Disaster Recovery rješenje bazirano na Cloud servisima

Mehanović, Enver

VELEUČILIŠTE
s pravom javnosti
BALTAZAR ZAPREŠIĆ
Zaprešić

Preddiplomski stručni studij
Informacijske tehnologije

ENVER MEHANOVIĆ

DISASTER RECOVERY RJEŠENJE BAZIRANO NA CLOUD SERVISIMA

PREDDIPLOMSKI ZAVRŠNI RAD

Zaprešić, 2022. godine

VELEUČILIŠTE
s pravom javnosti
BALTAZAR ZAPREŠIĆ
Zaprešić

Preddiplomski stručni studij
Informacijske tehnologije

PREDDIPLOMSKI ZAVRŠNI RAD

DISASTER RECOVERY RJEŠENJE BAZIRANO NA CLOUD SERVISIMA

Mentor:
Prof. dr. Vladimir Šimović

Student:
Enver Mehanović

Naziv kolegija:
PROJEKTIRANJE INFORMACIJSKIH SUSTAVA

JMBAG studenta:
1191017744

SADRŽAJ

SAŽETAK

Informacijski sustavi su ključni element današnjeg poslovanja. Informatizacijom je došlo do promjena procesa, pristupa i načina poslovanja. Velika konkurentnost na tržištu zahtijeva apsolutnu automatizaciju sustava, brzi pristup servisima bez obzira na vrijeme i lokaciju, sa bilo koje platforme. Količine podataka i zahtjevi na procesne resurse rastu eksponencijalno iz dana u dan. Uz sve te zahtjeve uvijek postoji mogućnost od neželjenih događaja, bilo prirodne ili ljudski uvjetovane prirode.

U ovom radu će se pokušati objasniti koncepti, strategija i glavni zahtjevi da bi se osigurao neometan rad informatičkih sustava bez obzira na svakodnevne prijetnje uključujući one manjeg opsega od kojih se lakše obraniti do onih sveobuhvatnih gdje dolazi do dislokacije kompletnog poslovanja. Dislokacija poslovanja ne uključuje samo informatičke sustave nego i ljudstvo, fizičke lokacije i ostale popratne aspekte poslovanja.

Ključne riječi: informacijski sustav, poslovanje, neželjeni događaj, strategija

Title in English: DISASTER RECOVERY SOLUTION BASED ON PUBLIC CLOUD SERVICES

ABSTRACT

Information systems are key element of today's business. Computerization has led to changes in processes, approaches and ways of doing business. Great competitiveness in the market requires absolute system automation, simple and seamless access to services regardless of time and location, platform agnostic. Data volume and requirements on process resources are growing exponentially daily. With all these requirements there is always the possibility of disastrous events, whether natural or human related.

This work will try to explain the concepts, strategy and main requirements in order to ensure the seamless operation of IT systems regardless of everyday threats including those of a smaller scale from which it is easier to defend along with ones on larger scale when is necessary to perform dislocation of the entire business. Business dislocation includes not only IT systems, but also manpower, physical locations and other aspects of the business.

Key words:information system, business, disastrous event, strategy

1. UVOD

Danas živimo u informatičkom dobu gdje se način poslovanja u gotovo svim granama društva i ekonomije temelji na informatizaciji. Zbog same konkurentnosti na tržištu i napretka tehnologije, svjedoci smo svakodnevnog uvođenja novih usluga, servisa i mogućnosti. Takav brzi tehnološki napredak ujedno prati i eksponencijalan rast kompleksnosti informatičkih sustava, povećava njihovu heterogenost i međuovisnost udaljenih servisa koji komuniciraju putem globalne mreže (Internet). Takvo moderno društvo predstavlja i donosi nove izazove kao što su stalna dostupnost servisa i različite vrste prijetnji. Dostupnost samih servisa spada pod infrastrukturno i aplikativno planiranje zaštite i brige o vezanim sustavima. Prijetnje mogu biti različiti neželjeni događaji poput hakerskih i terorističkih napada, prirodne katastrofe, ali i nesvjesne ljudske greške.

Svaki prekid kontinuiteta poslovanja, bez obzira na uzrok, možemo proglasiti poslovnom katastrofom koja, naravno, mogu imati različite nivoe težine i opsega; od lakših i brzo rješivih, do težih, kompleksnih. Bilo koji prekid poslovanja će na manji ili veći način generirati poslovnu štetu, bilo financijsku, reputacijsku, imovinsku ili neku drugu.

Jedini način obrane od bilo koje vrste neželjenih događaja jest unaprijed pripremljena sveobuhvatna strategija zaštite i oporavka od katastrofe. Strategiju čini opsežna dokumentacija koja unaprijed anticipira i definira postupke, tehnologije i rješenja u slučaju neželjenih događaja. Ne treba zaboraviti činjenicu kako traženu informaciju valja dosegnuti što brže, jeftinije i za korisnika pravovremeno, za korištenje (Šimović, 2010).

Cilj ovog rada obuhvatiti segment dislokacije pričuvnih podatkovnih centara u neki od javno dostupnih Cloud servisa i dati primjere softverske potpore implementaciji. Ovaj tip sustava se u najvećem broju slučaja aktivira prilikom težih katastrofa (požar, zemljotres, rat itd.) jer se radi o potpunom izmještanja svih informatičkih resursa sa primarne lokacije podatkovnog centra na sekundarnu (alternativnu). Također, samom pojavom tzv. "računarstva u oblacima" (engl.: cloud computing) i " Cloud servisa omogućeno je korištenje usluga moćnog hardvera i softvera gotovo svugdje i uvijek, te „su suvremeni informacijski sustavi sve više informacijsko-komunikacijski sustavi i mrežni (Šimović, Ružić-Baf, 2013).

2. OPORAVAK OD KATASTROFE *(eng. DISASTER RECOVERY)*

2.1 Definicija oporavka od katastrofe

Oporavak od katastrofe uključuje skup politika, alata i postupaka za omogućavanje oporavka ili kontinuiteta rada vitalne tehnološke infrastrukture i sustava nakon prirodne katastrofe ili katastrofe uzrokovane ljudskim djelovanjem. Plan Oporavka od katastrofe (*DR plan*) fokusiran je na informacijsku tehnologiju (IT) i/ili tehnološke sustave koji podržavaju kritične poslovne funkcije za razliku od pojma Kontinuiteta poslovanja *(eng. Business Continuity)*. DR plan uključuje održavanje svih bitnih aspekata funkcioniranja poslovanja unatoč značajnim neželjenim događajima. Kao takav se može smatrati podskupom Kontinuiteta poslovanja. Oporavak od katastrofe pretpostavlja da se primarna lokacija ne može oporaviti neko vrijeme i predstavlja proces vraćanja podataka i usluga na sekundarnu, unaprijed pripremljenu, lokaciju.[1]

2.1.1 Plan kontinuiteta poslovanja (eng. Business Continuity)

Kako smo i prethodno naveli, DR plan je podskup šireg plana Kontinuiteta poslovanja (BC plan) koji sveobuhvatno definira sposobnost poslovne organizacije da može nastaviti dostavljati svoje proizvode, usluge ili servise u slučaju nekog nepredviđenog incidenta prema unaprijed definiranom prihvatljivom Ugovoru o razini usluge *(eng. Service Level Agreement – SLA)*.

Plan Kontinuiteta poslovanja nije dio ovog rada, ali za bolje razumijevanje je svakako potrebno spomenuti neke elemente od kojih se sastoji:[2]

- Definiranje otpornosti sustava
- Planovi i procedure koje definiraju kontinuitet poslovanja
- Inventura svih vezanih sustava
- Analiza poslovnog utjecaja, prijetnji i različitih scenarija događaja iz kojih definiramo
    - Recovery Point Objective (RPO) – prihvatljiva količina podataka koji se mogu „izgubiti“
    - Recovery Time Objective (RTO) – prihvatljivo vrijeme oporavka usluge ili servisa
    - Consistency Objective (RCO) – definiran kao postotak koji definira prihvatljivu inkonzistentnost između povezanih distribuiranih sustava poslije neželjenog događaja (100% RCO znači da nema inkonzistentnosti između sustava)
- Definiranje potencijalnih prijetnji i rizika – primjeri su pandemija, zemljotres, požar, poplava, terorizam, nestanak struje, krađa, cyber napad itd.

[1] Disaster recovery – Wikipedia, https://en.wikipedia.org/wiki/Disaster_recovery, 27. kolovoza 2022.

[2] Business continuity planning – Wikipedia, https://en.wikipedia.org/wiki/Business_continuity_planning, 28. kolovoza 2022.

- Scenarij utjecaja – identificirati i dokumentirati potrebe u slučaju neželjenog događaja – primjeri su potreba za alternativnom lokacijom, prijevoznim sredstvima, medicinskom skrbi, pričuvni procesni sustavi

Plan Kontinuiteta poslovanja bi trebao u svakoj poslovnoj organizaciji biti kontinuirani proces koji se neprekidno evaluira, analizira, ispravlja i testira kao što pokazuje Slika 1.

Slika 1 – Business Continuity Planning životni vijek

Izvor: What is Bussiness Continuity Planning (28. kolovoz 2022.)

Primjeri ISO standarda za planiranje Kontinuiteta poslovanja[3]

- ISO 22300:2021 Security and resilience – Vocabulary
- ISO 22301:2019 Security and resilience – Business continuity management systems – Requirements
- ISO 22313:2020 Security and resilience – Business continuity management systems – Guidance on the use of ISO 22301
- ISO/TS 22317:2021 Security and resilience – Business continuity management systems – Guidelines for business impact analysis

[3] ISO standards, https://www.iso.org/search.html?q=business%20continuity&hPP=10&idx=all_en&p=0&hFR%5Bcategory%5D%5B0%5D=standard , 28. kolovoza 2022.

- ISO/TS 22318:2021 Security and resilience – Business continuity management systems – Guidelines for supply chain continuity
- ISO/TS 22330:2018 Security and resilience – Business continuity management systems – Guidelines for people aspects on business continuity
- ISO/TS 22331:2018 Security and resilience – Business continuity management systems – Guidelines for business continuity strategy
- ISO/TS 22332:2021 Security and resilience – Business continuity management systems – Guidelines for developing business continuity plans and procedures
- ISO/IEC/TS 17021-6:2015 Conformity assessment – Requirements for bodies providing audit and certification of management systems – Part 6: Competence requirements for auditing and certification of business continuity management systems
- ISO/IEC 27031:2011 Security techniques — Guidelines for information and communication technology readiness for business continuity

2.2 Povijest

1970-e godine

Porast digitalnih tehnologija doveo je i do porasta mogućnosti tehnoloških grešaka i problema. Prije toga, većina tvrtki držala je papirnate zapise, koji iako su podložni požarima i krađama, nisu ovisili o pouzdanoj IT infrastrukturi. Kako su tvrtke počele prihvaćati prednosti digitalnih tehnologija i informatizacije, postajale su svjesnije potencijalnih prekida u radu i problema uzrokovanih tehnološkim zastojima. Sedamdesetih godina prošlog stoljeća pojavile su se prve namjenske tvrtke koje su nudile usluge za oporavak od katastrofa.

Kako je to bila uslužna grana koja je bila nova i nerazvijena na tržištu, rane tvrtke koje su nudile uslugu oporavka od katastrofe su dolazile u tri oblika: vruća, topla i hladna mjesta. Tzv. vruća mjesta *(eng. Hot Site)* dupliciraju cjelokupnu infrastrukturu tvrtke, omogućujući nastavak rada praktički odmah nakon neželjenog događaja. Razumljivo je, međutim, da je ovakva metoda pružanja usluge izuzetno skupa. Topla mjesta *(eng. Warm Site)*, s druge strane, dopuštaju samo da se neki od temeljnih procesa visokog prioriteta štite odmah nakon havarije, čime se inicijalno provodi selekcija servisa, a rezultat je velika financijska ušteda u odnosu na vruća mjesta. Hladna mjesta *(eng. Cold Site)* ne dopuštaju trenutni nastavak bilo kakvih usluga nego se unaprijed izrađuju pričuvne kopije sustava i provodi se povrat podataka u slučaju prekida u radu. Ovom metodom kompanije najviše štede ali, najčešće, ujedno hladno mjesto pruža i alternativni prostor u slučaju katastrofe koja pogađa glavni ured. Ova metoda nosi najveće uštede ali ujedno i najdulje vrijeme oporavka od katastrofe.

1980-e godine

Propisi se uvode u SAD-u 1983. godine koji propisuju da nacionalne banke moraju imati sigurnosni plan koji se može testirati. Ubrzo su slijedile i druge industrijske grane, što je također potaknulo daljnji rast i razvoj tvrtki koje su nudile uslugu oporavka od katastrofa.

1990-e godine

Razvoj troslojne arhitekture odvojio je podatke od aplikacijskog sloja i korisničkog sučelja. To je održavanje i sigurnosno kopiranje podataka učinilo daleko lakšim procesom. Tijekom vremena se uočilo da veliki dio podataka vezanih na aplikacijski dio i korisnički dio je manje-više statičke prirode, dok su podaci koji se nalaze u bazama vrlo dinamični i podložni promjenama. Na taj način je došlo do selektivne izmjene rasporeda izrade pričuvnih kopija što je, posljedično, dovelo do iznimnih ušteda u cijeni, količini prostora za izrade kopija, vremenu oporavka i ostalim ključnim komponentama vezanim za oporavak od katastrofe.

2000-e godine

Napadi na Svjetske trgovinske centre 11. rujna snažno utječu na strategiju oporavka od katastrofa u SAD-u i inozemstvu. Nakon zločina, tvrtke su stavile veći naglasak na to da mogu brzo reagirati i oporaviti se u slučaju neočekivanih poremećaja.

Konkretno, tvrtke su nastojale osigurati oporavak njihovih ključnih servisa i vanjskih komunikacijskih kanala, kako iz altruističkih tako i iz konkurentnih razloga.

Relativno nova tehnologija virtualizacije poslužitelja čini oporavak od katastrofe višestruko bržim procesom. U tradicionalnim sustavima izrade pričuvnih kopija podataka koja se uglavnom oslanjala na korištenje tračnih uređaja, potpuna obnova je mogla potrajati danima dok se virtualni poslužitelji mogli obnoviti unutar nekoliko sati (ili manje) jer tvrtke više nisu morale zasebno obnavljati operativne sustave, poslužitelje i aplikacije nego bi se izrađivala pričuvna kopija kompletnog virtualnog poslužitelja *(eng. Virtual Machine – VM)*.

S virtualizacijom poslužitelja, mogućnost prebacivanja procesa na redundantne ili stand-by poslužitelje kada primarni poslužitelji postanu nedostupni iz bilo kojeg razloga, se također pokazalo kao izuzetno učinkovita metoda za prevenciju od neželjenih događaja.

2010-e godine do danas

Porast računalstva u oblaku omogućio je tvrtkama da eksternaliziraju svoje planove oporavka od katastrofa, poznate i kao oporavak od katastrofe kao uslugu *(eng. Disaster Recovery as a Service - DRaaS)*. Kao i kod drugih usluga u oblaku, takav pristup pruža brojne prednosti u smislu fleksibilnosti, vremena oporavka i troškova.

DRaaS je također izuzetno skalabilan čime se tvrtkama omogućuje da u slučaju širenja i smanjenja obima svog posla mogu izuzetno brzo provesti izmjene na pričuvnom sustavu jer će dobavljač usluge u oblaku *(eng. Cloud Service Provider – CSP)* dodijeliti potrebnu IT infrastrukturu, vrijeme i stručnost kako bi se osigurala pravilna provedba plana oporavka od katastrofa. Time se briga o resursima prebacuje na CSP-ove koji osiguravaju dostupnost resursa u danom trenutku, a uslugu naplaćuju prema količini i vremenu korištenja resursa. Oslobođenjem resursa npr. raskidom ugovora o pružanju usluge između tvrtke i CSP-a, pružatelj usluge preraspoređuje na drugog korisnika i vodi računa da svi resursi budu optimalno popunjeni. Neki CSP-ovi u slučaju viška slobodnih resursa nude tvrtkama resurse po diskontnim cijenama.

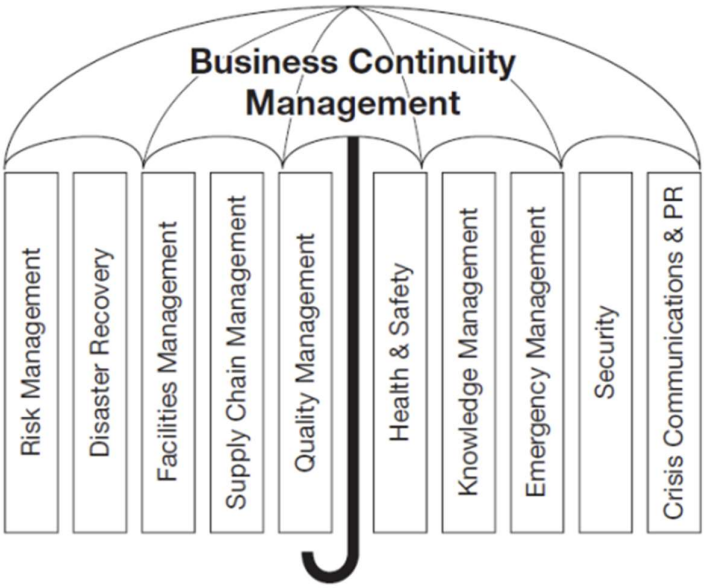
Ovakvim pristupom se oporavak ne temelji na sigurnosnim kopijama i poslužiteljima u stanju pripravnosti *(eng. Stand-by Servers)*, već na virtualne strojeve i skupove podataka, koji se mogu replicirati u roku od nekoliko sekundi ili minuta sa produkcijskim sustavima što im omogućuje pokretanje zamjenskog sustava uživo u roku od nekoliko minuta. Ono što je nekada bilo rješenje samo za najveće organizacije s velikom financijskom sposobnošću danas je dostupno svima.

Međutim, uz napredne usluge kao što je DRaaS koju omogućuju nove tehnologije, dolaze i nove vrste prijetnji. Budući da su zaposlenici povezani s Internetom i korporativnim sustavima, tvrtke će se morati nositi sa porastom zahtjeva revizora i osiguravajućih društava da ulažu i unapređuju sustave za zaštitu od prijetnji poput Ransomwarea[4], koji je sada osim na korisnička računala usmjeren i na poslužitelje tvrtki.

