Backup management

Dudjak, Mario

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA

Sveučilišni studij

BACKUP MANAGEMENT

Završni rad

Mario Dudjak

Osijek, 2016.

ELEKTROTEHNIČKI FAKULTET OSIJEK
Sveučilište Josipa Jurja Strossmayera u Osijeku

Obrazac Z1P - Obrazac za ocjenu završnog rada na preddiplomskom studiju

Osijek,

Odboru za završne i diplomske ispite

Prijedlog ocjene završnog rada

Ime i prezime studenta:	Mario Dudjak
Studij, smjer:	Preddiplomski, Računarstvo
Mat. br. studenta, godina upisa:	R3587, 2013.
Mentor:	Doc. dr. sc. Ivica Lukić
Sumentor:	Doc. dr. sc. Mirko Köhler
Naslov završnog rada:	Backup management
Primarna znanstvena grana rada:	
Sekundarna znanstvena grana (ili polje) rada:	
Predložena ocjena završnog rada:	
Kratko obrazloženje ocjene prema Kriterijima za ocjenjivanje završnih i diplomskih radova:	Primjena znanja stečenih na fakultetu: Postignuti rezultati u odnosu na složenost zadatka: Jasnoća pismenog izražavanja: Razina samostalnosti:

Potpis sumentora:	Potpis mentora:

Dostaviti:

1. Studentska služba

Potpis predsjednika Odbora: _____

Dostaviti:

1. Studentska služba

ETFOS
ELEKTROTEHNIČKI FAKULTET OSIJEK
Sveučilište Josipa Jurja Strossmayera u Osijeku

IZJAVA O ORIGINALNOSTI RADA

Osijek,

Ime i prezime studenta:	Mario Dudjak
Studij :	Računarstvo
Mat. br. studenta, godina upisa:	R3587, 2013.

Ovom izjavom izjavljujem da je rad pod nazivom**:**

Backup management

izrađen pod vodstvom mentora

Doc. dr. sc. Ivica Lukić

i sumentora

Doc. dr. sc. Mirko Köhler

moj vlastiti rad i prema mom najboljem znanju ne sadrži prethodno objavljene ili neobjavljene pisane materijale drugih osoba, osim onih koji su izričito priznati navođenjem literature i drugih izvora informacija.
Izjavljujem da je intelektualni sadržaj navedenog rada proizvod mog vlastitog rada, osim u onom dijelu za koji mi je bila potrebna pomoć mentora, sumentora i drugih osoba, a što je izričito navedeno u radu.

Potpis studenta:

Sadržaj

1. UVOD

U ovom završnom radu se obrađuju postojeće strategije izrade sigurnosnih kopija podataka (engl. *Backup*). U području informacijskih tehnologija, proces izrade sigurnosnih kopija podataka od velikog je značaja za poslovanje organizacija, u smislu očuvanja arhive znanja i integriteta organizacije. Arhiva znanja organizacije se sastoji od skupine podataka koji imaju određeno značenje i vrijednost. U svim fazama poslovanja organizacije, potrebno je određeno znanje o poslu koji se obavlja, tj. određen skup podataka. Rukovođenje tim skupom podataka, jedan je od ključnih poslova svake organizacije, a u ovom završnom radu opisana je teorijska podloga za izradu vlastitog rukovodstva sigurnosnim kopijama (engl. *Backup management*).

U prvom poglavlju glavnog dijela, prikazana je teorijska osnova na kojoj počiva koncept izrade sigurnosnih kopija. Istaknuta je svrha izrade sigurnosnih kopija i provedena je analiza učinaka, ali i troškova izrade sigurnosnih kopija. Objašnjeni su principi izrade osnovnih tipova, ali i kombiniranih funkcionalnih tipova sigurnosnih kopija.

U drugom poglavlju glavnog dijela, navedene su kategorije struktura podataka nad kojima se mogu izraditi sigurnosne kopije. Na temelju kombinacija osnovnih kategorija i osnovnih tipova sigurnosnih kopija, formirane su funkcionalne strategije za izradu sigurnosnih kopija. Za svaku funkcionalnu strategiju, objašnjen je njen princip izrade.

