuitenkin jonkin verran kuluja. Tavoitteena on kuitenkin päästä alle kymmenen euroon. AWS Well-Architected Labs valikoitui ympäristöksi siksi koska se on helppokäyttöinen ja harjoitukset ovat hyvin ohjattuja ja ne pyrkivät noudattamaan parhaita käytäntöjä. Toistettavuudella tarkoitetaan sitä, että opasta lukevat päätyvät samaan lopputulokseen.

Oppaan kohderyhmänä ovat opiskelijat, jotka erikoistuvat pilvipalveluihin ja ICT-infrastruktuureihin sekä ICT-alalla työskentelevät, joiden työhön liittyy pilvipalveluiden käyttö. Valmista raporttia voi hyödyntää suunniteltaessa toipumissuunnitelmaa omalle yritystoiminnalle, projekteihin tai esimerkiksi omaan opinnäytetyöhön liittyen.

Laadulliset kriteerit oppaalle ovat tekijän oma mielipide lopputuloksesta, saatu palaute sekä budjetissa (10 €) ja aikataulussa pysyminen. Oppaan 1. osan hyvästä onnistumisesta kertoo harjoitusten onnistuminen ja harjoituksille lisäarvon tuottaminen. Oppaan 2. osan hyvästä onnistumisesta kertoo onnistuneen ja helposti ymmärrettävän ja seurattavan harjoituksen kehittäminen.

6.2 Oppaan tuottamisen kuvaus

Kaikki oppaan 1. osan harjoitukset noudattavat samaa rakennetta. Harjoituksen vaiheet ovat

1. Infrastruktuurin pystytys mallinteilla
2. Sovelluksen toiminnan varmistaminen
3. Harjoituksessa tiedon ja palveluiden siirtämisessä passiiviselle alueelle käytettävien palveluiden toiminnan esitteleminen
4. Katastrofin simuloiminen estämällä pääsy aktiiviselle alueelle
5. Palauttamisen onnistumisen tarkistaminen, niin että sovellus toimii passiivisella alueella
6. Harjoituksessa käytettyjen resurssien tuhoaminen

Oppaan 2. osan harjoituksen vaiheet ovat seuraavat

1. Ensimmäinen asennuskerta Elastic Disaster Recovery palvelulle
2. AWS Replication Agent asentaminen lähde palvelimelle
3. Käynnistysasetusten määrittäminen
4. Harjoitus instanssin käynnistys
5. Katastrofin simulointi
6. Palauttamiseen käytettävän instanssin käynnistys
7. Palautuksen onnistumisen testaaminen
8. Harjoituksessa käytettyjen resurssien tuhoaminen

Molempien oppaiden harjoitukset tehdään AWS konsolissa. Tätä varten tarvitaan AWS tili. Harjoituksia varten on myös hyvä tehdä erillinen käyttäjä, jolla ei ole admin-oikeuksia tilille. Suurin osa harjoituksissa käytettävistä resursseista luodaan mallinteilla, tämä siksi, että se säästää aikaa ja voidaan keskittyä toipumissuunnitelman kannalta oleellisimpiin resursseihin. Harjoitusten lopuksi on tärkeää postaa kaikki luodut resurssit ja varmuuskopiot molemmilta alueilta, jotta vältytään ylimääräisiltä kuluilta.

7 Pohdinta

Työn tavoitteena oli tuottaa kaksiosainen opas. 1. osaan en ole kovin tyytyväinen. Osan lisäarvo ja hyödyllisyys ei vielä tällaisena ole kummoinen. 2. osaan olen tyytyväisempi. Siinä tehty harjoitus onnistui aivan kuten pitikin eikä vastaavanlaisia löytynyt pikaisella selaamisella netistä. Pidän sen tuomaa lisäarvoa oppaalle hyvänä. Määrittelemistäni laadullisista kriteereistä aikataulu ja budjetti ovat pitäneet. Kuluja on ollut n. 6 euroa.

Opas itsessään on mielestäni ajankohtainen, sillä luonnonkatastrofeja ja kyberhyökkäyksiä tapahtuu yhä enemmän, joten toipumissuunnitelmille on käyttöä. AWS valittuna pilvipalvelun tarjoajana on myös mielestäni perusteltu. On vaikea nähdä AWS:n menettävän merkitystä tulevina vuosina. Vastaavasta aiheesta ei myöskään ole aikaisempia opinnäytetöitä Theseuksessa.

AWS Well-Architected Labs on ympäristönä varsinkin opiskelijalle kätevä. Labroissa on hyvin hyödynnetty ilmaisia resursseja ja suurempienkin infrastruktuurien pystyttäminen (väliaikaisesti) on edullista ja mallinteiden avulla nopeaa. Harjoituksissa on kuitenkin ristiriitana se, että osa niistä tehdään manuaalisesti, vaikka tavoitteena on seurata parhaita käytäntöjä, mikä tässä tapauksessa tarkoittaisi automatisointia ja resurssien luomista infraa koodina tavalla.

Opasta voi hyödyntää pohjana omaa toipumissuunnitelmaa laatiessa. Opasta voisi kehittää vielä siten, että 1. osan harjoituksissa manuaalisia tehtäviä automatisoitaisiin ja lisättäisiin CloudFormation -mallinteihin. Samoin 2. osaan voisi kehittää samaa. Yleisesti parhaita käytäntöjä voisi noudattaa paremmin.

Lähteet

Alvarenga, G. 2022. What is the Shared Responsibility Model?. Luettavissa: https://www.crowdstrike.com/cybersecurity-101/cloud-security/shared-responsibility-model/. Luettu 29.3.2023.

Amazon Web Services. s.a. a. Cloud computing with AWS. Luettavissa: https://aws.amazon.com/what-is-aws/. Luettu 29.3.2023.

Amazon Web Services. 2021. Disaster Recovery of Workloads on AWS: Recovery in the Cloud. Luettavissa: https://docs.aws.amazon.com/whitepapers/latest/disaster-recovery-workloads-on-aws/disaster-recovery-workloads-on-aws.html. Luettu 4.4.2023.

Amazon Web Services. s.a. b. Regions and Availability Zones. Luettavissa: https://aws.amazon.com/about-aws/global-infrastructure/regions_az/. Luettu 4.4.2023.

Amazon Web Services. s.a. o. Well-Architected. Luettavissa: https://aws.amazon.com/architecture/well-architected. Luettu 30.3.2023.

Amazon Web Services. s.a. j. What is Amazon Aurora?. Luettavissa: https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/CHAP_AuroraOverview.html. Luettu 18.4.2023.

Amazon Web Services. s.a. i. What is Amazon Backup?. Luettavissa: https://docs.aws.amazon.com/aws-backup/latest/devguide/whatisbackup.html. Luettu 18.4.2023.

Amazon Web Services. s.a. n. What is Amazon CloudFront?. Luettavissa: https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Introduction.html. Luettu 18.4.2023.

Amazon Web Services. s.a. f. What is Amazon EC2?. Luettavissa: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/concepts.html. Luettu 18.4.2023.

Amazon Web Services. s.a. l. What is Amazon EC2 Auto Scaling?. Luettavissa: https://docs.aws.amazon.com/autoscaling/ec2/userguide/what-is-amazon-ec2-auto-scaling.html. Luettu 18.4.2023.

Amazon Web Services. s.a. q. What is Elastic Disaster Recovery?. Luettavissa: https://docs.aws.amazon.com/drs/latest/userguide/what-is-drs.html. Luettu 23.4.2023.

Amazon Web Services. s.a. h. What is Amazon Relational Database Service (Amazon RDS)?. Luettavissa: https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Welcome.html. Luettu 18.4.2023.

Amazon Web Services. s.a. g. What is Amazon S3?. Luettavissa: https://docs.aws.amazon.com/AmazonS3/latest/userguide/Welcome.html. Luettu 18.4.2023.

Amazon Web Services. s.a. d. What is Amazon VPC?. Luettavissa: https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html. Luettu 4.4.2023.

Amazon Web Services. s.a. m. What is AWS CloudFormation?. Luettavissa: https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/Welcome.html. Luettu 18.4.2023.

Amazon Web Services. s.a. k. What is Elastic Load Balancing?. Luettavissa: https://docs.aws.amazon.com/elasticloadbalancing/latest/userguide/what-is-load-balancing.html. Luettu 18.4.2023.

Butler, B. 2013. PaaS Primer: What is platform as a service and why does it matter?. Luettavissa: https://www.networkworld.com/article/2163430/paas-primer--what-is-platform-as-a-service-and-why-does-it-matter-.html. Luettu 6.5.2023.

Eliot, S. 2021a. Disaster Recovery (DR) Architecture on AWS, Part I: Strategies for Recovery in the Cloud. Luettavissa: https://aws.amazon.com/blogs/architecture/disaster-recovery-dr-architecture-on-aws-part-i-strategies-for-recovery-in-the-cloud/. Luettu 4.5.2023.

Eliot, S. 2021b. Disaster Recovery (DR) Architecture on AWS, Part II: Backup and Restore with Rapid Recovery. Luettavissa: https://aws.amazon.com/blogs/architecture/disaster-recovery-dr-architecture-on-aws-part-ii-backup-and-restore-with-rapid-recovery/. Luettu 4.5.2023.

Eliot, S. 2021c. Disaster Recovery (DR) Architecture on AWS, Part III: Pilot Light and Warm Standby. Luettavissa: https://aws.amazon.com/blogs/architecture/disaster-recovery-dr-architecture-on-aws-part-iii-pilot-light-and-warm-standby/. Luettu 4.5.2023.

Eliot, S. 2021d. Disaster Recovery (DR) Architecture on AWS, Part IV: Multi-site Active/Active. Luettavissa: https://aws.amazon.com/blogs/architecture/disaster-recovery-dr-architecture-on-aws-part-iv-multi-site-active-active/. Luettu 4.5.2023.

Eliot, S. & Valverde, L. 2018. The 6 Pillars of the AWS Well-Architected Framework. Luettavissa: https://aws.amazon.com/blogs/apn/the-6-pillars-of-the-aws-well-architected-framework/. Luettu 30.3.2023.

Haranas, M. 2023. Cloud Market Share Q4 2022: Microsoft Gains On AWS As Google Grows. Luettavissa: https://www.crn.com/news/cloud/cloud-market-share-q4-2022-microsoft-gains-on-aws-as-google-grows/6. Luettu 29.3.2023.

Hiles. A. 2002. The Complete Guide to IT Service Level Agreements. Rothstein Catalog On Service Level Books. 3. uudistettu painos. Rothstein. Brookfield. E-kirja. Luettu 20.4.2023.

IBM. 2021. IaaS vs. PaaS vs. SaaS. Luettavissa: https://www.ibm.com/cloud/learn/iaas-paas-saas. Luettu 6.5.2023.

Mell, P. & Grance, T. 2011. The NIST Definition of Cloud Computing, NIST. Luettavissa: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf. Luettu: 28.3.2023.

Merron, D. & Wickramasinghe, S. 2021. Infrastructure as Code (IaC): The Complete Beginner's Guide. Luettavissa: https://www.bmc.com/blogs/infrastructure-as-code/. Luettu: 28.3.2023.

Rouse, M. 2022. Infrastructure as a Service (IaaS). Luettavissa: https://www.techopedia.com/definition/141/infrastructure-as-a-service-iaas. Luettu 6.5.2023.

Turner, B. 2020. What is SaaS? Everything you need to know about Software as a Service. Luettavissa: https://www.techradar.com/news/what-is-saas. Luettu 6.5.2023.

VMware. s.a. a. What is Disaster Recovery?. Luettavissa: https://www.vmware.com/topics/glossary/content/disaster-recovery.html. Luettu 12.4.2023.

VMware. s.a. b. What is disaster recovery as a service (DRaaS)?. Luettavissa: https://www.vmware.com/topics/glossary/content/disaster-recovery-service-draas.html. Luettu 11.4.2023.

Wallenius, N. 2022. Tunnetko nämä neljä (4) jatkuvuudenhallinnan termiä?. Luettavissa: https://niklaswallenius.fi/jatkuvuussuunnittelu-termit/. Luettu 4.4.2023.

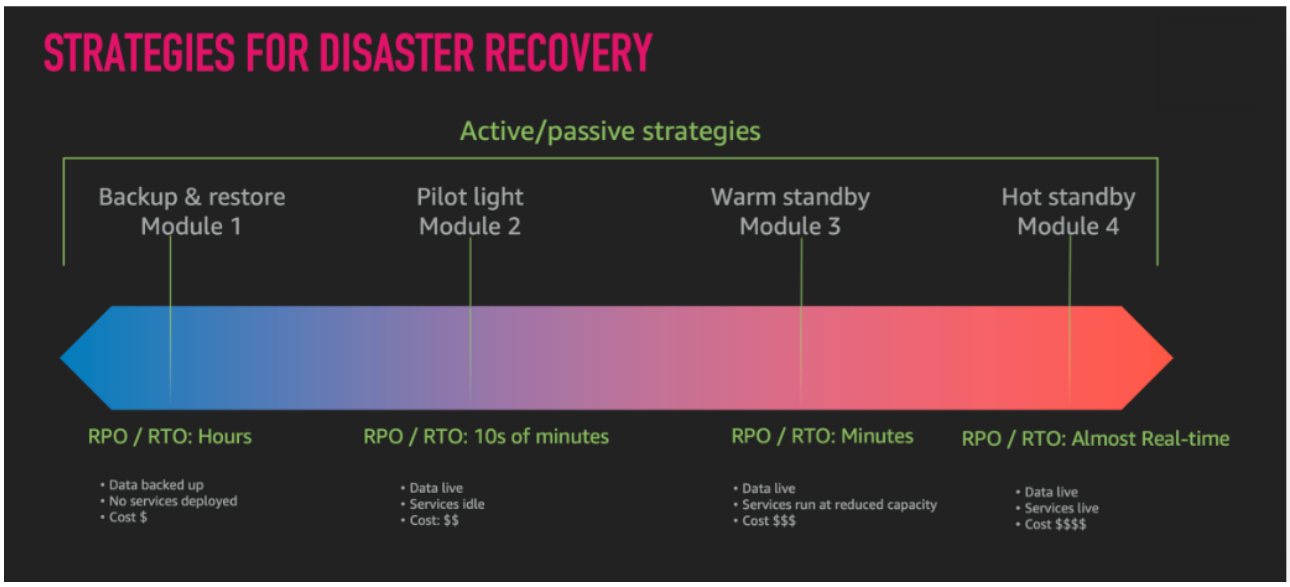
Liitteet

Liite 1. Toipumissuunnitelmavaihtoehtojen toteuttaminen harjoitusympäristössä

OSA 1

Tässä on tarkoitus läpikäydä wellarchitectedlabs.com-sivustolta löytyvät moduulit (kuva 12), joissa demonstroidaan eri vaihtoehtoja käytännön harjoituksilla. Sivusto sisältää yhteensä neljä moduulia.