Sve organizacija su potvrdile važnost održavanja kontinuiteta poslovanja i vjerodostojnog plana oporavka od katastrofa što se i odražava u prognozi rasta za taj sektor, a predviđa se da će tržište DRaaS-a do 2020. vrijediti 6,4 milijarde dolara.[5]

2.3 Upravljanje kontinuitetom poslovanja

Disaster recovery je dio cjelokupnog interdisciplinarnog procesa upravljanja kontinuitetom poslovanja.



Slika 2 – Business Continuity Management elementi

Izvor: Reuvid, J. (2005) The Secure Online Business Handbook

[4] Ucjenjivački softver (engl. ransomware) je vrsta štetnog softvera koja korisniku uskraćuje pristup računalnim resursima i traži plaćanje otkupnine za uklanjanje ograničenja. Neki oblici ransomwarea kriptiraju datoteke, dok drugi jednostavno zaključavaju sustav te prikazuju poruku koja korisnika nagovara na plaćanje otkupnine., Ransomware – Wikipedia, https://hr.wikipedia.org/wiki/Ransomware, 2. rujna 2022.

[5] A brief history of disaster recovery, https://www.comparethecloud.net/articles/a-brief-history-of-disaster-recovery/, 14. travnja 2022.

Upravljanje kontinuitetom poslovanja je proces koji u sebi sadržava mnoge, ne samo tehničke politike, za zaštitu od neželjenih događaja. Obuhvaća i upravljanje rizicima, imovinom, kvalitetom, logistikom, fizičkom zaštitom, zdravljem i sigurnošću djelatnika itd. Sve politike propisane upravljanjem kontinuiteta poslovanja se redovno revidiraju, nadopunjuju i unapređuju. Kako su svi djelatnici organizacije obuhvaćeni politikama kontinuiteta poslovanja, zadužene osobe se trebaju brinuti da su djelatnici upoznati sa politikama, provoditi edukaciju i stvarati svijest o sigurnosti, znanju i postupcima kod hitnih slučajeva.

3. DISASTER RECOVERY RJEŠENJE U CLOUD OKOLINI

3.1 Disaster recovery plan

Prije bilo kakvih radova na implementaciji DR rješenja, potrebno je izraditi kvalitetan plan i pokriti sve elemente. Primjer plana je prikazan u nastavku:[6]

1. Korak : Ciljevi plana oporavka od katastrofe
    a. Minimizirati prekide u regularnom poslovanju
    b. Ograničiti opseg prekida i štete
    c. Minimizirati financijski i reputacijski utjecaj na tvrtku
    d. Implementirati alternativne načine nastavka poslovanja
    e. Kontinuirano učiti i provoditi treninge za zaposlenike prema procedurama za slučaj katastrofe
    f. Osigurati neometanu i brzu obnovu svih ključnih servisa
2. Korak : Popis osoblja i zaduženja
    a. Izraditi i redovno ažurirati tablicu zaduženja svih osoba uključenih u aktivnosti oporavka od katastrofe (grupirati po zaduženjima)
        i. Ime i prezime
        ii. Pozicija u organizaciji
        iii. Adresa
        iv. Telefon
3. Korak : Popis aplikacija
    a. Izraditi listu svih ključnih aplikacija i servisa sa potrebnim informacijama (grupirati po profilima aplikacija)
        i. Naziv aplikacije
        ii. Kritičnost
        iii. Dobavljač
        iv. Komentari
        v. Kontakti (ako su potrebni vanjski kontakti)
4. Korak : Inventura hardvera
    a. Izraditi listu svog ključnog hardvera sa potrebnim informacijama
        i. Model
        ii. Proizvođač
        iii. Opis
        iv. Serijski broj
        v. Vlasništvo ili najam
        vi. Cijena
5. Korak : Procedure za izradu pričuvnih kopija podataka i servisa

[6] Example- Disaster recovery plan – IBM documentation, https://www.ibm.com/docs/en/i/7.3?topic=system-example-disaster-recovery-plan, 2. rujna 2022.

   a. Opisati detaljno na koji način se dnevno/tjedno/mjesečno provodi izrada pričuvnih kopija *(eng. Backup policies and procedures)*, definirati redovne provjere i alternativne lokacije u slučaju višestrukih kopija podataka
6. Korak : Procedure oporavka od katastrofe
   a. Iniciranje postupaka u hitnim slučajevima – navesti sve korake iniciranje postupka; prvi kontakt, organizacija DR tima, ustanoviti nivo nezgode, pokrenuti adekvatan plan oporavka, pratiti progres, kontaktirati alternativnu lokaciju i pokrenuti procedure, kontaktirati sve uključene osobe definirane u prethodnim točkama plana, kontaktirati i obavijestiti dobavljače usluga, obavijestiti krajnje korisnike o prekidu usluge
   b. Nastavak postupka po timovima – dodijeliti zadatke svim timovima, osigurati smještaj, logistiku i prijevoz djelatnicima za nastavak rada, prikupiti telefonske brojeve za kontakt, osigurati medicinsku pomoć (u slučaju potrebe)
   c. Puštanje u rad i provjera alternativne lokacije – timovi zaduženi za povrat podataka pokreću sustave i vraćaju podatke na alternativnoj lokaciji, osiguravaju mrežnu povezivost i testiraju ispravnost rada servisa i aplikacija
7. Korak : Povratak na primarnu lokaciju
   a. Nakon prestanka ili oporavka od katastrofalnog događaja i osiguravanja uvjeta na primarnoj lokaciji, pripremiti timove za povratak na primarnu lokaciju
   b. Osigurati sve potrebne resurse na primarnoj lokaciji (fizička lokacija, hardver, dostupnost el. energije, komunikacija itd.)
   c. Pokrenuti reverznu proceduru za povrat koja uključuje izrade pričuvnih kopija ili prijenos podataka sa sekundarne na primarnu lokaciju, podizanje primarne lokacije iz kopiranih ili prenesenih podataka i reinstalacija, puštanje u rad i testiranje
   d. Povrat zaposlenika na primarnu lokaciju i provjere dostupnosti servisa i aplikacija od strane djelatnika pojedinih odjela

3.2 Odabir pružatelja cloud usluge

Ako se organizacija odluči da svoju alternativnu (DR) lokaciju implementira kod nekog od DRaaS pružatelja usluga, koji su velikom broju slučajeva ujedno i pružatelji usluga javnih servisa u Cloudu, potrebno je voditi računa o više pokazatelja tako da se mitigira mogućnost bilo kakvog potencijalnog rizika.

Potrebno je voditi računa o kontroli pristupa sustavu, osobito u slučaju aktiviranja DR lokacije. Osigurati pristup kritičnim komponentama sustava i podataka je imperativ kao i spriječiti neovlašteni pristup da se izbjegne bilo kakvo potencijalno nanošenje štete. Svakako bi bilo dobro da pružatelj usluge ima implementiran SOC 2 standard (eng. Service Organization Control 2) gdje se može tražiti zadnji izvještaj. Kako SOC 2 standard nameće redovitu reviziju i nadzor od strane neovisnih revizijskih kuća, a uključuje sigurnost, dostupnost, povjerljivost,

integritet procesnih resursa i metrike privatnosti, na ovaj način se može vrlo brzo ustanoviti stanje DRaaS pružatelja usluga.

Kako se u slučaju DRaaS usluge, poslovni podaci, baze i aplikacije nalaze u cloud okruženju, izuzetno je bitna sigurnost podataka u samim cloud podatkovnim centrima. Iz tog razloga je potrebno provjeriti sa pružateljem usluga na koji način su podaci osigurani, tko od strane pružatelja usluga ima pristup, da li postoji redudancija između podatkovnih centara i da li se to može potvrditi dokumentacijom.

Svakako je provjeriti i SLA uvjete koje nudi pojedini pružatelj usluge i koliko brzo može reagirati na aktivaciju DR procedure, da li ima uvijek dovoljno procesnih resursa, podatkovnog prostora, komunikacijskih veza, kolika je njihova propusnost i, ako postoje, neki drugi parametri.

Jedni od važnijih parametara, osobito za budući planirani rast organizacije, jesu skalabilnost i elastičnost tj. u kojem kapacitetu i koliko brzo pružatelj usluga može osigurati dodatne resurse u slučaju potrebe. Eventualni podatak o planiranom širenju podatkovnih centara u budućnosti bi svakako bio poželjan.

Dostupnost pružatelja usluge je imperativ jer kako se organizacija štiti od neželjenih događaja, tako i pružatelj usluga je dužan štititi svoje podatkovne centre. Svaki od podatkovnih centara mora imati višestruke podatkovne linije po različitim trasama i višestruke izvore el. energije. SOC2 izvještaj može biti izvor podataka o gore navedenom.

Pružatelj usluga je također odgovoran da prema politikama načina zaštite i izrade pričuvnih kopija podataka vodi računa o tome da su pohranjeni na siguran način i da nije narušen integritet samih podataka niti na koji način.

Na zahtjev korisnika, pružatelj usluge treba osigurati nesmetanu kontrolu i testiranje DR procedura *(eng. Disaster Recovery Drill / Test Run)*.[7]

[7] 8 things to consider before choosing your DRaaS provider, https://www.msystechnologies.com/blog/8-things-to-consider-before-choosing-your-draas-provider/, 2. rujna 2022.

4. PRIMJER IMPLEMENTACIJE RJEŠENJA

Pružatelj usluga implementacije je fiktivna tvrtka „ITcom“. Klijent je fiktivna tvrtka „Contoso d.d.“.

4.1 Projekt sa Microsoft Azure Site Recovery (ASR) DRaaS servisom

4.1.1 U opsegu projekta

- Detaljno planiranje sustava za oporavak u slučaju katastrofe
- Konfiguracija Azure okoline (Site Recovery, Networking, Azure VM instance)
- Konfiguracija Azure Site Recovery sustava za Hyper-V okolinu
- Konfiguracija Azure Site Recovery sustava za fizičke poslužitelje
- Konfiguracija Domain Controller poslužitelja u Azure okolini
- Izrada procedura za testiranje DR okoline
- Izrada procedura za produkcijsku aktivaciju DR okoline
- Upravljanje projektom

4.1.2 Izvan opsega projekta

- Planiranje i izrada procesa i procedura za kontinuitet poslovanja (Business Continuity) nakon aktivacije sekundarnog podatkovnog centra
- Sve što nije navedeno u poglavlju „U opsegu projekta“

4.2 Koncept rješenja

4.2.1 Općenito

Korisnik Contoso d.d. je odlučio izgraditi sekundarnu lokaciju za svoj podatkovni centar u slučaju havarije na primarnoj lokaciji. Odabrano rješenje podrazumijeva replikaciju svih servisa u Microsoft javni oblak, testiranje repliciranih servisa u slučaju prekida rada primarnog podatkovnog centra te izradu sigurnosne kopije sekundarnog podatkovnog centra u slučaju pokretanja procedure prebacivanja servisa u Azure.

ITcom je pristupio sa prijedlogom rješenja koristeći Azure Site Recovery servis pomoću kojeg će replicirati servise i aplikacije korisnika u Azure javni oblak. Sam servis se sastoji od dvije komponente i obje će biti korištene za potrebe implementacije sekundarne lokacije podatkovnog centra.

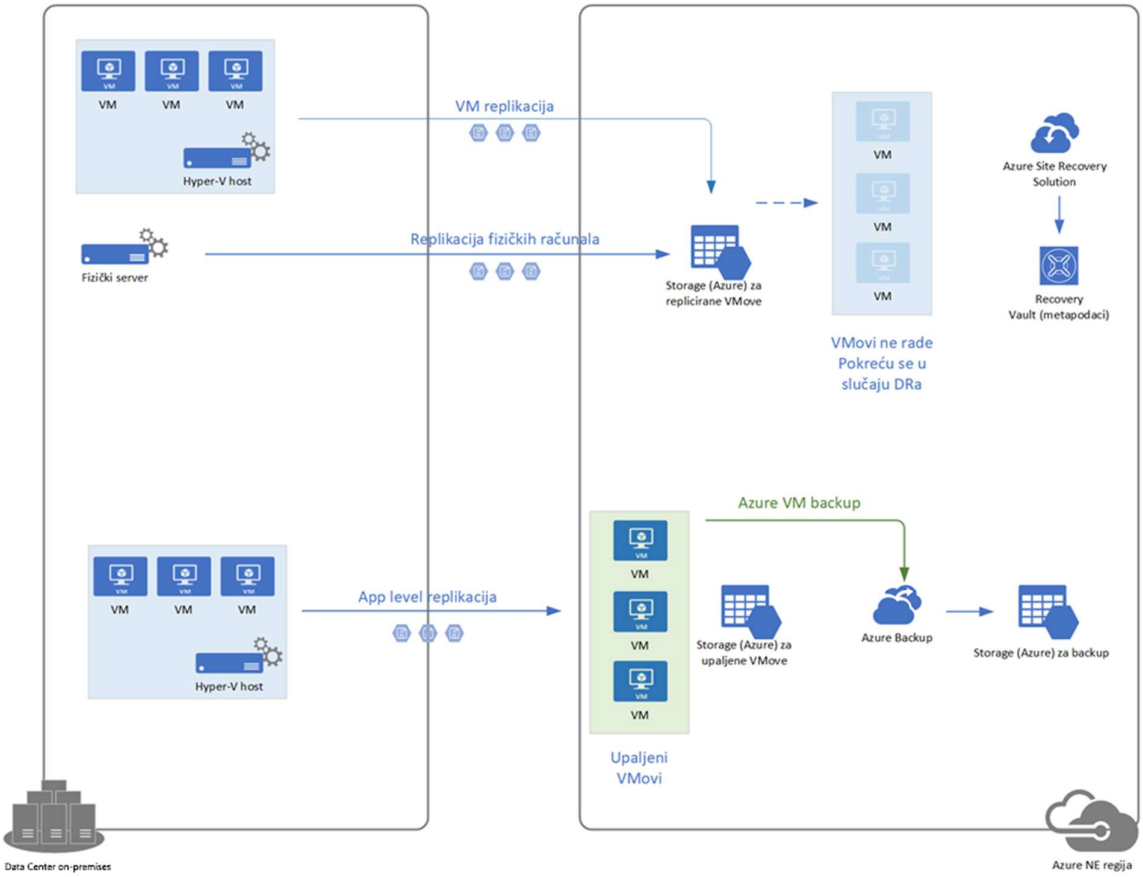
Site Recovery servis: omogućava poslovni kontinuitet replicirajući servise i aplikacije iz on-premises okoline u Azure javni oblak i pokrećući ih kada dođe do prekida rada u primarnom podatkovnom centru. Site Recovery servis replicira servise i aplikacije s virtualnih i fizičkih poslužitelja s primarne lokacije na sekundarnu. Kada se dogodi prekid rada primarne lokacije, pomoću Site Recovery servisa provodimo prebacivanje na sekundarnu lokaciju gdje

korisnikovi servisi i aplikacije nastavljaju s radom. Nakon osposobljavanja primarne lokacije za rad, sve replicirane servise i aplikacije možemo vratiti nazad.

Backup servis: Sprema sigurnosne kopije virtualnih poslužitelja te ih po potrebi vraća u zadnje kopirano stanje.

4.2.2 Shema sustava

4.2.2.1 Izgled sustava nakon implementacije DR rješenja



Slika 3 – ASR shema implementacije rješenja

4.2.3 Azure Site Recovery (ASR) za Hyper-V platformu

Ovaj dio dokumenta opisuje kako funkcionira ASR servis kada replikaciju provodimo s Hyper-V hosta u Azure data centar. ITcom je odabrao North Europe regiju Azure za sekundarnu lokaciju podatkovnog centra zbog najmanje udaljenosti, pa time i latencije između korisnika i Azure podatkovnog centra.

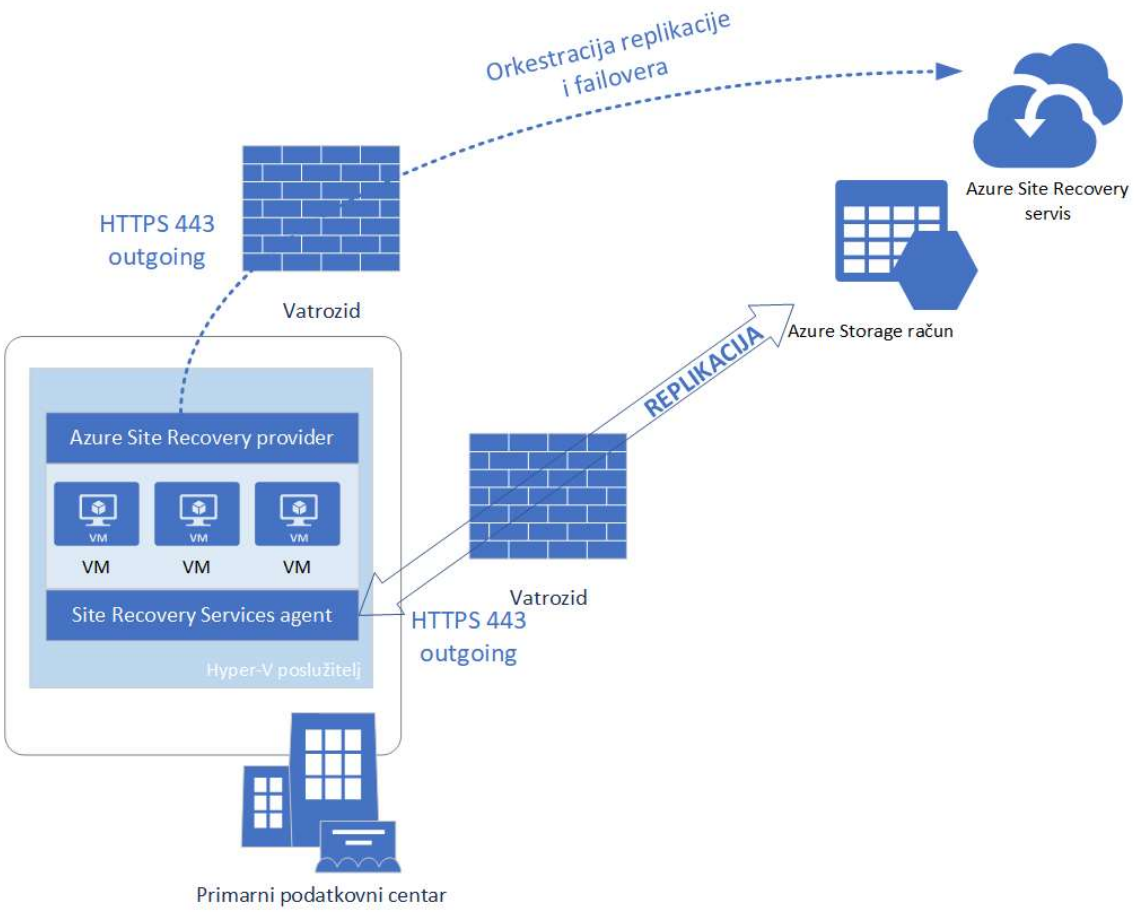
4.2.3.1 Arhitektura komponenti

Slijedeća tablica prikazuje općeniti pogled na komponente koje se koriste prilikom replikacije virtualnih mašina s Hyper-V poslužitelja na Azure. U ovom slučaju, Hyper-V poslužitelji nisu upravljani pomoću System Center Virtual Machine Manager sustava.

