Upravljanje kontinuitetom poslovanja kroz sigurnosno kopiranje poslužiteljskih računala - prikaz primjene Veeam tehnologije

Sabolić-Novaković, Damjan

VELEUČILIŠTE SUVREMENIH INFORMACIJSKIH TEHNOLOGIJA

STRUČNI PRIJEDIPLOMSKI STUDIJ INFORMACIJSKIH TEHNOLOGIJA

Damjan Sabolić-Novaković

ZAVRŠNI RAD

UPRAVLJANJE KONTINUITETOM POSLOVANJA KROZ SIGURNOSNO KOPIRANJE POSLUŽITELJSKIH RAČUNALA - PRIKAZ PRIMJENE VEEAM TEHNOLOGIJE

Zagreb, listopada 2024.

Veleučilište suvremenih informacijskih tehnologija
10000 Zagreb, Ulica Vjekoslava Klaića 7

Studij:	Stručni prijediplomski studij informacijskih tehnologija smjer računalni sustavi i mreže
Student:	**Damjan Sabolić-Novaković**
Matični broj:	2009151

Zadatak završnog rada

Predmet:	Arhitektura poslužiteljskih računala
Naslov:	**Upravljanje kontinuitetom poslovanja kroz sigurnosno kopiranje poslužiteljskih računala - prikaz primjene Veeam tehnologije**
Zadatak:	Rad istražuje primjenu sigurnosnog kopiranja poslužiteljskih računala u poslovnom okruženju s naglaskom na Veeam tehnologije. Naglašava važnost kontinuiteta poslovanja i potreba za pouzdanim rješenjima sigurnosnog kopiranja, različitih vrsta tehnologije, potrebe za njima i sl. Pregled tehnologije sigurnosnog kopiranja obuhvaća osnovne funkcionalnosti i mogućnosti te ujedno obrađuje različite vrste sigurnosnog kopiranja, njezine izrade, pohrane te kratki povijesni pregled. Definira funkcionalnosti Veeam rješenja i sigurnosnog kopiranja općenito te pruža uvid u performanse, pouzdanost i skalabilnost ovog rješenja. Kroz studije slučaja u radu u realnom okruženju istražuje se uspješna primjena Veeam tehnologije u stvarnim poslovnim scenarijima. Dodatno se ističe uloga Veeam tehnologije u budućnosti sigurnosnog kopiranja poslužiteljskih računala. Zaključak sažima ključne nalaze istraživanja i naglašava važnost tehnologije sigurnosnog kopiranja u osiguravanju kontinuiteta poslovanja u poslovnim okruženjima.
Mentor:	Dražen Novina, pred.
Zadatak uručen kandidatu:	1.2.2024.
Rok za predaju rada:	21.10.2024.
Rad predan:	_____

Povjerenstvo:

Saša Punčikar, pred.	član predsjednik	_____
Dražen Novina, pred.	mentor	_____
Dubravko Žižak, pred.	član	_____

SADRŽAJ

1 UVOD 5

2 TEORIJA SIGURNOSNOG KOPIRANJA 7
2.1 Uvod u sigurnosno kopiranje 7
2.1.1 Definicija i svrha sigurnosnog kopiranja 7
2.1.2 Značaj sigurnosnog kopiranja u modernom poslovanju 8
2.2 Osnovne vrste sigurnosnog kopiranja 9
2.2.1 Potpuno sigurnosno kopiranje (eng. *Full Backup*) 9
2.2.2 Inkrementalno sigurnosno kopiranje (eng. *Incremental Backup*) 10
2.2.3 Diferencijalno sigurnosno kopiranje (eng. *Differential Backup*) 10
2.3 Napredne tehnike sigurnosnog kopiranja 12
2.3.1 Zrcalno sigurnosno kopiranje (eng. *Mirror Backup*) 12
2.3.2 Kombinirano sigurnosno kopiranje (eng. *Combination Backup*) 13
2.3.3 Sintetičko sigurnosno kopiranje (eng. *Synthetic Backup*) 14
2.3.4 Neprekidno sigurnosno kopiranje (eng. *Continuous Data Protection*) 14

3 PRAVILA, STRATEGIJE I POSTUPANJA SIGURNOSNIM KOPIRANJEM (Napredne tehnike i primjena sigurnosnog kopiranja) 16
3.1 Integracija sigurnosnog kopiranja u poslovne procese 16
3.2 Pravila u sigurnosnom kopiranju 17
3.3 Definiranje ciljeva sigurnosnog kopiranja: 17
3.3.1 Procjena rizika i kritičnosti podataka i odabir odgovarajuće strategije 18
3.4 Planiranje i implementacija strategije sigurnosnog kopiranja 18
3.5 Sigurnost i izazovi sigurnosnog kopiranja 18
3.6 Točka oporavka i vrijeme oporavka (RTO i RPO) 20
3.7 Automatizacija i rasporedi sigurnosnog kopiranja: učinkovitost i pouzdanost 20
3.7.1 Automatizacija sigurnosnog kopiranja: 21
3.7.2 Pravljenje rasporeda sigurnosnog kopiranja 21
3.7.3 Kombinacija automatizacije i rasporeda: 21
3.8 Strategije i preporuke sigurnosnog kopiranja 21
3.9 Pravilo „3-2-1-1-0“ 22
3.9.1 Važnost pravila „3-2-1-1-0“ 23
3.9.2 Implementacija pravila „3-2-1-1-0“ 23

4 PRAKTIČNI RAD - PRIMJENA *VEEAM* TEHNOLOGIJE PRI STVARANJU I REPLICIRANJU SIGURNOSNE KOPIJE U STVARNOM POSLOVNOM OKRUŽENJU 24
4.1 Stvaranje zadatka sigurnosnog kopiranja 24
4.2 Oporavak podataka iz neke sigurnosne kopije 29
4.3 Replikacija sigurnosne kopije na udaljenu lokaciju 34

5 ZAKLJUČAK 37

LITERATURA 39

SAŽETAK 40

SUMMARY 41

POPIS SLIKA

Slika 1. Početni korak stvaranja nove sigurnosne kopije i zadavanja naziv 24
Slika 2. Odabir objekta nad kojim se vrši sigurnosno kopiranje 25
Slika 3. Odabir repozitorija za pohranu novog sigurnosnog kopiranja 25
Slika 4. Primjer konfiguracije čuvanja arhiva punih sigurnosnih kopija 26
Slika 5. Odabir sekundarne destinacije za pohranu 27
Slika 6. Prikaz odabrane opcije kopije sigurnosne kopije 27
Slika 7. Odabir dodatnih sigurnosnih opcija tijekom izrade nove sigurnosne kopije 27
Slika 8. Odabir optimalnih vremena za izradu automatiziranih sigurnosnih kopija 28
Slika 9. Prikaz dodatnih perioda za definiranje vremena izrade kopije 28
Slika 10. Odabir diska s kojeg se vrši oporavak 29
Slika 11. Odabir sistema iz kojeg se oporavljaju podaci 30
Slika 12. Odabir potrebnog razdoblja iz kojeg se datoteka oporavlja 30
Slika 13. Unošenje razloga povrata podataka iz sigurnosne kopije 31
Slika 14. Prikaz pretraživanja datoteka 32
Slika 15. Odabir dostupnih opcija mjesta gdje se podaci vraćaju 32
Slika 16. Prikaz potrebne autorizacije prethodne radnje 33
Slika 17. Vraćene mape dobivaju sufiks koji i vizualno označava da su obnovljene 33
Slika 18. Shema prikazuje veze lokalnog i udaljenog repozitorija 34
Slika 19. Izrada sigurnosne kopije na udaljenu lokaciju 35
Slika 20. Odabir željenog objekta 35
Slika 21. Odabir repozitorija i definiranje vremena izrade na udaljenoj lokaciji 36
Slika 22. Odabir načina prijenosa podataka (ovisi o licencama) 36

1 UVOD

U eri gdje su informacije nova valuta i gdje su podaci postali ključni pokretač uspjeha, upravljanje kontinuitetom poslovanja postaje, ne samo strateški imperativ već i, ključna komponenta korporativne otpornosti. U kontekstu neprestanih prijetnji podacima, od kibernetičkih napada do prirodnih katastrofa, sigurnosno kopiranje poslužiteljskih računala ne predstavlja samo tehničku potrebu, već i poslovnu mudrost. Tehnologija tvrtke *Veeam* kao predvodnik u industriji sigurnosnog kopiranja i oporavka, nudi sofisticirana rješenja koja poduzećima omogućuju da prevladaju izazove povezane s očuvanjem podataka i kontinuitetom poslovanja.

Ovaj rad istražuje kako tehnologija za sigurnosno kopiranje tvrtke *Veeam* transformira pejzaž sigurnosnog kopiranja poslužiteljskih računala, pružajući robusne, skalabilne i pouzdane metode zaštite ključnih podataka. S obzirom na sve veću kompleksnost informacijskih sustava, rad naglašava kako *Veeam*-ova inovativna rješenja adresiraju specifične potrebe modernih poduzeća, osiguravajući da njihovi podaci ostaju nedirnuti i dostupni čak i u najizazovnijim uvjetima.

Kroz prizmu najnovijih studija slučaja i empirijskih istraživanja, ovaj rad pruža uvid u stvarne prednosti koje takva tehnologija donosi organizacijama, ističući njezinu ulogu kao neizostavnog partnera u strategijama upravljanja rizicima i kontinuitetom poslovanja. Uzimajući u obzir trenutne trendove i buduće smjerove razvoja, rad razmatra što je u biti sigurnosno kopiranje, koje njegove vrste postoje te kako *Veeam* nastavlja oblikovati budućnost sigurnosnog kopiranja, postavljajući nove standarde u industriji i omogućujući poduzećima da se uspješno suočavaju s izazovima koji možda postoje.

Tema sigurnosnog kopiranja poslužiteljskih računala iznimno je važna jer predstavlja temelj zaštite podataka unutar svake organizacije. Ovaj rad pruža opis procesa sigurnosnog kopiranja kroz različite periode i u različitim uvjetima, istražuje tehnologije i metode koje se koriste u industriji, te potanko proučava, aktivno koristeći, *Veeam* tehnologiju kao jedno od vodećih rješenja dostupnih na tržištu.

Prikaz praktične primjene sigurnosnog kopiranja u svakodnevnom životu dodatno potvrđuje njegovu relevantnost. Od malih poduzeća do velikih korporacija, od obrazovnih institucija do zdravstvenih ustanova, svi se oslanjaju na pouzdane sustave za sigurnosno kopiranje kako bi osigurali spomenuti kontinuitet poslovanja i zaštitili svoje podatke od potencijalnih napada, tehničkih kvarova, prirodnih katastrofa, ali i naizgled jednostavnog – nespretnog rukovanja podacima ili povrata podataka uslijed kakvog nehotičnog manipuliranja.

U vremenu kada su podaci postali najvrjednija imovina mnogih organizacija, sigurnosno kopiranje više nije luksuz, već nužnost. Suvremene tehnologije sigurnosnog kopiranja, sa svojim inovativnim pristupom i naprednim funkcionalnostima, omogućuju poduzećima da se s pouzdanjem suoče s izazovima digitalnog doba. Budućnost sigurnosnog kopiranja je u stalnoj evoluciji, a kontinuirani razvoj i prilagodba novim tehnologijama osiguravaju da organizacije imaju pristup najsuvremenijim alatima za zaštitu svojih podataka i očuvanje kontinuiteta poslovanja. Ulaganje u pouzdana rješenja za sigurnosno kopiranje predstavlja ključan korak prema izgradnji otpornije budućnosti za svaku organizaciju.

Rad kroz konkretne primjere pokazuje kako se tehnologija sigurnosnog kopiranja primjenjuje u različitim scenarijima, čime se potvrđuje njezina neophodnost u modernom poslovnom okruženju.

Rad ujedno istražuje i ključne koncepte sigurnosnog kopiranja, uključujući različite tipologije poput potpunog (eng. *full*), inkrementalnog (eng. *incremental*) i diferencijalnog (eng. *differential*) načina, te njihove prednosti i nedostatke u različitim scenarijima upotrebe. Također je pozornost posvećena važnosti strategije oporavka od katastrofe i ulozi sigurnosnog kopiranja u osiguravanju kontinuiteta poslovanja čak i u najizazovnijim okolnostima, uzimajući u obzir ciljeve vremena oporavka (RTO) i ciljeve točke oporavka (RPO) s čime se rad ostalog, bavi u nastavku.

Kroz prizmu najnovijih tehnoloških dostignuća i najboljih praksi u industriji, ovaj rad pruža dubinski uvid u kompleksnost i važnost sigurnosnog kopiranja u današnjem digitalnom svijetu. Teoretizirano je kako organizacije mogu proaktivno pristupiti zaštiti od gubitka podataka, minimizirati vrijeme zastoja i osigurati nesmetan rad čak i u slučaju nepredviđenih događaja, čime se osigurava otpornost i kontinuitet poslovanja i ono najvažnije – odgovor na pitanje mogu li se datoteke uspješno obnoviti iz sigurnosnih kopija koje se potiho svakodnevno, samostalno, stvaraju u pozadini radnih procesa. Potonje je dokazano u praktičnom dijelu rada.

2 TEORIJA SIGURNOSNOG KOPIRANJA

2.1 Uvod u sigurnosno kopiranje

U kontekstu eksponencijalnog rasta volumena podataka i sveprisutne digitalne transformacije, sigurnosno kopiranje (eng. *Backup*) postaje ne samo preporučena praksa, već i esencijalna komponenta strategije upravljanja rizicima svake organizacije. Gubitak podataka, bilo uzrokovan hardverskim kvarovima, zlonamjernim softverom, prirodnim katastrofama ili ljudskim pogreškama, može imati katastrofalne posljedice, uključujući financijske gubitke, prekide poslovanja, narušavanje reputacije i gubitak povjerenja klijenata.

Sigurnosno kopiranje, u svojoj osnovi, predstavlja proces replikacije i pohrane podataka na sekundarnu lokaciju, koja može biti lokalna ili geografski odvojena, kao bi se osigurala njihova dostupnost i integritet u slučaju kompromitacije primarnog sustava. Ovaj proces obuhvaća širok spektar tehnologija i metodologija, od tradicionalnih metoda poput magnetskih vrpci do suvremenih rješenja temeljenih na oblaku, deduplikaciji[1] podataka i snimkama stanja (eng. *Snapshot*) tehnologijama.

2.1.1 Definicija i svrha sigurnosnog kopiranja

Sigurnosno kopiranje je proces dupliciranja i pohranjivanja podataka na sekundarnu lokaciju kako bi se osigurala njihova dostupnost u slučaju gubitka originalnih podataka iz raznih razloga. Ovaj proces uključuje stvaranje kopija važnih datoteka, baza podataka, konfiguracijskih datoteka i drugih kritičnih informacija, koje se zatim pohranjuju na različite medije kao što su vanjski diskovi, mrežni poslužitelji ili oblak.

Svrha sigurnosnog kopiranja je višestruka. Prvo i najvažnije, ono služi kao zaštita od gubitka podataka. U slučaju tehničkog kvara, poput prestanka rada ili oštećenja tvrdog diska, ili ljudske pogreške, poput slučajnog brisanja datoteka, sigurnosne kopije omogućuju brz i jednostavan oporavak izgubljenih podataka. Drugo, sigurnosno kopiranje pruža zaštitu od zlonamjernih napada, kao što su napadi ucjenjivačkog softvera (eng. *ransomware*), gdje napadači šifriraju podatke i zahtijevaju otkupninu za njihov povratak. Imati ažurirane sigurnosne kopije omogućuje korisnicima da obnove svoje sustave bez potrebe za plaćanjem otkupnine.