Moduulit on jaettu AWS Disaster Recovery -strategioihin. Kaikki moduulit käyttävät AWS:n tarjoamaa Javalla tehtyä Unishop-sovellusta ja jokainen moduuli korostaa eri toipumissuunnitelmaa ja AWS-palveluita, joissa on ominaisuuksia, jotka helpottavat toipumissuunnitelman toteuttamista. Jokaisessa moduulissa resurssit luodaan kahdelle alueelle, joista toisesta käytetään nimeä active - aktiivinen ja passive - passiivinen.



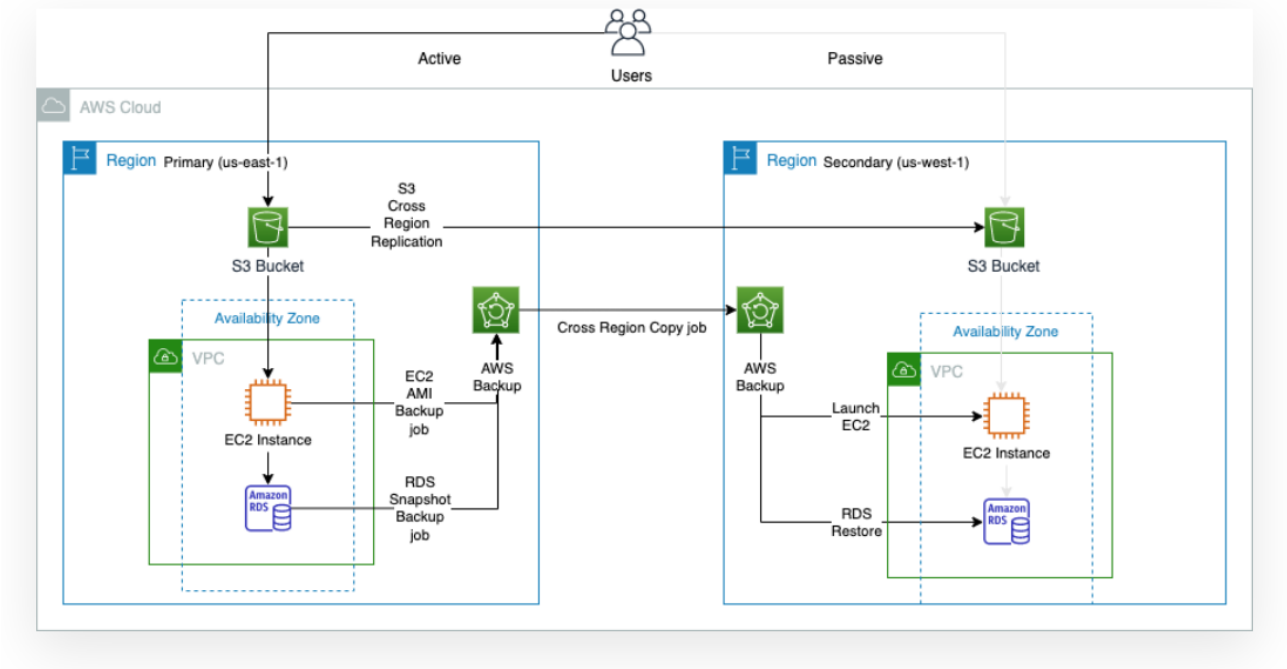
Kuva 12 Toipumisvaihtoehdot ja moduulit (Amazon Web Services 2023)

Tätä opinnäytetyötä tehdessä on AWS päivittänyt moduuleita ja vaihtanut Multi-site active/active moduulin Hot standby moduuliin ja lisännyt yhden uuden moduulin nimeltä Multi-Region Resilience with Route 53 ARC, tämä moduuli ei sisälly tähän. Multi-site active/active strategia eroaa Hot standby vaihtoehdosta lähinnä siten, että Hot standby:ssa reititys ohjataan vain yhdelle alueelle ja Multi-site vaihtoehdossa useille alueille esimerkiksi sijainnin tai latenssin perusteella.

Moduuli 1

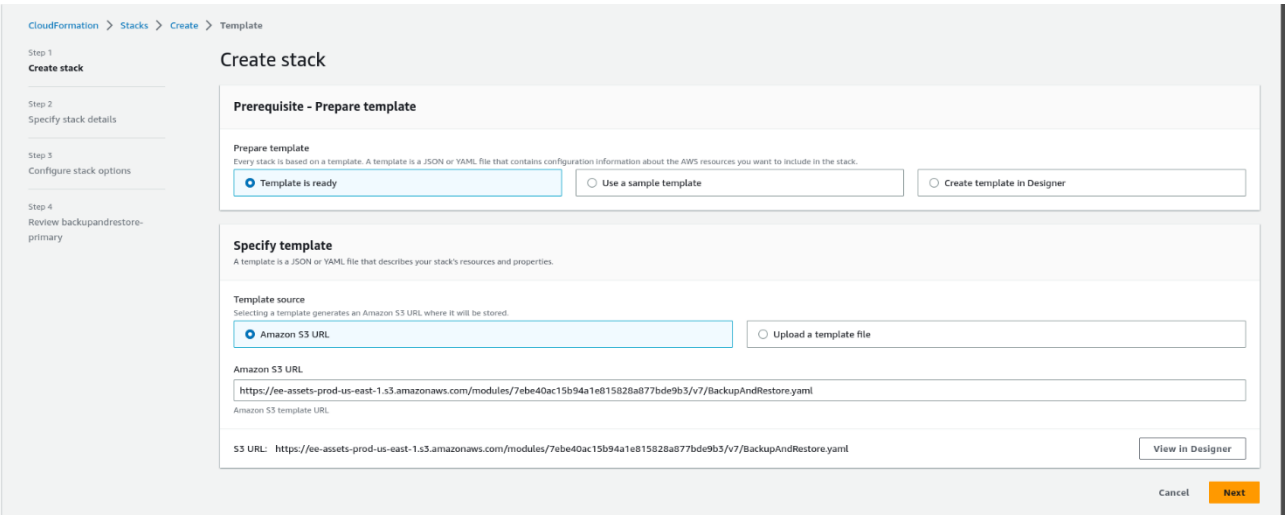
Ensimmäisessä moduulissa tehdään harjoitus backup and restore vaihtoehdolle (kuva 13). Arkkitehtuurissa tietokantana on MySQL RDS, Spring Boot Java sovellus pyörii EC2 instanssilla ja

käyttöliittymä (frontend) on S3 varastossa. AWS Backup palvelua hyödynnetään siirtämällä instanssin ja tietokannan varmuuskopiot passiiviselle alueelle. S3:n sisältö replikoitaan Cross-Region replication toiminnolla eli replikoidaan tieto toiselle alueelle.



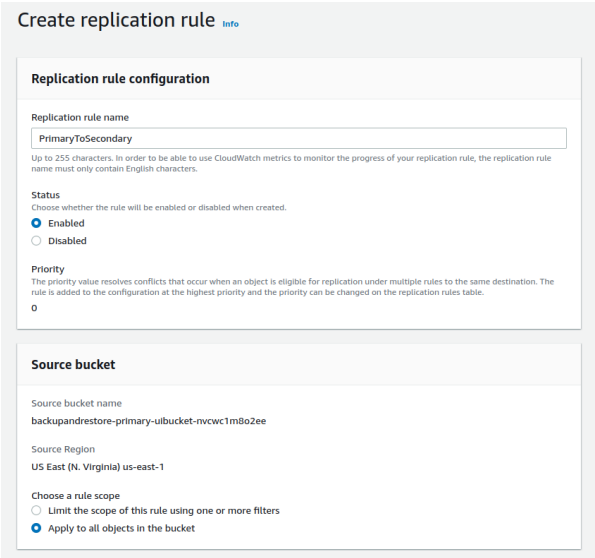
Kuva 13 Moduuli 1 arkkitehtuuri (Amazon Web Services 2023)

Ensimmäiseksi pystytetään infrastruktuuri molemmille alueille käyttämällä annettuja CloudFormation mallinteita.



Kuva 14 Aktiivisen alueen mallinteen pystyttäminen

Seuraavaksi tehdään asetus S3 varaston sisällön replikoimiselle passiiviselle alueelle. Frontend koodi kopioidaan aktiivisen alueen varastoon harjoituksen antamilla komennoilla, jotka ajetaan cloudshellissä.

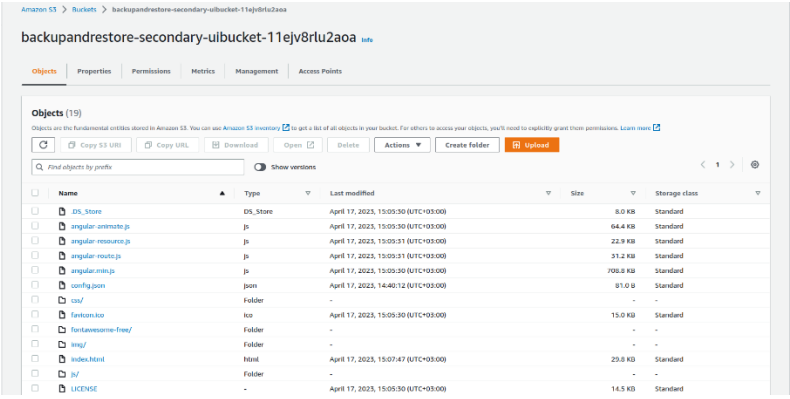


Kuva 15 Replikointia varten tarvittavat konfiguroinnit

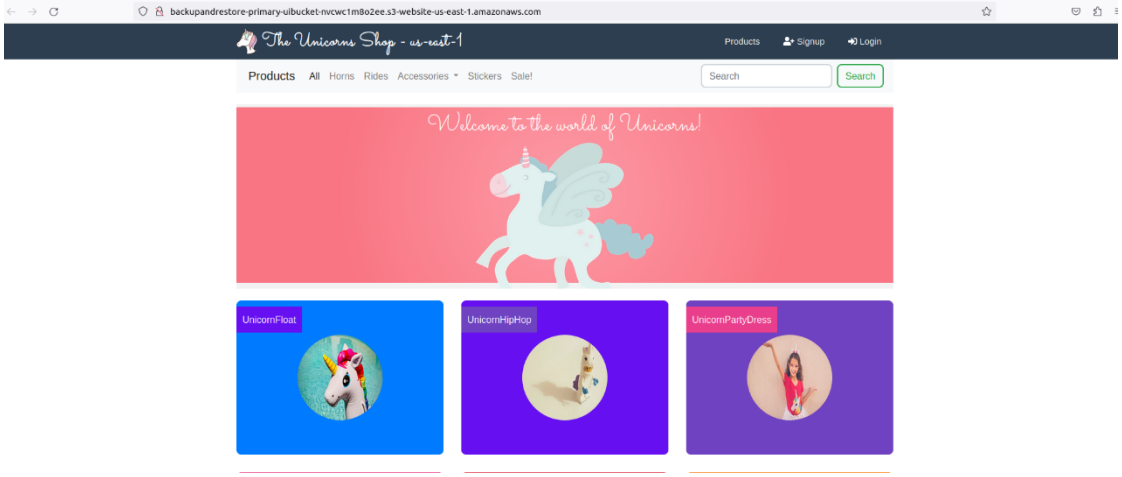
```
export S3_BUCKET=$(aws s3api list-buckets --region us-east-1 --output text --query 'Buckets[?starts_with(Name, `backupandrestore-primary-uibucket`) == `true`]'.Name)
aws s3 cp s3://ee-assets-prod-us-east-1/modules/630039b9022d4b46bb6cbad2e3899733/v1/UntShopUI/ s3://$S3_BUCKET/ --exclude "config.json" --recursive --grants read=uri=http://acs.amazonaws.com/groups/global/AllUsers
```

Kuva 16 Passiivisen alueen varaston konfigurointi tiedoston hakeminen

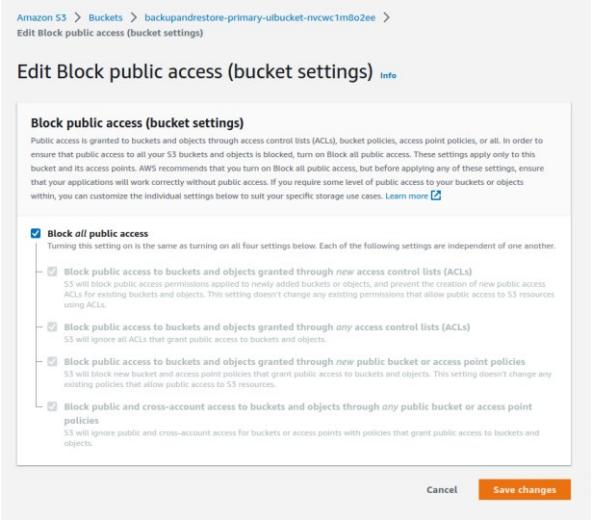
Tämän jälkeen varmistetaan, että molempien alueiden S3 varastot sisältävät frontend koodin ja aktiivisen alueen osoite vie toimivalle sovellukselle. Katastrofia demonstroidaan näissä moduuleissa estämällä pääsy aktiivisen alueen S3 varastoon.