U trećem poglavlju glavnog dijela, prikazano teorijsko razmatranje upotrijebljeno je pri izradi vlastitog rukovodstva sigurnosnim kopijama pomoću okruženja *SQL Server Management Studio.* Izabrano okruženje je jedno od najpoznatijih za istovremeno obavljanje poslova poput izrade baze podataka, konfiguriranje, upravljanje, pristupanje i manipuliranje podacima u bazi podataka i kreiranje objekata u bazi podataka.

Na kraju je u zaključku objašnjeno, kako je poželjno kombinirati sva tri osnovna tipa sigurnosnih kopija podataka, da bi se smanjio broj sigurnosnih kopija koje se moraju povratiti u slučaju problema, a time se smanjuje i vrijeme oporavka podataka. Također, zaključeno je kako je nemoguće unaprijed postaviti strategiju bez poznavanja svojstava baze podataka i načina korištenja podataka.

1.1. Zadatak završnog rada

Obraditi strategije izrade sigurnosnih kopija, tehnologije koje se koriste i moguće primjene. Usporediti samo troškove rukovodstva sigurnosnim kopijama s gubicima ako se on ne provodi. Iskoristiti najbolje tehnologije za razvoj vlastitog rukovodstva sigurnosnim kopijama.

2. OSNOVE SIGURNOSNIH KOPIJA PODATAKA

2.1. Važnost sigurnosnih kopija podataka i oporavka

Svaka organizacija koja koristi sustav za upravljanje bazom podataka (engl. *database management system*) zahtijeva administratora baze podataka (engl. *database administrator*) ili administracijsku grupu, kako bi se osiguralo učinkovito korištenje i implementacija baze podataka organizacije. Prema [1], administrator baza podataka je informacijski tehničar koji je odgovoran za osiguravanje stalne operativne funkcionalnosti i učinkovitosti baza podataka neke organizacije i programa koji pristupaju tim bazama podataka. Sustav za upravljanje bazom podataka je skup programa koji omogućuju krajnjem korisniku ili aplikacijskim programima dijeljenje i upravljanje podacima. On pruža sustavan način stvaranja, ažuriranja, pronalaženja i spremanja podataka u odgovarajućem obliku u bazi podataka. Sustav za upravljanje bazom podataka je odgovoran za osiguranje integriteta i sigurnosti podataka, kontrolu pristupa podacima, optimizaciju, automatizirano izvođenje, ponovno pokretanje i oporavak. Budući da većina današnjih organizacija koriste sustav za upravljanje bazom podataka, neovisno o njihovoj veličini, potreba za administratorima baza podataka je veća nego ikad.

Jedna od osnovnih zadaća administratora baza podataka je oporavak (engl. *Recovery*) podataka u slučaju problema. Problem može značiti bilo što od manjih tehničkih poteškoća, pogreška programa do prirodnih katastrofa koje gase organizaciju. Prema [2], problemi koji su uzrok oštećenju ili gubitku podataka svrstavaju se u 5 kategorija:

- Pogreške na tvrdom disku
- Neispravnost datoteka
- Destruktivni utjecaji (zaposlenici, virusi, hakeri)
- Prirodne katastrofe (požar, poplava,…)
- Slučajno brisanje ili prepisivanje datoteka

Prema [1], analitičari su pokazali da je 80% problema, koji su uzrok oštećenju ili gubitku podataka, posljedica grešaka u programima ili ljudskih pogrešaka. Administrator baza podataka mora biti spreman izvršiti oporavak podataka do razine na kojoj se oni opet mogu koristiti, bez obzira na vrstu problema i što je brže moguće.

Kako bi bio spreman za bilo koju vrstu oporavka, administrator baza podataka mora razviti strategiju sigurnosne kopije podataka, kako bi osigurao da se podaci ne izgube u slučaju nastanka jedne od vrste problema koji su uzrok oštećenju ili gubitku podataka. Prema [3], sigurnosna kopija podataka je kopija podataka koji se mogu koristiti za vraćanje (engl. *Restore*) i oporavak nakon nestanka. Sigurnosna kopija baze podataka se također može koristiti za premještanje kopije baze podataka na novo mjesto. Strategija sigurnosne kopije podataka mora biti primjenjiva na obradu baze podataka, tako da sadrži slikovne kopije podataka, kao i zapise učinjenih promjena nad podacima. Također, mora uzeti u obzir i sve aktivnosti koje nisu primarno aktivnosti nad bazom podataka, ali imaju posredan utjecaj na podatke.