Osim toga, sigurnosno kopiranje je ključno za kontinuitet poslovanja. U slučaju katastrofalnih događaja, poput požara ili poplava, sigurnosne kopije pohranjene na udaljenim lokacijama

[1] Institut za hrvatski jezik i jezikoslovlje, Struna, http://struna.ihjj.hr/naziv/deduplikacija/53099/ (pristupljeno 25.6.2024.)

omogućuju tvrtkama da brzo obnove svoje operacije i minimiziraju prekide u radu. Također, sigurnosno kopiranje omogućuje povijesno arhiviranje podataka, što može biti korisno za pravne ili regulatorne svrhe.

Postoje različite metode sigurnosnog kopiranja, uključujući potpuno, inkrementalno i diferencijalno kopiranje, svaka sa svojim prednostima i izazovima. Učinkovita strategija sigurnosnog kopiranja uključuje redovito izvođenje kopija, automatizaciju procesa, šifriranje podataka i redovito testiranje sigurnosnih kopija kako bi se osigurala njihova ispravnost i dostupnost.

2.1.2 Značaj sigurnosnog kopiranja u modernom poslovanju

U današnjem digitalnom svijetu, sigurnosno kopiranje podataka nije samo tehnička stvar, već ključni dio svakog poslovanja. Bez obzira na to koliko je tvrtka velika ili u kojoj industriji posluje, podaci su srž svega što radimo. Gubitak podataka, a koji može nastati iz niza razloga– od tehničkih kvarova i ljudskih pogrešaka do zlonamjernih napada ili prirodnih katastrofa – može imati katastrofalne posljedice. Redovito sigurnosno kopiranje osigurava da se važni podaci mogu brzo vratiti, što smanjuje prekide u poslovanju.

Osim što štiti od gubitaka podataka, sigurnosno kopiranje je ključno za održavanje poslovanja. U slučaju neočekivanih događaja, poput kibernetičkih napada ili kvara sustava, sigurnosne kopije omogućuju tvrtkama da brzo nastave s radom. To je ključno za održavanje povjerenja klijenata i izbjegavanje financijskih gubitaka.

Važno je napomenuti da sigurnosno kopiranje nije samo pitanje tehnologije, već i pravno pitanje. Mnoge industrije imaju stroge propise koji zahtijevaju redovito sigurnosno kopiranje i čuvanje podataka. Nepoštivanje tih propisa može dovesti do visokih kazni i pravnih problema. Sigurnosno kopiranje pomaže tvrtkama da ostanu u skladu sa zakonima i standardima.

Osim pravne zaštite potrebna je, dakako, i zaštita od kibernetičkih (op.: eng.: Cyber) prijetnji. Kibernetički napadi, poput korištenja ucjenjivačkog softvera, mogu zaključati ili uništiti podatke. Imati ažurirane sigurnosne kopije omogućuje tvrtkama da povrate svoje podatke bez plaćanja otkupnine, čime se smanjuje utjecaj takvih napada.

Na kraju, ali ne manje važno, sigurnosno kopiranje podataka je ključno za izgradnju povjerenja s klijentima. Klijenti očekuju da njihovi podaci budu sigurni i zaštićeni. Tvrtke koje mogu pokazati da imaju učinkovite mjere sigurnosnog kopiranja i oporavka podataka povećavaju povjerenje svojih klijenata, što može biti velika prednost.

2.2 Osnovne vrste sigurnosnog kopiranja

2.2.1 Potpuno sigurnosno kopiranje (eng. *Full Backup*)

Potpuno sigurnosno kopiranje predstavlja proces stvaranja kompletne kopije svih odabranih podataka u određenom trenutku. Ova kopija sadrži sve datoteke, aplikacije, konfiguracijske postavke i ostale relevantne informacije, bez obzira na to jesu li se promijenile od posljednjeg sigurnosnog kopiranja ili ne. Potpuno sigurnosno kopiranje odlikuje se sveobuhvatnošću, pružajući najopsežniju zaštitu podataka kroz replikaciju cjelokupnog odabranog skupa. Ovaj pristup rezultira iznimnom jednostavnošću oporavka, jer se svi potrebni podaci nalaze u jednoj, lako dostupnoj kopiji. Međutim, treba uzeti u obzir da potpuno sigurnosno kopiranje ima veće zahtjeve za prostorom za pohranu u usporedbi s drugim metodama, poput inkrementalnog ili diferencijalnog kopiranja. Nadalje, zbog kopiranja svih podataka, vrijeme izvršavanja može biti dulje u odnosu na druge strategije sigurnosnog kopiranja.

Potpuno sigurnosno kopiranje nudi brojne prednosti, ali i neke izazove. Prednosti potpunog sigurnosnog kopiranja uključuju jednostavan i brz oporavak, potpunu zaštitu podataka, pouzdanost i jednostavnost upravljanja.
Jednostavan i brz oporavak omogućava da su svi podaci dostupni u jednoj kopiji u slučaju gubitka ili oštećenja podataka. Time su podaci ujedno potpuno zaštićeni jer se kopira cjelokupni skup podataka, pružajući najvišu razinu sigurnosti i zaštite od gubitka informacija.
Takvim načinom izrade je dobivena i pouzdanost smanjujući tako rizik od pogrešaka tijekom oporavka, jer ne ovisi o lancu prethodnih sigurnosnih kopija. Ovakav je proces jednostavan za razumijevanje i implementaciju, što ga čini pogodnim za različite korisnike i organizacije.

S druge pak strane, prethodno spomenuti, izazovi vidljivi su kroz nekoliko aspekata, kao što su veliki zahtjevi za prostorom za pohranu, dugo vrijeme izvršavanja, veće opterećenje mreže i manja učestalost sigurnosnog kopiranja. U ovakvom načinu izrade sigurnosne kopije potrebno je znatno više prostora za pohranu u usporedbi s drugim metodama sigurnosnog kopiranja.
Uz znatnu količinu prostora potrebno je i duže vrijeme izvršavanja kako bi se takav prostor zapunio. Kopiranje svih podataka može potrajati dugo, posebno kod velikih količina podataka, što može utjecati na performanse sustava tijekom izvođenja sigurnosne kopije. Prijenos velikih količina podataka može opteretiti mrežnu infrastrukturu, posebno ako se sigurnosne kopije pohranjuju na udaljenoj lokaciji.
Zbog svega navedenog, zbog vremena i resursa potrebnih za potpuno sigurnosno kopiranje,

obično se ova vrsta sigurnosnog kopiranja izvodi rjeđe od drugih metoda, što može povećati rizik od gubitka podataka u slučaju incidenta između dvije sigurnosne kopije.

2.2.2 Inkrementalno sigurnosno kopiranje (eng. *Incremental Backup*)

Inkrementalno sigurnosno kopiranje predstavlja strategiju gdje se pri svakom novom ciklusu sigurnosnog kopiranja pohranjuju samo podaci koji su se promijenili od posljednjeg sigurnosnog kopiranja, bez obzira na to je li ono bilo potpuno ili inkrementalno. Ovaj pristup se temelji na ideji da se većina podataka unutar sustava ne mijenja često, što omogućuje značajne uštede u prostoru za pohranu i vremenu potrebnom za izvođenje sigurnosne kopije. Ključne karakteristike ovakvog načina izrade sigurnosne kopije podataka su učinkovitost, brzina, fleksibilnost. Inkrementalno sigurnosno kopiranje ističe se svojom učinkovitošću, jer kopira samo promjene podataka, što rezultira manjim sigurnosnim kopijama i bržim izvršavanjem. Ova fleksibilnost omogućuje češće sigurnosne kopije, smanjujući rizik od gubitka podataka između ciklusa.

Inkrementalno sigurnosno kopiranje ima nekoliko prednosti, a učinkovito korištenje prostora, brzo izvođenje i mogućnost češćih sigurnosnih kopija su neke od njih. Inkrementalne kopije zauzimaju manje prostora jer pohranjuju samo promjene od posljednje sigurnosne kopije, što je idealno za okruženja s ograničenim kapacitetom pohrane. Budući da se prenose samo izmijenjeni podaci, inkrementalne kopije se izvode brže od potpunih, čime se štedi vrijeme i resursi. Zbog svoje brzine i učinkovitosti, inkrementalne kopije omogućuju češće sigurnosno kopiranje, smanjujući rizik od gubitka podataka u slučaju incidenta.
Unatoč spomenutim prednostima, složenost oporavka i ovisnost o integritetu lanca sigurnosnih kopija, pokazuju da postoje i neki nedostatci ovakvog načina sigurnosnog kopiranja i oporavka. Oporavak podataka zahtijeva vraćanje posljednje potpune sigurnosne kopije i svih naknadnih inkrementalnih kopija, što može biti vremenski zahtjevno i složenije.
Ako je bilo koja od inkrementalnih kopija u lancu oštećena ili nedostupna, oporavak podataka može biti nepotpun ili nemoguć, zbog ovisnosti o integritetu cjelokupnog lanca.

2.2.3 Diferencijalno sigurnosno kopiranje (eng. *Differential Backup*)

Diferencijalno sigurnosno kopiranje predstavlja strategiju gdje se pri svakom novom ciklusu sigurnosnog kopiranja pohranjuju samo podaci koji su se promijenili od posljednjeg potpunog sigurnosnog kopiranja. Za razliku od inkrementalnog pristupa, gdje se svaka nova kopija temelji na prethodnoj, diferencijalno kopiranje uvijek referencira posljednju potpunu kopiju. Učinkovitost diferencijalnog sigurnosnog kopiranja je da je učinkovitije od potpunog kopiranja

jer se ne kopiraju svi podaci svaki put, ali je manje učinkovito od inkrementalnog jer se s vremenom povećava količina podataka za kopiranje.
Iako je ovakav način kopiranja brži od potpunog sigurnosnog kopiranja, sporije je od inkrementalnog, jer se količina podataka za kopiranje povećava s vremenom od posljednjeg potpunog sigurnosnog kopiranja. Oporavak podataka u slučaju kakva nemila događaja, zahtijeva samo posljednju potpunu kopiju i posljednju diferencijalnu kopiju, što je jednostavnije i brže od oporavka kod inkrementalnog kopiranja. Za razliku od inkrementalnog kopiranja, oporavak ne ovisi o nizu međusobno povezanih kopija, što smanjuje rizik od neuspjelog oporavka zbog oštećenja jedne od kopija u lancu čime ovakav način sigurnosnog kopiranja pokazuje manju ovisnost o lancu sigurnosnih kopija.
Diferencijalno sigurnosno kopiranje je posebno korisno kada je tražena ravnoteža između učinkovitosti i jednostavnosti oporavka podataka. Ova metoda je idealna u situacijama kada se podaci mijenjaju umjerenom brzinom, jer nudi brže sigurnosno kopiranje od potpunog, ali i jednostavniji oporavak od inkrementalnog. U slučajevima gdje je pouzdanost oporavka od ključne važnosti, diferencijalno kopiranje se ističe zbog svoje manje ovisnosti o lancu sigurnosnih kopija, čime se smanjuje rizik od neuspjelog oporavka. Međutim, ako se podaci mijenjaju vrlo brzo, diferencijalne kopije mogu postati prevelike i dugotrajne za izvođenje, što može utjecati na učinkovitost ovog pristupa.

Prednosti diferencijalnog sigurnosnog kopiranja su učinkovitije korištenje prostora za pohranu od potpunog kopiranja, jednostavniji i brži oporavak od inkrementalnog kopiranja i manja ovisnost o lancu sigurnosnih kopija. Diferencijalno kopiranje pohranjuje samo promjene od posljednje potpune kopije podataka, što rezultira manjim sigurnosnim kopijama i optimiziranim korištenjem prostora za pohranu, posebno u usporedbi s potpunim kopiranjem koje uvijek stvara potpuno novu kopiju svih podataka. Za oporavak podataka potrebna je samo posljednja diferencijalna kopija, što značajno ubrzava proces u usporedbi s inkrementalnim kopiranjem gdje je potrebno primijeniti sve inkrementalne kopije od posljednjeg potpunog sigurnosnog kopiranja. Za razliku od inkrementalnog kopiranja, diferencijalno kopiranje nije toliko osjetljivo na oštećenja ili gubitak pojedinačnih kopija u lancu, što povećava pouzdanost oporavka podataka.

Unatoč navedenim prednostima, diferencijalno sigurnosno kopiranje ima, naravno, i svoje nedostatke. Manje je učinkovito od inkrementalnog kopiranja u smislu korištenja prostora i brzine izvođenja. Kako vrijeme prolazi od posljednjeg potpunog sigurnosnog kopiranja,

diferencijalne kopije postaju sve veće jer uključuju sve promjene od tog trenutka. To može dovesti do sporijih sigurnosnih kopija i veće potrošnje prostora za pohranu u usporedbi s inkrementalnim kopiranjem, koje pohranjuje samo promjene od posljednjeg kopiranja (bilo potpunog ili inkrementalnog). Kako bi se spriječilo da diferencijalne kopije postanu prevelike i dugotrajne, potrebno je redovito izvoditi potpune sigurnosne kopije. To može zahtijevati dodatne resurse i vrijeme u usporedbi s inkrementalnim kopiranjem, gdje potpune kopije nisu toliko česte.

2.3 Napredne tehnike sigurnosnog kopiranja

2.3.1 Zrcalno sigurnosno kopiranje (eng. *Mirror Backup*)

Zrcalno sigurnosno kopiranje predstavlja strategiju gdje se stvara točna kopija izvornih podataka na drugoj lokaciji, obično u stvarnom vremenu ili s minimalnim kašnjenjem. Ova kopija, često nazivana i "zrcalna slika", u svakom trenutku odražava stanje izvornih podataka, pružajući najbrži mogući oporavak u slučaju incidenta. Zrcalna kopija je uvijek ažurna i sinkronizirana s izvornim podacima, što omogućuje trenutni oporavak u slučaju gubitka ili oštećenja originala. U slučaju kvara primarnog sustava, zrcalna kopija može odmah preuzeti ulogu produkcijskog sustava, minimizirajući vrijeme zastoja i osiguravajući kontinuitet poslovanja. Ovakav način izrade sigurnosne kopije obično zahtijeva minimalnu konfiguraciju i održavanje, što pojednostavljuje proces sigurnosnog kopiranja. Budući da se stvara potpuna kopija podataka, zrcalno kopiranje zahtijeva jednaku količinu prostora za pohranu kao i izvorni podaci. Održavajući samo trenutno stanje podataka znači da se u slučaju potrebe za oporavkom starije verzije datoteke moraju koristiti druge metode sigurnosnog kopiranja. Ako se izvorni podaci, pak, oštete ili zaraze zlonamjernim softverom, te promjene se odmah repliciraju na zrcalnu kopiju, što može ugroziti integritet sigurnosne kopije.
Zrcalno sigurnosno kopiranje predviđeno je za sustave gdje je vrijeme zastoja neprihvatljivo i brzi oporavak od ključne važnosti, jer pruža najbrži način vraćanja u funkciju. Također se često koristi za osiguravanje visoke dostupnosti aplikacija, gdje se u slučaju kvara jednog sustava automatski prebacuje na zrcalnu kopiju. Ova funkcija je korisna i za baze podataka koje se često ažuriraju, osiguravajući tako uvijek dostupne najnovije informacije.