Kuva 17 Replikoinnin onnistumisen varmistaminen



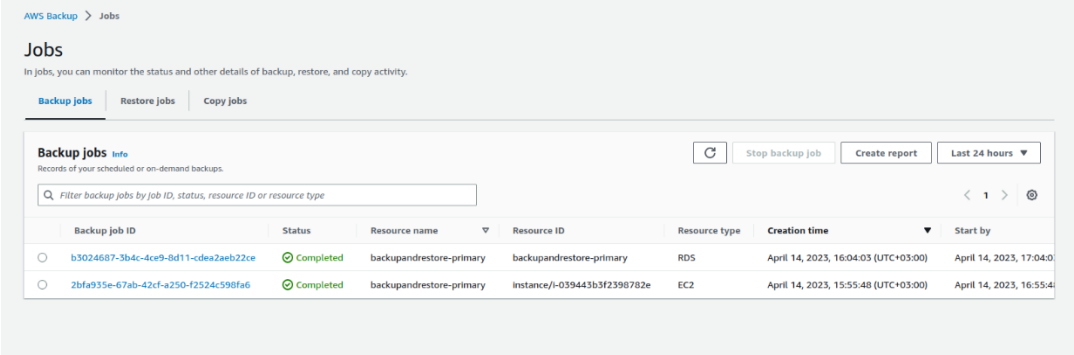
Kuva 18 Sovelluksen toiminnan varmistaminen



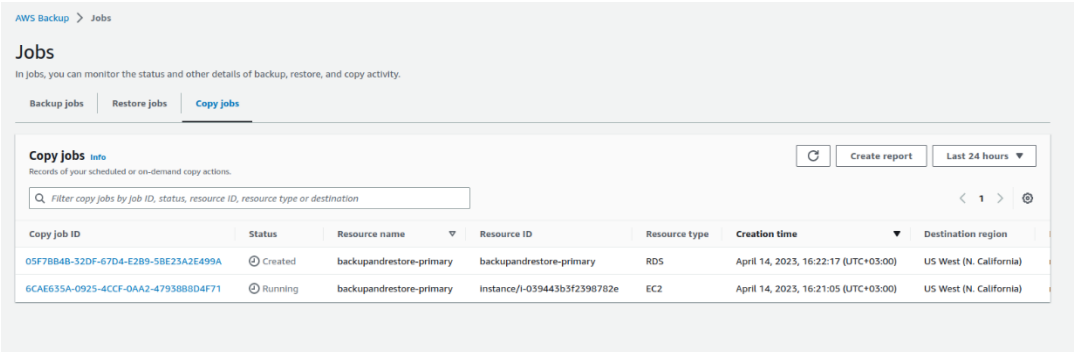
Kuva 19 Katastrofia simuloidaan estämällä julkinen pääsy varastossa oleviin tiedostoihin

Kuva 20 Aktiiviseen alueeseen ei enää pääse

Varmuuskopiointi passiiviselle alueelle tehdään AWS Backup palvelulla, joka harjoituksessa tehdään manuaalisesti siten, että ensin tehdään backup job kopioitavista resursseista (EC2 ja RDS) ja jotka kopioidaan passiiviselle alueelle, josta ne palautetaan (restore).



Kuva 21 Varmuuskopioidut resurssit



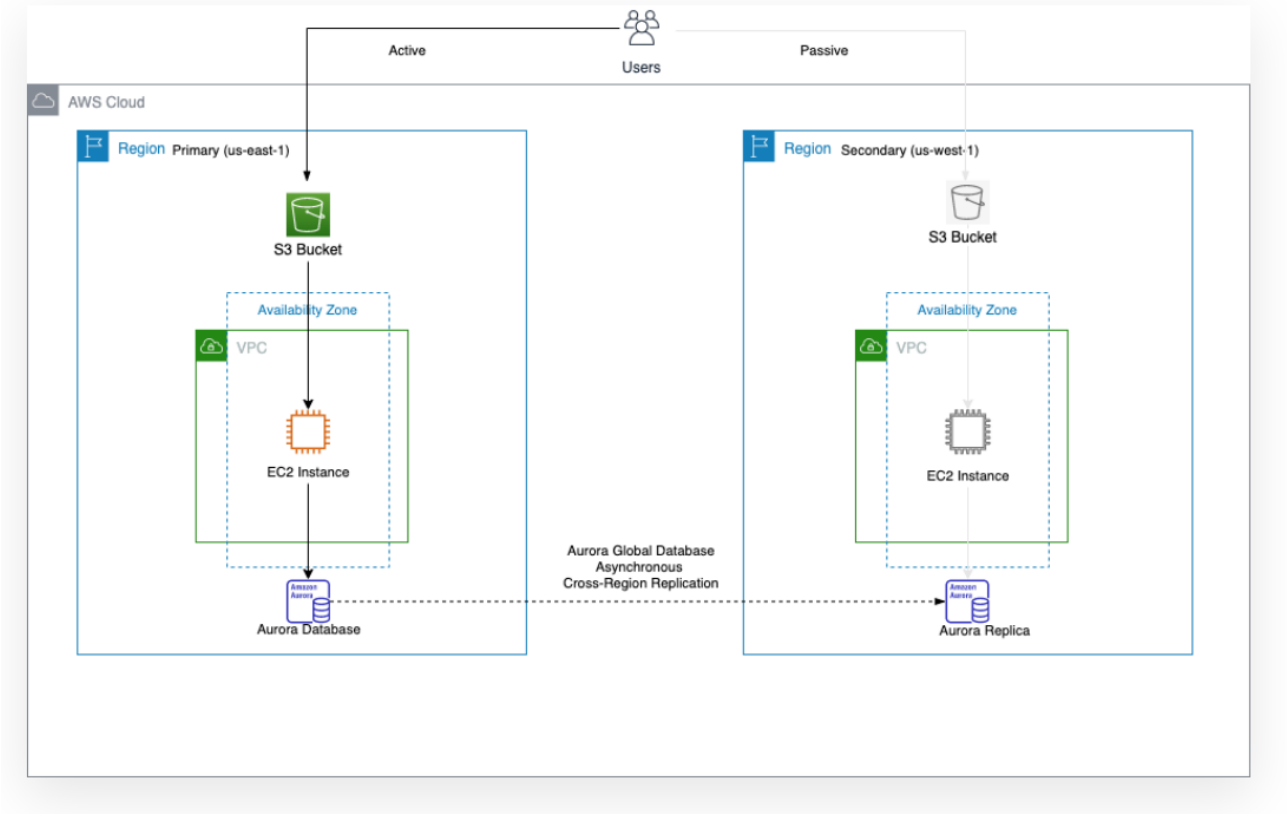
Kuva 22 Varmuuskopioiden kopioiminen passiiviselle alueelle

Kun palautus on tehty, tarkistetaan, että passiivisen alueen S3 varaston antama URL vie toimivaan osoitteeseen.

Lopuksi kaikki resurssit tuhotaan molemmilta alueilta kulujen säästämiseksi järjestyksessä S3:n sisältö, CloudFormation mallinne ja AWS Backup.

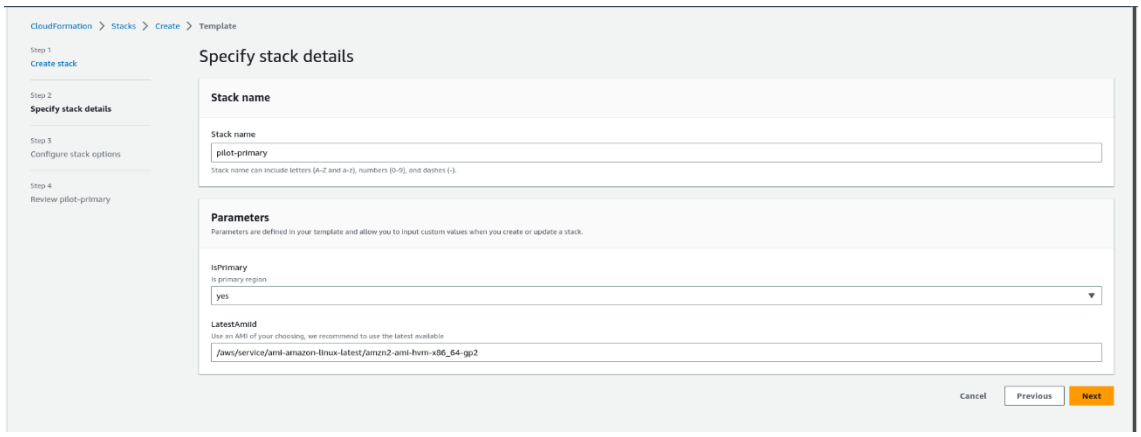
Moduuli 2

Toisessa moduulissa tehdään harjoitus pilot light vaihtoehdolle (kuva 23). Arkkitehtuuri on muuten sama paitsi, että tietokantana on Aurora. Tässä harjoituksessa resurssit siirretään passiiviselle alueelle niin, että instanssista luodaan AMI, jonka avulla instanssi pystytetään toiselle alueelle. Tietokanta siirtyy passiiviselle alueelle Auroran global database ominaisuuden avulla. Tämän harjoituksen CloudFormation mallinteissa frontend koodit sisältyvät jo S3 varastoon, joten sitä ei tarvitse tehdä.



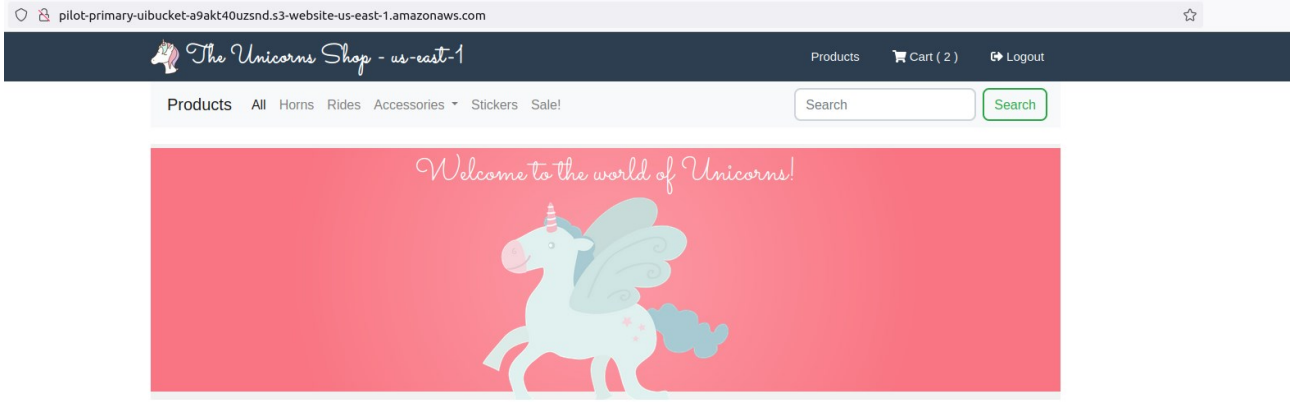
Kuva 23 Moduuli 2 arkkitehtuuri (Amazon Web Services 2023)

Tämän harjoituksen mallinteet hyödyntävät parametrejä. Ajettaessa aktiivisen alueen mallinne IsPrimary parametrin arvoksi annetaan yes ja passiivisessa alueessa arvoksi no.



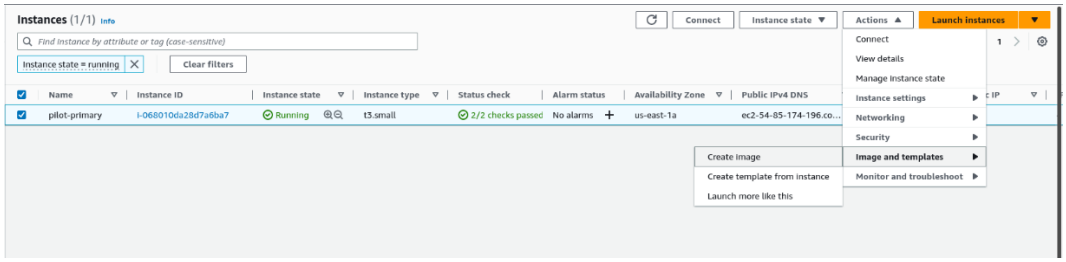
Kuva 24 Passiivisen alueen mallinteen pystytys

Aktiivisen alueen sivulle tehdään tili ja ostoskoriin laitetaan asioita, jotta voidaan testata tiedon siirtämistä onnistuneesti passiiviselle alueelle.