Komponenta	Zahtjev	Detalji
Azure	Azure pretplata, Azure storage račun i Azure mreža	Svi replicirani podaci se spremaju u Azure storage račun. Azure virtualne mašine se kreiraju pomoću repliciranih podataka kada se dogodi prebacivanje servisa iz primarnog u sekundarni podatkovni centar. Kada se Azure virtualna mašina kreira, spaja se na Azure virtualnu mrežu.
Hyper-V	Prilikom implementacije ASR servisa, svi Hyper-V serveri i Hyper-V klasteri se dodaju u Azure Hyper-V lokacije. Azure Site Recovery Provider i Recovery Services agent se instaliraju na svaki samostalni Hyper-V poslužitelj i na svaki čvor Hyper-V klastera	Provider orkestrira replikaciju s ASR servisom putem Interneta. Recovery Services agent upravlja samom replikacijom podataka. Komunikacija oba ova servisa s Azure javnim oblakom je kriptirana. Podaci koji se repliciraju u Azure storage račun su također kriptirani.
Hyper-V virtualne mašine	Jedna ili više virtualnih mašina	Na virtualnu mašinu nije potrebno ništa specifično instalirati.

Tablica 1 – ASR komponente sustava

4.2.3.1.1 Hyper-V u Azure replikacija



Slika 4 – ASR koncept replikacije Hyper-V virtualizacijskog sustava

4.2.3.2 Proces replikacije i oporavka

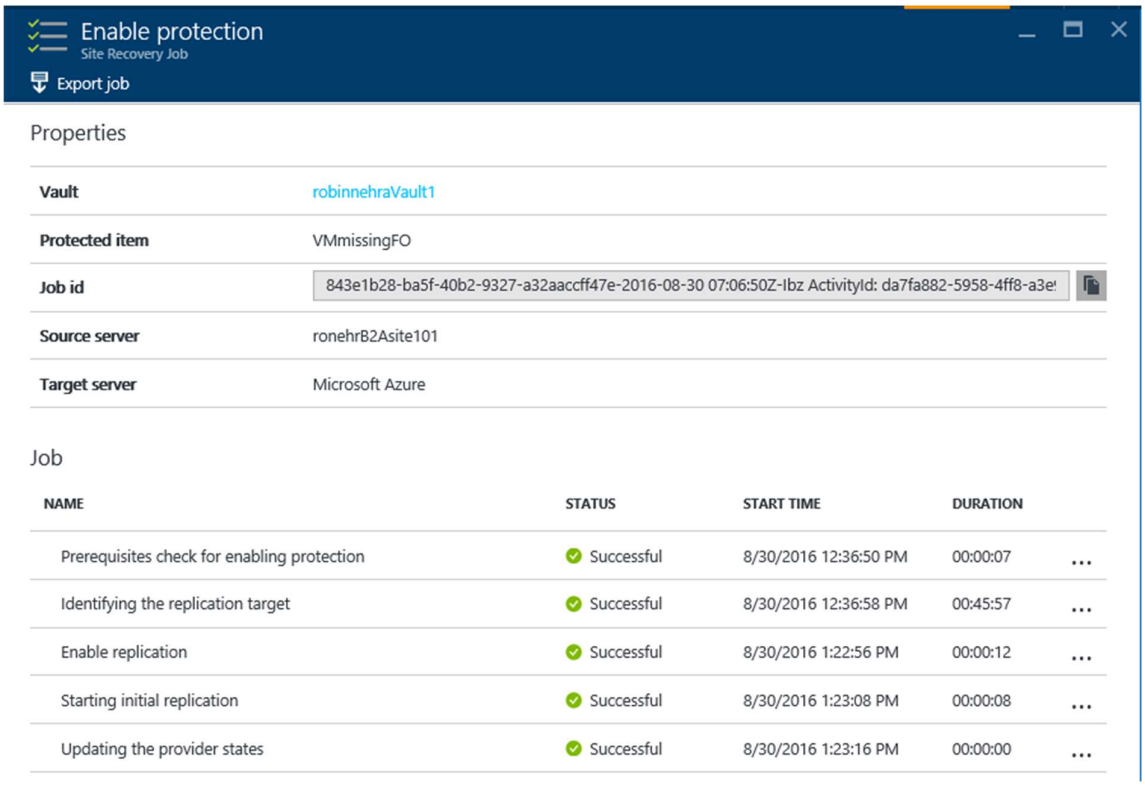
4.2.3.2.1 Uključivanje zaštite

1. Nakon što uključimo zaštitu za Hyper-V u Azure portalu ili na on-premises serverima, započinje proces zaštite
2. Započinje proces provjere virtualnog poslužitelja da li je u skladu s traženim zahtjevima, prije nego se pokrene CreateReplicationRelationship[8], da bi se podesili replikacijsku parametri koje smo zadali

[8] CreateReplicationRelationship method, https://msdn.microsoft.com/library/hh850036.aspx , 5. rujna 2022.

3. Proces započinje replikaciju pozivajući StartReplication[9] metodu da bi se pokrenula potpuna inicijalna replikacija virtualne mašine i da bi se disk virtualne mašine poslao u Azure
4. Ovaj proces možemo nadgledati u Jobs izborniku Azure portala

Slika 5 – ASR nadzor zadataka



Slika 6 – ASR konfiguracija zaštite VM-a

[9] StartReplication method, https://msdn.microsoft.com/library/hh850303.aspx , 5. rujna 2022.

4.2.3.2.2 Inicijalna replikacija podataka

1. Kada se pokrene inicijalna replikacija, Hyper-V kreira snapshot
2. Virtualni diskovi virtualnih mašina se jedan po jedan repliciraju, sve dok se svi ne kopiraju u Azure. Ovo može potrajati, ovisno o veličini virtualne mašine i propusnosti mreže.
3. Ako se prilikom replikacije dogode promjene na virtualnim diskovima, Hyper-V Replica Replication Tracker proces prati te promjene u Hyper-V logovima (.hrl). Ovi logovi se nalaze u istom direktoriju kao i virtualni diskovi. Svaki disk ima svoju .hrl datoteku koja se šalje na sekundarno spremište podataka. Snapshot i logovi zauzimaju diskovne resurse dok je u tijeku inicijalna replikacija.
4. Kada se završi inicijalna replikacija virtualnih diskova, snapshot virtualnog poslužitelja se briše
5. Sve delta promjene koje su se u međuvremenu dogodile, sinkroniziraju se i spajaju se s repliciranim diskom

4.2.3.2.3 Finaliziranje procesa zaštite

1. Nakon što se završi inicijalno proces replikacije, pokreće se proces Finalize protection on the virtual machine. On konfigurira mrežu i ostale post-replikacijske postavke, tako da virtualna mašina bude u potpunosti zaštićena
2. U ovom trenutku možemo provjeriti postavke virtualne mašine da smo sigurni da je spremana za potencijalno prebacivanje u Azure. Već sad možemo napraviti i testno prebacivanje virtualne mašine.

4.2.3.3 Replikacije delta vrijednosti

1. Nakon inicijalne replikacije, sukladno s postavkama replikacijskih politika, započinje proces replikacije delta vrijednosti
2. Hyper-V Replica Replication Tracker proces prati promjene na virtualnim diskovima kroz .hrl datoteke. Svaki disk koji se replicira ima svoju povezanu .hrl datoteku
3. Ove log datoteke se šalju u korisnikovo spremište podataka u Azure-u. Kada datoteka dođe u Azure, promjene na primarnom disku se porate kroz dodatnu log datoteku u istom direktoriju
4. Prilikom inicijalne delta replikacije, virtualnu mašinu možemo nadgledati u Azure portalu

4.2.3.3.1 Proces ponovne sinkronizacije

1. Ukoliko dođe do pogrešaka prilikom delta replikacije a potpuna replikacija bi bila neisplativa u pogledu brzine mreže ili vremena, tada se virtualna mašina označava za ponovnu sinkronizaciju.

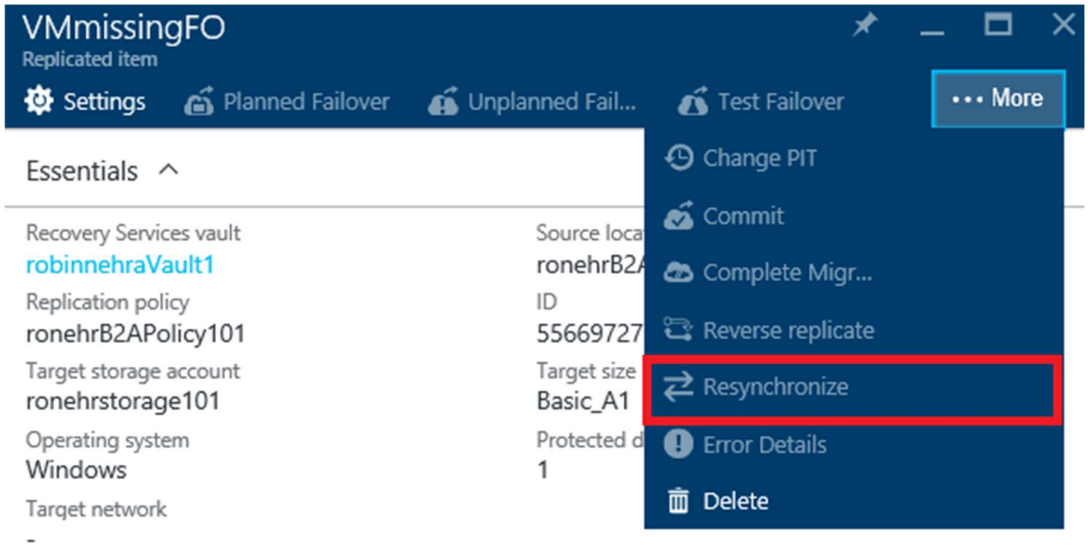
    - Na primjer, ukoliko .hrl datoteka dosegne 50% veličine diska, virtualna mašina će biti označena za ponovnu sinkronizaciju

- Prema zadanim vrijednostima, ponovna sinkronizacija se događa automatski van radnog vremena

2. Ponovna sinkronizacija šalje samo delta promjene

   - Izračunavanjem kontrolnih vrijednosti polazišne i odredišne virtualne mašine smanjuje se količina podataka koje je potrebno sinkronizirati
   - Koristi se fixed-block algoritam koji dijeli polazišne i odredišne datoteke u blokove fiksne veličine
   - Generira se kontrolna vrijednost za svaki blok. Ovo se koristi da bi odredili koje blokove s polazišne virtualne mašine treba primijeniti na odredišnu

3. Nakon što se završi proces ponovne sinkronizacije, normalna delta replikacija preuzima replikaciju.
4. Ako ne želimo čekati da se dogodi ponovna sinkronizacija van radnog vremena, proces možemo pokrenuti i ručno. Na primjer, ako se dogodi iznenadni pad sustava. Da bi ovo napravili, u Azure portalu potrebno je odabrati virtualnu mašinu i onda opciju Resynchronize.



Slika 7 – ASR resinhronizacija

4.2.3.3.2 Proces ponovnog pokušaja sinkronizacije

Ako se dogodi pogreška u replikaciji, ugrađene su opcije ponovnog pokušaja replikacije. Ponovni pokušaj je klasificiran kako je opisano u tablici.

Kategorija	Detalji
Greške od kojih se ne možemo oporaviti	Ponovni pokušaj replikacije se neće dogoditi. Virtualna mašina će biti u statusu Critical i potrebna je intervencija administratora. Primjeri ovakvih pogrešaka su prekid u lancu virtualnih diskova, neispravan status replicirane virtualne mašine, greške u mrežnoj autentifikaciji, autorizacijske pogreške

Greške od kojih se možemo oporaviti	Ponovni pokušaj se događa prilikom definiranog intervala, koristeći eksponencijalni pomak koji povećava interval ponovnog pokušaja od početka prvog pokušaja za 1, 2, 4, 8, i 10 minuta. Ako se pogreška nastavi, pokušajte svakih 30 minuta. Primjeri uključuju mrežne pogreške, malo prostora na disku i malo radne memorije.

Tablica 2 - ASR klasifikacija grešaka u replikaciji

4.2.3.4 Proces prebacivanja rada virtualne mašine na Azure i povratak nazad (failover i failback)

1. Možemo pokrenuti planirano ili neplanirano prebacivanje s lokalnog Hyper-V VM-a u Azure. Ako se pokrene planirano prebacivanje u Azure, izvorne virtualne mašine se isključuju kako bi se osigurali od gubitka podataka. Pokrenite neplanirano prebacivanje ako primarna lokacija nije dostupna.
2. Možemo prebaciti jednu po jednu virtualnu mašinu ili možemo kreirati planove za oporavak (recovery plan), da bi orkestrirali prebacivanje više virtualnih mašina odjedanput.
3. Kada se završi prva faza prebacivanja, u Azure portalu bi trebali vidjeti kreiranu repliku virtualne mašine. Ukoliko je potrebno, toj mašini možemo dodijeliti javnu IP adresu.
4. Prebacivanje možemo potvrditi (commit), te početi pristupati servisima i aplikacijama na virtualnoj mašini u Azure javnom oblaku.

Kada je infrastruktura u primarnom podatkovnom centru ponovno uspostavljena, možemo pokrenuti proces vraćanja virtualnih mašina iz Azure javnog oblaka u primarni podatkovni centar.

1. Pokrenimo planirani povrat s Azure na primarni podatkovni centar

    - **Minimalni prekid rada (Minimum downtime):** Ako koristimo ovu opciju, ASR sinkronizira podatke prije povrata. Provjerava promjenjuje blokova podataka, preuzima ih i sprema u primarni podatkovni centar, dok virtualna mašina u Azure radi te time smanjuje trajanje prekida rada. Kada ručno definiramo da se treba dogoditi prebacivanje i kad ono treba završiti, Azure virtualna mašina se gasi, kopiraju se finalne delta promjene i započinje proces prebacivanja.
    - **Potpuno preuzimanje (Full download):** Ova opcija sinkronizira podatke prilikom prebacivanja virtualne mašine. Ova opcija prvo preuzme cijeli virtualni disk. Brže je jer nema provjere kontrolnih vrijednosti ali je prekid rada duži. Ova opcija se koristi ukoliko je replika virtualne mašine u Azure-u dugo radila ili ukoliko je virtualna mašina u primarnom podatkovnom centru izbrisana.
    - **Kreiraj VM (Create VM):** Možemo prebacivanje napraviti na postojeću ili na novu virtualnu mašinu. Možemo specificirati da ASR kreira novu virtualnu mašinu ako ona već ne postoji.

2. Nakon što početna sinkronizacija završi, odabiremo opciju završetka prebacivanja. Nakon što proces završi, možemo se prijaviti na virtualnu mašinu u primarnom podatkovnom centru i provjeriti da li sve radi kako je očekivano. Virtualna mašina u Azure javnom oblaku je zaustavljena.

3. Nakon toga potvrđujemo prebacivanje te servisima i aplikacijama pristupamo putem virtualne mašine u primarnom podatkovnom centru.
4. Nakon što prebacimo virtualne mašine, uključujemo obrtanje replikacije tako da se virtualne mašine iz primarnog podatkovnog centra ponovno repliciraju u Azure javni oblak.

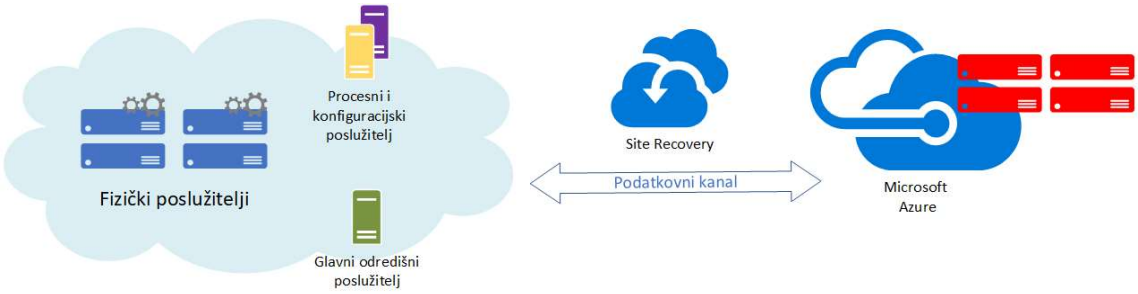
4.2.4 Azure Site Recovery za fizičke poslužitelje

4.2.4.1 Komponente arhitekture

Komponenta	Zahtjevi	Detaljne informacije
Azure	Azure pretplata i Azure virtualna mreža	Replicirani podaci s fizičkih poslužitelja se spremaju u Azure storage račun. Pomoću repliciranih podataka se kreira virtualna mašina kada pokrenemo prebacivanje. Nakon toga se virtualna mašina spaja na Azure mrežu.
Konfiguracijski poslužitelj (Configuration server)	Jedna fizička mašina ili VMware virtualna mašina na kojoj se pokreću Site Recovery komponente. Virtualna mašina pokreće konfiguracijski, procesni i glavni odredišni poslužitelj	Koordinira komunikaciju između primarnog podatkovnog centra i Azure-a te upravlja replikacijom podataka.
Procesni poslužitelj (Process server)	Instalira se zajedno s konfiguracijskim poslužiteljem	Služi kao replikacijski gateway. Prima replikacijske podatke, optimizira ih pomoću kompresije, enkripcije i korištenjem među spremnika te ih šalje u Azure spremište podataka. Procesni server instalira i Mobility service na poslužitelje koje želimo replicirati. Ako okolina počne rasti možemo dodati još procesnih poslužitelja.
Glavni odredišni poslužitelj (Master target server)	Instalira se zajedno s konfiguracijskim poslužiteljem	Upravlja replikacijskim podacima prilikom prebacivanja virtualnih mašina nazad u primarni podatkovni centar. Ako okolina počne rasti možemo dodati još glavnih odredišnih poslužitelja.
Replicirani poslužitelji	Mobility service se instalira na svaki poslužitelj koji želimo replicirati	Preporuka je da se omogući automatska instalacija Mobility servisa s procesnog servera. Po potrebi, Mobility service se može i ručno instalirati ili pomoću SCCMa i sl.