Prednosti zrcalnog sigurnosnog kopiranja su najbrži mogući oporavak podataka, minimalno vrijeme zastoja i jednostavnost upravljanja
Nedostaci zrcalnog sigurnosnog kopiranja su vidljivi kroz velike zahtjeve za prostorom za pohranu, ograničenu zaštitu od povijesnih podataka i osjetljivost na greške i napade.

Zrcalno sigurnosno kopiranje predstavlja moćan alat za osiguravanje kontinuiteta poslovanja i brzog oporavka kritičnih sustava. Iako ima određene nedostatke, njegova sposobnost da pruži trenutnu repliku podataka čini ga nezamjenjivim u situacijama gdje je brzina oporavka od najveće važnosti.

2.3.2 Kombinirano sigurnosno kopiranje (eng. *Combination Backup*)

Kombinirano sigurnosno kopiranje, kako mu i samo ime govori, predstavlja strategiju koja kombinira različite metode sigurnosnog kopiranja, poput potpunog, inkrementalnog i diferencijalnog, kako bi se postigla optimalna ravnoteža između učinkovitosti, brzine i pouzdanosti. Ovaj pristup omogućuje organizacijama da prilagode svoju strategiju sigurnosnog kopiranja specifičnim potrebama različitih vrsta podataka i aplikacija.
Kombinirano sigurnosno kopiranje omogućuje organizacijama da odaberu najbolju kombinaciju metoda za različite vrste podataka i aplikacija, uzimajući u obzir njihovu kritičnost, učestalost promjena i zahtjeve za oporavkom.
Kroz kombiniranje različitih metoda, moguće je optimizirati korištenje prostora za pohranu, vrijeme izvršavanja sigurnosnih kopija i brzinu oporavka podataka. Implementacija i upravljanje kombiniranim sigurnosnim kopiranjem mogu biti složeniji od korištenja samo jedne metode, jer zahtijeva pažljivo planiranje i koordinaciju različitih vrsta sigurnosnih kopija.
Kombinirano sigurnosno kopiranje koristi se u okruženjima s različitim vrstama podataka i aplikacija jer omogućuje prilagodbu strategije specifičnim potrebama svakog sustava. Kombiniranjem različitih metoda, moguće je osigurati brzi oporavak kritičnih podataka, dok se za manje važne podatke mogu koristiti metode koje su učinkovitije u pogledu prostora za pohranu. Kombinirano sigurnosno kopiranje omogućuje pronalaženje optimalnog balansa između učinkovitosti, brzine i pouzdanosti, ovisno o specifičnim potrebama organizacije.

Prednosti kombiniranog sigurnosnog kopiranja su fleksibilnost u prilagodbi strategije sigurnosnog kopiranja, optimizacija korištenja resursa i vremena te mogućnost postizanja ravnoteže između učinkovitosti, brzine i pouzdanosti.
Nedostaci kombiniranog sigurnosnog kopiranja su složenija implementacija i upravljanje te potreba za pažljivim planiranjem i koordinacijom.

Kombinirano sigurnosno kopiranje predstavlja svestran i prilagodljiv pristup zaštiti podataka, omogućavajući organizacijama da iskoriste prednosti različitih metoda sigurnosnog kopiranja i prilagode ih svojim specifičnim potrebama. Iako zahtijeva dodatno planiranje i upravljanje, ova

strategija pruža optimalnu ravnotežu između učinkovitosti, brzine i pouzdanosti, osiguravajući da su podaci zaštićeni i dostupni u svakom trenutku.

2.3.3 Sintetičko sigurnosno kopiranje (eng. *Synthetic Backup*)

Sintetičko sigurnosno kopiranje predstavlja naprednu strategiju koja koristi postojeće sigurnosne kopije, poput potpunih i inkrementalnih, za stvaranje novih, virtualnih potpunih sigurnosnih kopija bez potrebe za ponovnim kopiranjem svih podataka s izvornog sustava. Ovaj pristup omogućuje značajne uštede u prostoru za pohranu, vremenu i resursima, posebno u okruženjima s velikim količinama podataka.
Sintetičko sigurnosno kopiranje eliminira potrebu za čestim potpunim sigurnosnim kopiranjem, što smanjuje opterećenje sustava, mreže i prostora za pohranu. Stvaranje sintetičkih kopija je znatno brže od izvođenja potpunog sigurnosnog kopiranja, jer se podaci ne prenose s izvornog sustava. Kopije podataka stvorene ovom metodom mogu se stvarati na zahtjev ili prema unaprijed definiranom rasporedu, pružajući veću fleksibilnost u upravljanju sigurnosnim kopijama. Implementacija i upravljanje može biti složenije od tradicionalnih metoda, jer zahtijeva specijalizirani softver i pažljivo planiranje. Ovakvo kopiranje je idealno za okruženja s velikim količinama podataka, gdje bi često potpuno sigurnosno kopiranje bilo previše zahtjevno u pogledu vremena i resursa.
Sintetičko kopiranje smanjuje opterećenje jer se podaci ne prenose s izvornog sustava, a kopije se mogu stvarati na zahtjev, što omogućuje brzi pristup podacima u slučaju potrebe. Sintetičke se kopije temelje na postojećim potpunim i inkrementalnim sigurnosnim kopijama, što znači da njihova pouzdanost ovisi o integritetu tih kopija.

Prednosti sintetičkog sigurnosnog kopiranja su učinkovito korištenje prostora za pohranu, brzo stvaranje sigurnosnih kopija te veća fleksibilnost u upravljanju sigurnosnim kopijama.
Kao nedostatke je moguće istaknuti složeniju implementaciju i upravljanje te ovisnost o integritetu postojećih sigurnosnih kopija.

Sintetičko sigurnosno kopiranje predstavlja inovativni pristup zaštiti podataka koji omogućuje organizacijama da učinkovito upravljaju velikim količinama podataka i smanje opterećenje sustava. Iako zahtijeva specijalizirani softver i pažljivo planiranje, njegove prednosti u pogledu učinkovitosti, brzine i fleksibilnosti čine ga vrijednim alatom za moderna IT okruženja.

2.3.4 Neprekidno sigurnosno kopiranje (eng. *Continuous Data Protection*)

Neprekidno sigurnosno kopiranje podataka predstavlja najnapredniju strategiju sigurnosnog

kopiranja koja omogućuje kontinuirano praćenje i snimanje svih promjena podataka u stvarnom vremenu. Za razliku od tradicionalnih metoda koje se izvode u određenim intervalima, ova metoda osigurava da je svaka promjena podataka, čak i najmanja, odmah zaštićena i dostupna za oporavak. Neprekidno sigurnosno kopiranje kontinuirano prati i bilježi sve promjene čim se dogode, pružajući najvišu razinu zaštite od gubitka podataka. To znači da u slučaju incidenta, može vratiti stanje na bilo koju točku u vremenu, čak i nekoliko sekundi prije nego što se problem dogodio, čime se minimiziraju gubitci. Ovo je posebno važno za kritične sustave gdje je svaka sekunda važna. Oporavak podataka je izuzetno brz, jer se ne moraju primjenjivati nikakve dodatne sigurnosne kopije. To omogućuje minimalno vrijeme zastoja i brzi povratak u operativno stanje.

Prednosti neprekidnog sigurnosnog kopiranja koje valja posebno izdvojiti su neprekidna zaštita, minimalni gubitak podataka i brzi oporavak. Omogućuje najvišu razinu zaštite podataka, osiguravajući da se svaka promjena odmah replicira i zaštiti. Oporavak podataka moguć je na bilo koju točku u vremenu, čak i na nekoliko sekundi prije incidenta, a vrijeme oporavka je gotovo trenutno, što minimizira vrijeme zastoja i potencijalne gubitke.
Neki od nedostataka neprekidnog sigurnosnog kopiranja su visoki zahtjevi za resursima i složenost implementacije i upravljanja. Ovakav način izrade sigurnosnih kopija zahtijeva značajne resurse u pogledu procesorske snage, memorije i prostora za pohranu, jer se sve promjene podataka moraju kontinuirano pratiti i bilježiti. To može biti izazov za organizacije s ograničenim resursima. Implementacija i upravljanje ovakvim rješenjima mogu biti složeniji od tradicionalnih metoda sigurnosnog kopiranja, jer zahtijevaju specijalizirani softver i stručnost. To može zahtijevati dodatna ulaganja u obuku i podršku.

Neprekidno sigurnosno kopiranje je idealno za sustave i aplikacije gdje je čak i najmanji gubitak podataka neprihvatljiv, poput financijskih transakcija, medicinskih podataka ili sustava za kontrolu industrijskih procesa. Okruženja s visokim zahtjevima za dostupnošću, koja zahtijevaju da su podaci uvijek dostupni i ažurni, a što je ključno za aplikacije koje zahtijevaju kontinuirani rad bez prekida, također su još jedno mjesto gdje neprekidni sustav kopiranja može pružiti svoj potencijal.

3 PRAVILA, STRATEGIJE I POSTUPANJA SIGURNOSNIM KOPIRANJEM (NAPREDNE TEHNIKE I PRIMJENA SIGURNOSNOG KOPIRANJA)

3.1 Integracija sigurnosnog kopiranja u poslovne procese

Sigurnosno kopiranje nije samo tehnički zadatak koji se izvodi u pozadini. Ono ima dubok utjecaj na poslovne procese, donošenje odluka i cjelokupnu strategiju upravljanja rizicima unutar organizacije. U današnjem digitalnom dobu, pouzdano sigurnosno kopiranje omogućuje organizacijama da donose informirane odluke, minimiziraju rizike i osiguraju kontinuitet poslovanja čak i u najizazovnijim situacijama. Utjecaj sigurnosnog kopiranja na poslovne odluke je velik i nastavlja rasti. Znajući da su podaci sigurno zaštićeni, menadžment može donositi odluke s većim samopouzdanjem, bez straha od gubitka ključnih informacija. Sposobnost brzog oporavka podataka omogućuje organizacijama da budu inovativnije i eksperimentiraju s novim idejama, znajući da imaju sigurnosnu mrežu u slučaju neuspjeha.
Pouzdano sigurnosno kopiranje omogućuje organizacijama da se šire na nova tržišta i uvode nove proizvode i usluge, bez straha od gubitka podataka ili prekida poslovanja. Mnoge industrije imaju stroge propise o čuvanju i zaštiti podataka. Sigurnosno kopiranje pomaže organizacijama da ispune te zahtjeve i izbjegnu potencijalne kazne.

Sigurnosno kopiranje je prva linija obrane od gubitka podataka uzrokovanog hardverskim kvarovima, kibernetičkim napadima, prirodnim katastrofama ili ljudskim pogreškama. U slučaju incidenta, sigurnosno kopiranje omogućuje brzi oporavak podataka i minimizira vrijeme zastoja, čime se smanjuju financijski gubici i utjecaj na reputaciju. Kopije koje su pohranjene izvan mreže ili su nepromjenjive pružaju zaštitu od ucjenjivačkog softvera napada, jer napadači ne mogu šifrirati ili izbrisati te kopije. Ovakav pouzdani proces omogućuje organizacijama da nastave s radom čak i u slučaju katastrofe, čime se osigurava kontinuitet poslovanja i zadovoljstvo kupaca.

Integracija sigurnosnog kopiranja u poslovne procese ključna je za donošenje informiranih odluka, smanjenje rizika i osiguravanje dugoročnog uspjeha organizacije. Ulaganje u pouzdano rješenje za sigurnosno kopiranje nije samo tehnička potreba, već i strateška investicija koja se višestruko isplati kroz povećanu otpornost, agilnost i konkurentnost na tržištu.

3.2 Pravila u sigurnosnom kopiranju

Pravila u sigurnosnom kopiranju su ključna za osiguravanje učinkovite zaštite podataka i minimiziranje rizika od gubitka informacija. Nekoliko najvažnijih pravila su redovitost, pohrana na različite medije, pohrana na udaljenoj lokaciji, nepromjenjivost, testiranje oporavka te dokumentiranje i praćenje.

Redovito sigurnosno kopiranje osigurava da su kopije podataka ažurne i da možete oporaviti podatke do najnovije moguće točke u vremenu. Pohranjivanje sigurnosnih kopija na različite medije (npr. tvrdi disk, magnetska vrpca, cloud) smanjuje rizik od gubitka svih kopija u slučaju kvara jednog medija. Čuvanje barem jedne kopije podataka na udaljenoj lokaciji štiti od lokalnih katastrofa poput požara, poplave ili krađe. Korištenje nepromjenjivih kopija ili kopija koje su fizički odvojene od mreže (eng. *air-gapped*) sprječava zlonamjerni softver da izbriše ili šifrira sigurnosne kopije. Redovito testiranje procesa oporavka osigurava da su sigurnosne kopije ispravne i da je moguće brzo vratiti i podatke u slučaju potrebe. Vođenje detaljne dokumentacije o strategiji sigurnosnog kopiranja i redovito praćenje njenog izvršavanja omogućuje vam da identificirate potencijalne probleme i unaprijedite proces.

Ova pravila su temelj svake uspješne strategije sigurnosnog kopiranja. Pridržavajući se ovih pravila, organizacije mogu značajno smanjiti rizik od gubitka podataka i osigurati kontinuitet poslovanja čak i u najizazovnijim situacijama.

3.3 Definiranje ciljeva sigurnosnog kopiranja:

Definiranje ciljeva sigurnosnog kopiranja predstavlja ključni korak u izgradnji učinkovite strategije zaštite podataka. Bez jasno definiranih ciljeva, organizacije riskiraju neučinkovito korištenje resursa, nepotpunu zaštitu podataka i poteškoće u oporavku u slučaju incidenta.

Potrebno je identificirati kritične podatke za poslovanje, uključujući baze podataka, aplikacije, konfiguracijske datoteke i druge važne informacije. Učestalost sigurnosnog kopiranja ovisi o vrsti podataka i njihovoj važnosti za poslovanje. Kritični podaci koji se često mijenjaju zahtijevaju češće sigurnosno kopiranje. Realna procjena raspoloživih resursa također je bitna u odabiru rješenja za sigurnosno kopiranje koje se uklapa u neki budžet. Vrijeme oporavka (eng. *Recovery Time Objective* - RTO) definira maksimalno prihvatljivo vrijeme zastoja u slučaju incidenta. Što je RTO kraći, to je potrebna brža i pouzdanija strategija oporavka. Točka oporavka (eng. *Recovery Point Objective* – RPO) definira maksimalnu količinu podataka koju je korisnik spreman izgubiti u slučaju incidenta. Što je RPO manji, to je potrebno češće sigurnosno kopiranje.

Jasni definirani ciljevi omogućuju usmjeravanje resursa na najkritičnije podatke i izbjegavanje nepotrebnog trošenja na manje važne informacije. Definirati RTO i RPO pomaže u odabiru strategije sigurnosnog kopiranja koja omogućava brzi oporavak podataka u slučaju incidenta.
U mnogim industrijama postoje propisi o čuvanju i zaštiti podataka. Jasno definirani ciljevi sigurnosnog kopiranja pomažu u ostvarenju pravilnog sigurnosnog kopiranja.
Vizija omogućuje praćenje i mjerenje uspješnosti strategije sigurnosnog kopiranja te daje mogućnost prilagođavanja prema potrebi.