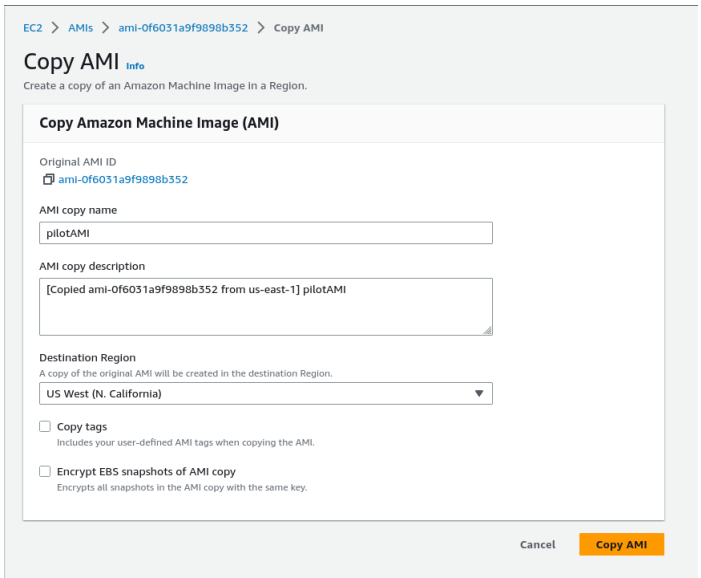


Kuva 25 Sovelluksen toiminnan varmistus

Instanssista tehty AMI kopioidaan manuaalisesti passiiviselle alueelle.



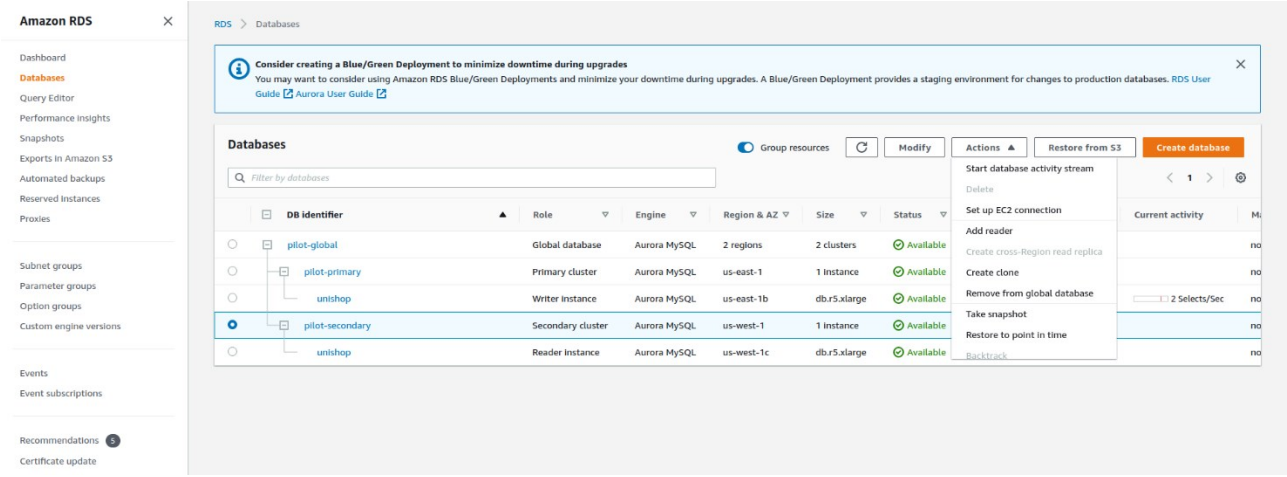
Kuva 26 AMI:n luominen



Kuva 27 AMI:n kopioiminen passiiviselle alueelle

Aurora tietokannan palauttamiseen on kaksi eri lähestymistapaa, Managed planned failover ja Managed unplanned failover. Tässä käytetään jälkimmäistä eli suunnittelematonta tapaa.

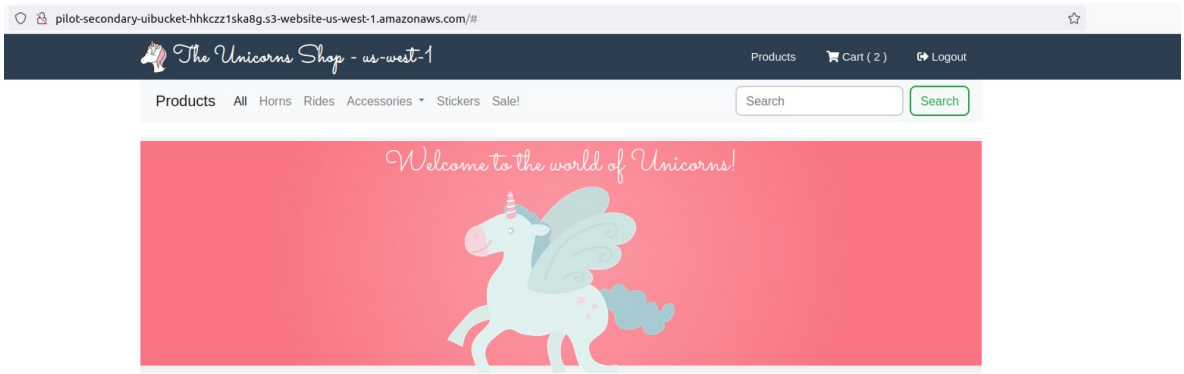
Auroran toissijainen klusteri, joka sijaitsee passiivisella alueella, ylennetään itsenäiseksi tietokannaksi.



Kuva 28 Auroran tietokannat

Aikaisemmin passiiviselle alueelle kopioitu AMI pystytetään uudelle instanssille.

Nyt passiivisen alueen sivu toimii ja aikaisemmin aktiivisen alueen sivulla ostoskoriin laitetut tavarat ovat myös siellä.



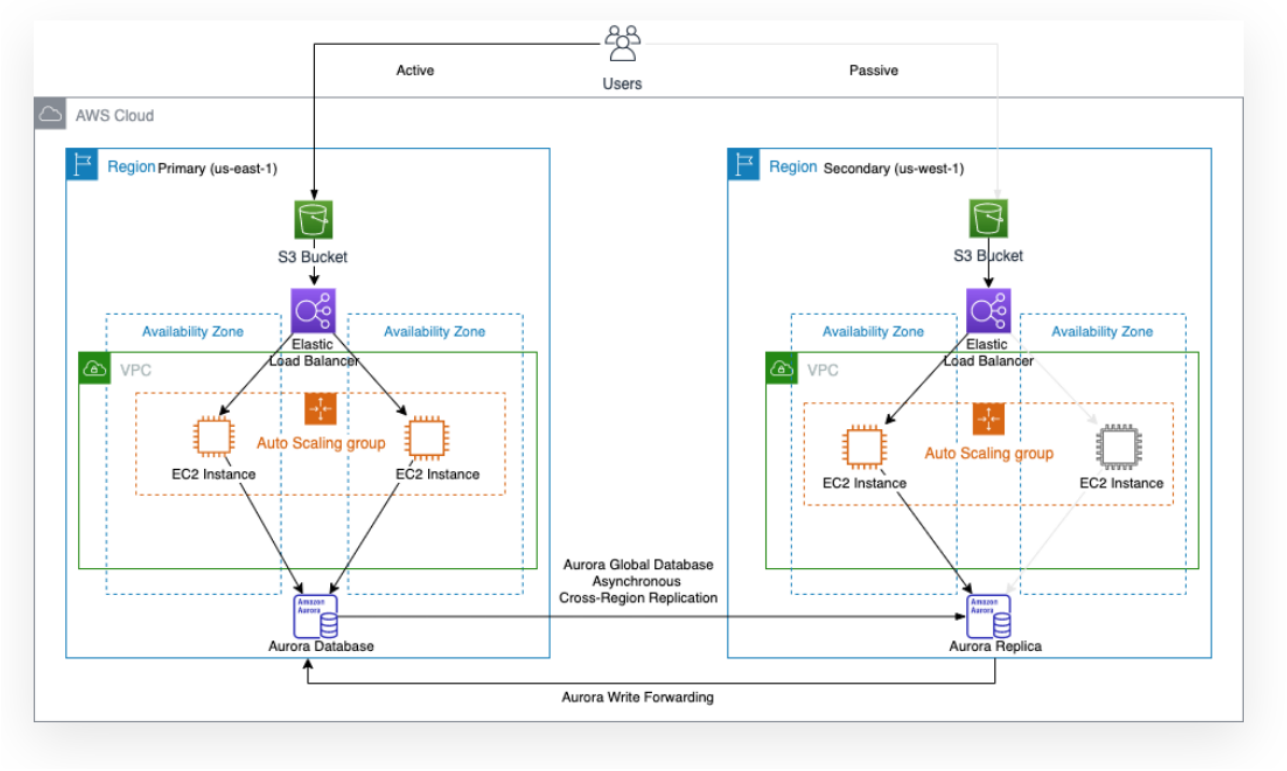
Kuva 29 Sovellus toimii passiivisella alueella

Lopuksi kaikki resurssit tuhotaan molemmilta alueilta kulujen säästämiseksi järjestyksessä S3, Aurora, EC2 ja muotit. Mallinteissa passiivisen alueen mallinne poistetaan ensin. Tietokannoissa ensin poistetaan kirjoittavat instanssit (writer instance) ja lopuksi global database.

Moduuli 3

Kolmannessa moduulissa tehdään harjoitus warm standby vaihtoehdolle (kuva 30). Tässä erona aikaisempaan on, että arkkitehtuurissa hyödynnetään kuormantasausta (load balancing) ja

instanssien automaattista skaalautumista (auto scaling). Tietokantana toimii edelleen Aurora, jonka write forwarding ominaisuutta hyödynnetään tiedon siirrossa.



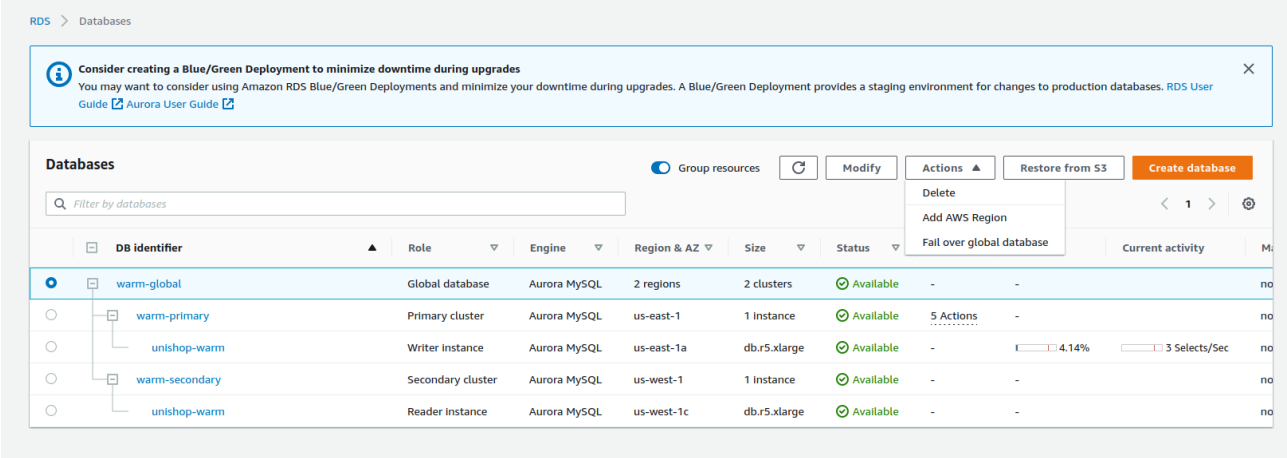
Kuva 30 Moduuli 3 arkkitehtuuri (Amazon Web Services 2023)

Tässä harjoituksessa hyödynnetään aikaisemman tavoin mallinteiden kohdalla parametrejä. Tällä kertaa käytetään kahta eri parametriä IsPrimary ja IsPromote. IsPrimary parametriä käytetään samalla tavoin kuin aikaisempien mallinteiden luonnissa. IsPromote käytetään myöhemmin.

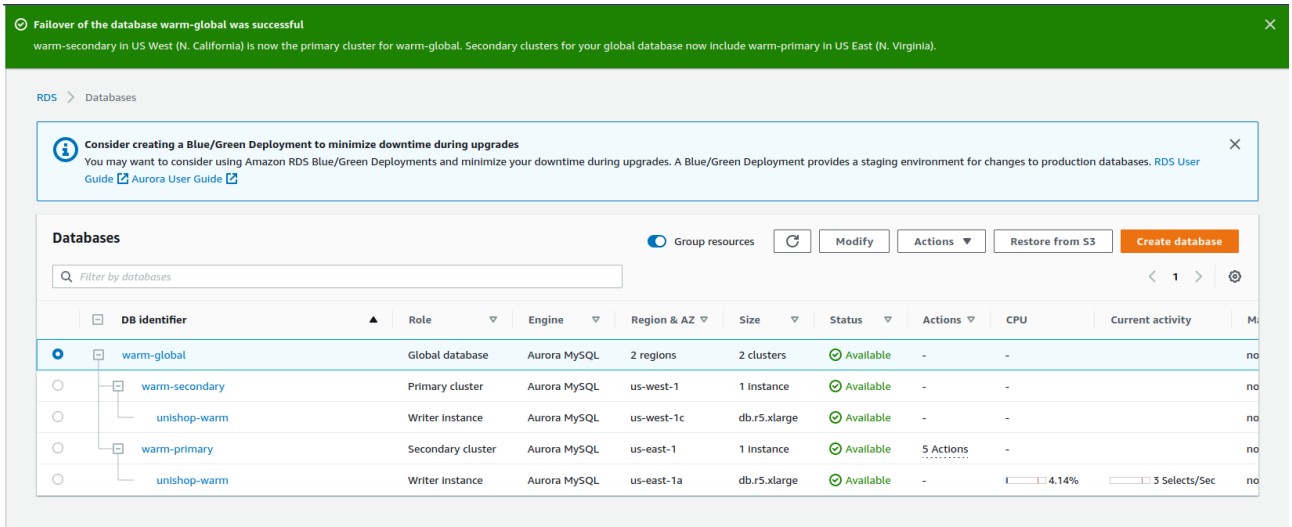
Aktiivisella alueella olevalle sivustolle tehdään tili ja ostoskorin sisältö aikaisemman harjoituksen tavoin.