Općenito, svrha sigurnosne kopije podataka i oporavka je zaštititi bazu podataka od gubitka podataka i rekonstruirati bazu podataka u slučaju gubitka podataka. Prema [4], zadaci koje uključuje izrada strategije sigurnosne kopije podataka su sljedeći :

- Planiranje i testiranje odgovora na različite vrste kvarova
- Podešavanje okružja baze podataka za sigurnosno kopiranje i oporavak
- Postavljanje rasporeda izrade sigurnosne kopije podataka
- Praćenje okružja sigurnosne kopije podataka
- Rješavanje problema u sigurnosnoj kopiji podataka
- Oporavak od gubitka podataka

Administrator baza podataka, osim zadataka koje uključuje izrada strategije sigurnosne kopije podataka, može obavljati i druge poslove vezane uz sigurnosnu kopiju podataka i oporavak. Dvije osnovne takve zadaće su očuvanje podataka (engl. *Data preservation*) i prijenos podataka (engl. *Data transfer*). Očuvanje podataka uključuje stvaranje kopije baze podataka za dugotrajnu pohranu, a prijenos podataka uključuje premještanje podataka iz jedne baze podataka na drugu ili s jednog računala na drugo.

2.2. Analiza učinaka i troškova sigurnosne kopije podataka

Sposobnost vraćanja baze podataka iz važeće kopije je vitalni dio osiguranja neprekidnosti poslovanja organizacije. Kako bi organizacija mogla izvršiti oporavak podataka u svakom trenutku, sigurnosne kopije podataka bi se trebale nastojati izrađivati što češće, nad što većim opsegom podataka te koristeći najbolje tehnologije izrade sigurnosne kopije podataka. No, primarna funkcija cilja organizacija je ostvarivanje dobiti ili stvaranje novih učinaka s obzirom na raspoložive resurse. Prilikom izrade sigurnosne kopije podataka, organizacija mora uložiti određene resurse, kao što su novčana ulaganja, kapitalna dobra i radni kapital. U računovodstvenim izvješćima organizacija, taj utrošak resursa će se prikazivati kao rashod organizacije i negativno će utjecati na financijsko poslovanje organizacije u cilju ostvarivanja dobiti.

Kako bi organizacije osigurale mogućnost povratka podataka nužnih za svoje poslovanje uz minimalan trošak, obavezane su izraditi plan povratka podataka (engl. *Data recovery plan*). Prema [5], plan povratka podataka je skup radnji koje administratori baza podataka poduzimaju za rukovanje štetnim događajima koji mogu utjecati na dostupnost okružja njihovih baza podataka. Dva ključna pokazatelja koja se uzimaju u obzir prilikom izrade plana povratka podataka su: količina izgubljenih podataka koje si organizacija može priuštiti u slučaju štetnog događaja i novčani iznos koji je organizacija voljna platiti u svrhu očuvanja podataka čak i slučaju kada ne dođe do štetnog događaja. Ta dva suprotstavljena pokazatelja se određuju analizom prijetnji (engl. *Threat analysis*) i analizom poslovnih i operativnih zahtjeva.

Analiza prijetnji je jedan od dijelova izrade plana povratka podataka u kojoj se pokušavaju predvidjeti sve potencijalne prijetnje koje se analiziraju i kao rezultat daju posljedice tih prijetnji, tj. vrste mogućih oštećenja podataka. Prema [5], prijetnje se klasificiraju s obzirom na njihov izvor: Tehnička oprema (engl. *Hardware*), Programska oprema (engl. *Software*), ljudi i okoliš. Po pojedinom izvoru, moguće su sljedeće prijetnje:

1. Tehnička oprema:
    a. Oštećenje tvrdog diska
    b. Oštećenje ulazno – izlaznih komponenata
    c. Kvar mikroprocesora i memorije
    d. Kolaps poslužitelja (engl. *Server*)