3.3.1 Procjena rizika i kritičnosti podataka i odabir odgovarajuće strategije

Po postavljenim ciljevima sljedeće je identificirati i procijeniti potencijalne rizike koji mogu ugroziti podatke, poput hardverskih kvarova, kibernetičkih napada, prirodnih katastrofa ili ljudskih pogrešaka. Također je važno procijeniti kritičnost različitih vrsta podataka za poslovanje, kao na primjer koji su podaci ključni za svakodnevne operacije, a koji su manje važni. Ova procjena pomaže odrediti prioritete i usmjeriti resurse na najkritičnije podatke.

3.4 Planiranje i implementacija strategije sigurnosnog kopiranja

Planiranje sigurnosnog kopiranja nije jednokratan zadatak, već kontinuirani proces koji se mora redovito preispitivati i prilagođavati promjenama u poslovnom okruženju i tehnologiji. Ulaganje vremena i resursa u ovu fazu ključno je za izgradnju robusne strategije koja osigurava zaštitu podataka i kontinuitet poslovanja u slučaju nepredviđenih događaja.

3.5 Sigurnost i izazovi sigurnosnog kopiranja

Sigurnosno kopiranje, iako ključno za zaštitu podataka, samo po sebi ne garantira potpunu sigurnost. U današnjem digitalnom dobu, gdje su kibernetički napadi sve sofisticiraniji i učestaliji, organizacije se suočavaju s brojnim izazovima u osiguravanju integriteta i povjerljivosti svojih sigurnosnih kopija.

Sigurnosni aspekti sigurnosnog kopiranja obuhvaćaju zaštitu od neovlaštenog pristupa, zaštitu od zlonamjernog softvera i integritet podataka. Sigurnosne kopije moraju biti zaštićene od neovlaštenog pristupa, kako fizičkog tako i logičkog. To uključuje kontrolu pristupa fizičkim medijima za pohranu, kao i implementaciju sigurnosnih mjera poput jakih lozinki, autentifikacije s više faktora i šifriranja podataka. Sigurnosne kopije mogu biti meta ucjenjivačkog softvera i drugih vrsta zlonamjernog softvera. Korištenje nepromjenjivih kopija ili kopija koje su fizički odvojene od mreže može pomoći u zaštiti od ovih prijetnji. Važno je osigurati da nisu oštećene ili izmijenjene. Redovito testiranje i provjera integriteta podataka

ključni su za održavanje pouzdanosti sigurnosnih kopija.

Izazovi u sigurnosnom kopiranju su brojni, a tek neki od njih se javljaju u vidu kibernetičkih napada, ljudskih grešaka, hardverskih kvarova ili prirodne katastrofe. Ucjenjivački softver, napadi uskraćivanja usluge (*DDoS*[2]) i drugi oblici kibernetičkih napada mogu ugroziti sigurnost sigurnosnih kopija. Slučajno brisanje datoteka, pogrešne konfiguracije ili nepažljivo rukovanje sigurnosnim kopijama mogu dovesti do gubitka podataka. Kvarovi diskova, servera ili drugih komponenti infrastrukture za sigurnosno kopiranje mogu dovesti do nedostupnosti podataka. Požari, poplave ili druge prirodne katastrofe mogu uništiti sigurnosne kopije koje se čuvaju na istoj lokaciji kao i izvorni podaci.

Šifriranje, kontrola pristupa, geografska distribucija kopija i druge ideje daju zadovoljavajuće rezultate u nezaustavljivom pronalaženju adekvatnog osiguranja sigurnosnih kopija. Šifriranje podataka u sigurnosnim kopijama štiti ih od neovlaštenog pristupa, čak i ako fizički mediji za pohranu budu ukradeni ili izgubljeni. Implementacija stroge kontrole pristupa sigurnosnim kopijama osigurava da samo ovlaštene osobe imaju pristup podacima. Korištenje nepromjenjivih kopija ili kopija koje su fizički odvojene od mreže sprječava zlonamjerni softver da ih izmijeni ili izbriše. Redovito testiranje procesa oporavka i provjera integriteta podataka osiguravaju da su sigurnosne kopije ispravne i spremne za upotrebu u slučaju incidenta. Pohranjivanje sigurnosnih kopija na različitim geografskim lokacijama smanjuje rizik od gubitka svih kopija u slučaju lokalne katastrofe. Implementacija politika za upravljanje životnim ciklusom podataka osigurava da se sigurnosne kopije čuvaju samo onoliko dugo koliko je potrebno, čime se optimizira korištenje prostora za pohranu.

Šifriranje podataka i kontrola pristupa ključni su elementi sigurnosti sigurnosnog kopiranja. Organizacije moraju pažljivo upravljati ključevima za šifriranje i osigurati da samo ovlaštene osobe imaju pristup tim ključevima i sigurnosnim kopijama. Također je važno redovito preispitivati i ažurirati politike pristupa kako bi se osiguralo da su u skladu s promjenama u poslovnim potrebama i sigurnosnim rizicima.
U konačnici, sigurnost sigurnosnog kopiranja zahtijeva socijalno osviješten pristup koji uključuje kombinaciju tehničkih mjera, organizacijskih politika i kontinuirane edukacije

[2] DDoS je napad uskraćivanja usluga. Napad je specifičan po generiranju pozamašne količine mrežnog prometa u svrhu zasićenja resursa mreže i poslužitelja.

zaposlenika. Kroz implementaciju najboljih praksi i korištenje naprednih tehnologija, organizacije mogu osigurati da njihovi podaci ostaju sigurni i dostupni čak i u najizazovnijim okolnostima.

3.6 Točka oporavka i vrijeme oporavka (RTO i RPO)

Vrijeme oporavka *(eng. Recovery Time Objective* (RTO)) i točka oporavka (eng. *Recovery Point Objective* (RPO)) su dva ključna parametra u planiranju oporavka od katastrofe i sigurnosnog kopiranja podataka. Oni definiraju koliko brzo i do koje točke u vremenu organizacija treba moći oporaviti svoje podatke nakon incidenta.

Vrijeme oporavka predstavlja maksimalno prihvatljivo vrijeme zastoja sustava ili aplikacije nakon incidenta, unutar kojeg se podaci moraju oporaviti i sustav vratiti u funkciju. Drugim riječima, RTO definira koliko dugo organizacija može tolerirati prekid poslovanja prije nego što to počne imati ozbiljne posljedice.

Točka oporavka predstavlja maksimalnu količinu podataka koju organizacija može prihvatiti izgubiti u slučaju incidenta. To je vremenski interval između posljednjeg uspješnog sigurnosnog kopiranja i trenutka incidenta. Što je RPO manji, to je manji potencijalni gubitak podataka.

Primjer:

- Ako organizacija ima RTO od 4 sata, to znači da mora moći oporaviti svoje podatke i vratiti sustav u funkciju unutar 4 sata od trenutka incidenta.
- Ako organizacija ima RPO od 1 sata, to znači da je spremna prihvatiti gubitak podataka koji su nastali unutar posljednjeg sata prije incidenta.

Definiranje vremena oporavka i točke oporavka ključno je za odabir odgovarajuće strategije sigurnosnog kopiranja i planiranje oporavka od katastrofe. Organizacije moraju pažljivo procijeniti kritičnost svojih sustava i podataka te odrediti prihvatljive razine rizika kako bi postavile realne ciljeve vremena i točaka oporavka. Što su ti ciljevi stroži (npr. kraći RTO i manji RPO), to su potrebna sofisticiranija i skuplja rješenja za sigurnosno kopiranje i oporavak.

3.7 Automatizacija i rasporedi sigurnosnog kopiranja: učinkovitost i pouzdanost

U svijetu gdje se količina podataka neprestano povećava, a kibernetičke prijetnje postaju sve sofisticiranije, ručno upravljanje sigurnosnim kopiranjem više nije održivo. Automatizacija i pravilno definiranje rasporeda sigurnosnog kopiranja postaju ključni elementi svake uspješne strategije zaštite podataka.

3.7.1 Automatizacija sigurnosnog kopiranja:

Automatizacija sigurnosnog kopiranja podrazumijeva korištenje softverskih alata i skripti za automatsko pokretanje, izvršavanje i praćenje procesa sigurnosnog kopiranja, bez potrebe za ručnom intervencijom. Eliminira rizik od zaboravljanja ili nepravilnog izvođenja sigurnosnog kopiranja, što je čest uzrok gubitka podataka. Automatizacija omogućuje optimizaciju procesa sigurnosnog kopiranja, čime se štede i vrijeme i resursi. Osigurava da se sigurnosno kopiranje izvodi redovito i prema unaprijed definiranom rasporedu, bez obzira na ljudski faktor.
Automatizacija omogućuje jednostavno prilagođavanje rastućim količinama podataka i promjenama u IT infrastrukturi.

3.7.2 Pravljenje rasporeda sigurnosnog kopiranja

Definiranje optimalnog rasporeda sigurnosnog kopiranja ključno je za postizanje ravnoteže između zaštite podataka i učinkovitosti sustava. Prilikom izrade rasporeda treba uzeti u obzir faktore kao što su kritičnost podataka, učestalost promjena, dostupni resursi i vrijeme izvršavanja. Podaci koji su ključni za poslovanje trebaju se češće sigurnosno kopirati od manje važnih podataka. Podaci koji se često mijenjaju zahtijevaju češće sigurnosno kopiranje kako bi se smanjio rizik od gubitka podataka u slučaju incidenta. Raspored sigurnosnog kopiranja treba biti prilagođen raspoloživim resursima, poput propusnosti mreže i prostora za pohranu. Sigurnosno kopiranje treba izvoditi u vrijeme kada će najmanje utjecati na performanse sustava i korisničko iskustvo.

3.7.3 Kombinacija automatizacije i rasporeda:

Kombinacija automatizacije i pravilno definiranog rasporeda omogućuje organizacijama da izgrade pouzdan i učinkovit sustav sigurnosnog kopiranja. Automatizacija osigurava da se sigurnosno kopiranje izvodi redovito i bez grešaka, dok raspored osigurava da se podaci kopiraju optimalnom učestalošću, uzimajući u obzir njihovu kritičnost i učestalost promjena.
U današnjem dinamičnom IT okruženju, gdje se podaci neprestano mijenjaju i rastu, automatizacija i rasporedi sigurnosnog kopiranja predstavljaju ključne alate za zaštitu podataka i osiguravanje kontinuiteta poslovanja. Kroz pažljivo planiranje i implementaciju ovih strategija, organizacije mogu minimizirati rizik od gubitka podataka i izgraditi otpornost na nepredvidive događaje.

3.8 Strategije i preporuke sigurnosnog kopiranja

U današnjem svijetu, gdje se podaci smatraju najvrjednijom imovinom organizacija, a kibernetičke prijetnje i tehnološki kvarovi vrebaju iza svakog digitalnog ugla, sigurnosno

kopiranje postaje ne samo preporučena praksa, već i neizostavan dio strategije upravljanja rizicima. Međutim, učinkovito sigurnosno kopiranje zahtijeva više od pukog stvaranja kopija podataka. Potrebna je dobro osmišljena strategija koja uzima u obzir specifične potrebe organizacije, vrstu podataka, razinu rizika i dostupne tehnologije.

Definiranje ciljeva sigurnosnog kopiranja, procjena rizika i kritičnosti podataka te odabir odgovarajuće metode dobar su početak u stvaranju dobre strategije. Definiranje ciljeva slijedi provedba testiranja i provjere oporavka podataka kako bi se osigurala funkcionalnost i spremnost za slučaj incidenta. Sljedeća je implementacija automatiziranih procesa za pojednostavljenje i optimizaciju sigurnosnog kopiranja. Usvajanje provjerene strategije za sigurnosno kopiranje koja uključuje tri kopije podataka na dva različita medija, s jednom kopijom izvan lokacije, tako zvano pravilo „3-2-1-1-0“, može pomoći za lakše kretanje u provedbu . Dobra strategija također uključuje implementaciju mjera zaštite sigurnosnih kopija od neovlaštenog pristupa, gubitka ili oštećenja, a vođenje detaljne dokumentacije o strategiji sigurnosnog kopiranja i redovito praćenje njenog izvršavanja zaokružuje dobru strategiju u smislenu cjelinu.

Slijedeći ove preporuke i prilagođavajući ih svojim specifičnim potrebama, organizacije mogu izgraditi robusnu strategiju sigurnosnog kopiranja koja im omogućava da se s pouzdanjem suoče s izazovima digitalnog doba i zaštite svoje najvrjednije resurse - podatke.

3.9 Pravilo „3-2-1-1-0“

„3-2-1-1-0“ je strategija sigurnosnog kopiranja podataka koja se smatra vrhunskim standardom u zaštiti podataka od raznih rizika. Ova strategija se razvila iz ranije, dobro poznate i opće prihvaćene „3-2-1“ strategije, dodajući dodatne slojeve sigurnosti kako bi se nosila sa sve sofisticiranijim prijetnjama u digitalnom dobu.
Potrebno je imati najmanje tri kopije važnih podataka: originalnu kopiju i dvije sigurnosne kopije. Sigurnosne kopije pohraniti na najmanje dva različita medija, poput tvrdog diska, magnetske vrpce, ili cloud pohrane. Ovo osigurava da ako jedan medij zakaže, podaci su i dalje dostupni na drugom. Jedna od sigurnosnih kopija treba biti pohranjena na fizički odvojenoj lokaciji od primarnog sustava. To štiti podatke od lokalnih katastrofa poput požara, poplave ili krađe. **J**edna nepromjenjiva kopija (eng. *immutable*) ili kopija koja je fizički odvojena od mreže. Ovaj dodatni sloj zaštite osigurava da podaci ne mogu biti izmijenjeni ili izbrisani, čak ni od strane ucjenjivačkog softvera ili kakvog drugog zlonamjernog softvera. Cilj je imati nula

grešaka prilikom oporavka podataka. Redovitim testiranjem sigurnosne kopije osigurava se da su podaci potpuni i da se mogu uspješno oporaviti u slučaju kakve izvanredne potrebe.

3.9.1 Važnost pravila „3-2-1-1-0“

U današnjem svijetu, gdje su kibernetički napadi i gubitak podataka sve češći, 3-2-1-1-0 pravilo pruža sveobuhvatnu zaštitu podataka. Ova strategija kombinira redundanciju, raznolikost medija, geografsku razdvojenost i nepromjenjivost kako bi osigurala da podaci budu sigurni i dostupni čak i u najnepovoljnijim scenarijima.