Aikaisemmassa harjoituksessa Auroran palautuksessa käytettiin suunnittelematonta tapaa. Tässä käytetään toista vaihtoehtoa Managed Planned Failover.

RDS sivulla valitaan global database ja klikataan Fail over global database ja valitaan passiivisella alueella oleva toissijainen klusteri uudeksi ensisijaiseksi klusteriksi kuvat 31 ja 32.

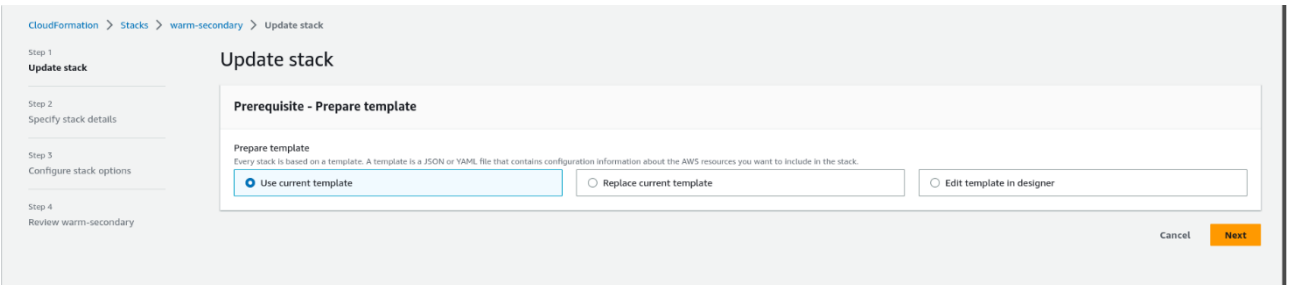


Kuva 31 Auroran tietokantojen muuttaminen

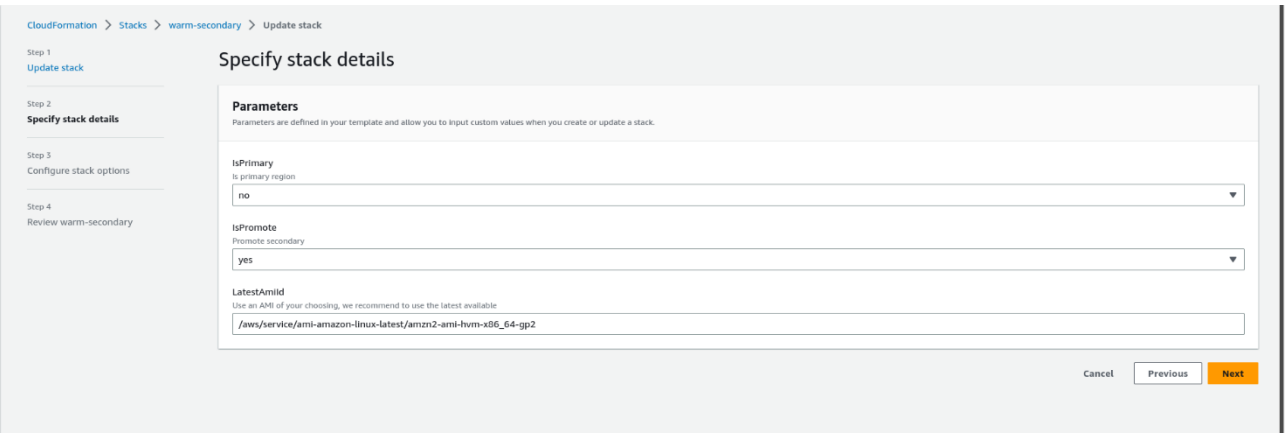


Kuva 32 Muutosten vahvistaminen

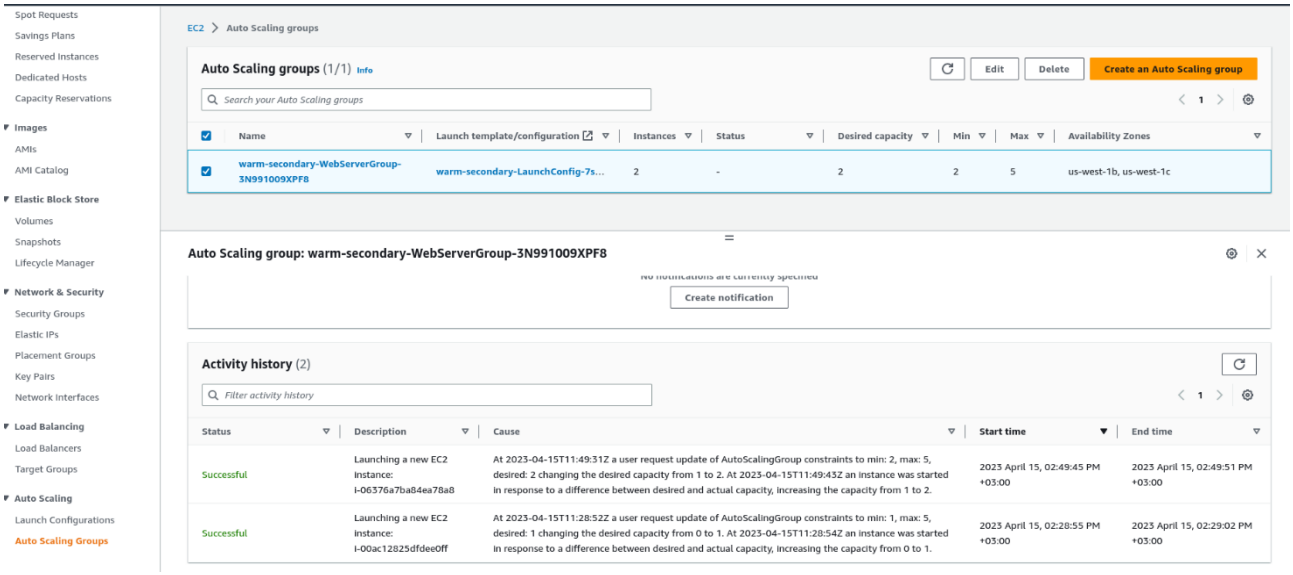
Passiivisen alueen instanssit käynnistetään tässä mallinteen avulla. Valitaan passiivisen alueen mallinne ja valitaan update (kuva 33) ja vaihdetaan IsPromote parametrin arvoksi yes (kuva 34). Mallinteessa sovellus ottaa yhteyden ylennettyyn Aurora klusteriin ja Auto Scaling Groupsin asetuksissa haluttujen instanssien määrä kasvaa samaan mitä se oli aktiivisella alueella (kuva 35).



Kuva 33 Mallin päivittäminen

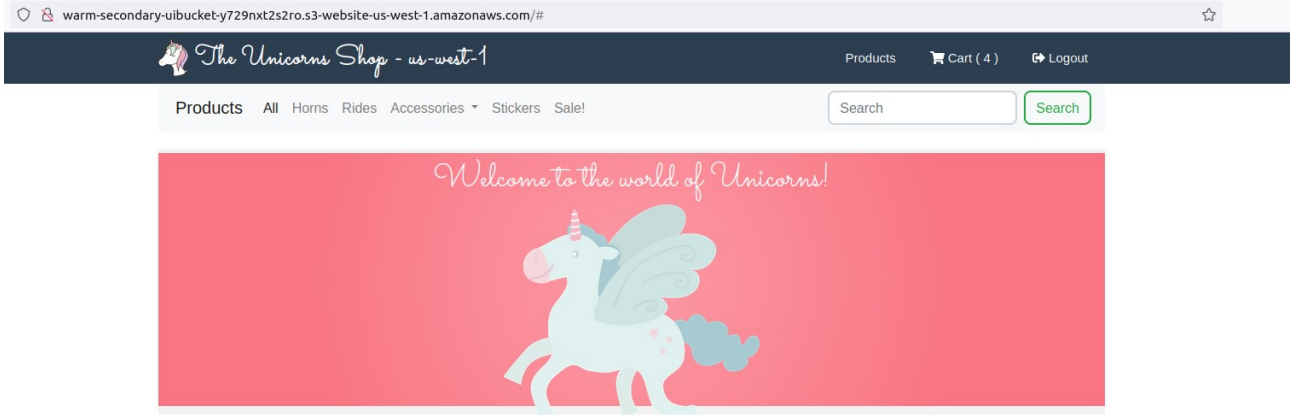


Kuva 34 Parametrin arvon vaihtaminen



Kuva 35 Passiiviselle alueelle pystytetään automaattisesti kaksi instanssia

Aikaisemman harjoituksen tavoin aikaisemmin aktiivisen alueen sivulla ostoskoriin laitetut tavarat ovat edelleen siellä. Tässä vaihtoehdossa passiivisen alueen sivusto itse on koko ajan saavutettavissa.

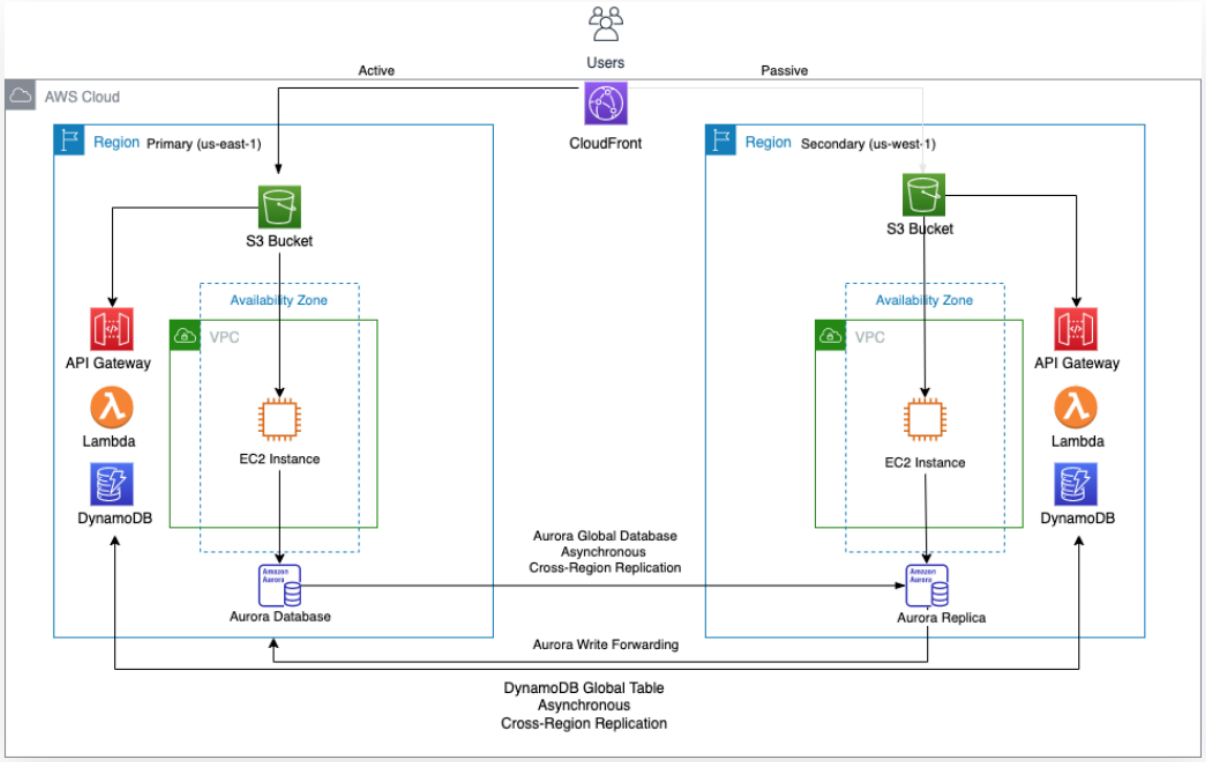


Kuva 36 Passiivisen alueen sovelluksen ostoskoriin on ilmestynyt aktiivisella alueella lisätyt tuotteet

Lopuksi kaikki resurssit tuhotaan samalla tavalla kuin aikaisemminkin molemmilta alueilta järjestyksessä S3, Aurora, ja mallinteet.