Tablica 3 - ASR lista komponenata arhitekture

4.2.4.1.1 Arhitektura rješenja replikacije fizičkih poslužitelja u Azure



Slika 8 – ASR koncept replikacije fizičkih poslužitelja

4.2.4.2 Proces replikacije

1. Podesimo okolinu, uključujući poslužitelje u primarnom podatkovnom centru i servise u Azure javnom oblaku. U Recovery Service spremištu, definiramo polazišne izvore replikacije i odredišne ciljeve replikacije, podesimo konfiguracijski poslužitelj, kreiramo replikacijsku politiku i uključimo replikaciju.

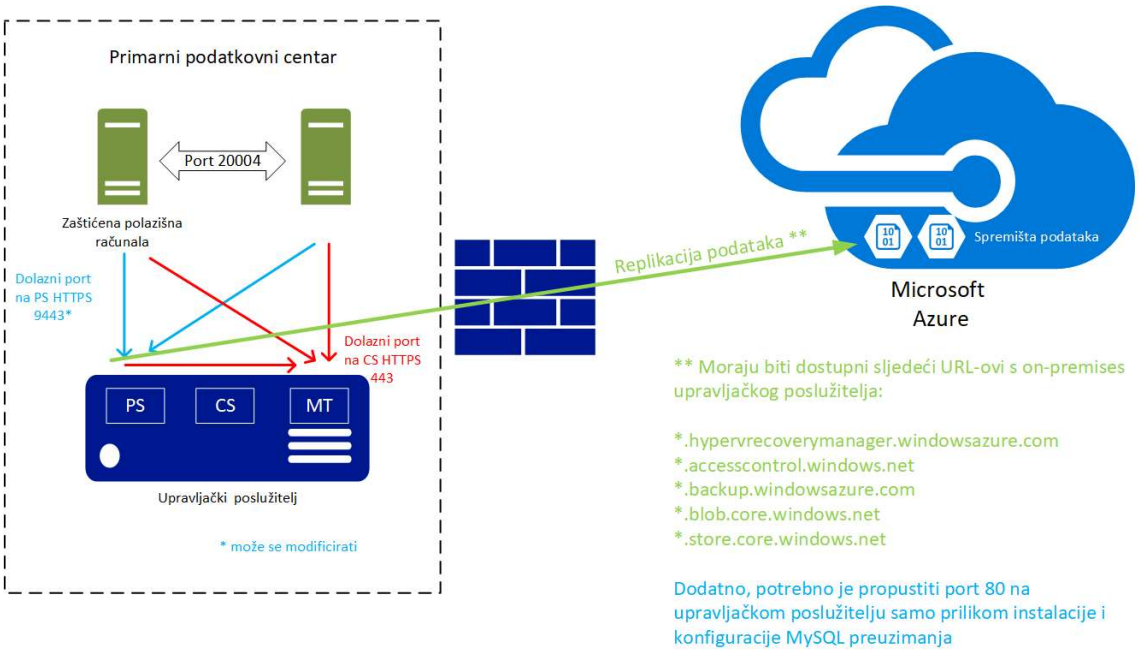
2. Poslužitelji se repliciraju u skladu s replikacijskom politikom te se odmah pokreće replikacija inicijalne kopije podataka u Azure spremište podataka.

3. Nakon što inicijalna replikacija završi, počinje replikacija delta promjena u Azure. Promjene koje se događaju na poslužiteljima se prate kroz .hrl datoteke.

    - Poslužitelji komuniciraju s konfiguracijskim poslužiteljem na HTTPS portu 443 dolazno, za potrebe upravljanja replikacijom
    - Poslužitelji šalju replikacijske podatke proces poslužitelju na HTTPS portu 9443 dolazno (moguće je promijeniti port)
    - Konfiguracijski poslužitelj orkestrira upravljanje replikacijom s Azure javnim oblakom na HTTPS portu 443 odlazno.
    - Procesni poslužitelj prima podatke od poslužitelja koje repliciramo, optimizira ih i kriptira te ih šalje u Azure spremište podataka putem odlaznog porta 443.
    - Ako uključimo konzistentnost više virtualnih mašina, mašine u toj replikacijskoj grupi komuniciraju međusobno na portu 20004. Konzistentnost više virtualnih mašina se koristi kada mašine grupiramo u replikacijsku grupu koja dijeli aplikacije koje moraju biti konzistentne u slučaju pada servisa.

4. Sav promet se replicira na Azure putem javnih točaka spremišta podataka, preko Interneta. Po potrebi možemo koristiti i Express Route Microsoft peering[10]. Repliciranje prometa putem S2S VPN tunela prema Azure javnom oblaku nije podržano.

4.2.4.2.1 Proces replikacije fizičkih poslužitelja u Azure



Slika 9 – ASR replikacija fizičkih poslužitelja

4.2.4.3 Proces prebacivanja resursa na Azure i natrag u primarni podatkovni centar

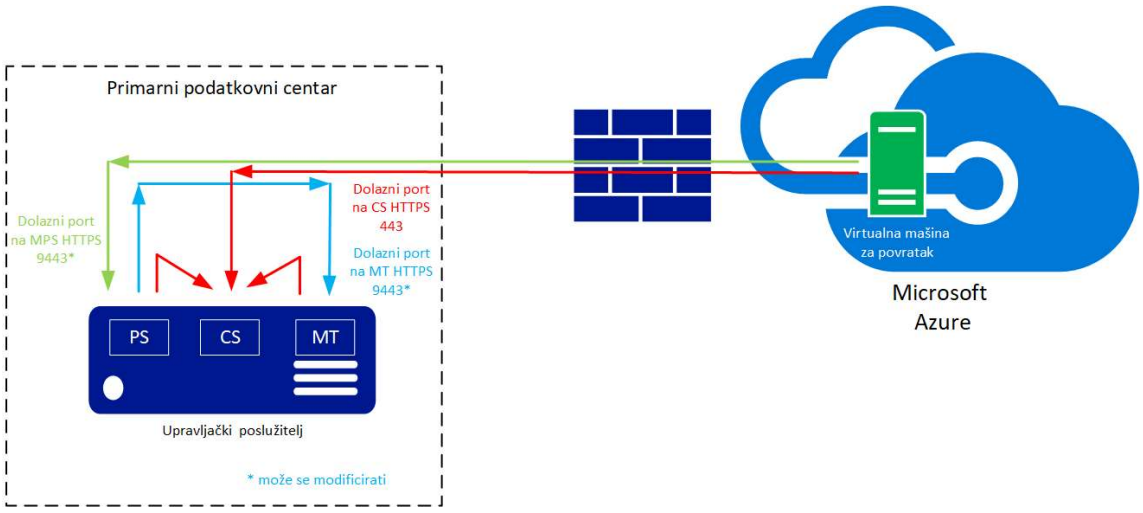
Nakon što smo podesili replikaciju i pokrenuli nekoliko testova prebacivanja poslužitelja u Azure da bi provjerili ispravnost konfiguracije, možemo početi koristiti servis po potrebi. Imajmo na umu sljedeće informacije:

- Planirano prebacivanje nije podržano
- Kad radimo vraćanje poslužitelja iz Azure-a u primarni podatkovni centar moramo ih vratiti na VMware okolinu.
- Možemo prebaciti jedno računalo u Azure ili napraviti planove za oporavak (recovery plan) i prebaciti više poslužitelja odjedanput
- Kada pokrenemo prebacivanje, virtualne mašine se kreiraju u Azure javnom oblaku iz repliciranih podataka
- Nakon što pokrenemo inicijalno prebacivanje, potvrđujemo da ćemo od tada servisima i aplikacijama pristupati na Azure virtualnim mašinama

[10] https://docs.microsoft.com/en-us/azure/expressroute/expressroute-circuit-peerings#microsoftpeering

- Kada oporavimo primarni podatkovni centar, možemo početi proces vraćanja virtualnih mašina iz Azure javnog oblaka
- Potrebno je imati infrastrukturu za povrat u primarni podatkovni centar, a to uključuje:
    - Privremeni procesni poslužitelj u Azure-u: Da bi napravili povrat iz Azure javnog oblaka, podesimo Azure virtualnu mašinu da bude procesni poslužitelj, koji onda upravlja replikacijom iz Azure-a. Nakon što vratimo sve mašine nazad, ovu virtualnu mašinu možemo izbrisati.
    - VPN veza: Potrebno je imati VPN ili Express route vezu između Azure-a i primarnog podatkovnog centra
    - Odvojeni glavni odredišni poslužitelj: Prema zadanoj postavci, glavni odredišni poslužitelj koji je instaliran skupa s konfiguracijskim poslužiteljem, na on-premises VMware virtualnoj mašini, upravlja procesom prebacivanja natrag u primarni podatkovni centar. Međutim, ako nam treba velika propusnost podataka i prebacujemo veliku količinu podataka, preporuka je da imamo odvojeni glavni odredišni poslužitelj za ovu svrhu.
    - Politika povratka (failback policy): Da bi replicirali podatke nazad na primarni podatkovni centar moramo imati politiku povratka. Ona se automatski kreira kada kreiramo replikacijsku politiku iz primarnog podatkovnog centra u Azure javni oblak
    - VMware infrastrukture: Za povratak poslužitelja iz Azure javnog oblaka u primarni podatkovni centar moramo imati spremnu VMware infrastrukturu. Ne možemo napraviti povratak na fizičko računalo. Ukoliko je izvorni poslužitelj i dalje funkcionalan, preporučeni proces povrata je backup podataka na virtualnom poslužitelju u Azure-u i restore na fizički poslužitelj.
- Nakon što su sve komponente spremne, povratak se događa u tri faze:
    - Faza 1: Ponovna zaštita Azure virtualnih mašina tako da repliciraju iz Azure javnog oblaka na VMware infrastrukturu u primarnom podatkovnom centru.
    - Faza 2: Pokrenemo proces prebacivanja na primarni podatkovni centar
    - Faza 3: Nakon sto su sve mašine prebačene, ponovno uključimo replikaciju.

4.2.4.3.1 Povratak na VMware infrastrukturu iz Azure javnog oblaka



Slika 10 – ASR povratak podataka na primarnu lokaciju VMWare

4.2.5 Backup sustav tijekom DR produkcije

Ukoliko dođe do katastrofalnog događaja na primarnom podatkovnom centru i korisnik mora prebaciti svoje resurse u sekundarni podatkovni centar koji se nalazi u Azure javnom oblaku, javlja se potreba izrade sigurnosnih kopija tih virtualnih mašina.

Korisnik je definirao da se sigurnosna kopija resursa u sekundarnom podatkovnom centru mora raditi ukoliko se sekundarni podatkovni centar koristi više od 72 sata.

Za ovaj scenarij ITcom je odabrao Azure backup kao rješenje. Azure Backup omogućava spremanje sigurnosne kopije jedne ili više virtualnih mašina smještenih u Azure javni oblak. Sami proces je moguće i automatizirati. Konfiguracija Azure Backup servisa se radi prilikom kreiranja virtualne mašine ili naknadno kroz sam Azure portal, po potrebi je moguće dodijeliti Azure politike na određeni skup virtualnih mašina koje će onda automatski te virtualne mašine konfigurirati za Azure Backup.

4.2.5.1 Azure Backup proces

Evo kako Azure Backup radi sigurnosne kopije Azure virtualnih mašina:

1. Za sve virtualne mašine koje su odabrane da im se napravi sigurnosna kopija, Azure Backup pokreće proces prema rasporedu koji sami definiramo

2. Prilikom izrade prve sigurnosne kopije, ukoliko je virtualna mašina upaljena, instalira se ekstenzija za kreiranje sigurnosnih kopija
    - Za Windows virtualnu mašinu instalira se VMSnapshot ekstenzija
    - Za Linux virtualnu mašinu instalira se VMSnapshotLinux ekstenzija

3. Za pokrenute Windows virtualne mašine koje su pokrenute, Azure Backup koordinira s Windows Volume Shadow Copy servisom (VSS) da bi se kreira aplikacijski konzistentna slika sustava (snapshot)
    - Prema zadanoj postavci, Azure backup radi potpunu VSS sigurnosnu kopiju
    - Ako Azure Backup ne može napraviti aplikacijski konzistentnu sliku sustava onda se kreira datotečno konzistentna slika spremišta podataka u kojem se nalazi virtualna mašina

4. Za Linux virtualnu mašinu, Azure backup radi datotečno konzistentnu sliku spremišta podataka u kojem se nalazi virtualna mašina. Da bi napravili aplikacijski konzistentnu sliku sustava potrebno je ručno prilagoditi pre i post skripte unutar virtualne mašine

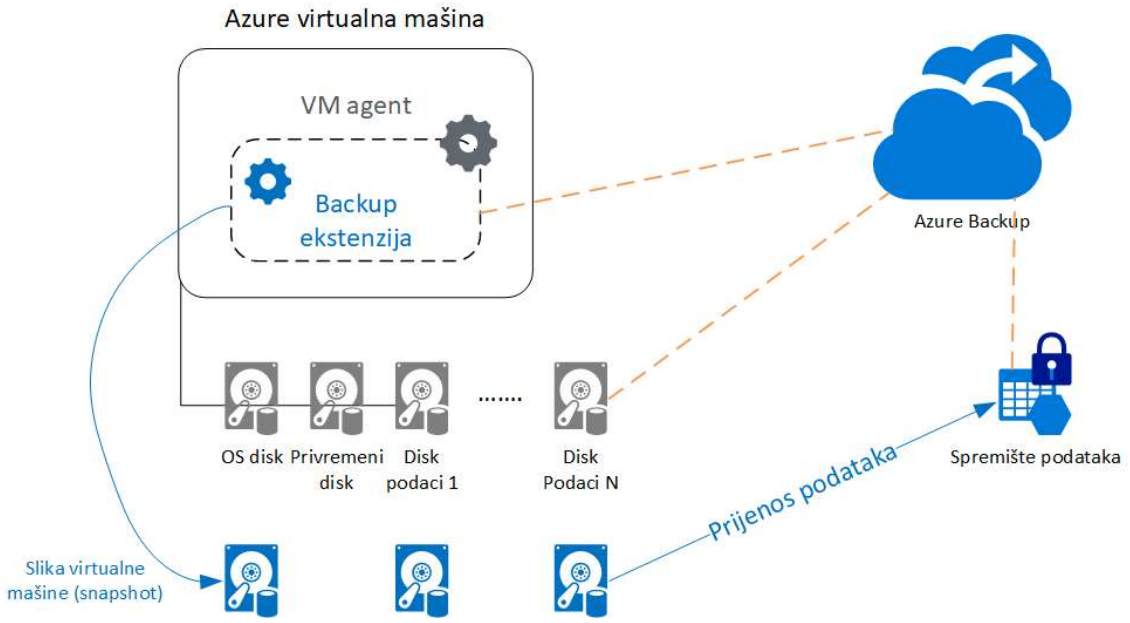
5. Nakon što Azure Backup naravi kopiju podataka, sprema ih u spremište podataka u Azure-u

    - Proces spremanja kopija je optimiziran tako da se kreira kopija svakog diska virtualne mašine paralelno
    - Za svaki disk za koji se radi sigurnosna kopija, Azure Backup prebacuje samo one blokove podataka koji su se promijenili (delta) od prošle sigurnosne kopije

- Kopije podataka možda neće odmah biti kopiranje u spremište podataka. U vremenima velikog opterećenja, kopiranje može potrajati nekoliko sati. Ukupno vrijeme kreiranja kopije virtualne mašine je manje od 24 sata kada su podešene dnevne politike kreiranja sigurnosnih kopija

6. Nakon što na Windows virtualnoj mašini uključimo opciju Azure Backupa, dogode se određene promjene:
   - Instalira se Microsoft Visual C++ 2013 Redistributable(x64) - 12.0.40660 u virtualnu mašinu
   - Volume Shadow Copy servis je podešen da se pokreće automatski prilikom paljenja virtualne mašine
   - Doda se IaaSVmProvider Windows servis

7. Kada je prijenos podataka gotov, slika virtualne mašine se briše i kreira se točka povrata (recovery point)



Slika 11 – ASR shema tijeka podataka

4.2.5.2 Kriptiranje sigurnosnih kopija Azure virtualnih mašina

Azure Backup kriptira sigurnosne kopije virtualnih mašina korištenjem Storage Service Encryption (SSE). Azure Backup može kreirati sigurnosne kopije virtualnih mašina koje su kriptirane korištenjem Azure enkripcije.

Enkripcija	Detaljne informacije	Podrška
Azure Disk enkripcija	Azure enkripcija kriptira i OS disk i diskove s podacima za Azure virtualne mašine.	Azure Backup podržava kreiranje sigurnosnih kopija za upravljane i neupravljanje Azure

Enkripcija	Detaljne informacije	Podrška
	Azure Disk enkripcija se integrira s BitLocker enkripcijskim ključevima (BEK), koji se čuvaju u spremištu ključeva (key vault) kao tajna informacija. Azure Disk enkripcija se također integrira i s Azure Key Vault enkripcijskim ključevima (KEK)	virtualne mašine koje su kriptirane s samo s BEK, ili s BEK i KEK. I BEK i KEK imaju svoje sigurnosne kriptirane kopije. Pošto postoje sigurnosne kopije BEK i KEK, korisnici s dovoljnom razinom ovlasti ih mogu vratiti iz sigurnosne kopije. Ovi korisnici mogu također vratiti i kriptiranu virtualnu mašinu. Kriptirane ključeve i tajne ne mogu čitati neautorizirani korisnici ili sama Azure platforma.
SSE	Pomoću SSE, Azure spremišta podataka omogućavaju enkripciju podataka automatski kriptirajući podatke prije nego ih spremi. Azure spremište podataka također dekriptira podatke prije nego ih dohvati.	Azure Backup koristi SSE da bi kriptirao sigurnosne kopije Azure virtualnih mašina

Tablica 4 - ASR opcije enkripcije

4.2.5.3 Kreiranje sigurnosne kopije (snapshot)

Azure Backup kreira sigurnosne kopije u skladu s definiranim rasporedom.