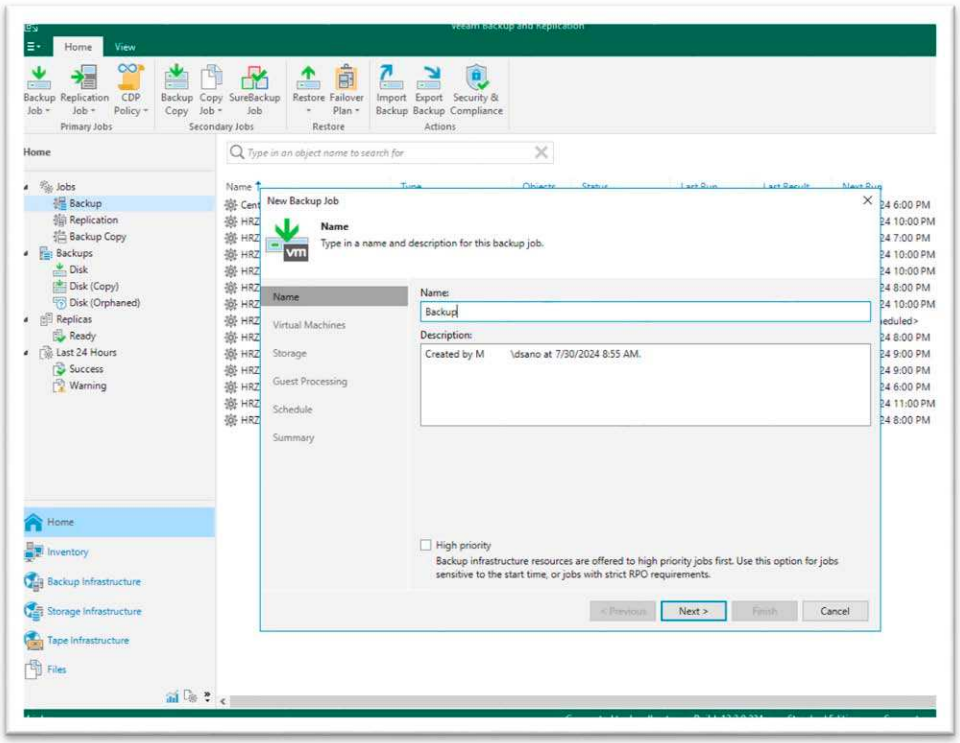
3.9.2 Implementacija pravila „3-2-1-1-0“

Implementacija ovog pravila može uključivati kombinaciju različitih tehnologija i pristupa, poput lokalnih i oblak rješenja za pohranu, softvera za sigurnosno kopiranje s podrškom za nepromjenjive kopije, te redovitog testiranja oporavka podataka. Iako može zahtijevati određena ulaganja, ova strategija pruža neprocjenjiv mir i sigurnost znajući da su podaci zaštićeni od širokog spektra prijetnji.

4 PRAKTIČNI RAD - PRIMJENA *VEEAM* TEHNOLOGIJE P RI STVARANJU I REPLICIRANJU S IGURNOSNE KOPIJE U STVARNOM POSLOVNOM OKRUŽENJU

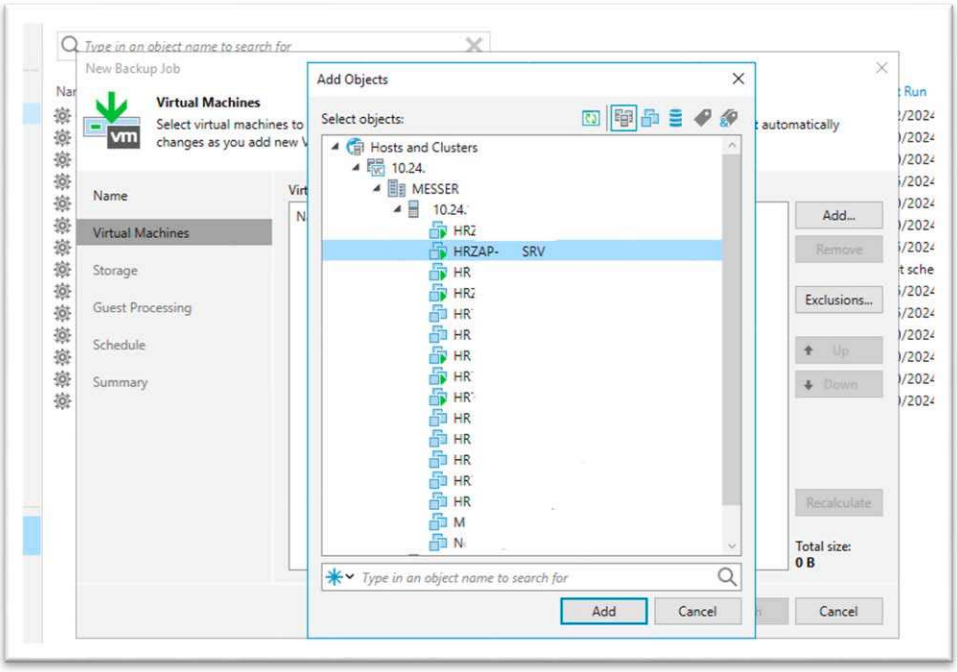
4.1 Stvaranje zadatka sigurnosnog kopiranja

Za potrebe nekog sigurnosnog kopiranja ovaj dio rada prikazuje stvaranje sigurnosne kopije i dodjeljivanje odgovarajućih svojstva istoj. Konkretno je stvorena sigurn osna kopij a jedne virtualne mašine. Početni korak zahtijeva izabrati opciju kre iranja novog z adatka za željeni posao. Zadavanje n aziva pomaže u razlikovanju različitih vrsta zadataka, ovisno o individualnim potrebama poslovanja i korištenju ranije opisanih tehnologija stvaranja sigurnosnih kopija (Slika 1).

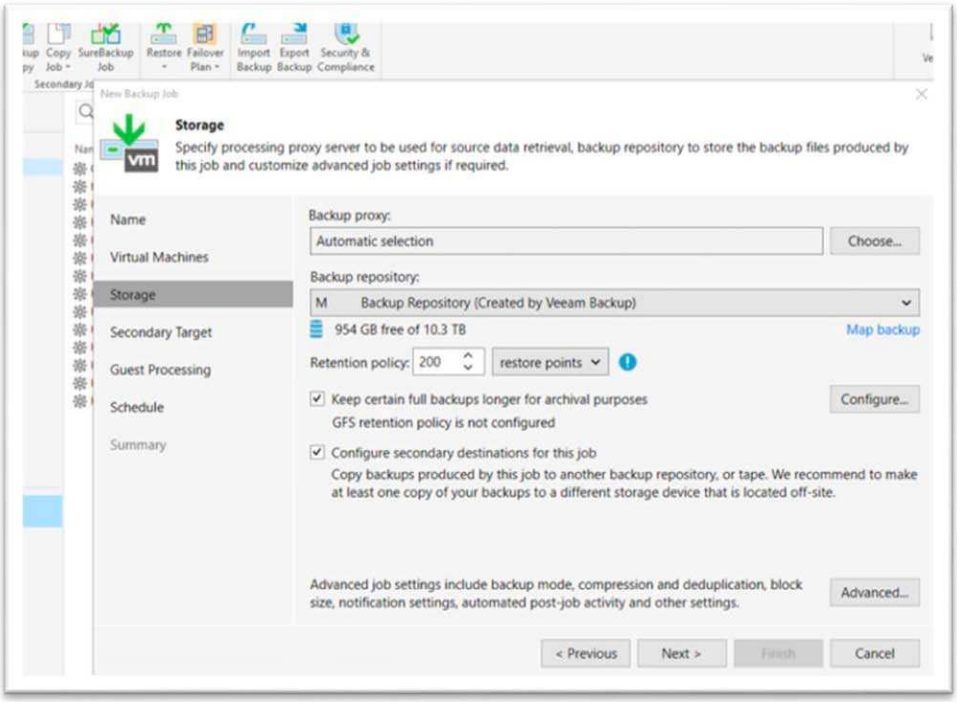


Slika 1. Početni korak stvaranja nove sigurnosne kopije i zadavanja naziv

Potom sli jedi oda bir objekta (Slika 2) nad kojim se vrši stvaranje sigurnosne kopije i repozitorija (Slika 3) unutar kojeg ista po početku stvaranja biva pohranjena.



Slika 2. Odabir objekta nad kojim se vrši sigurnosno kopiranje



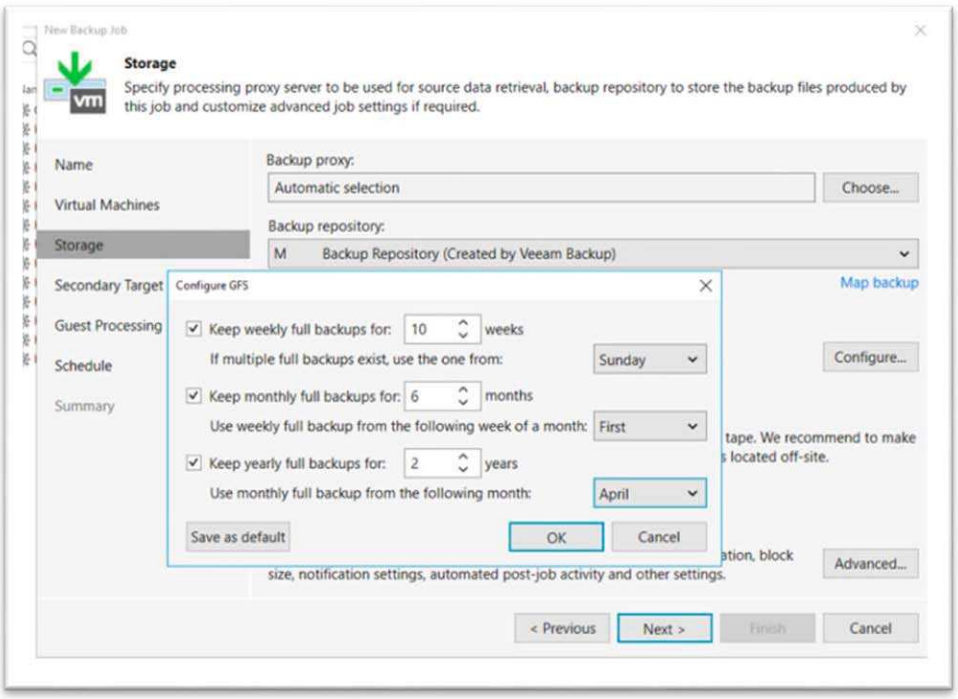
Slika 3. Odabir repozitorija za pohranu novog sigurnosnog kopiranja

Kod odabira prostora za pohranu kreirajući novi zadatak, odabrana je i opcija sekundarne destinacije na koju je ovaj zadatak (posao sigurnosnog kopiranja) spreman (Slika 3). Vidljive su opcije u kojima se bira mjesto (repozitorij) pohrane. Tijekom postavljanja novih zadataka sigurnosnih kopija, tijekom gotovo cijelog procesa, vidljive su informacije o pre ostalom,

odnosno korištenom, prostoru koji je dostupan u nekom repozitoriju. Potonje može poslužiti kao dobra informacija za planiranja i momentalno odlučivanje o korištenju nekog prostora za pohranu.

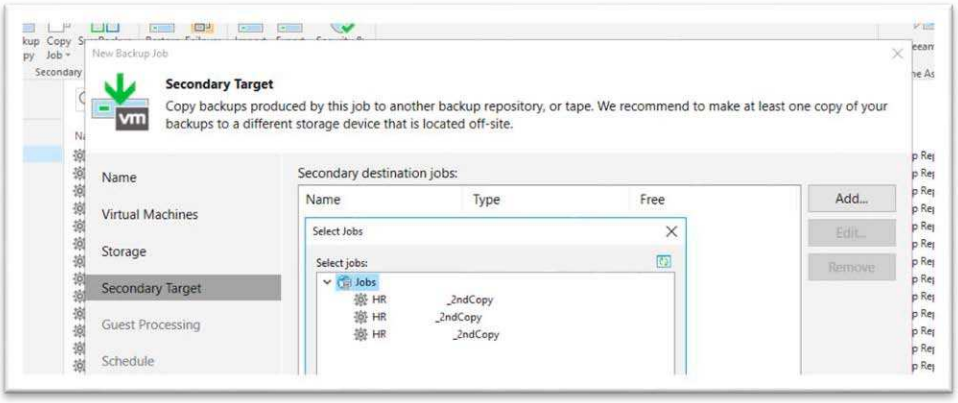
Važno je, tijekom ovog procesa, odabrati dodatne opcije koje mogu poboljšati sigurnosne kopije, a koje postoje kao opcije prilikom stvaranja sigurnosne kopije *Veeam* softverskim rješenjem.

Naime, tzv. *Grandfather-son* (GFS) nudi dodatne opcije stvarajući sintetičku sigurnosnu kopiju. U ovom slučaju dodane su opcije koje, osim potpune sigurnosne kopije, neovisno o inkrementalnim sigurnosnim kopijama, čuvaju pune sigurnosne kopije u određenim razdobljima, prema dodijeljenim pravilima (Slika 4).

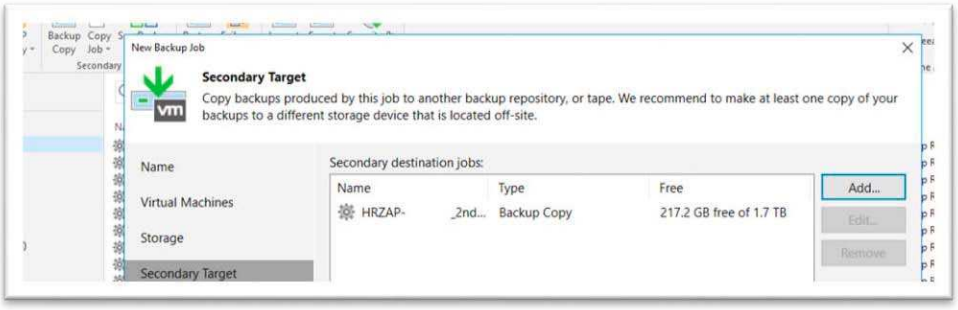


Slika 4. Primjer konfiguracije čuvanja arhiva punih sigurnosnih kopija

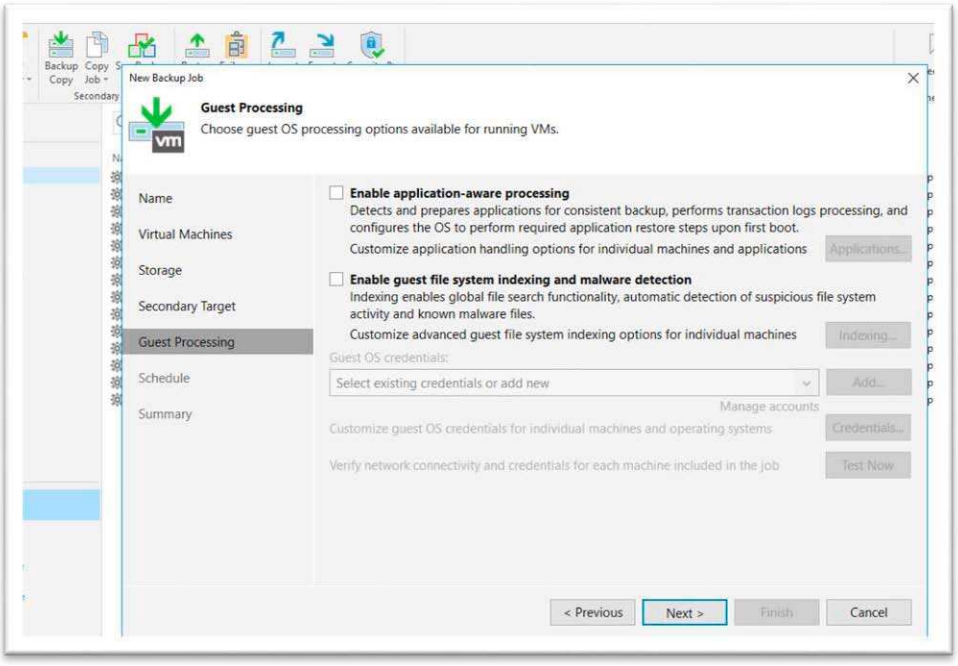
U sljedećim koracima je dostupna opcija odabira druge, dodatne, destinacije na koju se kopira sigurnosna kopija (Slika 5). Ista je definiran kao (sigurnosna) kopija sigurnosne kopije (op.: eng. *Backup copy*) (Slika 6). Zatim slijedi mogućnost odabira dodatnih opcija koje omogućavaju dodatni sloj zaštite pri izradi sigurnosne kopije, a njihov odabir ovisi o stvarnim potrebama i načinu korištenja sustava i kasnije sigurnosnih kopija (Slika 7).