Moduuli 4

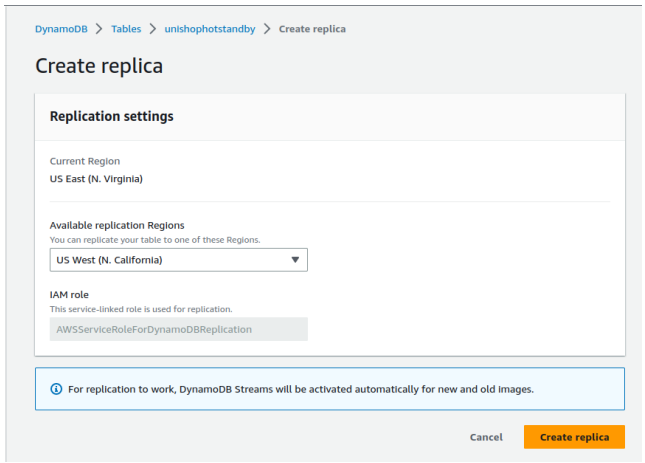
Neljännessä moduulissa tehdään harjoitus hot standby vaihtoehdolle (kuva 37). Tässä sovellus on tuotettu API Gateway ja AWS Lambda palveluilla, mutta se ei ole oleellista harjoituksen kannalta. Tässä tietokantana on sekä Aurora että DynamoDB. Aurora sisältää käyttäjätiedot ja DynamoDB ostoskorin sisällön. Cloudfrontia käytetään sisällönjakamiseen.



Kuva 37 Moduuli 4 arkkitehtuuri (Amazon Web Services 2023)

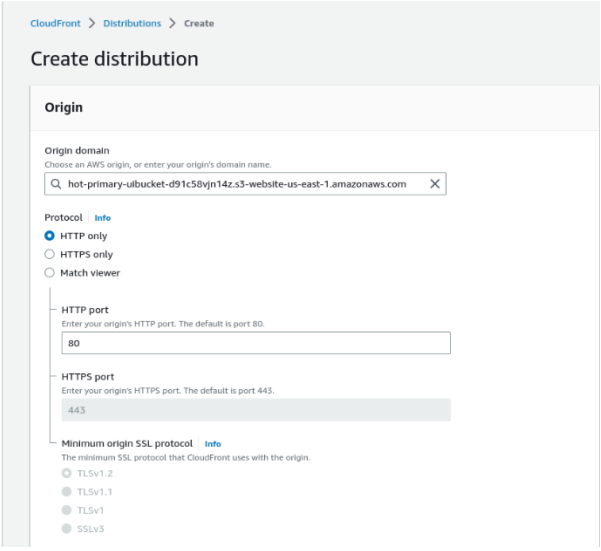
Tässä molempien alueiden infra pystytetään mallinteiden avulla samalla tavalla kuin 2. moduulissakin. Myös sovelluksen testaaminen toimii samoin.

Tietokantaa varten käytetään DynamoDB:n global tables toimintoa, jolla tehdään replika passiiviselle alueelle.

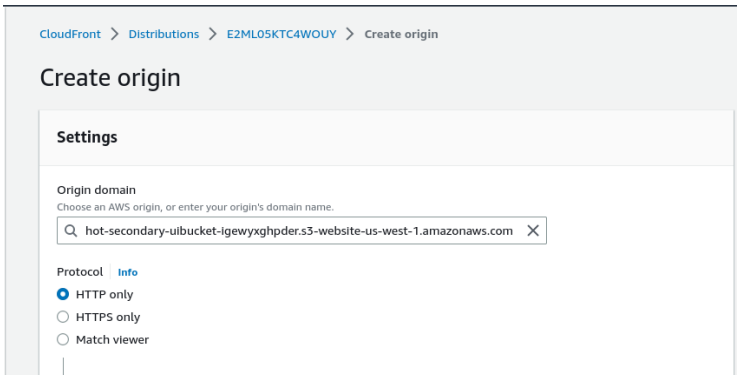


Kuva 38 Replikan tekeminen

CloudFront jakelun origin domainiksi annetaan aktiivisen alueen sivuston URL (kuva 39) ja vaihto-ehtoiseksi originiksi passiivisen alueen sivuston URL (kuva 40).

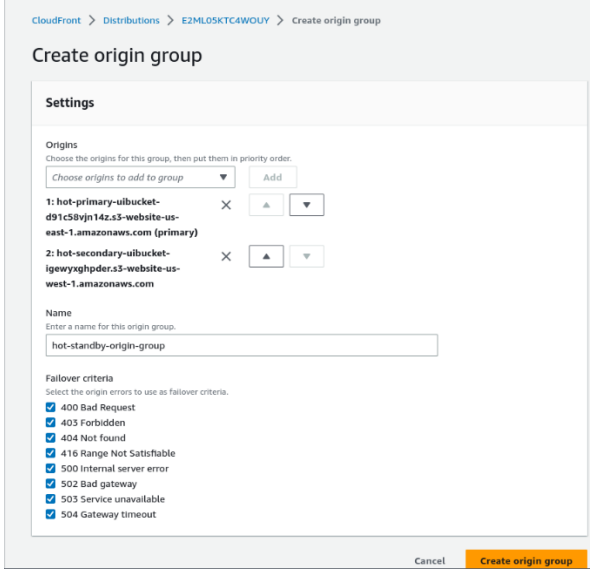


Kuva 39 Origin asettaminen



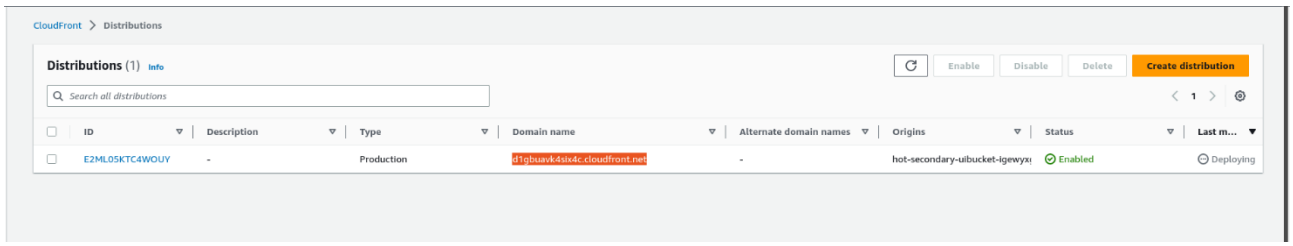
Kuva 40 Vaihtoehtoisen origin asettaminen

Tämän lisäksi tehdään origin group, johon lisätään molempien alueiden S3 varastot ja asetetaan kriteerit vialle (kuva 41).

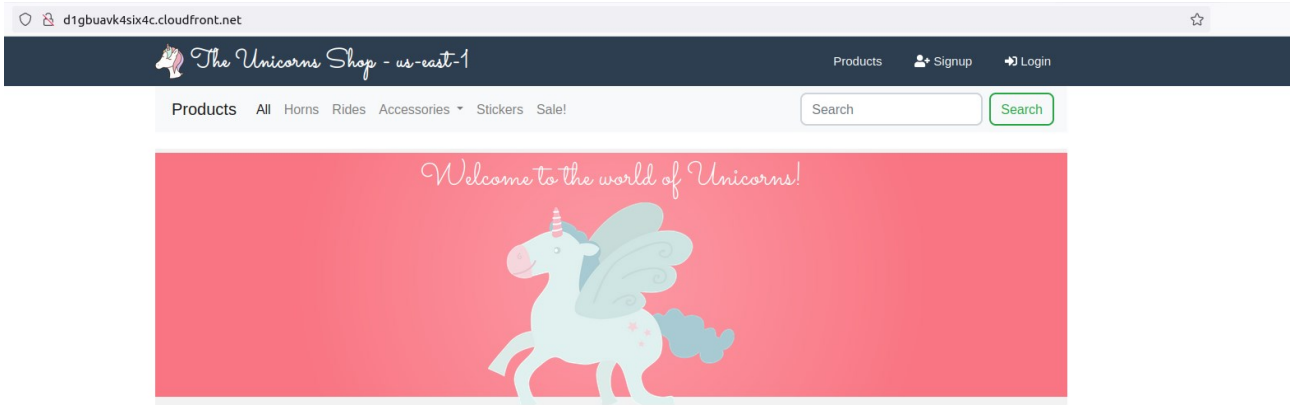


Kuva 41 Origin group asetusten tekeminen

Lopuksi varmistetaan jakelun toimivuus kopioimalla domain name, josta pitäisi avautua sivusto aktiiviselta alueelta (kuvat 42 ja 43).



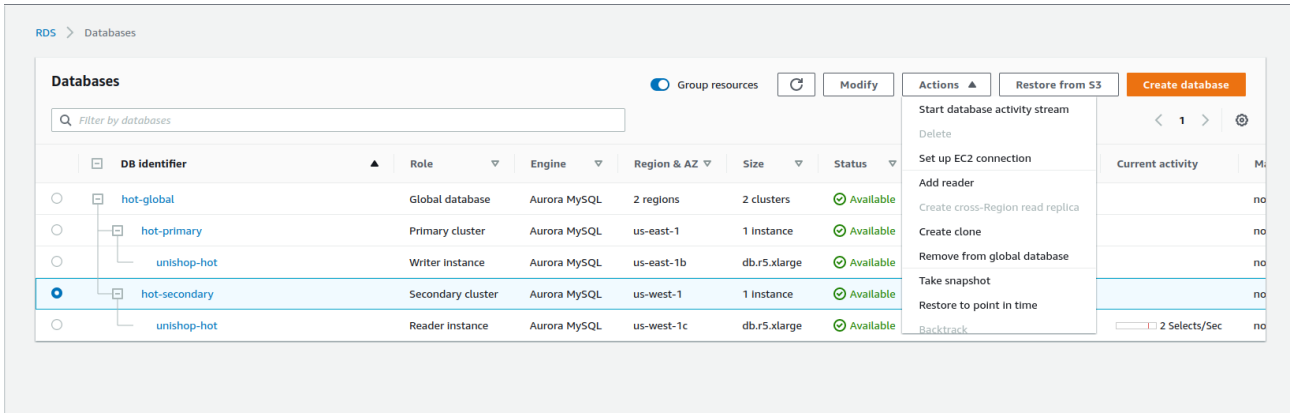
Kuva 42 Osoitteen kopioiminen



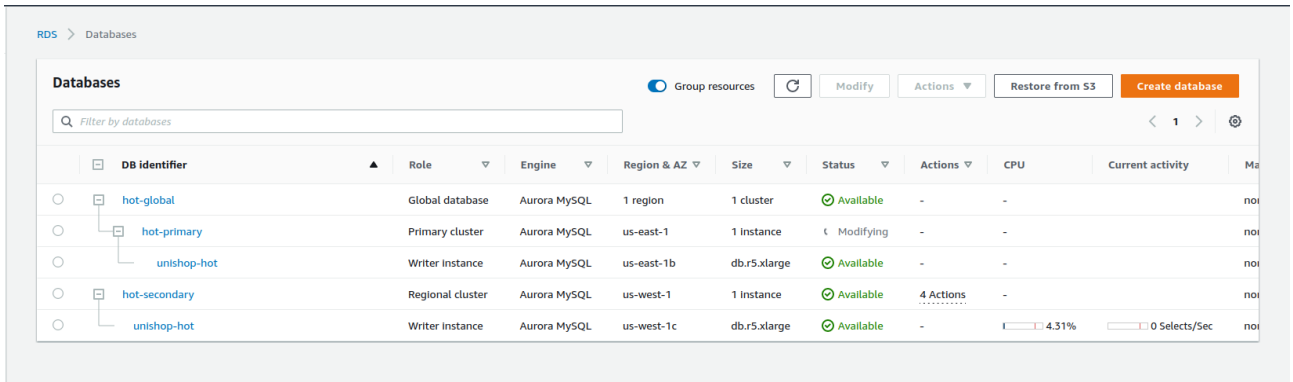
Kuva 43 URL:n toimivuuden varmistaminen

Katastrofia simuloidaan taas estämällä pääsy aktiivisen alueen S3 varastoon.

Käyttäjätiedot tallentava Aurora palautetaan passiiviselle alueelle samalla tavalla kuin 2. moduulissa.

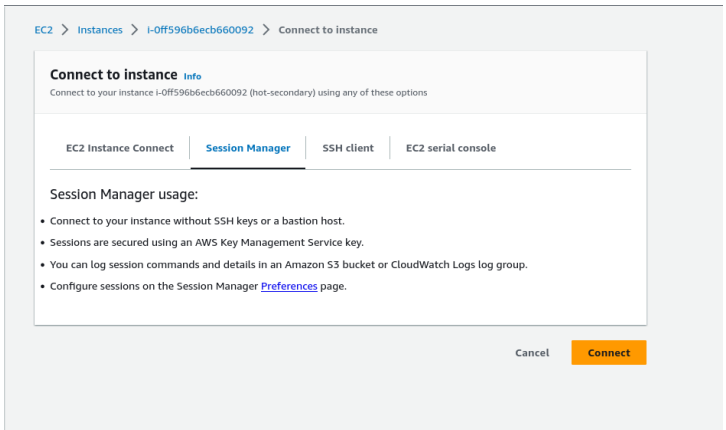


Kuva 44 Auroran tietokantojen muokkaaminen

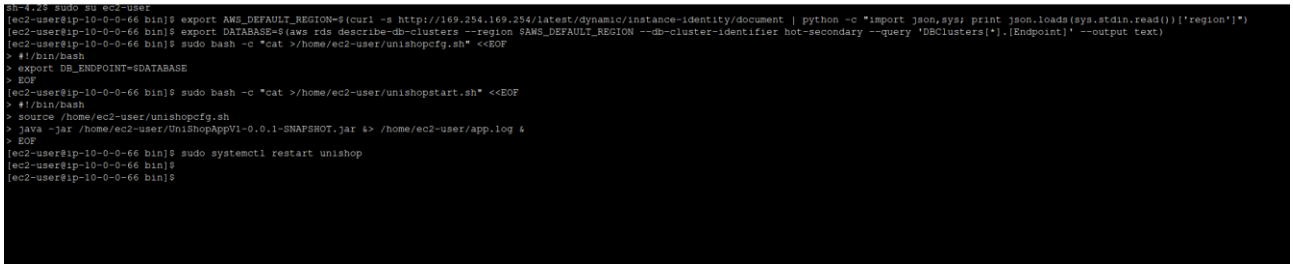


Kuva 45 Tietokantojen muutosten varmistaminen

Kolmannesta moduulista poiketen instanssia ei yhdistetä ylennettyyn klusteriin ajamalla mallinnetta eri parametrillä, vaan siten, että System Manager palvelun avulla otetaan yhteys passiivisen alueen instanssiin (kuva 46) ja ajetaan skripti ja uudelleenkäynnistyksen jälkeen sovellus osoittaa ylennettyyn instanssiin (kuva 47).