- Windows virtualne mašine: Za Windows virtualne mašine, Backup servis koordinira s VSS servisom i kreira aplikacijski konzistentne sigurnosne kopije.
  - Prema zadanoj postavci, Azure backup radi potpunu VSS sigurnosnu kopiju
  - Da bi promijeni ovu postavku i podesili da Azure Backup radi VSS kopiju, potrebno je modificirati ključeve u registru pomoću sljedeće komade:

    REG ADD "HKLM\SOFTWARE\Microsoft\BcdrAgent" /v USEVSSCOPYBACKUP /t REG_SZ /d TRUE /f

- Linux virtualne mašine: Da bi napravili aplikacijski konzistentnu sliku sustava potrebno je ručno prilagoditi pre i post skripte unutar virtualne mašine.
  - Azure Backup pokreće samo ručno napravljene pre i post skripte
  - Ako se skripte uspješno pokrenu, Azure Backup označava tu sigurnosnu kopiju kao aplikativno konzistentnu. Imajmo na umu da smo mi odgovorni za konzistentnost aplikacija kada koristimo ručno napravljene skripte
  - Kako konfigurirati skripte možemo pronaći na ovom linku https://docs.microsoft.com/en-us/azure/backup/backup-azure-linux-app-consistent

4.2.5.3.1 Konzistentnost sigurnosne kopije

Ova tablica objašnjava različite tipove konzistentnosti sigurnosne kopije podataka:

Kopija	Detalji	Oporavak	Imajmo na umu

Aplikacijski konzistentno	Aplikacijski konzistentne sigurnosne kopije hvataju sadržaj memorije i I/O operacija na čekanju. One koriste VSS writer servis (pre i post skripte na Linux mašinama) da bi osigurale konzistentnost aplikacijskih podataka prije nego što se kreira sigurnosna kopija.	Virtualna mašina se pali, nema korupcije podataka ili gubitaka. Aplikacija se pokreće u konzistentnom stanju	Windows: Svi VSS zapisi su uspješni Linux: pre i post skripte su konfigurirane i uspješno izvršene
Datotečno konzistentno	Omogućavaju konzistentnost kreiranjem kopije svih datoteka u istom trenutku	Virtualna mašina se pali, nema korupcije podataka ili gubitaka. Aplikacija mora imati svoje rješenje koje će se pobrinuti da su podaci koji su vraćeni ujedno i konzistentni.	Windows: Neki VSS zapisi nisu prošli Linux: prema zadanoj vrijednosti (ako pre i post skripte nisu konfigurirane ili nisu uspješno izvršene)
Crash konzistentno	Obično se događaju ako se Azure virtualna mašina ugasi prilikom kreiranja sigurnosne kopije. Samo oni podaci koji su u tom trenutku na diskovima se spremaju. Ovaj tip konzistentnosti ne garantira konzistentnost podataka niti aplikacija.	Iako nema garancije, virtualna mašina se obično upali i nakon toga odradi provjeru diska te pokuša popraviti greške koje su došle radi korupcije podataka ako ih ima. Sve informacije kose su bile u memoriji ili operacije koje nisu zapisane na disk su izgubljene. Aplikacije moraju implementirati svoju metodu verifikacije podataka. Na primjer, baza podataka može iskoristiti svoje transakcijske logove.	Virtualna mašina je u ugašenom stanju

Tablica 5 - ASR tipovi konzistentnosti sigurnosne kopije podataka

4.2.5.4 Što imati na umu prilikom izrada i povrata sigurnosne kopije

Komponente i procesi	Detalji
Disk	Sigurnosne kopije diskova unutar virtualne mašine događaju se paralelno. Na primjer, ako virtualna mašina ima 4 diska, Backup servis pokušava napraviti sigurnosnu kopiju sva 4 diska paralelno. Sigurnosna kopija je inkrementalna.
Planiranje	Da bi smanjili promet povezan s kreiranjem sigurnosnih kopija, kreirajte sigurnosne kopije različitih virtualnih mašina u različito vrijeme.
Priprema sigurnosnih kopija	Ne zaboravimo na pripremu prije kreiranja sigurnosnih kopija. Priprema uključuje instalaciju ili nadogradnju ekstenzija te pokretanje kreiranja sigurnosne kopije u skladu s definiranim rasporedom.
Prijenos podataka	Imajmo na umu vrijeme koje je potrebno da Azure Backup identificira inkrementalne promjene od prijašnje sigurnosne kopije. Prilikom inkrementalne kopije, Azure Backup određuje promjene izračunavajući kontrolni zbroj blokova. Ako je blok promijenjen, označava se za transfer u spremište podataka.

	Može doći do razlike u vremenu između kreiranja sigurnosne kopije i prebacivanja u Azure spremište podataka U vremenima velikog prometa, može proći i do osam sati dok se sigurnosna kopija ne procesira.
Inicijalna sigurnosna kopija	Iako je potpuno kreiranje sigurnosne kopije za inkrementalnu sigurnosnu kopiju manje od 24 sata, to možda neće biti tako za inicijalnu sigurnosnu kopiju. To vrijeme ovisi o veličini i količini podataka koje Azure Backup treba procesirati.
Red čekanja na oporavak	Azure Backup procesira zadatke oporavka iz više spremišta podataka paralelno, te ih sve stavlja u red čekanja.
Oporavak kopije	Prilikom procesa oporavka, podaci se kopiraju iz Azure Backup servisa u spremište podataka Ukupno vrijeme trajanja oporavka ovisi o IOPS-ima te o propusnosti spremišta podataka Da bi smanjili vrijeme kopiranja, odaberimo spremište podataka koje nije opterećeno pisanjem i čitanjem od strane drugih aplikacija

Tablica 6 - ASR lista zadataka o kojima treba voditi računa

4.2.5.4.1 Performanse sigurnosnih kopija

Ovi scenariji najčešće utječu na ukopno vrijeme kreiranja sigurnosne kopije:

- Dodavanje novih diskova u zaštićenu Azure virtualnu mašinu: Ako je virtualna mašina u procesu kreiranja inkrementalne sigurnosne kopije a mi dodamo novi disk, vrijeme izrade sigurnosne kopije će se povećati. Ukupno vrijeme sigurnosne kopije može biti i veće od 24 sata zbog inicijalne replikacije cijelog novog diska i inkrementalnih kopija postojećih diskova.
- Fragmentacija diskova: Operacije kreiranja sigurnosnih kopija su brze ako su podaci na disku zapisani u neprekidnom nizu (contiguous). Ako su podaci fragmentirani, kreiranje sigurnosne kopije je sporije.
- Promjene na diskovima (churn): Ako diskovi na kojima se radi inkrementalna sigurnosna kopija imaju dnevno više od 20GB promjena, kreiranje sigurnosne kopije može potrajati duže (više od 8 sati).
- Verzije sigurnosnih kopija: Posljednja verzija sigurnosne kopije (poznata kao Instant Restore verzija) koristi optimiziraniji proces detekcije promjena nego što je to uspoređivanje kontrolnih brojena na blokovima. Ali, ako koristimo Instant Restore i izbrišemo sigurnosnu kopiju, Azure Backup servis se vraća na stari algoritam provjere blokova. U ovom slučaju će proces kreiranja sigurnosne kopije trajati duže od 24 sata ili neće biti uspješan.

4.2.5.5 Preporuke

Microsoft ima sljedeće preporuke glede konfiguracije sigurnosnih kopija:

- Promijenimo zadane postavke u rasporedu kreiranja sigurnosnih kopija tako da se resursi optimalno koriste

- Ukoliko radimo povrat virtualne mašine iz jednog spremišta sigurnosnih kopija, preporučenoj je da se za povrat mašina sprema u drugom spremištu podataka.
- Za sigurnosne kopije virtualnih mašina koje koriste Premium spremišta podataka, s Instant Restore opcijom, preporučamo da se alocira 50% više slobodnog prostora od spremišta podataka koje je nužno samo za prvu kopiju. 50% nije potrebno za dodatne kopije.
- Oporavak iz v1 spremišta podataka će biti gotov unutar nekoliko minuta jer se kopija nalazi u istom spremištu podataka dok povrat iz v2 spremišta podataka može potrajati duže. U slučaju kada su podaci u v12 spremištu podataka, preporuka je da se koristi Instant Restore opcija.
- Ako u jednom spremištu podataka imamo više od 10 diskova, preporuka je da neke diskove prebacimo u druga spremišta podataka.

4.2.6 Azure okolina

4.2.7 Način povezivanja Azure okoline

Sva infrastruktura koje je u podatkovnim centrima međusobno je povezana putem HT veza preko centralne HT lokacije u Zagrebu. ITcom predlaže da HT ostvari ExpressRoute vezu prema Azure podatkovnom centru koji se nalazi u sjevernoj Europi (Dublin). Azure ExpressRoute je privatna dedicirana konekcija iz korisnikovog podatkovnog centra prema Azure podatkovnom centru. Omogućava veću propusnost i nižu latenciju od standardnog S2S VPN tunela.

Dok sekundarna lokacija radi samo u stanju pripravnosti, putem ExpressRoute konekcije će prolaziti replikacijski promet domain controller poslužitelja, Exchange i SQL baza. Predviđeno je da se za tu svrhu ostvari konekcija brzine 1 Gbps.

Kada se sekundarna lokacija aktivira zbog katastrofe primarne lokacije, u Azure podatkovnom centru će se upaliti dodatnih 70+ virtualnih poslužitelja i svi korisnici koji su se do tada spajali na primarni podatkovni centar će se sada spajati na Azure putem ExpressRoute veze. ExpressRoute brzina se može podići na 2, 5 ili 10 Gbps. ITcom je predvidio da će se ExpressRoute podići s 1 na 2 Gbps. Povećanje ExpressRoute brzine sa strane Azure-a je jednostavna radnja (promjena VPN Gateway SKU-a, promjena ExpressRoute circuit propusnosti), ali HT na svojoj strani mora osigurati potrebnu opremu koja može podnijeti minimalno 2 Gbps propusnosti.

4.2.8 Okolina u stanju pripravnosti

U Azure podatkovnom centru će postojati virtualni poslužitelji koji će biti stalno ili povremeno upaljeni kako bi se u slučaju aktivacije sekundarnog podatkovnog centra mogli brže i jednostavnije preuzeti servisi i role s primarnog podatkovnog centra. Slijedeća tablica sadržava popis poslužitelja s njihovim karakteristikama i kratkim opisom.

Virtualni poslužitelj	Karakteristike	Opis
Domain Controller 1	Veličina instance: D4s v3 vCPU: 4 RAM: 16 GB Diskovi: 1 x P6 (64 GB) za operativni sustav; 1 x P6 (64 GB) za NTDS bazu	Domain controller za domenu domena.local i DNS. Poslužitelj će biti stalno upaljen.
Domain Controller 2	Veličina instance: D4s v3 vCPU: 4 RAM: 16 GB Diskovi: 1 x P6 (64 GB) za operativni sustav; 1 x P6 (64 GB) za NTDS bazu	Domain controller za domenu sub.domena.local i DNS. Poslužitelj će biti stalno upaljen.

Tablica 7 - ASR lista cloud poslužitelja u pripravnosti

4.2.9 Okolina u stanju produkcije

U slučaju neplaniranog prebacivanja produkcije u Azure okolinu, u istoj će se kreirati sve potrebne virtualne mašine s svim potrebnim resursima za nastavak poslovanja onih servisa koji su obuhvaćeni DR procedurama. Sljedeća tablica prikazuje mapiranja on-premises virtualnih i fizičkih mašina u Azure okolini.

Poslužitelj	Azure VM	Disk 1	Disk 2	Disk 3	Disk 4	Disk 5	Disk 6	Disk 7
Server A	E4_v3	E15	E15	E20				
Server B	E4_v3	P6						
Server C	F4s_v2	P6						
Server D	F2s_v2	E6						
Server E	E2_v3	E10	E20					
Server F	F8s_v2	P10						
Server G	F8s_v2	P10						

Tablica 8 - ASR mapiranje odgovarajućih virtualnih mašina

4.2.10 Performanse diskova u Azure-u

Azure podatkovni centar ima puno različitih tipova diskova kojima je definirana veličina diska, propusnost, i količina I/O operacija u sekundi (IOPS). U slijedećim tablicama prikazane su vrijednosti za tri vrste diskova, Standard HDD, Standard SSD i Premium SSD (također

dostupno i na ovoj poveznici: https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disks-types).

Standard Disk Type	S4	S6	S10	S15	S20	S30	S40	S50	S60	S70	S80
Disk size in GiB	32	64	128	256	512	1,024	2,048	4,096	8,192	16,384	32,767
IOPS per disk	Up to 500	Up to 500	Up to 500	Up to 500	Up to 500	Up to 500	Up to 500	Up to 500	Up to 1,300	Up to 2,000	Up to 2,000
Throughput per disk	Up to 60 MiB/sec	Up to 60 MiB/sec	Up to 60 MiB/sec	Up to 60 MiB/sec	Up to 60 MiB/sec	Up to 60 MiB/sec	Up to 60 MiB/sec	Up to 60 MiB/sec	Up to 300 MiB/sec	Up to 500 MiB/sec	Up to 500 MiB/sec

Standard SSD sizes	E4	E6	E10	E15	E20	E30	E40	E50	E60	E70	E80
Disk size in GiB	32	64	128	256	512	1,024	2,048	4,096	8,192	16,384	32,767
IOPS per disk	Up to 120	Up to 240	Up to 500	Up to 500	Up to 500	Up to 500	Up to 500	Up to 500	Up to 2,000	Up to 4,000	Up to 6,000
Throughput per disk	Up to 25 MiB/sec	Up to 50 MiB/sec	Up to 60 MiB/sec	Up to 60 MiB/sec	Up to 60 MiB/sec	Up to 60 MiB/sec	Up to 60 MiB/sec	Up to 60 MiB/sec	Up to 400 MiB/sec	Up to 600 MiB/sec	Up to 750 MiB/sec

Premium SSD sizes	P4	P6	P10	P15	P20	P30	P40	P50	P60	P70	P80
Disk size in GiB	32	64	128	256	512	1,024	2,048	4,096	8,192	16,384	32,767
IOPS per disk	Up to 120	Up to 240	Up to 500	Up to 1,100	Up to 2,300	Up to 5,000	Up to 7,500	Up to 7,500	Up to 16,000	Up to 18,000	Up to 20,000
Throughput per disk	Up to 25 MiB/sec	Up to 50 MiB/sec	Up to 100 MiB/sec	Up to 125 MiB/sec	Up to 150 MiB/sec	Up to 200 MiB/sec	Up to 250 MiB/sec	Up to 250 MiB/sec	Up to 500 MiB/sec	Up to 750 MiB/sec	Up to 900 MiB/sec

Tablica 9 - ASR liste performansi virtualnih diskova

Iz priloženih tablica se vidi da diskovi P30 kakvi se mogu koristiti za npr. MS Exchange i SQL Server baze podataka podržavaju 5000 IOPS-a po disku i 200 MiB/sec (~209 MB/sec) propusnosti po disku. Diskove je moguće i agregirati pomoću Storage Spaces funkcionalnosti koja je dio Windows Server operativnog sustava. Tako se za SQL Server diskove može koristiti Storage Spaces pool od 8 P30 diskova što može povećati propusnost na maksimalnih 40 000 IOPS-a i 1600 MiB/s. Međutim, svaka veličina instance virtualnog poslužitelja u Azure-u ima svoja ograničenja što znači da je propusnost VM instance prema diskovima ograničavajući faktor, a ne sami diskovi. Detaljne karakteristike VM instanci u Azure-e se nalaze na slijedećim poveznicama:

- https://docs.microsoft.com/en-us/azure/virtual-machines/windows/sizes
- https://docs.microsoft.com/en-us/azure/virtual-machines/linux/sizes

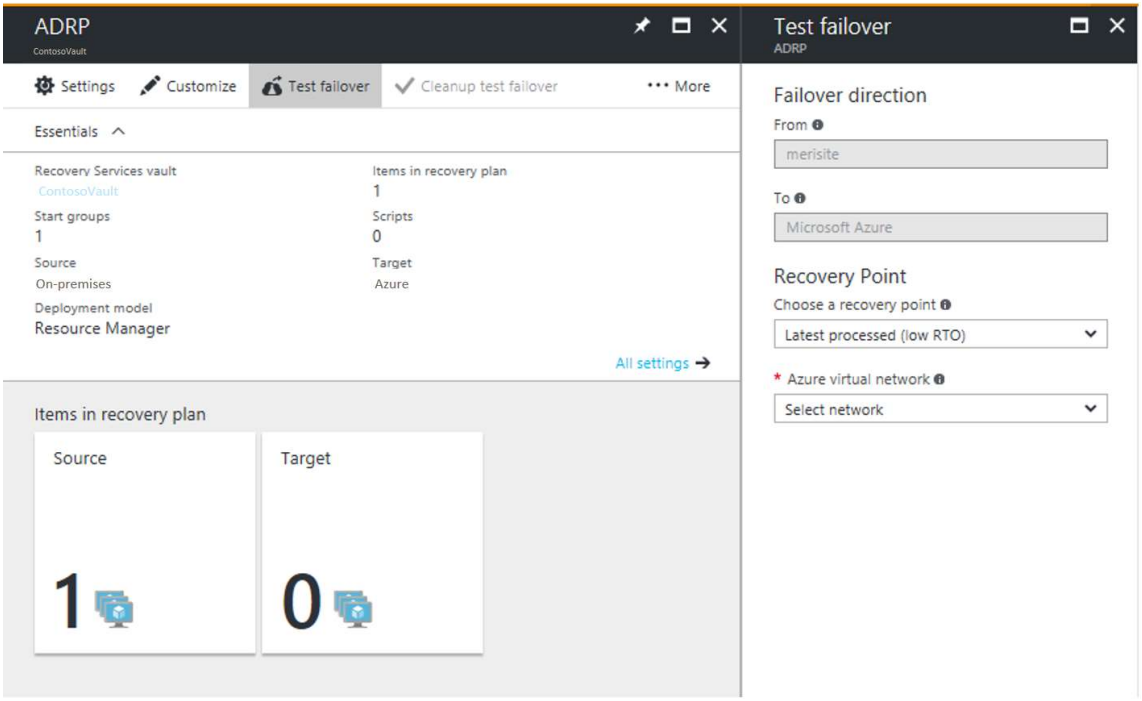
4.2.11 Aktivacija/deaktivacija DR sustava u svrhu testiranja

4.2.11.1 Azure Site Recovery

Test aktivacije DR sustava radimo u svrhu validacije replikacije i DR strategije, bez gubitka podataka ili prekida u radu servisa. Test DR sustava ne utječe na produkcijsku okolinu niti na postojeću replikaciju. Test možemo pokrenuti na specifičnim virtualnim mašinama ili na većem broju virtualnih mašina korištenjem planova za oporavak.