Slika 5. Odabir sekundarne destinacije za pohranu



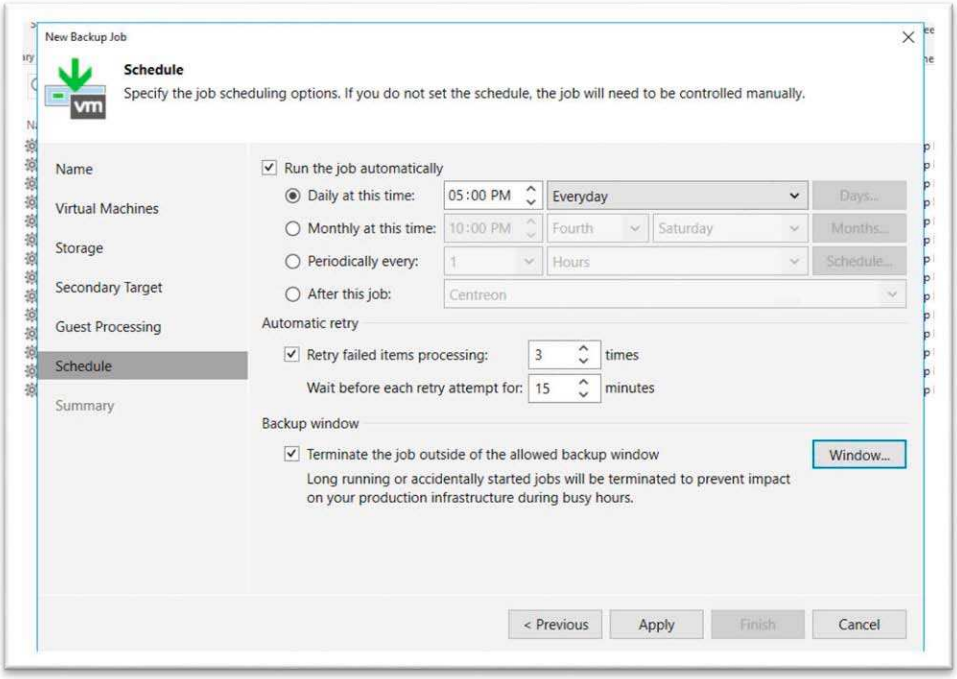
Slika 6. Prikaz odabrane opcije kopije sigurnosne kopije



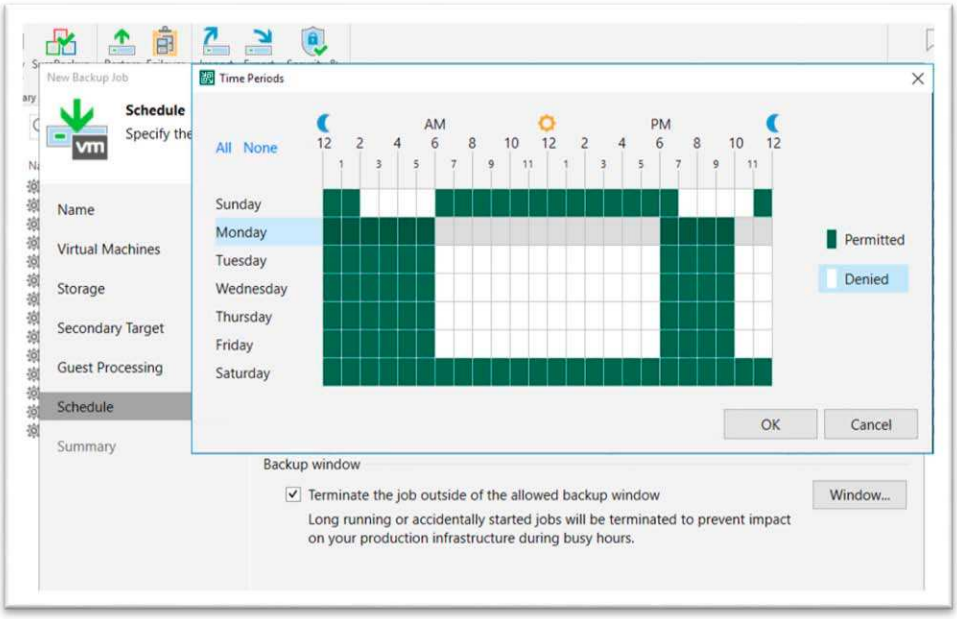
Slika 7. Odabir dodatnih sigurnosnih opcija tijekom izrade nove sigurnosne kopije

Nakon odabira željenih opcija same izrade, slijedi definiranje i odabir vremena kada sigurnosna biva izrađena. Moguće je odabrati dnevnu, mjesečnu, periodičku izradu ili po nekom drugom

završenom zadatku (Slika 8). Uz definirano vrijeme izrade sigurnosne kopije postoji i mogućnost odabira načina ponašanja sustava pri izradi sigurnosne kopije, ako eventualno dođe do greške i neuspjelog pokušaja izvršenja zadatka. Uz definirano vrijeme kada se kopija treba raditi prema redovitom rasporedu, dostupna je i dodatna mogućnost odabira vremenskih okvira unutar kojih se kopije ne smiju izrađivati, odnosno koje je vrijeme dozvoljeno i poželjno za izradu (Slika 9).



Slika 8. Odabir optimalnih vremena za izradu automatiziranih sigurnosnih kopija



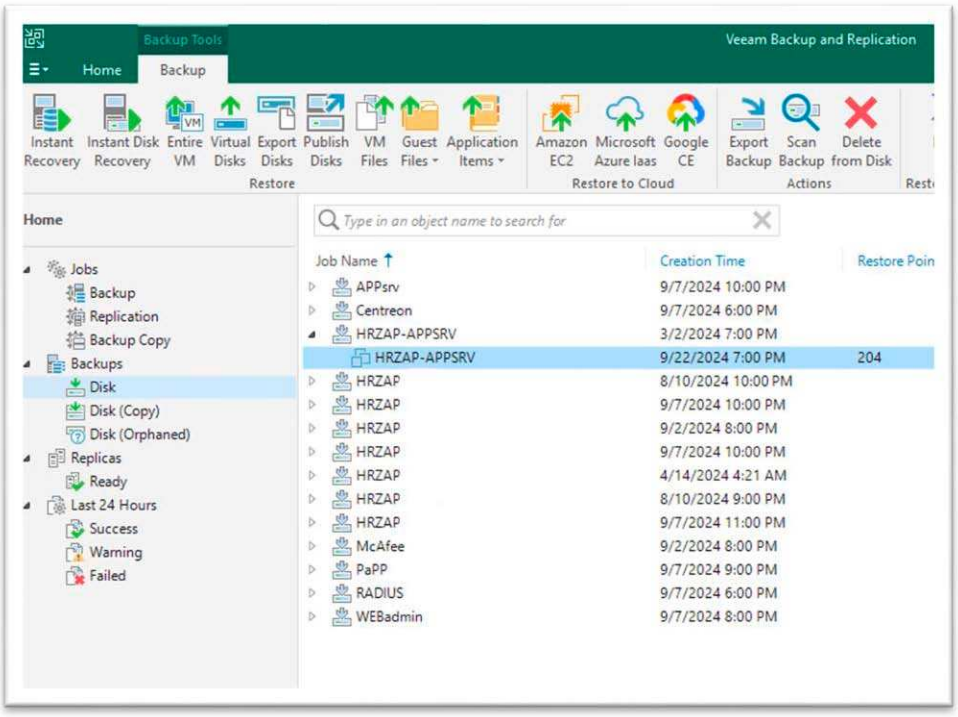
Slika 9. Prikaz dodatnih perioda za definiranje vremena izrade kopije

4.2 Oporavak podataka iz neke sigurnosne kopije

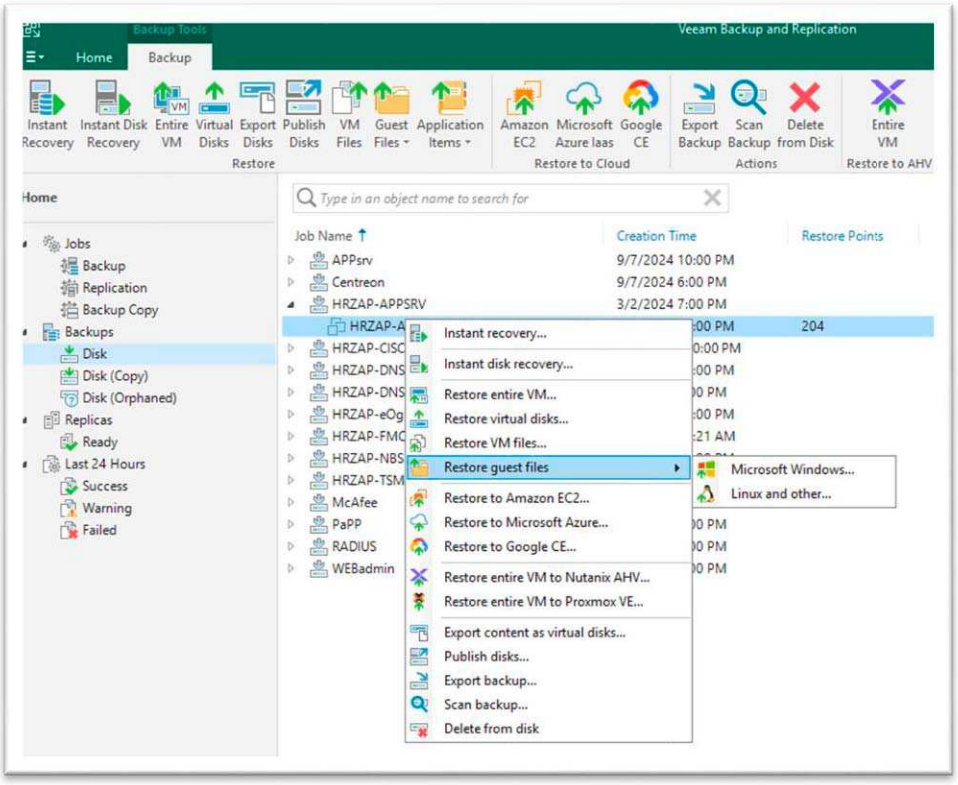
Kao jedan od primjera pravilnog i adekvatnog korištenja sigurnosne kopije, u životnim situacijama, rekreirana je situacija u kojoj je potrebno oporaviti niz datoteka iz mrežno dijeljenog diska. U sljedećim koracima, kroz slike, je prikazano vraćanje tih datoteka.

Za potrebe ovog rada korištena je dostupna verzija programa za sigurnosno kopiranje i repliciranje podataka „Veeam Backup & Replication 12“.

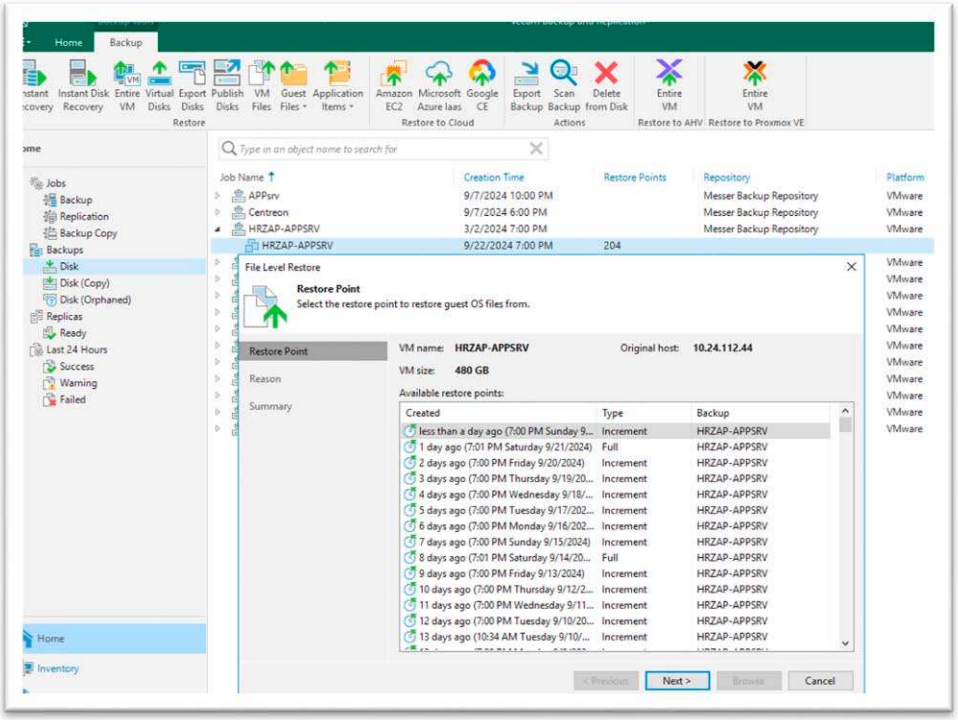
Za početak je potrebno odabrati odgovarajuću virtualnu mašinu, odnosno disk koji želimo oporaviti, odnosno u navedenom slučaju podataka ili niz podataka koji je potrebno oporaviti s nekog diska (Slika 10). Po odabiru željenog diska, na primjer, virtualne mašine potrebno je odabrati sistem iz kojeg se datoteke oporavljaju (Slika 11). Potom slijedi odabir neke željene, od dostupnih vremenskih točaka, iz koje je potrebno oporaviti datoteke (Slika 12).