2. Programska oprema:
    a. Rizici vezani za nadogradnje i zakrpe
    b. Pogreške programske opreme
    c. Računalni virusi
3. Ljudi:
    a. Slučajno brisanje podataka
    b. Netočno ažuriranje podataka
    c. Slučajne pogreške administratora baza podataka
    d. Namjerne pogreške administratora baza podataka
    e. Neovlašteni pristup podacima ili poslužitelju
4. Okoliš:
    a. Požar, poplava
    b. Potres, tornado
    c. Krađa ili civilni poremećaj

Jedan od dijelova izrade plana povratka podataka je i analiza poslovnih zahtjeva. Prilikom analize poslovnih zahtjeva potrebno je razmotriti sljedeće kriterije: vrijednost podataka, promjenjivost podataka, veličina baze podataka i upotreba podataka. Pod kriterijem vrijednosti podataka, podrazumijeva se vrijednost podataka organizacije, tj. pokušava se utvrditi koliki bi bio trošak organizacije zbog izgubljenih podataka, po raznim jedinicama podataka (jedan dan transakcija, jedan sat informacija…). Kriterij promjenjivosti podataka pokušava utvrditi koliko često se mijenjaju podaci unutar baze podataka organizacije. Promjenjive baze podataka zahtijevaju česte izrade sigurnosnih kopija. Kriterijem veličine baze podataka utvrđuje se koliko je velika baza podataka i prema tome zaključuje koliko će dugo trajati izrada sigurnosne kopije takve baze podataka i oporavak baze podataka u slučaju oštećenja ili gubitka podataka.

Kriterijem upotrebe podataka se utvrđuje koliko vremena se baza podataka organizacije koristi s obzirom na radno vrijeme organizacije i prema tome se utvrđuje vrijeme izrade sigurnosne kopije baze podataka kako bi se smanjio utjecaj sigurnosnih postupaka na poslovanje organizacije. Primjerice, ako se baza podataka ne koristi izvan radnog vremena, poželjno je izvršiti sigurnosnu kopiju baze podataka kada korisnici ne rade, kako bi se podaci mogli brže oporaviti u slučaju kvara. No, ako su podaci organizaciji potrebni u svakom trenutku, tj. dvadeset i četiri sata dnevno i sedam dana tjedno, sigurnosnu kopiju je poželjno izraditi u trenutku kada

ima najmanji utjecaj na sustav. Takvom planu povratka podataka će biti potrebno manje vremena za izvođenje, ali će oporavak podatka u slučaju kvara duže trajati.

Plan povratka podataka također treba uzeti u obzir i operativne zahtjeve. Najrelevantniji operativni zahtjevi plana povrataka podataka su sigurnost, učinak i upravljivost. Sigurnost je najosjetljiviji operativni zahtjev za razmatranje, jer su sigurnosne kopije podataka izloženije fizičkim napadima od baza podataka koje sadrže. Ispunjavanje zahtjeva sigurnosti podrazumijeva očuvanje povjerljivosti, integriteta i raspoloživosti podataka. Stvarne mjere za ispunjavanje navedenih sigurnosnih zahtjeva bile bi: sprječavanje neovlaštenog kopiranja sigurnosne kopije podataka, sprječavanje neovlaštenog brisanja sadržaja sigurnosne kopije podataka i sprječavanje krađe medija na kojima su pohranjene sigurnosne kopije podataka.

Provedbom usporedbe rezultata analize prijetnji i analize operativnih i poslovnih zahtjeva, mogu se formirati ciljevi izrade sigurnosnih kopija. Tri temeljna cilja izrade sigurnosnih kopija su:

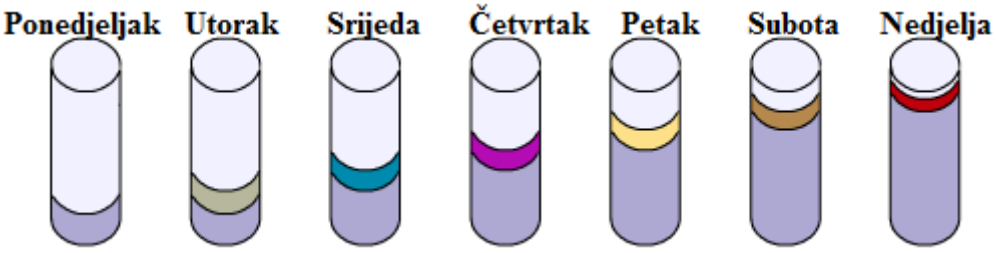
1. Povrat izgubljenih podataka
2. Minimalizacija količine izgubljenih podataka
3. Minimalizacija troška oporavka podataka.