4.2.11.2 Pokretanje DR testa

Ova procedura opisuje kako pokrenuti test DR okoline za plan oporavka jer je to češći slučaj. Za informacije o tome kako napraviti DR test za samo jednu virtualnu mašinu pogledati upute na ovoj poveznici: https://docs.microsoft.com/en-us/azure/site-recovery/tutorial-dr-drill-azure#run-a-test-failover-for-a-single-vm.



Slika 12 – ASR pokretanje DR testa

1. Unutar Azure portala otvorimo Site Recovery opciju, odaberimo Recovery plans, pa ime plana te odaberimo opciju Test failover.

2. Odaberimo točku oporavka u koju želimo napraviti povrat. Dostupne su nam sljedeće opcije:

- **Zadnji procesirani:** Ova opcija vraća sve virtualne mašine koje su obuhvaćene recovery planom na zadnju točku oporavka koji je procesiran od strane Site Recovery servisa. Da bi vidjeli koja je zadnja točka oporavka za specifičnu virtualnu mašinu, možemo pogledati pod postavkama opciju Latest Recovery Points. Ova opcija omogućava nizak RTO jer se vrijeme ne troši na procesiranje neprocesuiranih podataka.
- **Zadnji aplikacijski konzistentni:** Ova opcija vraća sve virtualne mašine koje su obuhvaćene recovery planom na zadnju točku oporavka koja je aplikativno konzistentna.
- **Zadnji:** Ova opcija prvo procesira sve podatke koji su poslane u Site Recovery servis**,** da bi se kreirala točka povrata za sve virtualne mašine prije vraćanja mašine. Ova opcija nudi najniži RPO radi toga jer će vraćena virtualna mašina imati sve informacije do trenutka kada je pokrenut Site Recovery proces.
- **Zadnji s više procesiranih virtualnih mašina:** Ova opcija je dostupna u recovery planovima koji imaju jednu ili više virtualnih mašina s uključenom opcijom višestruke konzistentnosti. Virtualne mašine s upaljenom opcijom se vraćaju na zajedničku točku konzistentnosti. Druge virtualne mašine se vraćaju na zadnju procesiranu točku konzistentnosti.
- **Prilagođeno:** Ovi opciju koristimo kada određenu virtualnu mašinu želimo vratiti u točno određenu točku povrata

3. Odaberimo Azure virtualnu mrežu u koju ćemo napraviti povrat virtualnih mašina

    - Site Recovery servis će pokušati kreirati testnu virtualnu mašinu u subnetu s istim imenom i IP adresom koja je dodijeljena u Compute and network postavkama virtualne mašine
    - Ako takav subnet u Azure virtualnoj mreži nije dostupan, onda se virtualna mašina kreira u prvom subnetu po abecednom redu
    - Ako u subnetu nije dostupna ista IP adresa, virtualna mašina dobije prvu dostupnu IP adresu iz subneta

4. Ako radimo povrat u Azure i uključena je enkripcija podataka, u postavkama pod Encryption key, odaberimo certifikat koji je dodijeljen prilikom instalacije Providera. Ako enkripcija nije uključena, ovaj korak možemo ignorirati.

5. Sam proces vraćanja virtualnih mašina možemo pratiti u Jobs kartici. U Azure portalu bi trebali vidjeti i repliku testne virtualne mašine.

6. Da bi pokrenuli RDP vezu prema Azure virtualnoj mašini trebat će nam javna IP adresa ili direktna veza prema Azure virtualnoj mreži s naše lokacije (S2S VPN, P2S VPN ili Express Route)

7. Kada provjerimo da sve radi kako treba, odaberimo opciju Cleanup test failover. Ovime brišemo sve virtualne mašine koje su kreirane prilikom DR testiranja.

8. U polju notes možemo zabilježiti sve što smo primijetili tijekom pokretanja DR testa.

Job

NAME	STATUS	START TIME	DURATION	
Prerequisites check for the recovery plan	Successful	5/3/2017 3:48:14 PM	00:00:04	...
Create the test environment	Successful	5/3/2017 3:48:19 PM	00:00:01	...
▼ Recovery plan failover	Successful	5/3/2017 3:48:20 PM	00:01:14	...
SQLServer	Successful	5/3/2017 3:48:20 PM	00:01:14	...
▼ Group 1: Start (1)	Successful	5/3/2017 3:49:35 PM	00:01:40	...
SQLServer	Successful	5/3/2017 3:49:35 PM	00:01:40	...
Finalizing the recovery plan	Successful	5/3/2017 3:51:16 PM	00:00:00	...

Slika 13 – ASR pokretanje DR testa lista zadataka

Kada pokrenemo DR test, događa se sljedeće:

1. **Preduvjeti:** Pokreće se provjera preduvjeta da bi servis bio siguran da se sam proces testiranja može pokrenuti
2. **Prebacivanje:** Priprema se proces i prebacuju se podaci tako da se mogu kreirati Azure virtualne mašine
3. **Zadnji:** Ukoliko smo odabrali zadnju točku povrata, kreira se točka povrata od podataka koju su poslani u servis
4. **Start:** Ovaj korak kreira virtualne mašine korištenjem procesiranih podataka iz prethodnog koraka

4.2.11.2.1 Vremenski moment prebacivanja

U sljedećim scenarijima, prebacivanje zahtijeva dodatni međukorak koji obično traje oko 8 do 10 minuta da se završi:

- VMware virtualne mašine koje imaju Mobility servis stariji od verzije 9.8
- Fizički poslužitelji
- VMware Linux virtualne mašine
- Hyper-V Virtualne mašine zaštićene kao fizički poslužitelji
- VMware virtualne mašine u kojima sljedeći driveri nisu boot driveri
    - storvsc
    - vmbus
    - storflt
    - intelide
    - atapi
- VMware virtualne mašine koje nemaju uključen DHCP, bez obzira da li koriste DHCP ili statičnu IP adresu

4.2.11.3 Kreiranje virtualne mreže za DR testiranje

Preporuka je da se za testiranje DR scenarija u Azure kreira testna virtualna mreža koja je izolirana od produkcije. Testna mreža je prema zadanim postavkama prilikom kreiranja izolirana od ostalih mreža te bi trebala oponašati postavke produkcijske mreže:

- Testna mreža bi trebala imati jednak broj subneta kao i produkcijska mreža. Subneti bi trebali imati ista imena.
- Testna mreža bi trebala koristiti isti raspon IP adresa
- Prepravimo DNS testne mreže s IP adresama definiranim u postavkama DNS virtualne mašine

4.2.11.4 Testiranje DR scenarija u produkcijsku mrežu sekundarne lokacije

Iako je preporučeno da se DR testiranje izvodi u izoliranoj mreži, ukoliko testiranje želite napraviti u produkcijskoj mreži sekundarne lokacije imajmo na umu sljedeće:

- Pobrinimo se da je primarna virtualna mašina ugašena kada radimo DR test. Ukoliko nije, imat ćemo dvije virtualne mašine s istim identitetom, koje u istom trenutku rade u istoj mreži. Ovo može dovesti do neželjenih posljedica.
- Sve promjene koje radimo na testnoj virtualnoj mašini nakon prekida DR testiranje su nepovratno izgubljene. Ove promjene se ne repliciraju na primarnu virtualnu mašinu.
- Testiranje u produkcijskoj okolini dovodi do prekida u radu aplikacija. Korisnici ne bi trebali koristiti aplikacije na testiranim virtualnim mašinama.

4.2.11.5 Priprema Active Directory i DNS servisa

Da bi pokrenuli testiranje za aplikacije, treba nam kopija produkcijskog Active Directory okruženja u testom okruženju. Za više informacije pročitajmo informacije na sljedećoj poveznici: https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-active-directory#test-failover-considerations.

4.2.11.6 Priprema za povezivanje na virtualne mašine nakon testnog prebacivanja

Ako se na virtualnu mašinu želimo spojiti putem RDP ili SSH protokola, moramo zadovoljiti sljedeće uvjete.

Prebacivanje	Lokacija	Akcija
Azure virtualna mašina s Windows OS	On-premises virtualna mašina prije prebacivanja	Da bi pristupili Azure virtualnoj mašini putem Interneta uključimo RDP i pobrinimo se da na Public mrežnoj kartici propustimo odgovarajuće TCP i UDP portove. Da bi pristupili Azure virtualnoj mašini putem S2S tunela, uključimo RDP na mašini i provjerimo da je RDP uključen u postavkama lokalnog vatrozida. Operativna SAN politika mora biti odešena na OnlineAll (https://support.microsoft.com/kb/3031135). Ukoliko je mašina u

		statusu nadogradnje operativnog sustava nećemo se moći spojiti na nju putem RDP protokola.
Azure virtualna mašina s Windows OS	Azure virtualna mašina nakon prebacivanja	Dodajmo javnu IP adresu za virtualnu mašinu. Mrežne sigurnosne postavke moraju omogućavati RDP vezu. Provjerimo Boot diagnostics virtualne mašine da smo sigurni da se upalila. Ukoliko imamo dodatnih problema pogledajmo sljedeće preporuke https://social.technet.microsoft.com/wiki/contents/articles/31666.troubleshooting-remote-desktop-connection-after-failover-using-asr.aspx.
Azure virtualna mašina s Linux OS	On-premises virtualna mašina prije prebacivanja	Pobrinimo se da Secure Shell servis je pokrenut odmah nakon pokretanja virtualne mašine. Provjerimo pravila vatrozida da dopuštaju spajanje na SSH portove.
Azure virtualna mašina s Linux OS	Azure virtualna mašina nakon prebacivanja	Mrežne sigurnosne postavke moraju omogućavati SSH vezu. Dodajmo javnu IP adresu na virtualnu mašinu. Provjerimo Boot diagnostics virtualne mašine da smo sigurni da se upalila.

Tablica 10 - ASR uvjeti za spajanje na virtualnu mašinu nakon testnog prebacivanja

Ukoliko imamo problema s povezivanjem nakon prebacivanja virtualne mašine, pratimo ove korake za rješavanje problema https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-failover-to-azure-troubleshoot.

4.2.12 Active Directory

U Azure podatkovnom centru će se nalaziti dva Domain Controller poslužitelja, jedan za domenu contoso.local, a drugi za domenu sub.contoso.local. Sama replikacija baze podataka koja sadrži sve objekte u Active Directory sustavu poput korisnika, računala i poslužitelja se odvija automatski kroz ugrađeni replikacijski mehanizam i nije ga potrebno posebno konfigurirati za potrebe DR podatkovnog centra. Iz tog razloga nema posebne procedure za prebacivanje Domain Controller servisa niti u svrhu testiranja niti u svrhu produkcijske aktivacije DR podatkovnog centra. Virtualni poslužitelji i servisi koji se aktiviraju u sekundarnom podatkovnom centru će kroz „Domain Controller Locator“ proces pronaći najbliži Domain Controller. Da bi taj proces radio, svi poslužitelji koji se aktiviraju u

sekundarnom podatkovnom centru će imati primarni i sekundarni DNS podešen tako da pokazuju upravo na dva Domain Controller poslužitelja u Azure-u. To će se dogoditi automatski prilikom paljenja virtualnih poslužitelja zato što će se na razini VNet objekta u Azure-u biti konfigurirane IP adrese za primarni i sekundarni DNS.

4.3 Aktivacija/deaktivacija DR sustava u slučaju potrebe

4.3.1 Azure Site Recovery

4.3.1.1 Preduvjeti

1. Prije pokretanja prebacivanja virtualnih mašina i fizičkih poslužitelja na sekundarnu lokaciju preporuka je da se napravi test prebacivanja
2. Prije pokretanja same DR procedure potrebno je pripremiti mrežne parametre na sekundarnoj lokaciji

Tablica prikazuje koje opcije postoje u Azure Site Recovery servisu.

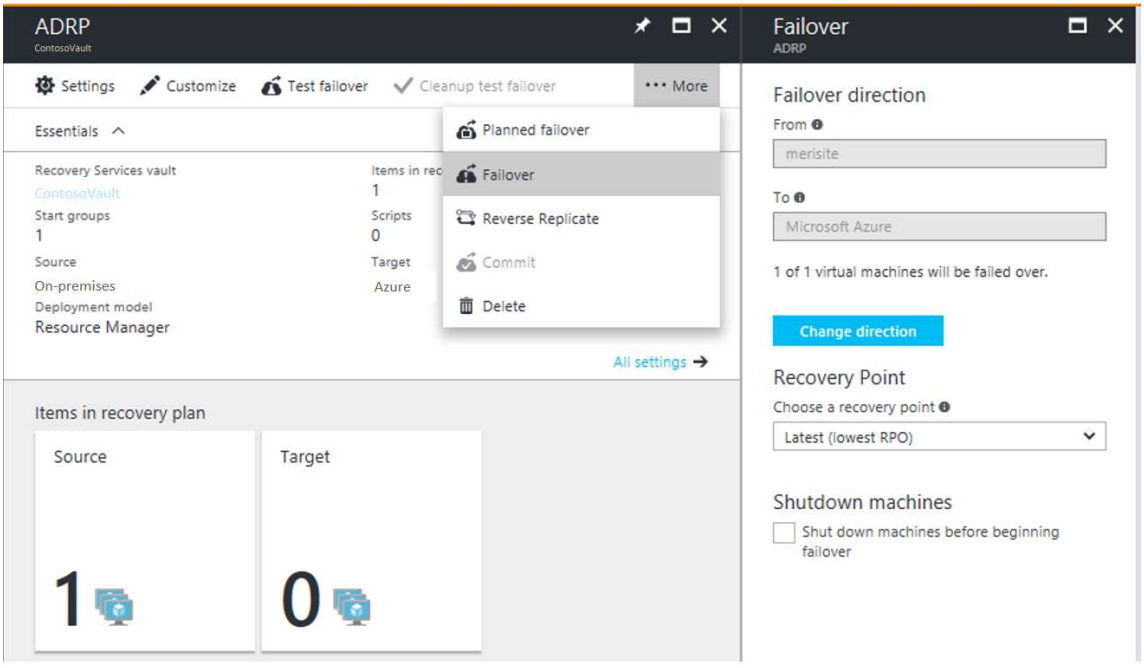
Scenarij	Zahtjevi za povrat aplikacija	Hodogram za Hyper-V
Planirano prebacivanje kada anticipiramo prekid rada podatkovnog centra	Nema gubitka podataka u aplikacijama kad se radi planirana aktivnost	ASR replicira podatke prema frekvenciji kopiranja koju je definirao korisnik. Planirano prebacivanje se koristi da bi se nadvladala ta frekvencija repliciranja i da bi se replicirali finalni podaci prije nego se pokrene prebacivanje. 1. Planirajmo prozor održavanje prema poslovnim procesima tvrtke 2. Obavijestimo korisnike o prestanku rada aplikacija 3. Ugasimo sve aplikacije koje koriste korisnici 4. Pokrenimo Planned failover. Virtualne mašine koje su on-premises se automatski gase Efektivni gubitak podataka u aplikacijama = 0 Zapisnik o točkama povrata je dostupan ako netko želi koristiti stariju točku povrata (do 24 sata za Hyper-V).

		Ako je replikacija zaustavljena duže od retencijskog okvira, korisnik i dalje može napraviti prebacivanje na zadnju dostupnu replikacijsku točku.
Neplanirano prebacivanje zbog iznenadnog događaja (požar, poplava…)	Minimalni gubitak podataka u aplikacijama	1. Pokrenimo DR plan 2. Pokrenimo Unplanned Failover korištenjem ASR servisa na zadnju točku replikacije

Tablica 11 - ASR opcije servisa

4.3.1.2 Pokrenimo prebacivanje

Ova procedura opisuje kako pokrenuti test DR okoline za plan oporavka. Za informacije o tome kako napraviti prebacivanje za samo jednu virtualnu mašinu pogledati upute na ovoj poveznici: https://docs.microsoft.com/en-us/azure/site-recovery/vmware-azure-tutorial-failover-failback#run-a-failover-to-azure.



Slika 14 – ASR pokretanje prebacivanja VM-ova

1. Unutar Azure portala otvorimo Site Recovery opciju, odaberimo Recovery plans, pa ime plana te odaberimo opciju Failover.

2. Odaberimo točku oporavka u koju želimo napraviti povrat. Dostupne su nam sljedeće opcije:

- **Zadnji procesirani:** Ova opcija vraća sve virtualne mašine koje su obuhvaćene recovery planom na zadnju točku oporavka koji je procesiran od strane Site Recovery servisa. Da bi vidjeli koja je zadnja točka oporavka za specifičnu virtualnu mašinu, možemo pogledati pod postavkama opciju Latest Recovery Points. Ova opcija omogućava nizak RTO jer se vrijeme ne troši na procesiranje neprocesuiranih podataka.
- **Zadnji aplikacijski konzistentni:** Ova opcija vraća sve virtualne mašine koje su obuhvaćene recovery planom na zadnju točku oporavka koja je aplikativno konzistentna.
- **Zadnji:** Ova opcija prvo procesira sve podatke koji su poslane u Site Recovery servis**,** da bi se kreirala točka povrata za sve virtualne mašine prije vraćanja mašine. Ova opcija nudi najniži RPO radi toga jer će vraćena virtualna mašina imati sve informacije do trenutka kada je pokrenut Site Recovery proces.
- **Zadnji s više procesiranih virtualnih mašina:** Ova opcija je dostupna u recovery planovima koji imaju jednu ili više virtualnih mašina s uključenom opcijom višestruke konzistentnosti. Virtualne mašine s upaljenom opcijom se vraćaju na zajedničku točku konzistentnosti. Druge virtualne mašine se vraćaju na zadnju procesiranu točku konzistentnosti.
- **Zadnji s više procesiranih virtualnih mašina aplikacijski konzistentan:** Ova opcija je dostupna u recovery planovima koji imaju jednu ili više virtualnih mašina s uključenom opcijom višestruke konzistentnosti. Virtualne mašine s upaljenom opcijom se vraćaju na zajedničku točku aplikacijske konzistentnosti. Druge virtualne mašine se vraćaju na zadnju procesiranu točku konzistentnosti.
- **Prilagođeno:** Ovi opciju koristimo kada određenu virtualnu mašinu želimo vratiti u točno određenu točku povrata

Napomena: Opcija odabira točke povrata je dostupna samo kada povrat radimo u Azure javni oblak.