Slika 10. Odabir diska s kojeg se vrši oporavak



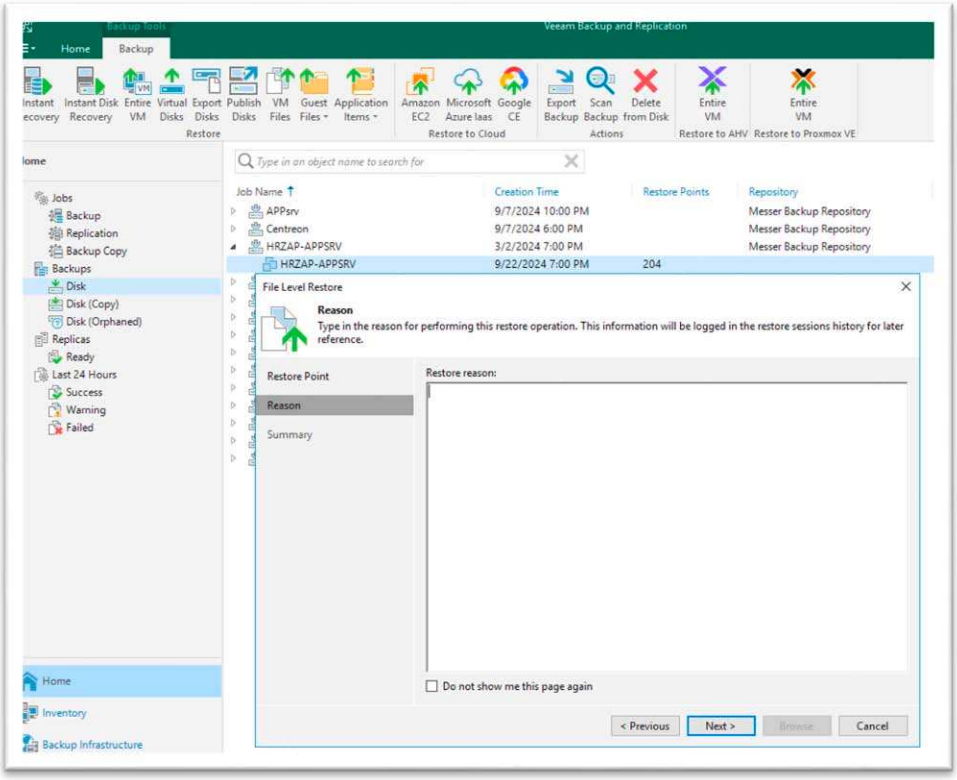
Slika 11. Odabir sistema iz kojeg se oporavljaju podaci



Slika 12. Odabir potrebnog razdoblja iz kojeg se datoteka oporavlja

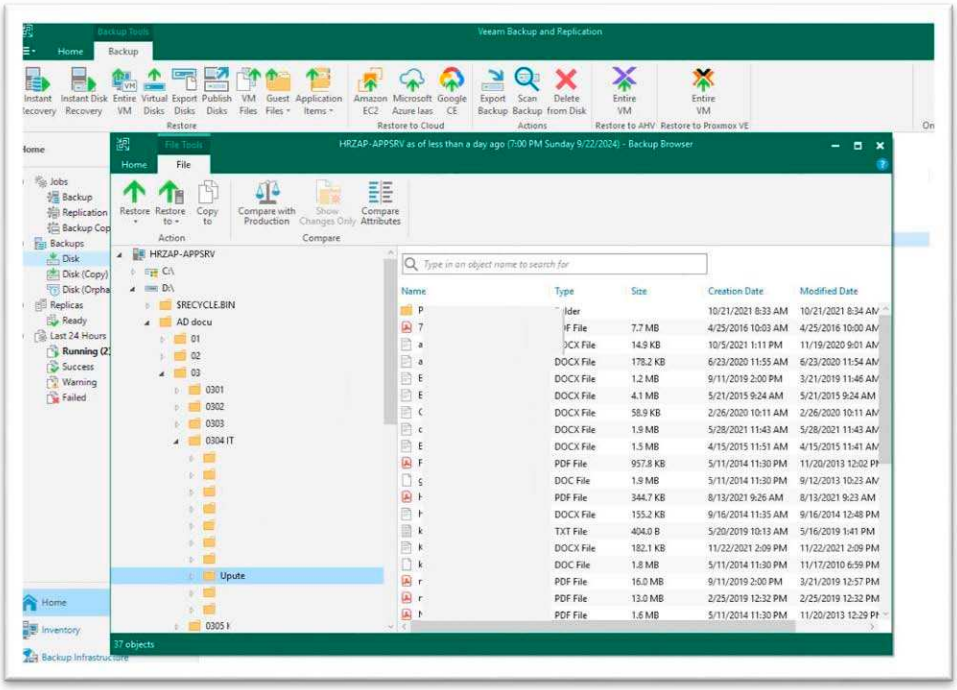
Kako bi cijelo proces oporavka bio pravilno dokumentiran i praćen, potrebno je navesti razlog

zbog kojeg se vrši određena promjena u sistemu (Slika 13).



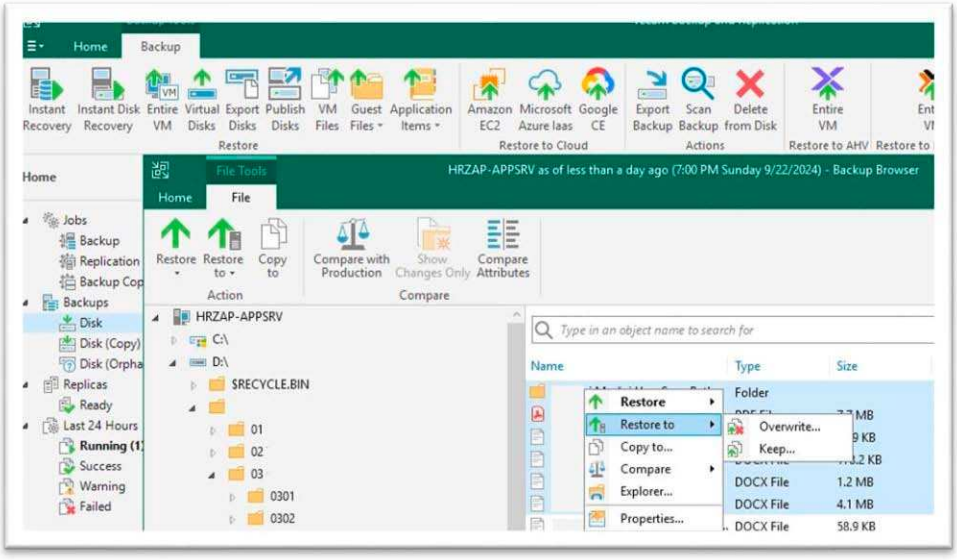
Slika 13. Unošenje razloga povrata podataka iz sigurnosne kopije

Nakon što je unesen razlog, sljedeći zaslon raspisuje sve što je prethodno odabrano za željeni povrat datoteka iz sigurnosne kopije, te je na sljedećem koraku potrebno odabrati datoteku ili datoteke za kojima postoji potreba da se obnove iz željene sigurnosne kopije (Slika 14).

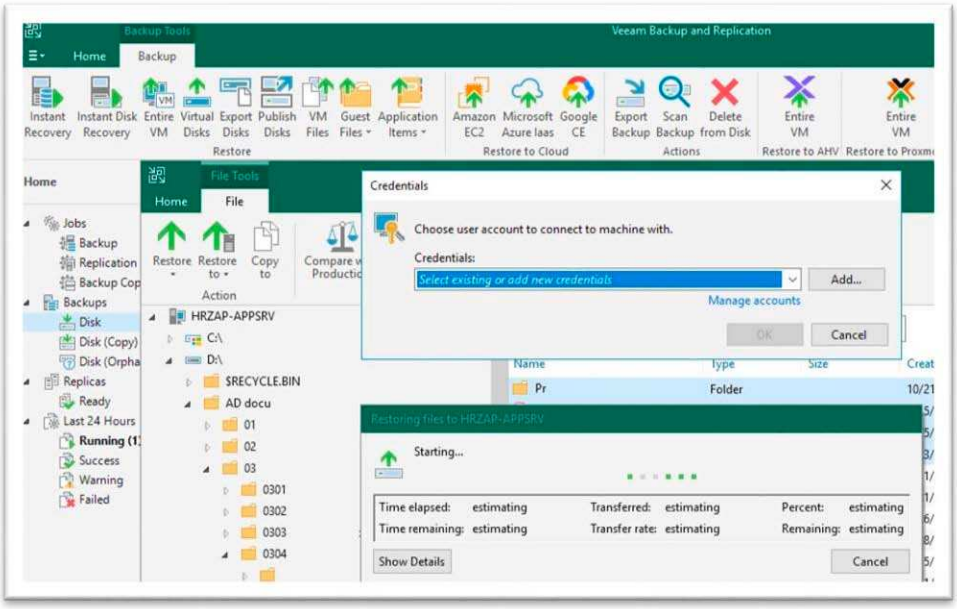


Slika 14. Prikaz pretraživanja datoteka

Nakon odabira datoteka koje je potrebno obnoviti potrebno je izabrati jednu od opcija gdje je datoteku moguće zamijeniti prethodnom, na istom mjestu ili zadržati izmijenjenu datoteku i datoteku iz povrata podataka na istom mjestu ili je obnovljene podatke moguće pohraniti na neko novo dostupno mjesto (Slika 15). Cijelu je proceduru potom potrebno autorizirati pripadajućim računom, kako bi se spriječile kakve eventualne neželjene i neautorizirane radnje (Slika 16).

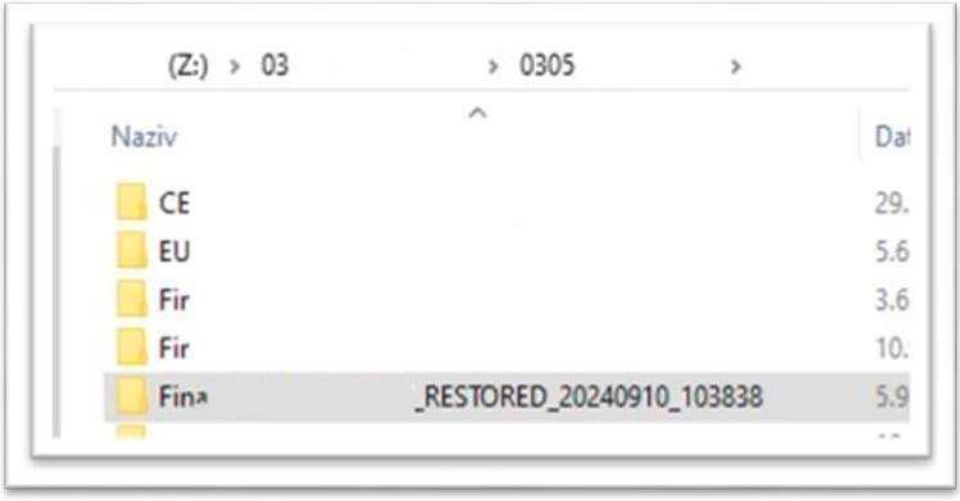


Slika 15. Odabir dostupnih opcija mjesta gdje se podaci vraćaju



Slika 16. Prikaz potrebne autorizacije prethodne radnje

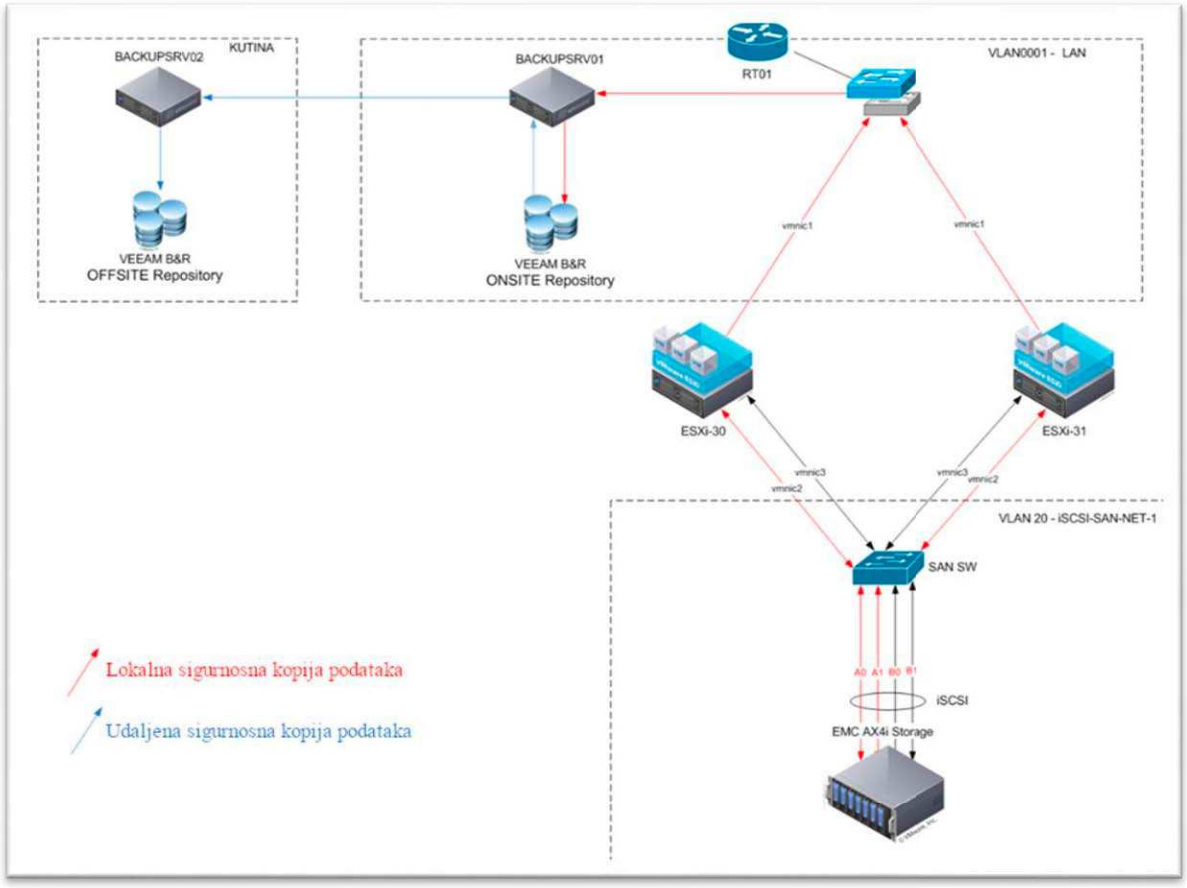
Nakon potvrde program, jedno izvjesno vrijeme koje mu je potrebno za oporavak, odrađuje oporavak, te potom javlja da je izvršeno učinjeno. Nakon toga je preporučljivo dokument otvoriti u prozoru za pregled datoteka i uvjeriti se da je proces zaista odrađen. Vizualni identifikator ukazuje na datoteke iz povrata tako što, recimo, vršna mapa, dobiva sufiks „RESTORED“, kao što je prikazano na slici niže (Slika 17). Također, dodaju se datum i vrijeme obrade kako bi se jasno naznačilo kada je obnova izvršena.