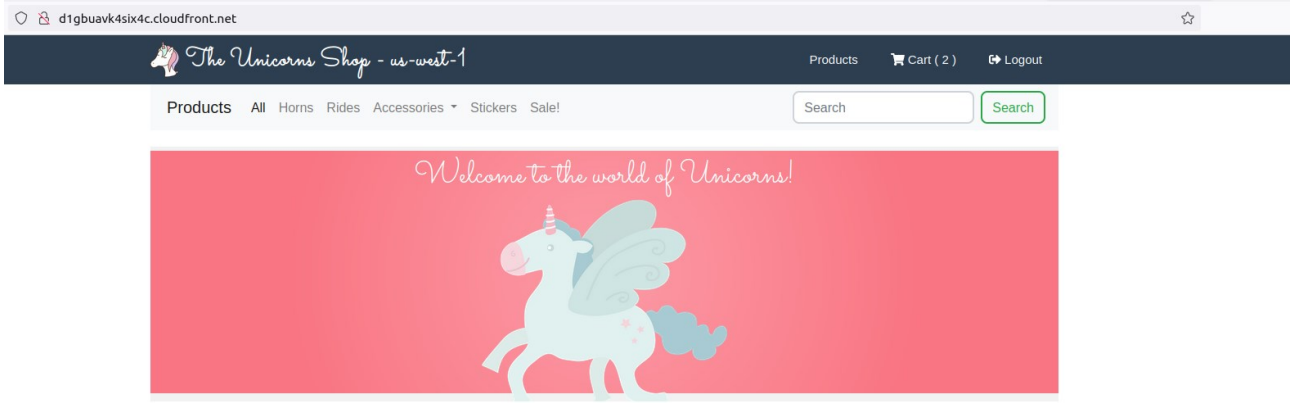


Kuva 46 Yhteyden muodostaminen



Kuva 47 Skriptin ajaminen

Päivittämällä CloudFrontin antamaa domain osoitetta sovellus siirtyy passiiviselle alueelle.



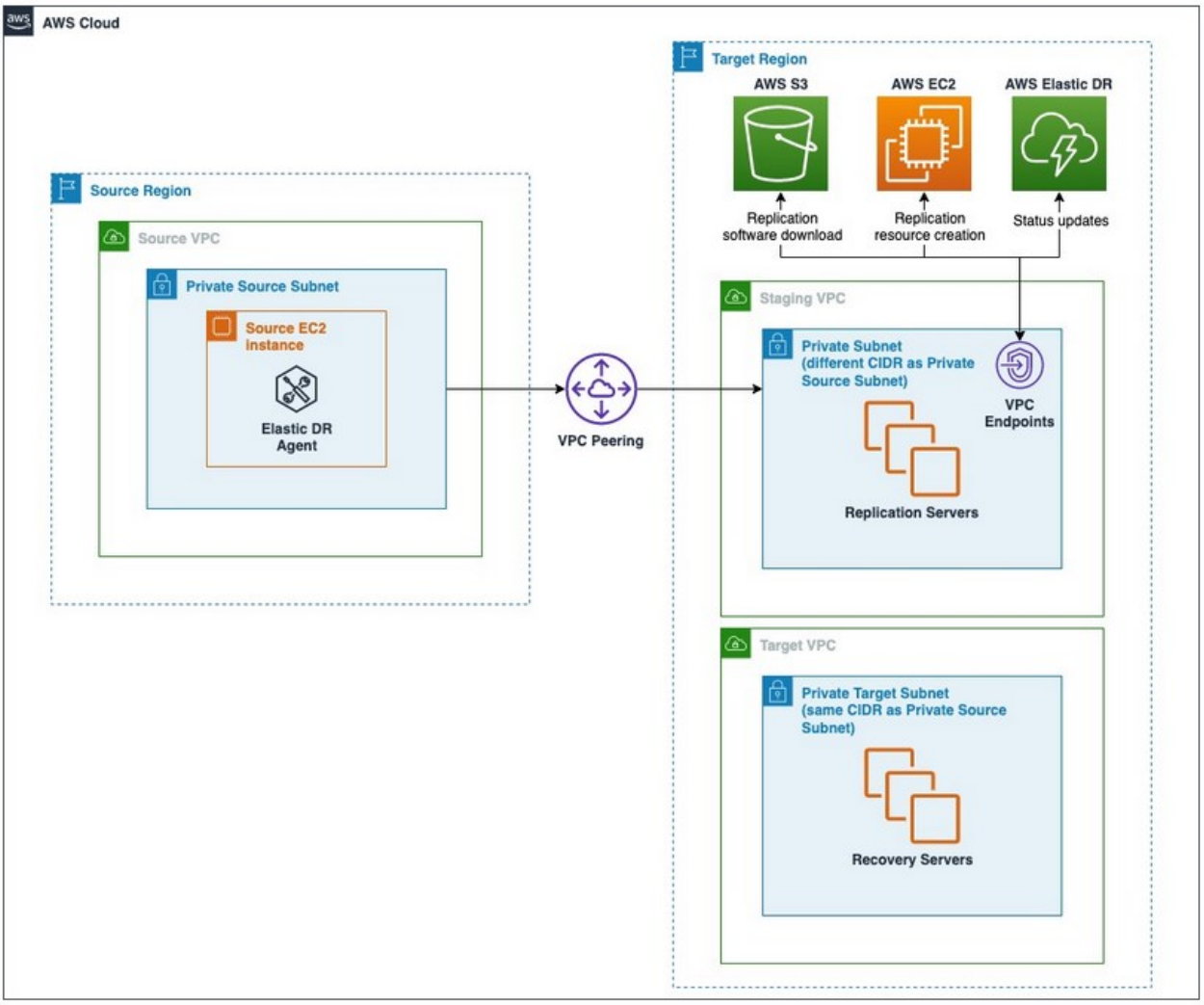
Kuva 48 Päivittämisen jälkeen us-eat-1 on muuttunut us-west-1

Lopuksi kaikki resurssit tuhotaan samalla tavalla kuin aikaisemminkin molemmilta alueilta järjestyksessä S3, DynamoDB, CloudFront, Aurora, ja mallinteet

OSA 2

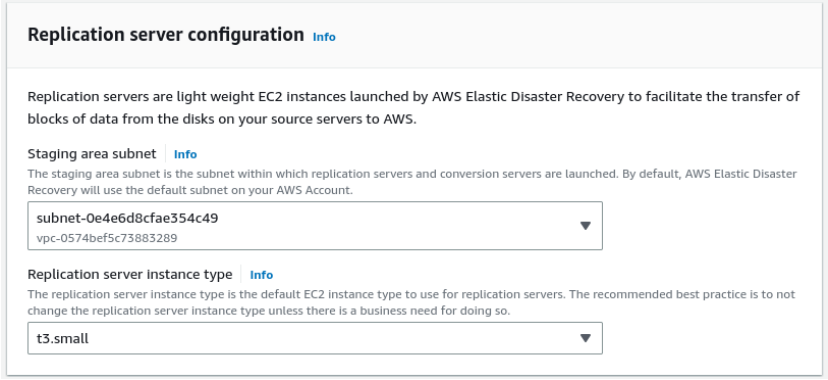
Elastic Disaster Recovery

Tässä harjoituksessa tehdään toipumissuunnitelma wordpress-sovellukselle (kuva 49). Wordpress sovellus on asennettu yhdelle instanssille eu-north-1 alueelle ja se siirretään harjoituksessa us-east-1 alueelle.

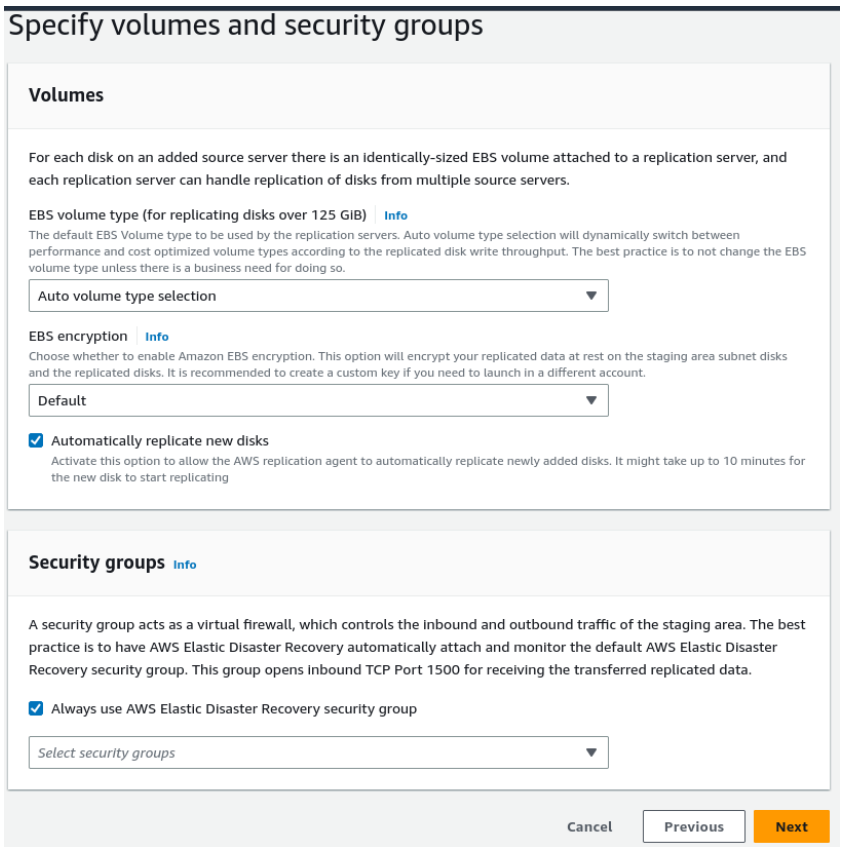


Kuva 49 Elastic Disaster Recovery harjoituksen arkkitehtuuri

Ensin Elastic Disaster Recovery palvelulle konfiguroidaan käytettävä aliverkko, instanssin tyyppi ja security group:ina käytetään palvelun itsensä luomaa, joka avaa portit 443 ja 1500 (kuvat 50 ja 51).



Kuva 50 Replikointi serverin asetukset



Kuva 51 Replikointi serverin asetukset

Seuraavaksi asennetaan agentti Wordpress sovellusta käyttävälle Linux koneelle (kuvat 52, 53, 54).

```
bitnami@ip-172-26-12-254:~$ wget -O ./aws-replication-installer-init.py https://aws-elastic
-disaster-recovery-us-east-1.s3.us-east-1.amazonaws.com/latest/linux/aws-replication-instal
ler-init.py
--2023-04-22 08:00:06--  https://aws-elastic-disaster-recovery-us-east-1.s3.us-east-1.amazo
naws.com/latest/linux/aws-replication-installer-init.py
Resolving aws-elastic-disaster-recovery-us-east-1.s3.us-east-1.amazonaws.com (aws-elastic-d
isaster-recovery-us-east-1.s3.us-east-1.amazonaws.com)... 52.217.93.120, 52.217.94.216, 52.
216.62.242, ...
Connecting to aws-elastic-disaster-recovery-us-east-1.s3.us-east-1.amazonaws.com (aws-elast
ic-disaster-recovery-us-east-1.s3.us-east-1.amazonaws.com)|52.217.93.120|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 27705 (27K) [binary/octet-stream]
Saving to: ‘./aws-replication-installer-init.py’

./aws-replication-inst 100%[===========================>]  27.06K  --.-KB/s    in 0.1s

2023-04-22 08:00:07 (246 KB/s) - ‘./aws-replication-installer-init.py’ saved [27705/27705]
```

Kuva 52 Tarvittavan Python-tiedoston lataaminen

```
bitnami@ip-172-26-12-254:~$ sudo python3 aws-replication-installer-init.py
The installation of the AWS Replication Agent has started.
AWS Region Name: us-east-1
AWS Access Key ID: AKIA2C7N7Y6L7C2NVBWM
AWS Secret Access Key:
Identifying volumes for replication.
Choose the disks you want to replicate. Your disks are: /dev/xvda,/dev/nvme0n1
To replicate some of the disks, type the path of the disks, separated with a comma (for exa
mple, /dev/sda, /dev/sdb). To replicate all disks, press Enter:
```

Kuva 53 Python-tiedoston ajaminen konfigurointi

```
Identified volume for replication: /dev/nvme0n1 of size 20 GiB
All volumes for replication were successfully identified.
Downloading the AWS Replication Agent onto the source server... Finished.
Installing the AWS Replication Agent onto the source server... Finished.
Syncing the source server with the Elastic Disaster Recovery Console... Finished.
The following is the source server ID: s-3776fd540af244aac.
The AWS Replication Agent was successfully installed.
bitnami@ip-172-26-12-254:~$
```