3. Ako su neke virtualne mašine prebačene prije i sada je ta virtualna mašina aktivna na primarnoj i sekundarnoj lokaciji, pomoću opcije Change direction možemo odabrati na koju lokaciju će se dogoditi prebacivanje
4. Ako radimo povrat u Azure i uključena je enkripcija podataka (samo kada je virtualna mašina zaštićena putem VMMa), u postavkama pod Encryption key, odaberimo certifikat koji je kreiran prilikom zaštite virtualne mašine na VMMu.
5. Odaberimo opciju Shut-down machine before beginning failover ako želimo da Site Recovery pokuša ugasiti virtualnu mašinu na primarnoj lokaciji prije prebacivanja. Čak i ako servis ne uspije ugasiti virtualnu mašinu proces prebacivanja se nastavlja

Napomena: Ako su Hyper-V virtualne mašine zaštićene. Opcija gašenja virtualnih mašina također pokuša sinkronizirati on-premises podatke koji još nisu bili poslani u servis prije nego pokrene prebacivanje.

6. Tijek prebacivanja možemo pratit ina Jobs kartici. U slučaju grešaka prilikom prebacivanja recovery plan se izvršava sve do kraja.
7. Nakon prebacivanja, provjerimo da su virtualne mašine pokrenute tako da se pokušamo u njih prijaviti. Ako se želimo prebaciti u neku drugu točku replikacije to možemo napraviti pomoću opcije Change recovery point.

8. Nakon što smo zadovoljni s rezultatima prebacivanja virtualnih mašina, možemo odabrati opciju Commit da bi potvrdili prebacivanje. Commit opcija briše sve točke povrata dostupne u servisu te opcija Change recovery point opcija više nije dostupna.

4.3.1.3 Planirano prebacivanje

Virtualne mašine i fizički poslužitelji zaštićeni putem Site Recovery servisa podržavaju i planirano prebacivanje. Planirano prebacivanje je proces u kojem nema gubitka aplikacijskih podataka. Kada se pokrene planirano prebacivanje, prvo se gase polazne virtualne mašine, sinkroniziraju se svi podaci te započinje proces prebacivanja.

4.3.1.4 Zadatak prebacivanja

Job

NAME	STATUS	START TIME	DURATION	
Prerequisites check for the recovery plan	Successful	5/3/2017 4:01:19 PM	00:00:02	...
Create the environment	Successful	5/3/2017 4:01:22 PM	00:00:00	...
▼ All groups shutdown (1)	Successful	5/3/2017 4:01:23 PM	00:01:54	...
Shutdown: Group 1 (1)	Successful	5/3/2017 4:01:23 PM	00:01:54	...
▼ Recovery plan failover	Successful	5/3/2017 4:03:18 PM	00:01:38	...
SQLServer	Successful	5/3/2017 4:03:18 PM	00:01:38	...
▼ Group 1: Start (1)	Successful	5/3/2017 4:04:57 PM	00:01:45	...
SQLServer	Successful	5/3/2017 4:04:57 PM	00:01:45	...
Finalizing the recovery plan	Successful	5/3/2017 4:06:43 PM	00:00:00	...

Slika 15 – ASR pokretanje prebacivanja VM-ova lista zadataka

Kada pokrenemo proces prebacivanja, uključeni su sljedeći koraci:

1. **Preduvjeti:** Pokreće se provjera preduvjeta da bi servis bio siguran da se sam proces prebacivanja može pokrenuti
2. **Prebacivanje:** Priprema se proces i prebacuju se podaci tako da se mogu kreirati Azure virtualne mašine
3. **Zadnji:** Ukoliko smo odabrali zadnju točku povrata, kreira se točka povrata od podataka koju su poslani u servis
4. **Start:** Ovaj korak kreira virtualne mašine korištenjem procesiranih podataka iz prethodnog koraka

Upozorenje: Nemojte nikada prekidati postupak prebacivanja kada ga jednom pokrenete! Prije nego se pokrene proces prebacivanja, replikacija se zaustavlja. Ako prekinemo prebacivanje nakon sto ga pokrenemo, sam proces staje ali virtualna mašina neće ponovno pokrenuti proces replikacije. Replikacija se ne može ponovno pokrenuti.

4.3.1.5 Vrijeme potrebno za prebacivanje u Azure

U određenim slučajevima, prebacivanje virtualnih mašina zahtijeva dodatne međukorake koji traju od 8 do 10 minuta. U sljedećim slučajevima to vrijeme može biti i duže:

- VMware virtualne mašine koje imaju Mobility servis stariji od verzije 9.8
- Fizički poslužitelji
- VMware Linux virtualne mašine
- Hyper-V Virtualne mašine zaštićene kao fizički poslužitelji
- VMware virtualne mašine u kojima sljedeći driveri nisu boot driveri
    - storvsc
    - vmbus
    - storflt
    - intelide
    - atapi
- VMware virtualne mašine koje nemaju uključen DHCP, bez obzira da li koriste DHCP ili statičnu IP adresu

4.3.1.6 Korištenje skripti u koraku prebacivanja

Neke akcije se mogu automatizirati prilikom procesa prebacivanja. Možemo koristiti skripte ili Azure automatizaciju u recovery planovima za tu svrhu.

4.3.2 Active Directory

Nema posebnih procedura za aktivaciju Active Directory sustava.

4.4 CloudEndure DRaaS Servis

4.4.1 CloudEndure sustav

CloudEndure Disaster Recovery je SaaS servis *(eng. Software as a Service)* koji omogućuje organizacijama da brzo i jednostavno prebace svoju strategiju oporavka od katastrofe na Amazon Web Services (AWS) iz postojećih fizičkih ili virtualnih podatkovnih centara, privatnih oblaka ili drugih javnih oblaka, uz podršku oporavka od katastrofe između regija ili zona u AWS-u. CloudEndure je u inicijalno nastao kao zasebna tvrtka koja je nudila DR rješenje između različitih izvora i ciljeva, ali naposlijetku ga je kupila kompanija Amazon Web Services i „asimilirala“ u svoju ponudu cloud servisa kao DR rješenje.

CloudEndure izvodi kontinuiranu replikaciju na razini bloka i sprema neaktivnu kopiju u ciljnu infrastrukturu, koja koristi manji postotak računanja, pohrane i memorije od primarnog mjesta ; to dovodi do minimalnog RTO-a (cilj vremena oporavka) i RPO-a (ciljane točke oporavka) kada dođe do potrebe oporavka od katastrofalnog događaja. Implementacija se provodi na način da se na sve poslužitelje koje se namjerava štititi instalira vrlo lagani agent i samo inicijalno konfigurira. Nakon toga se agent „javlja“ cloud SaaS servisu odakle se nadalje sve konfigurira i podešava. Kako agent radi u pozadini i troši izuzetno malo resursa, nakon inicijalne konfiguracije nema više potrebe da se bilo što podešava na samom poslužitelju. Preko CloudEndure portala administrator upravlja svim postavkama i politikama zaštite, kreira planove, provodi DR testiranja itd. Jedno od najboljih svojstava CloudEndure sustava jest izuzetno ekonomičan način korištenja resursa u cloudu.

Prilikom inicijalnog dodavanja prvog poslužitelja u DR servis, CloudEndure u korisnikovoj AWS pretplati automatski kreira jednu vrlo nezahtjevnu i povoljnu virtualnu mašinu sa prilagođenom verzijom Linuxa *(eng. Synchronization Controller)* koja je za korisnika tzv. „black box“ i nema mogućnosti spajanja i podešavanja. Nakon toga u ovisnosti koliko izvorni štićeni poslužitelj ima diskova, mapira se isti broj povoljnih tzv. spinning diskova bez obzira i ako se na izvornom poslužitelju koriste performansni SSD diskovi *(eng. Solid State Drive)*. CloudEndure analizira i pohranjuje sve metapodatke o izvornom poslužitelju (CPU, RAM, OS itd.) i nakon toga započinje inicijalnu sinkronizaciju diskova koja ovisi o brzini veze između korisnika i cloud servisa. Kada oba diskovna sustava dostignu stanje sinkronizacije, nastavlja se samo delta sinkronizacija koja prebacuje sa izvorne lokacije na cloud servis samo izmjenjene podatke, ali ujedno vodi računa da su podaci na cloud servisu konzistentni *(eng. Crash Consistent)*. Nakon toga možemo krenuti u bilo kojem trenutku sa test DR ili pravom aktivacijom DR-a. Važno je napomenuti da jedna instanca Synchronization Controllera podržava približno 15 diskova, neovisno o broju štićenih poslužitelja.

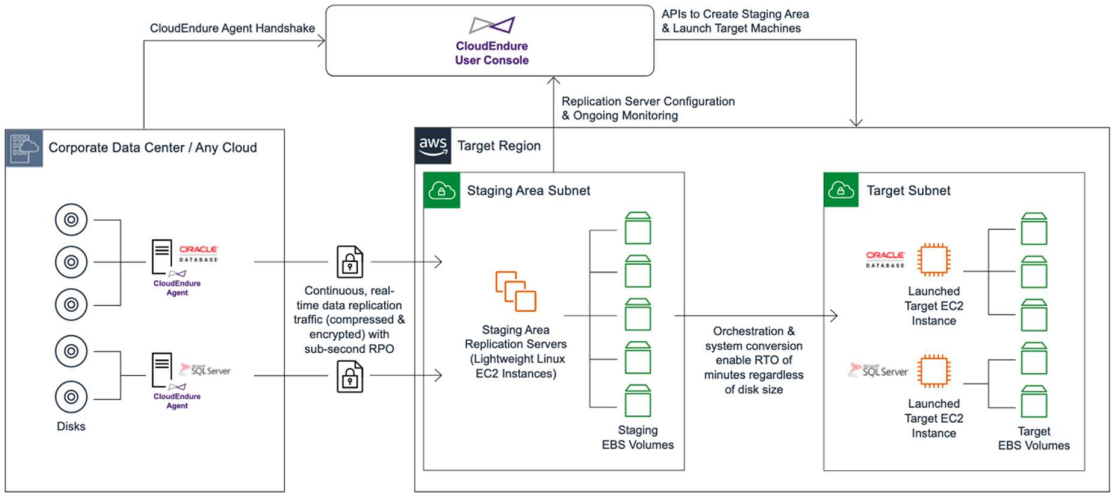
Prilikom poketanja DR testa ili iniciranja pravog DR slučaja *(eng. Failover)*, CloudEndure servis kreira specijalnu privremenu Linux virtualnu mašinu *(eng. Converter Controller)* koja služi za transformaciju pričuvnog sinkroniziranog diska u pravi ciljni disk koji će se povezati sa novom virtualnom mašinom u cloudu. Nakon što sustav iz meta podataka kreira novu virtualnu mašinu performansama najsličniju izvornoj, Converter Controller transformira

diskove i spaja ih na novu mašinu. Nakon toga se mašina pokreće i tu završava procedura. CloudEndure servis uništava Converter Controller mašinu i sustav odlazi u status Failovered.

Metoda povratka *(eng. Failback)* je prilično slična zato ne bi ulazio u dublje tehničke detalje.

Samo CloudEndure rješenje se može koristiti ujedno i kao servis za kontinuirano sigurnosno kopiranje i Live migraciju pojedinih sustava, a ne samo kao DR rješenje.

CloudEndure DR je tzv. "application agnostic" rješenje te ima mogućnost repliciranja sustava neovisno da li se radi o fizičkoj, virtualnoj ili infrastrukturi temeljenoj na drugom cloud servisu uključujući (Amazon Web Services (AWS), Google Cloud Platform (GCP) i Microsoft Azure).



Slika 16 – CloudEndure shema

Izvor: CloudEndure , 20. ožujka 2022.

5. ZAKLJUČAK

Namjera i cilj ovog rada je pokazati i naglasiti na koji način su danas bitni informatički sustavi kako u poslovanju tako i u svim granama ljudske djelatnosti. Također smo svjesni koliko su takvi sustavi postali kompleksni, međusobno povezani i do neke mjere javno dostupni.

Uključujući u obzir sve navedeno, svaki dan smo svjedoci kako takvi su takvi sustavi podložni različitim vrstama neželjenih događaja. Radom smo pokrili segment koji se odnosi na planiranje i sustav oporavka od katastrofalnih događaja. Na veliki broj neželjenih događaja najčešće ne možemo utjecati, ali se kvalitetnim planiranjem unaprijed, pravovremenom obukom, redovnim testiranjima i kontinuiranim poboljšanjima možemo zadržati dostupnost i konkurentnost na tržištu, osigurati sigurnost djelatnika i imovine.

Ideja na kojoj se temeljio cijeli ovaj rad je dislokacija pričuvnih podatkovnih centara u neki od javno dostupnih Cloud servisa. Takvim pristupom se, u odnosu na stari konvencionalni pristup, višestruko pojednostavio, ubrzao i smanjio financijski teret na svaku organizaciju koja se odluči na ovakav pristup izradi plana kontinuiteta poslovanja čime smo postigli inicijalni cilj.

6. IZJAVA

Izjava o autorstvu završnog rada i akademskoj čestitosti

Ime i prezime studenta: Enver Mehanović

Matični broj studenta: 1191017744

Naslov rada: Disaster Recovery rješenje bazirano na Cloud servisima

Pod punom odgovornošću potvrđujem da je ovo moj autorski rad čiji niti jedan dio nije nastao kopiranjem ili plagiranjem tuđeg sadržaja. Prilikom izrade rada koristio sam tuđe materijale navedene u popisu literature, ali nisam kopirao niti jedan njihov dio, osim citata za koje sam naveo autora i izvor te ih jasno označio znakovima navodnika. U slučaju da se u bilo kojem trenutku dokaže suprotno, spreman sam snositi sve posljedice uključivo i poništenje javne isprave stečene dijelom i na temelju ovoga rada.

Potvrđujem da je elektronička verzija rada identična onoj tiskanoj te da je to verzija rada koju je odobrio mentor.

Datum	Potpis studenta
_____	_____

7. POPIS LITERATURE

7.1 Knjige i članci

Reuvid, Jonathan, (2005) The Secure Online Business Handbook; A Practical Guide to Risk Management and Business Continuity (4th Edition)

Šimović, Vladimir, Uvod u informacijske sustave, 2. dopunjeno i izmijenjeno izdanje, Golden Marketing – Tehnička knjiga i Učiteljski fakultet Sveučilišta u Zagrebu, Zagreb, 2010.

Šimović, Vladimir, Maja Ružić-Baf, Suvremeni informacijski sustavi, Sveučilište Jurja Dobrile u Puli, Pula, 2013.

7.2 Internetski izvori

[1] *Disaster recovery – Wikipedia*. Preuzeto s https://en.wikipedia.org/wiki/Disaster_recovery (27. kolovoza 2022.)

[1] *Business continuity planning – Wikipedia*. Preuzeto s https://en.wikipedia.org/wiki/Business_continuity_planning (28. kolovoza 2022.)

[1] *ISO standards*. Preuzeto s https://www.iso.org/search.html?q=business%20continuity&hPP=10&idx=all_en&p=0&hFR%5Bcategory%5D%5B0%5D=standard (28. kolovoza 2022.)

[1] *Ransomware – Wikipedia*. Preuzeto s https://hr.wikipedia.org/wiki/Ransomware (2. rujna 2022.)

[1] *A brief history of disaster recovery*. Preuzeto s https://www.comparethecloud.net/articles/a-brief-history-of-disaster-recovery/ (14. travnja 2022.)

[1] *Example- Disaster recovery plan – IBM documentation*. Preuzeto s https://www.ibm.com/docs/en/i/7.3?topic=system-example-disaster-recovery-plan (2. rujna 2022.)

[1] *8 things to consider before choosing your DRaaS provider*. Preuzeto s https://www.msystechnologies.com/blog/8-things-to-consider-before-choosing-your-draas-provider/ (2. rujna 2022.)

[1] *CreateReplicationRelationship method*. Preuzeto s https://msdn.microsoft.com/library/hh850036.aspx (5. rujna 2022.)

[1] *StartReplication method*. Preuzeto s https://msdn.microsoft.com/library/hh850303.aspx (5. rujna 2022.)

[1] *Microsoft peering for Express Route Circuit*. Preuzeto s https://docs.microsoft.com/en-us/azure/expressroute/expressroute-circuit-peerings#microsoftpeering (5. rujna 2022.)

8. POPIS SLIKA, TABLICA I GRAFIKONA

8.1 Popis slika

8.2 Popis tablica

ŽIVOTOPIS

CURRICULUM VITAE

OSOBNE INFORMACIJE

Enver Mehanović

Španovićeva 5

+385 95 9021 353

Enver.Mehanovic@outlook.com

Datum rođenja: 27.12.1973.

RADNO ISKUSTVO

srp 2019 - danas — Arhitekt rješenja

Span d.d.

Arhitektura informatičkih rješenja (on-prem i Cloud based). Rad sa različitim, većinom Microsoft, tehnologijama i proizvodima uz različita Cloud pružatelje usluga (Azure, AWS).

svi 2016 - danas — Inženjer rješenja, Konzalting za rješenja

Span d.o.o.

AD Migracije
RDS rješenja
Active Directory
Printing rješenja
AWS rješenja

NPS rješenja
Podrška korisnicima (TAM)

lis 2015 - ožu 2016 Sistem inženjer, Podrška i upravljanje infrastrukturom

Span d.o.o.