2.3. Osnovni tipovi sigurnosne kopije podataka

Nakon kreiranja plana povratka podataka, koji uključuje analizu prijetnji, poslovnih i operativnih zahtjeva, sljedeći korak administratora baza podataka je formiranje strategije za izradu i rukovanje sigurnosnom kopijom podataka i procesom oporavka podataka ukoliko bude potrebno. Kako bi stvorio takvu strategiju, administrator baza podataka mora razlikovati različite tipove sigurnosnih kopija podataka. Postoje tri osnovna tipa sigurnosnih kopija podataka: potpuni (engl. *Full*), diferencijalni (engl. *Differential*) i zapis izvršenih promjena (engl. *Log*).

2.3.1. Potpuna sigurnosna kopija podataka

Potpuna sigurnosna kopija podataka čini kopiju svih upotrijebljenih stranica baze podataka (engl. *Database pages*), što znači da kopira sve podatke iz baze podataka. Također i odstranjuje svaku praznu stranicu u bazi podataka. Stranica baze podataka je jedna od unutarnjih struktura u bazi podataka, koja služi za organiziranije spremanje podataka u bazi podataka. Stranica baze podataka može biti različite veličine (8KB, 16KB, 64KB…). Prema [1], potpuna sigurnosna kopija podataka je potpuna kopija svih podataka u bazi podataka u vrijeme kada se potpuna sigurnosna kopija podataka izvršava. Potpune sigurnosne kopije podataka također kopiraju i udvostručuju zapise izvršenih transakcija nad podacima (engl. *Transaction logs*), pri čemu se u obzir uzimaju sve izvršene transakcije ali i transakcije koje su se odvijale tijekom izrade sigurnosne kopije podataka. To svojstvo omogućuje očuvanje integriteta transakcija, prilikom povratka podataka iz sigurnosne kopije podataka. U ovom kontekstu, transakcija podrazumijeva dvosmjernu razmjenu podataka između organizacije i osobe ili programa koji koristi podatke iz baze podataka organizacije radi obavljanja određenog posla.

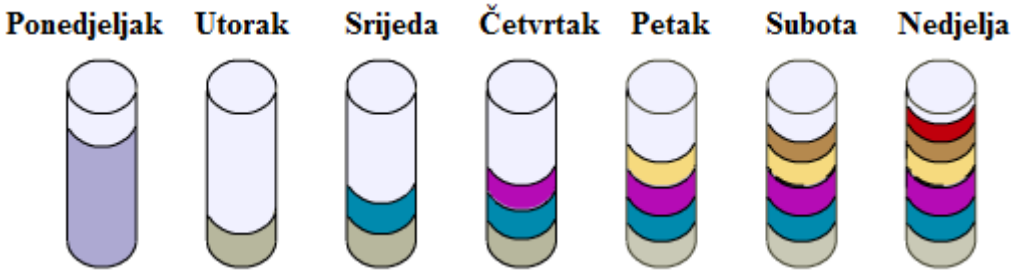


Sl. 2.1.: Princip izrade potpune sigurnosne kopije podataka [2]

Potpune sigurnosne kopije podataka predstavljaju temelj za izradu strategija za rukovanje sigurnosnom kopijom podataka, u slučajevima krađe podataka, gubitka ili oštećenja većine fizičkih medija na kojima su podaci spremljeni. U takvim slučajevima, dostupnost pune sigurnosne kopije podataka, sigurno pohranjene na posebnom položaju, može biti jedini put za povratak svih podataka organizacije koji bi se potom smjestili na novi poslužitelj. Ako uz punu sigurnosnu kopiju podataka, postoje i diferencijalna sigurnosna kopija i zapis učinjenih promjena nad podacima, podaci iz baze podataka će se gotovo potpuno oporaviti na stanje u kojem su bili prije teškog oštećenja. No, ako potpuna sigurnosna kopija podataka nikad nije bila kreirana, neće postojati ni diferencijalna sigurnosna kopija ni zapis učinjenih promjena, jer je potpuna sigurnosna kopija podatka preduvjet za oboje, tj. takozvana temeljna sigurnosna kopija podataka (engl. *Base backup*). Tada postoji vrlo mala vjerojatnost za oporavak podataka.