Kuva 54 Agentin asentaminen onnistui

Source servers (1) Info

Actions | Replication | Initiate recovery job

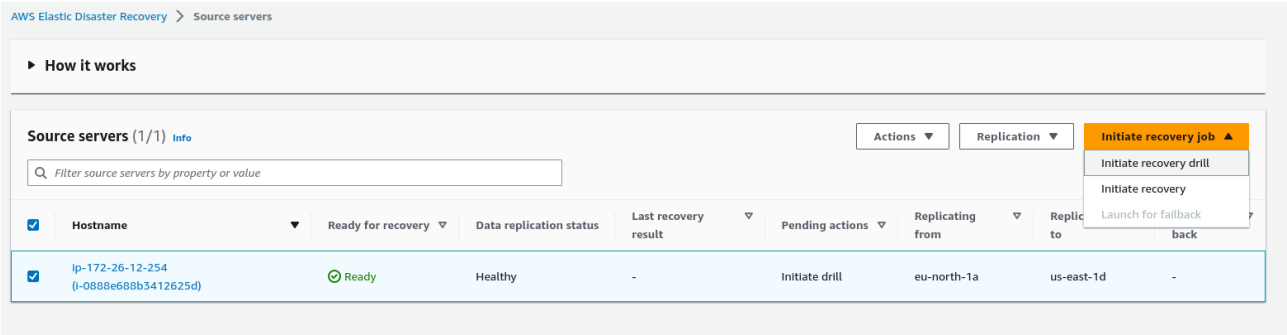
Filter source servers by property or value

Hostname	Ready for recovery	Data replication status	Last recovery result	Pending actions	Replicating from	Replicating to	Failing back
ip-172-26-12-254 (i-0888e688b3412625d)	Ready	Healthy	-	Initiate drill	eu-north-1a	us-east-1d	-

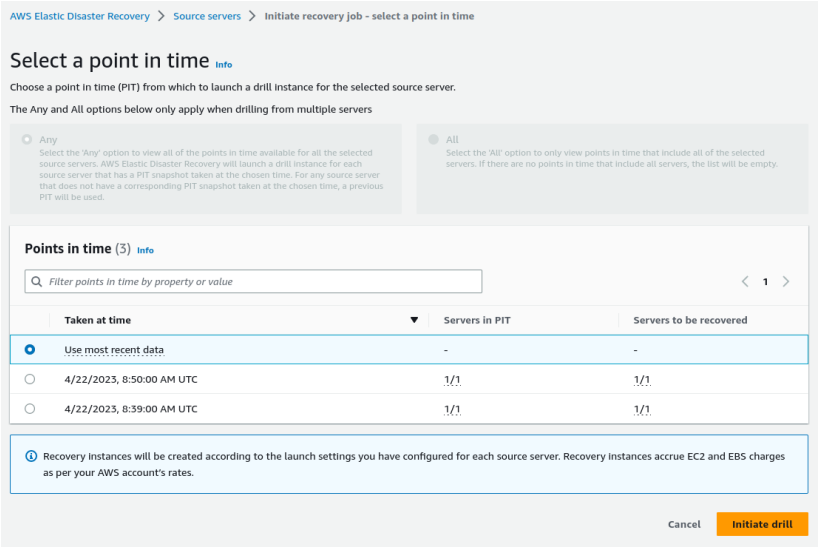
Kuva 55 Agentin asennuksen jälkeen instanssi ilmestyy source servers -välilehdelle

Tässä vaiheessa konfiguroidaan uuden instanssin asetukset, siis sille jolle palautus pystytetään. Avataan sille portit 80 ja 443 (kuva 62). Lisäksi valitaan instanssin koko ja haluttu aliverkko, johon instanssi pystytetään. Instanssille voidaan halutessa antaa sama ip-osoite, joka sillä oli alun perin, mutta havainnollistamisen takia tässä sille annetaan eri osoite.

Seuraavaksi suoritetaan harjoitus instanssin replikoinnille toiselle alueelle ja onnistuneen harjoituksen jälkeen itse varsinainen siirtäminen (kuvat 56 ja 57).

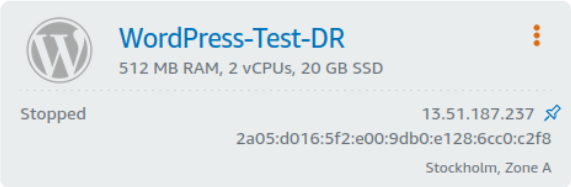


Kuva 56 Valitaan recovery drill eli harjoituspalautus



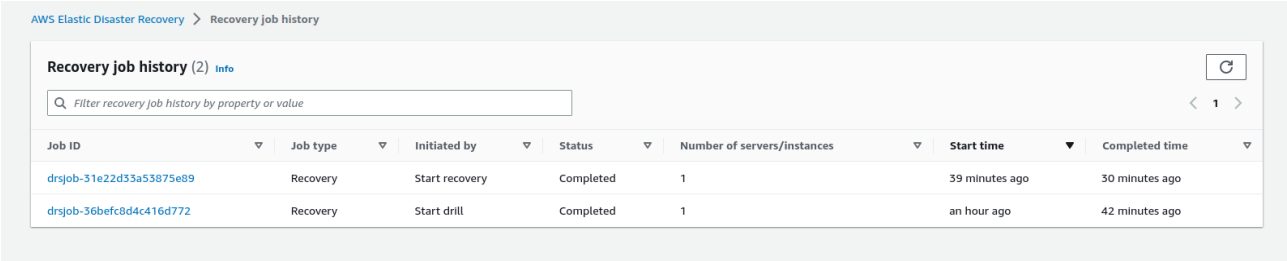
Kuva 57 Valitaan haluttu varmuuskopio

Onnistuneen harjoituksen jälkeen (kuva 59) simuloidaan katastrofia sammuttamalla EC2-instanssi, jolla Wordpress sovellus on. Lopuksi käytetyt resurssit tuhotaan.

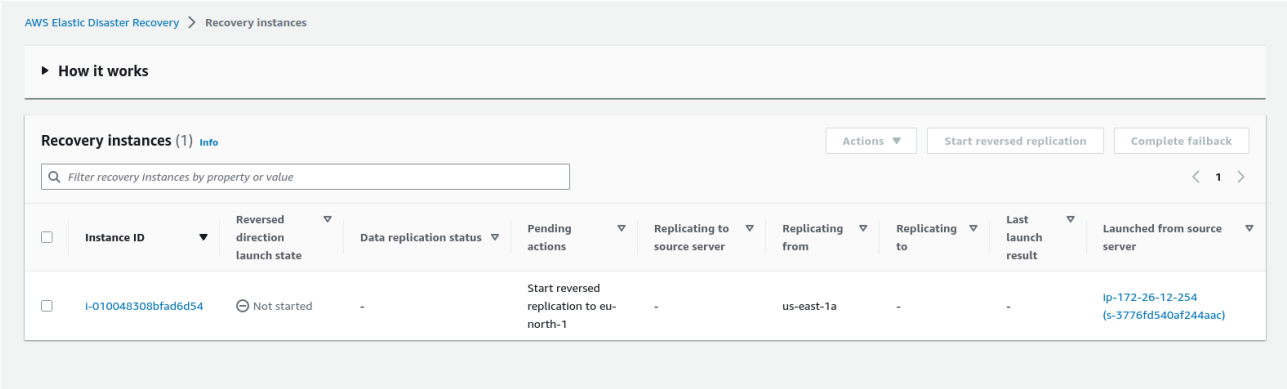


Kuva 58 Katastrofin simulointi

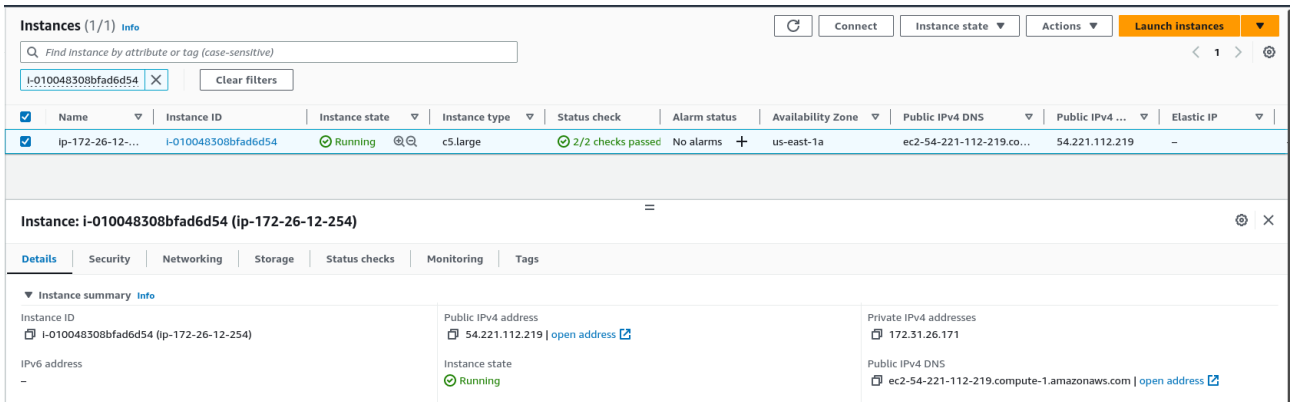
Kun palautus on valmis, nähdään Recovery instances -välilehdellä uusi instanssi ja (kuva 60), jonka ip-osoite kopioidaan (kuva 61) ja sitten testataan, onko sovellus saatavilla (kuva 63).



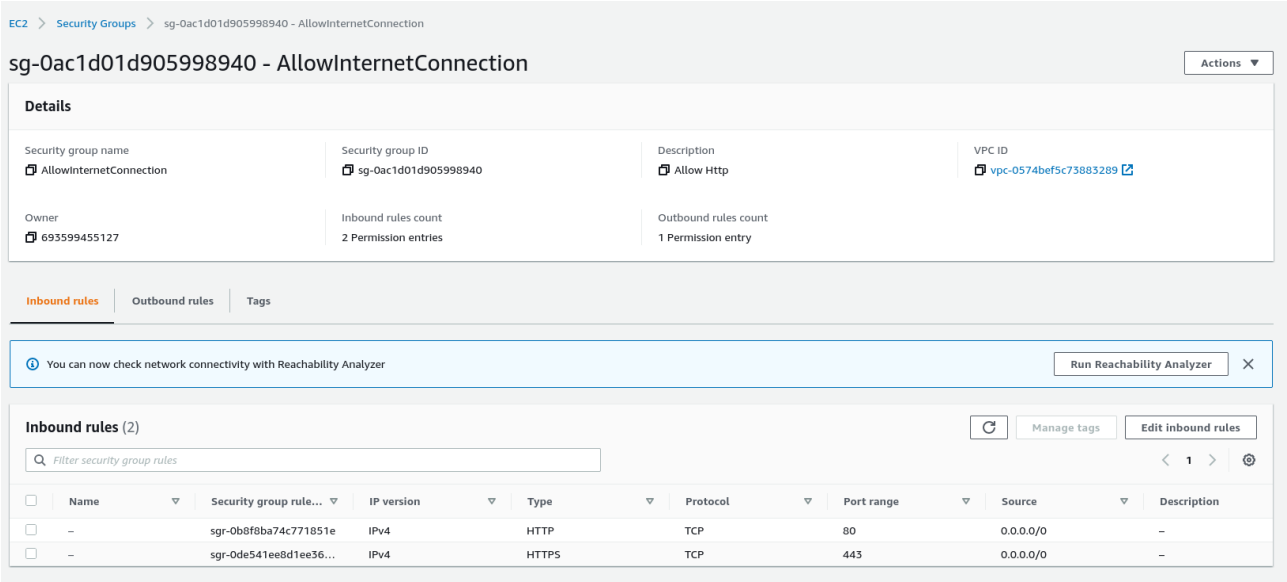
Kuva 59 Työhistoria, jossa näkyy kaksi tehtyä työtä



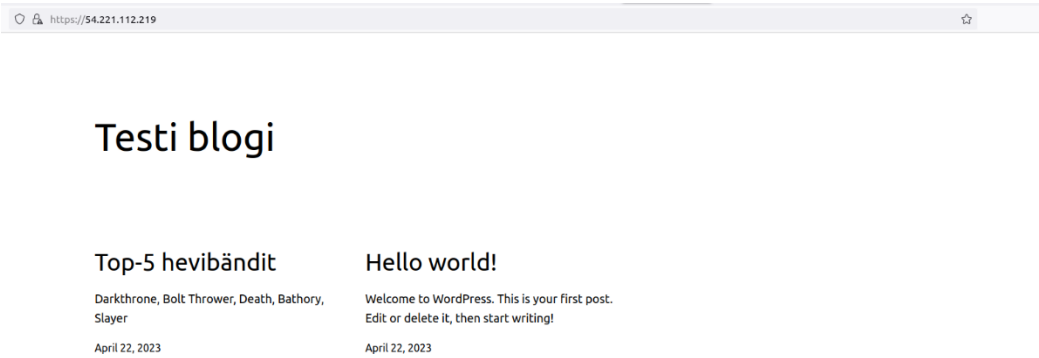
Kuva 60 Replikoitu EC2-instanssi



Kuva 61 Uusi EC2-instanssi uudella alueella



Kuva 62 . Security group, jossa http ja https liikenne sallittu



Kuva 63 Wordpress sovellus toimii uudella alueella uudella ip-osoitteella