Upravljanje, održavanje i rješavanje problema IT sustava za klijente
Planiranje i provođenje migracija AD-a
Podrška klijentima
Savjetovanje klijenata vezano za implementacije sustava i aplikacija
Praćenje korisničke infrastrukture
Rad s različitim Microsoftovim tehnologijama (Exchange, MSO, AD, ADMT, Powershell itd.)

vel 2007 - tra 2015 Zamjenik voditelja odjela informatike

Banco Popolare Croatia d.d.

Upravljanje i razvoj IT sustava
Voditelj tima za IT projekte
Član tima više IT projekata
Planiranje i konfiguriranje mrežne opreme i telekomunikacijskih veza, implementacija novih mrežnih rješenja (poboljšanje kvalitete i performansi)
Organizacija i rad na sistemskoj i korisničkoj podršci
Upravljanje nabavama vezanim za IT i odnosi partnera / dobavljača / outsourcinga
Upravljanje i nadzor provedbi aktivnosti koje se odnose na regulatorne zahtjeve za
odgovarajuće upravljanje informacijskim sustavima unutar banke (regulator - HNB, revizijske kuće)

lip 2002 - vel 2007 Senior sistem inženjer (Stručnjak za sigurnost)

HVB Bank Croatia d.d. (later Splitska banka d.d.)

Upravljanje i razvoj IT sustava
Član projektnih timova na mnogim IT projektima
Priprema, instalacija i konfiguracija poslužitelja baziranih na Windows i Linux platformi
Organizacija i rad na sistemskoj i korisničkoj podršci

ožu 1998 - lip 2002 Serviser, Savjetnik u prodaji, Savjetnik za tendere

MSan grupa d.o.o., King računala d.o.o.

IT hardverske usluge
Izgradnja i instalacija poslužitelja i stolnih računala
Planiranje i savjetovanje prodaje u trgovini
Pomoć i savjetovanje za klijente
Planiranje tendera i projektna dokumentacija za velike nabave IT opreme
Upravljanje nabavom i IT odnosima s dobavljačima

PROJEKTI

Naziv projekta	Erste bank - AVD POC
Klijent	Erste bank
Tehnologije	Azure Active Directory, Azure Files, Azure Windows Virtual Desktop, Microsoft Active Directory
Uloga na projektu	**Span d.d. - Voditelj projekta**
Trajanje	veljača 2022 - danas
Opis projekta	Dizajn i implementacija testnog POC AVD rješenja za potrebe zamjene postojećeg on-prem VDI rješenja baziranog na MS RDS VDI rješenju.

Naziv projekta	HPB - Infrastrukturna i aplikacijska analiza
Klijent	HPB
Tehnologije	Azure Migrate
Tehnologije (ručni unos)	CAST, Silk
Uloga na projektu	**Span d.d. - Voditelj projekta**
Trajanje	siječanj 2022 - danas
Opis projekta	Asistencija prilikom instalacije Azure Migrate appliancea, pomoć prilikom konfiguracije, prikupljanje metrika, provođenje radionica, analiza aplikacija pomoću alata CAST, analiza svih prikupljenih podataka i izrada završnog dokumenta prijedloga migracije servera, servisa i baza u Azure Cloud.

Naziv projekta	Erste bank - analiza infrastrukture
Klijent	Erste bank
Tehnologije	Azure Active Directory, Azure Migrate
Uloga na projektu	**Span d.d. - Voditelj projekta**
Trajanje	listopad 2021 - ožujak 2022
Opis projekta	Podrška implementaciji Azure Assessment appliance-a, podešavanje, prikupljanje metrika, provođenje radionica, analiza svih podataka i izrada dokumentacije sa preporukama za migraciju servera i servisa u Azure Cloud.

Naziv projekta	Tate & Lyle - Luebeck i Lodz migracija servera u Azure
Klijent	Tate & Lyle
Tehnologije	Azure File Sync, Azure Site Recovery (Microsoft)
Uloga na projektu	**Span d.d. - Voditelj projekta**
Trajanje	veljača 2021 - ožujak 2022

Opis projekta	Priprema, planiranje i migracija servera na lokacijama Luebeck i Lodz u Azure.

Naziv projekta	SOPH
Klijent	McDonalds (but not limited to)
Tehnologije	Backup Veeam B&R, Converged management HPE OneView, Microsoft Active Directory, Microsoft Hyper-V
Uloga na projektu	**Span d.d. - Voditelj projekta**
Trajanje	siječanj 2021 - siječanj 2022
Opis projekta	Dizajn Spanovog OPH (On-Premise Hosting) rješenja kao zamjena za postojeće Zynstra OPH rješenje u McDonaldsu.

Naziv projekta	Konsolidacija RDS farme u Newsec-u
Tehnologije	Azure Networking, Azure SQL Database Managed Instance, Azure Storage, Remote Desktop Services
Uloga na projektu	**Span d.d. - Voditelj projekta**
Trajanje	svibanj 2019 - listopad 2021
Opis projekta	Pregled postojećeg sustava, izrada dizajna novog rješenja, implementacija.

Naziv projekta	Nadogradnja RDS farme u Newsec Norway
Tehnologije	Microsoft Active Directory, Remote Desktop Services
Uloga na projektu	**Span d.d. - Voditelj projekta**
Trajanje	prosinac 2019 - rujan 2021
Opis projekta	Pregled i analiza postojećeg rješenja. Izrada dizajna novog rješenja. Implementacija.

Naziv projekta	Valamar - analiza spremnost za migraciju u Azure
Klijent	Valamar Riviera

Tehnologije	Azure Active Directory, Azure Migrate
Uloga na projektu	**Span d.d. - Voditelj projekta**
Trajanje	veljača 2021 - kolovoz 2021
Opis projekta	Instalacija Azure Migrate appliance-a. Monitoring i analiza postojećeg sustava i izrada dokumentacije za migraciju servera i servisa u Azure Cloud.

Naziv projekta	Tate & Lyle - WVD POC za APAC
Klijent	Tate & Lyle
Tehnologije	Azure Active Directory, Azure Files, Azure Windows Virtual Desktop, Microsoft Active Directory
Uloga na projektu	**Span d.d. - Voditelj projekta**
Trajanje	ožujak 2021 - svibanj 2021
Opis projekta	Dizajn i implementacija AVD rješenja za potrebe POC-a i testiranja pristupa klijenata i instalacije aplikacija. Usporedba sa postojećim Citrix rješenjem.

Naziv projekta	HCK - konsolidacija poslužiteljske infrastrukture
Klijent	HCK - Croatian Red Cross
Tehnologije	Backup Veeam B&R, Exchange, Microsoft Active Directory, Office 365, Vmware, Windows Server 2016
Uloga na projektu	**Span d.o.o. - Voditelj projekta**
Trajanje	siječanj 2019 - prosinac 2020
Opis projekta	Instalacija novih servera, podizanje nove domene, instalacija Exchange servera i implementacija O365 hibridnog rješenja, implementacija backupa.

Naziv projekta	Valamar - instalacija ADFS-a za potrebe on-prem MFA
Klijent	Valamar Riviera

Tehnologije	Active Directory Federation Services, Azure Active Directory, Microsoft Active Directory, NPS
Uloga na projektu	**Span d.d. - Voditelj projekta**
Trajanje	srpanj 2020 - studeni 2020
Opis projekta	Dizajn i implementacija ADFS HA farme u korisnikovu okolinu za potrebe lokalnog MFA rješenja. Integracija sa zadanim sustavima.

Naziv projekta	MZLZ - Azure VDI
Klijent	MZLZ
Tehnologije	Azure Active Directory, Azure Windows Virtual Desktop
Uloga na projektu	**Span d.d. - Voditelj projekta**
Trajanje	svibanj 2020 - kolovoz 2020
Opis projekta	Dizajn i implementacija WVD rješenje za potrebe POC-a.

Naziv projekta	Implementacija OPH rješenja u McDonald's Francuska
Tehnologije	Windows Server, Zynstra
Uloga na projektu	**Span d.d. - Voditelj projekta**
Trajanje	ožujak 2019 - siječanj 2020
Opis projekta	Implementacija on-prem hosting rješenja tvrtke Zynstra. Podešavanje mreže i instalacija poslužitelja.

Naziv projekta	McD Francuska - implementacija OPH rješenja
Tehnologije	Zynstra
Uloga na projektu	**Span d.d. - Voditelj projekta**
Trajanje	ožujak 2019 - siječanj 2020
Opis projekta	Implementacija OPH rješenja u DC McD u Francuskoj. Instalacija VM-ova na OPH sustav.

Naziv projekta	CH McD pregled i analiza Grupnih AD politika
Klijent	McDonalds CH
Tehnologije	Microsoft Active Directory
Uloga na projektu	**Span d.o.o. - Voditelj projekta**
Trajanje	srpanj 2018 - prosinac 2018
Opis projekta	Revidiranje postojećih grupnih politika u CH McD Market OU-u. Kreiranje novih, optimizacija.

Naziv projekta	Valamar - Implementacija visokodostupnog RDS rješenja
Klijent	Valamar Riviera d.d.
Tehnologije	LoadBalancer KEMP, Remote Desktop Services, SQL Server, Windows Server 2016
Uloga na projektu	**Span d.o.o. - Član tima**
Trajanje	siječanj 2018 - rujan 2018
Opis projekta	Instalacija nove RDS farme, podešavanje visoke dostupnosti, podešavanje print sustava, pristupa izvana itd.

Naziv projekta	Migracija restoranske mreže u McDonald's UK marketu
Tehnologije	Active Directory Migration Tool, Microsoft Active Directory, Powershell
Uloga na projektu	**Span d.o.o. - Član tima**
Trajanje	siječanj 2017 - ožujak 2018
Opis projekta	McD UK migracija restoranskih korisničkih računa i mailbox-a iz legacy domene u GAD.

Naziv projekta	OTP pregled i analiza Active Direcotry imeničkog servisa
Tehnologije	Microsoft Active Directory, Powershell

Uloga na projektu	**Span d.o.o. - Voditelj projekta**
Trajanje	prosinac 2017 - siječanj 2018
Opis projekta	Analiza rada AD sustava u mreži OTP banke i dostava dokumentacije i preporuka.

Naziv projekta	Ured predsjednice RH - pregled sustava
Tehnologije	Powershell, Windows Server
Uloga na projektu	**Span d.o.o. - Voditelj projekta**
Trajanje	prosinac 2017 - siječanj 2018
Opis projekta	Analiza i pregled svih poslužitelja u mreži UP RH. Kreiranje izvještaja sa preporukama.

Naziv projekta	Migracija McDonald's BPS korisničkih računa
Tehnologije	Active Directory Migration Tool, Microsoft Active Directory
Uloga na projektu	**Span d.o.o. - Voditelj projekta**
Trajanje	studeni 2017 - siječanj 2018
Opis projekta	Migracija vanjskih McD korisnika iz legacy domene u GAD prema tablicama.

Naziv projekta	McDonalds migracija marketa
Tehnologije	Active Directory Migration Tool, Microsoft Active Directory, Powershell
Uloga na projektu	**Span d.o.o. - Član tima**
Trajanje	svibanj 2016 - siječanj 2018
Opis projekta	Migracija više marketa iz legacy domene u GAD u McD mreži (marketi: ES, CH, BA, SI, RS itd).

Naziv projekta	McDonald's Kanada - implementacija RDS rješenja

Tehnologije	Remote Desktop Services, Windows Server
Uloga na projektu	**Span d.o.o. - Član tima**
Trajanje	travanj 2017 - listopad 2017
Opis projekta	Implementacija novog RDS sustava u McD Kanada.

Naziv projekta	McDonald's Finska - Instalacija RDS "jump" poslužitelja
Tehnologije	Remote Desktop Services, Windows Server
Uloga na projektu	**Span d.o.o. - Voditelj projekta**
Trajanje	lipanj 2016 - rujan 2017
Opis projekta	Implementacija novog RDS jump poslužitelja prema potrebama korisnika.

Naziv projekta	McDonald's Latinska Amerika - instalacija imeničkih poslužitelja (DC)
Tehnologije	Microsoft Active Directory, SMART (SCCM), SMART (SCOM)
Uloga na projektu	**Span d.o.o. - Član tima**
Trajanje	ožujak 2017 - srpanj 2017
Opis projekta	Implementacija više DC-a u McD mreži za potrebe Latinske Amerike.

Naziv projekta	McDonald's EU Ženeva - relokacija ureda
Tehnologije	Active Directory Migration Tool, Microsoft Active Directory
Uloga na projektu	**Span d.o.o. - Voditelj projekta**
Trajanje	studeni 2016 - ožujak 2017
Opis projekta	Gašenje EU Ženevskog ureda; prebacivanje korisnika i računala prema tablicama u urede u drugim zemljama, prebacivanje velikih količina podataka, accounta itd.

Naziv projekta	McDonald's - instalacija Azure imeničkih poslužitelja (DC)
Tehnologije	Microsoft Active Directory, SMART (SCCM), SMART (SCOM)
Uloga na projektu	**Span d.o.o. - Član tima**
Trajanje	srpanj 2016 - rujan 2016
Opis projekta	Implementacija više DC poslužitelja u McD mreži na Azure platformi.

Naziv projekta	IBM Sterling Connect:Direct implementacija rješenja
Tehnologije	IBM Tivoli Netcool/OmniBus
Tehnologije (ručni unos)	IBM Connect:Direct
Uloga na projektu	**Banco Popolare Croatia d.d. - Voditelj projekta**
Trajanje	siječanj 2015 - ožujak 2015
Opis projekta	Implementacija Connect:Direct MQ sustava za potrebe sigurne razmjene podataka sa trećim stranama.

Naziv projekta	Etički test mrežnih slabosti
Tehnologije	Linux
Tehnologije (ručni unos)	Various tools
Uloga na projektu	**Banco Popolare Croatia d.d. - Voditelj projekta**
Trajanje	ožujak 2014 - kolovoz 2014
Opis projekta	Provođenje etičkog penetracijskog testiranja za potrebe povećanja sigurnosti mreže banke.

Naziv projekta	Implementacija rješenja za upravljanje zapisima - Splunk Enterprise
Tehnologije	Firewall Cisco, Networking Cisco, Windows Server

Tehnologije (ručni unos)	Splunk SIEM solution
Uloga na projektu	**Banco Popolare Croatia d.d. - Voditelj projekta**
Trajanje	svibanj 2013 - veljača 2014
Opis projekta	Implementacija Splunk Enterprise sustava za log management.

Naziv projekta	Fortinet implementacija IPS rješenja - Banco Popolare Croatia
Tehnologije	FortiAnalyzer, Fortigate
Tehnologije (ručni unos)	Fortinet network appliances
Uloga na projektu	**Banco Popolare Croatia d.d. - Voditelj projekta**
Trajanje	siječanj 2012 - siječanj 2013
Opis projekta	Implementacija cluster Fortigate sustava za potrebe IPS-a u mreži banke. U sustav uključen FortiAnalyzer i FortiManager.

OBRAZOVANJE I TRENING

lis 2018 - ruj 2021 **Veleučilište Baltazar Zaprešić**

Informacijske tehnologije

Studij u tijeku

ruj 1988 - kol 1992 **Tehničar za elektroniku**

Tehnička škola za elektrotehniku Ruđer Bošković

TEHNIČKE VJEŠTINE

Active Directory, Amazon Web Services, Android, Azure, Azure Virtual Desktop, Cisco Technologies, Excel, Group Policy, Hardware, iCloud, IIS, Infrastructure assesment and planning, iOS, Microsoft Office, Networking, O365, Poitsharp, PowerBI, Powershell, Veeam Backup & Replication, Windows 10, Windows Phone, Windows Server

CERTIFIKATI

Amazon — AWS Solutions Training for Partners: Big Data and Analytics

Vrijedi od 14.09.2017. do Nije definirano.

Amazon — AWS Solutions Training for Partners: Foundations Course

Vrijedi od 13.09.2017. do Nije definirano.

Amazon — Big Data & Analytics E-Learning

Vrijedi od 31.08.2017. do Nije definirano.

Amazon — AWS Business Professional Online

Vrijedi od 21.09.2017. do Nije definirano.

Amazon — AWS Solutions Training for Partners: AWS for Windows (Techincal Online)

Vrijeme valjanosti certifikata nije definirano.

Kvadra Consulting — Osnove informacijske sigurnosti po normi ISO/IEC 27001

Vrijeme valjanosti certifikata nije definirano.

Microsoft DataSec BootCamp

Vrijeme valjanosti certifikata nije definirano.

Microsoft Microsoft Certified Professional

Vrijedi od 18.07.2016. do Nije definirano.

Microsoft Microsoft Certified Solutions Associate: Windows Server 2012

Vrijedi od 12.03.2018. do Nije definirano.

Microsoft Microsoft Certified: Azure Solutions Architect Expert

Vrijedi od 11.07.2019. do 11.07.2023..

Amazon AWS Certified Cloud Practitioner

Vrijedi od 10.02.2020. do Nije definirano.

Microsoft Microsoft Certified: Azure Virtual Desktop Specialty

Vrijedi od 20.09.2021. do 20.09.2023..

Amazon AWS Certified Solutions Architect – Associate

Vrijedi od 15.03.2022. do 15.03.2025..

ISPITI

Microsoft	70-410 Installing and Configuring Windows Server 2012
Microsoft	70-411 Administering Windows Server 2012
Microsoft	70-210 Installing, Configuring, and Administering Microsoft Windows 2000 Professional
Microsoft	70-215 Installing, Configuring, and Administering Microsoft Windows 2000 Server
Microsoft	Microsoft Windows 2000 Network & Operating System Essentials
Microsoft	70-412 Configuring Advanced Windows Server 2012 Services
Microsoft	AZ-300 Microsoft Azure Architect Technologies
Microsoft	AZ-301 Microsoft Azure Architect Design
Microsoft	Exam AZ-140: Configuring and Operating Microsoft Azure Virtual Desktop
Amazon	AWS Certified Solutions Architect – Associate
Amazon	AWS Cloud Practitioner

JEZIČNE VJEŠTINE

	RAZUMIJEVANJE		GOVOR		PISANJE
	Slušanje	Čitanje	Interakcij	Produkcij	
Hrvatski	C2	C2	C2	C2	C2
Engleski	C1	C1	B2	B2	B2
Njemački	A1	A1	A1	A1	A1

Razine: A1/A2: Temeljni korisnik - B1/B2: Samostalni korisnik - C1/C2: Iskusni korisnik
Zajednički europski referentni okvir za jezike