Slika 17. Vraćene mape dobivaju sufiks koji i vizualno označava da su obnovljene

4.3 Replikacija sigurnosne kopije na udaljenu lokaciju

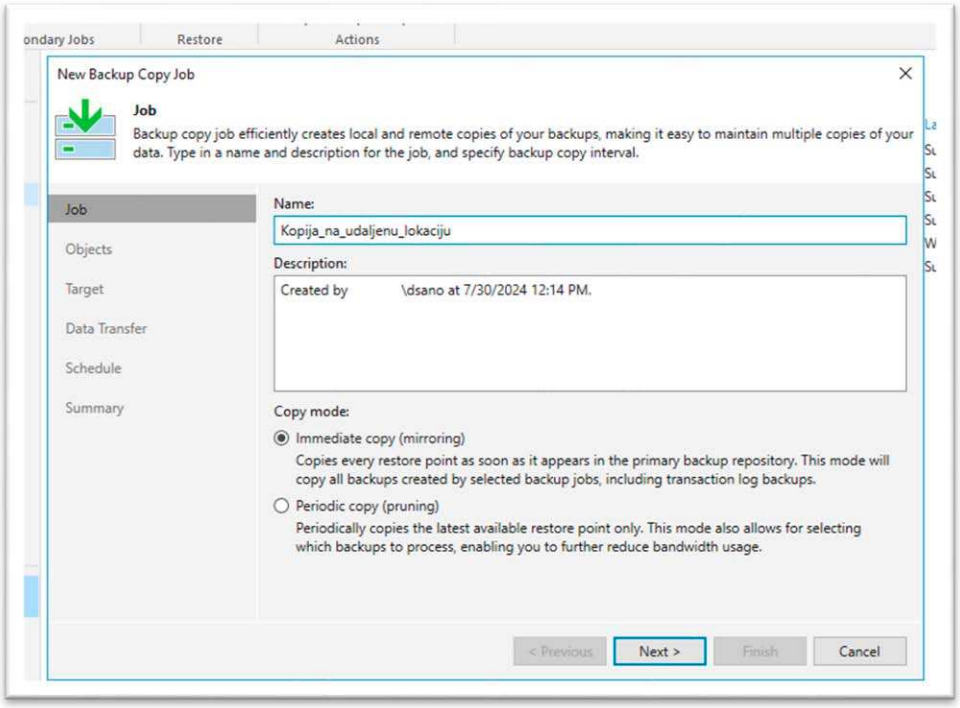
Kao dodatna mjera zaštite kojom se vodi i pravilo „3-2-1-1-0“, potrebno je postaviti izradu sigurnosne kopije na udaljenu, najbolje i geografski dislociranu, lokaciju. U ovom slučaju koristi se repliciranje sigurnosne kopije na geografski udaljenu lokaciju, odnosno u drugi grad. Za ovaj primjer napravljena je ujedno i kopija sigurnosne kopije i to na udaljenu lokaciju i pripadajući repozitorij. Na shemi ispod (Slika 18) prikazana su 2 geografski dislocirana repozitorija. Prikazano je kako se vrši izrada sigurnosne kopije unutar iste lokalne mreže i kako se replikacija vrši van lokalnog repozitorija na drugi, udaljeni.



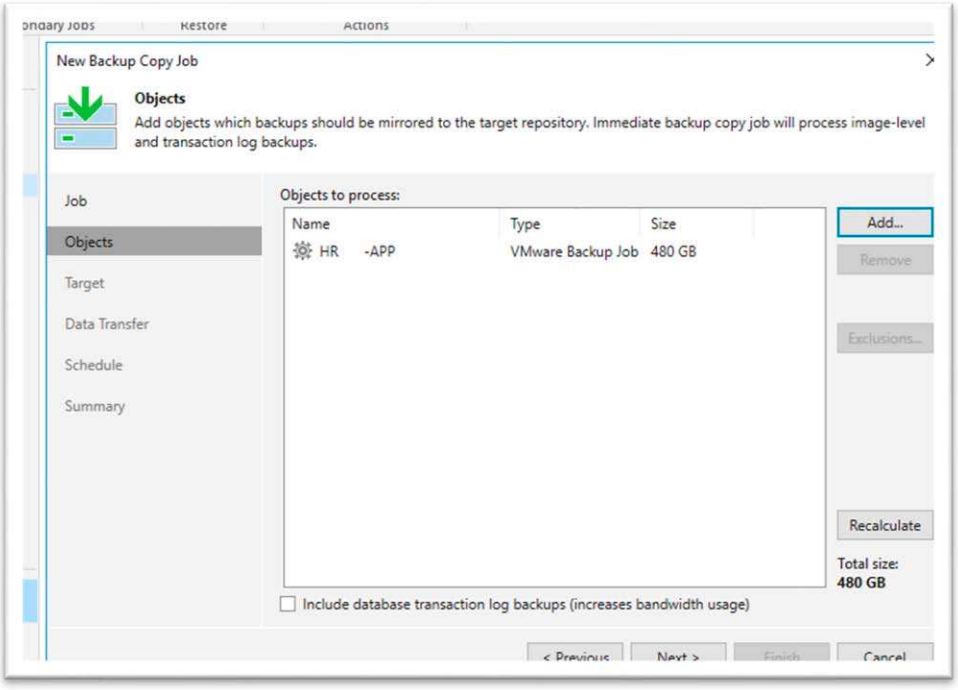
Slika 18. Shema prikazuje veze lokalnog i udaljenog repozitorija

Početak izrade kopije postojeće sigurnosne kopije započinje jednako kao i izrada regularne sigurnosne kopije s razlikom što se u početnom koraku bira način na koji se kopiranje izvršava (Slika 19). Tako su ponuđene dvije opcije, od kojih je prva orijentirana na momentalno kopiranje svih stvorenih točki vraćanja, a druga nudi kopiranje samo posljednje točke vraćanja izvorne sigurnosne kopije. Odabir ovisi o mogućnostima sistema te utječe li to na produktivni tijek. Po odabranoj opciji, potrebno je definirati objekt za kojim postoji potreba da se štiti

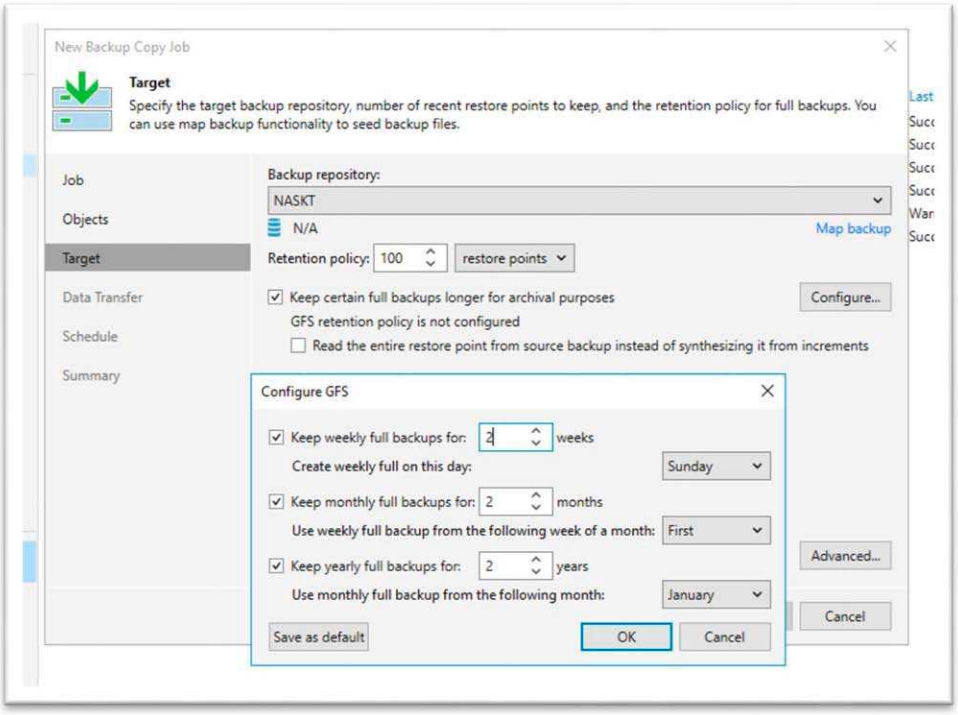
stvaranjem kopije (Slika 20). Kada je sustavu definirano, od strane korisnika, koji je željeni objekt za kojim postoji potreba da se dodatno zaštiti, bira se dostupni i željeni repozitorij na udaljenoj lokaciji te učestalost izrade kopija (Slika 21) .



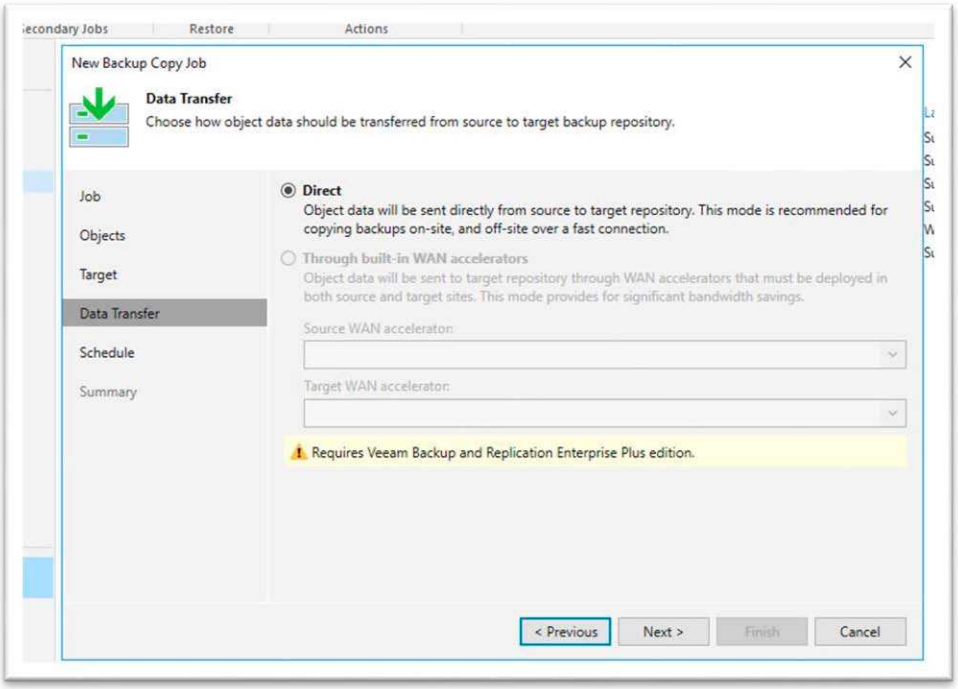
Slika 19. Izrada sigurnosne kopije na udaljenu lokaciju



Slika 20. Odabir željenog objekta



Slika 21. Odabir repozitorija i definiranje vremena izrade na udaljenoj lokaciji



Slika 22. Odabir načina prijenosa podataka (ovisi o licencama)

Posljednji korak uključuje odabir načina prijenosa podataka. On može biti direktan ili upućen preko posebnih *Veeam*-ovim WAN ubrzivača propusnosti (Slika 22).

5 ZAKLJUČAK

U današnjem svijetu, podaci su postali srž svakog poslovanja, a prijetnje poput kibernetičkih napada ili čak običnih tehničkih kvarova su, nažalost, svakodnevica. Zbog toga, sigurnosno kopiranje podataka više nije nešto što možemo odgađati ili smatrati opcionalnim - to je apsolutna nužnost.

Pregledom širokog spektara metoda sigurnosnog kopiranja, od onih tradicionalnih poput potpunog i inkrementalnog, pa sve do onih modernijih poput diferencijalnog, sintetičkog i neprekidnog kopiranja vidljiv je čitam jedan niz mogućnosti koje stoje na raspolaganju potencijalnim korisnicima. Ono što je postalo jasno jest da ne postoji univerzalno rješenje. Svaka organizacija je jedinstvena i ima svoje specifične potrebe, pa je ključno prilagoditi strategiju sigurnosnog kopiranja tim potrebama.

Dobra strategija počinje postavljanjem jasnih ciljeva i temeljitom procjenom rizika. Potrebno je razumjeti koje su informacije najkritičnije, a zatim odabrati pravu kombinaciju metoda sigurnosnog kopiranja koja pruža najbolju zaštitu. Automatizacija procesa i definiranje rasporeda sigurnosnog kopiranja olakšavaju svakodnevicu i osiguravaju da se kopije stvaraju redovito, bez potrebe za stalnim ručnim intervencijama. Govoreći o najboljim praksama, pravilo „3-2-1-1-0“ predstavlja vrh standarda koji nudi višeslojnu zaštitu od raznih prijetnji.

Iako bi se dalo zaključiti i suprotno, sigurnosno kopiranje nije samo tehnički zadatak za IT odjel. To je strateška odluka koja omogućuje organizacijama da donose informirane odluke, minimiziraju rizike i nastave s radom čak i kada se dogodi nešto neočekivano. Ulaganje u pouzdana rješenja za sigurnosno kopiranje i kontinuirano praćenje i poboljšavanje strategije su ključni za izgradnju otpornosti i osiguranje dugoročnog uspjeha u ovom digitalnom dobu.

Na kraju krajeva, sigurnosno kopiranje nije priča samo o zaštiti podataka. Radi se o očuvanju povjerenja klijenata, zaštiti reputacije tvrtke i osiguravanju da poslovanje nastavlja funkcionirati bez obzira na izazove. U vremenu i okruženju gdje su informacije gotovo najvažnija imovina, sigurnosno kopiranje služi poput police osiguranja koja svakoj organizaciji daje mir i sigurnost u (potencijalno) nesigurnim vremenima.

Unatoč prijetnjama koje su sveprisutne i, na kraju krajeva, neizbježne dobro je znati da organizacije, velike i male tvrtke i pojedinci mogu više vremena posvetiti produktivnosti svakog novog dana i posvetiti se idejama koje pospješuju sveopću kreativnost, a da su manje zabrinuti za sigurnost plodova svoga rada. Kako je i navedeno, postoje mnoge opcije kako

proizvesti zadovoljavajuće sigurnosne kopije podataka, a ovim radom je željeno pokazati i kako je moguće napraviti sigurnosne kopije podataka na lokaciji gdje su potrebne kao i njihove zaštitne iteracije van lokacije.

Praktična primjena *Veeam* tehnologije u ovom radu potvrđuje njenu efikasnost i pouzdanost u zaštiti podataka. S lakoćom je postignut željeni cilj oporavka, što ulijeva povjerenje u sposobnost sustava da odgovori na stvarne izazove. Posebno je zadovoljavajuće što se povrat datoteka odvijao točno onako kako je predviđeno u teoretskom dijelu, što potvrđuje vrijednost pažljivog planiranja i odabira adekvatnih alata.

LITERATURA

1. Preston, W. Curtis, (2021.), *Modern Data Protection Ensuring Recoverability of All Modern Workloads*, O'Reilly Media, Inc.
2. Nelson, Steven, (2011.), *Pro Data Backup and Recovery*, Apress
3. Veeam® Software, *Veeam* Blog, https://www.veeam.com/blog/ (Pristupljeno 20. 6. 2024)

SAŽETAK

U digitalnom dobu, gdje su podaci ključna imovina, sigurnosno kopiranje je neizostavno za zaštitu od gubitka, krađe ili oštećenja informacija. Kroz različite strategije poput potpunog, inkrementalnog, diferencijalnog, sintetičkog i neprekidnog kopiranja, organizacije mogu prilagoditi zaštitu svojim potrebama. Automatizacija, rasporedi i pravila poput 3-2-1-1-0 osiguravaju učinkovitost i pouzdanost. Ulaganje u sigurnosno kopiranje je strateška odluka koja štiti podatke, osigurava kontinuitet poslovanja i gradi povjerenje, omogućujući organizacijama da uspješno plove digitalnim svijetom.

Ključne riječi: sigurnosno kopiranje, sigurnosna kopija, Veeam, zaštita podatka, oporavak, podaci

SUMMARY

In the digital age, where data is a key asset, backup is essential protection against information loss, theft or damage. Through different strategies such as full, incremental, differential, synthetic and continuous backup, organizations can tailor protection to their needs. Automation, schedules and rules like 3-2-1-1-0 ensure efficiency and reliability. Investing in backup is a strategic decision that protects data, ensures business continuity and builds trust, enabling organizations to successfully navigate the digital world.

Keywords: backup, copy backup, Veeam, data protection, recovery, data