2.3.2. Diferencijalna sigurnosna kopija podataka

Diferencijalna sigurnosna kopija podataka je dizajnirana kako bi se smanjilo vrijeme trajanja izrade sigurnosne kopije podataka. Princip izrade diferencijalne sigurnosne kopije podataka je kopiranje samo onih stranica baze podataka koje su se promijenile od posljednje izrade potpune sigurnosne kopije podataka, umjesto kopiranja svih upotrijebljenih stranica. Prema [3], diferencijalna sigurnosna kopija podataka je sigurnosna kopija podataka koja se temelji na potpunoj sigurnosnoj kopiji podataka cjelovite ili djelomične baze podataka koja sadrži samo podatke koji su promijenjeni od posljednje izrade potpune sigurnosne kopije podataka. Slično kao i potpuna sigurnosna kopija podataka, diferencijalna sigurnosna kopija podataka također kopira zapis izvršenih transakcija nad podacima kako bi osigurala očuvanje transakcijskog integriteta.

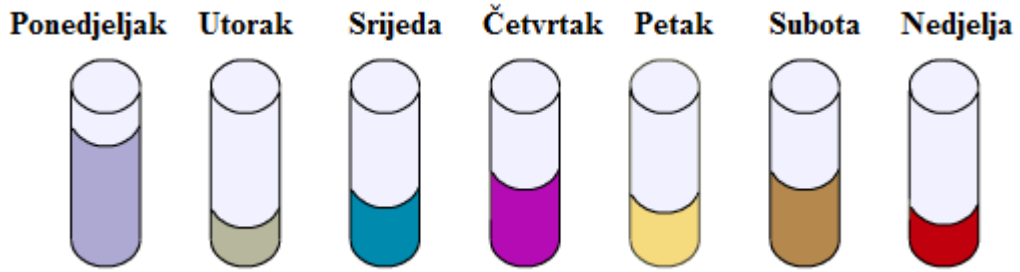


Sl. 2.2.: Princip izrade diferencijalne sigurnosne kopije podataka [2]

Svaka uzastopna diferencijalna sigurnosna kopija podataka kopira podatke od posljednje potpune sigurnosne kopije podataka, tj. promjene nad podacima su kumulativne. Na taj način, u slučaju gubitka ili oštećenja podataka, potrebno je povratiti podatke iz posljednje potpune sigurnosne kopije podataka i posljednje diferencijalne sigurnosne kopije podataka. Osnovna prednost diferencijalne sigurnosne kopije podataka u odnosu na potpunu sigurnosnu kopiju podataka je što zahtijeva manje vremena za obradu, jer sadrži manje podataka ukoliko se sigurnosne kopije izvode redovito. Osim toga, izrada diferencijalne sigurnosne kopije podataka nasuprot potpune sigurnosne kopije podataka je ušteda prostora, tj. računalnih resursa.

2.3.3. Zapis izvršenih promjena (engl. *log backup*)

Jedina vrsta sigurnosne kopije podatka koja zapravo ne kopira stranice baze podataka je zapis izvršenih promjena. Zapis izvršenih promjena, kao i druga dva osnovna tipa sigurnosnih kopija podataka, kopira zapis izvršenih transakcija nad podacima. Nakon što kopira taj zapis, zapis izvršenih promjena izbaci dio zapisa izvršenih transakcija, koji nije potreban aktivnim transakcijama. Prema [3], zapis izvršenih promjena je sigurnosna kopija zapisa izvršenih transakcija koji uključuje sve zapise izvršenih transakcija koji nisu bili kopirani u prethodnom zapisu izvršenih promjena.



Sl. 2.3.: Princip izrade zapisa izvršenih promjena [2]

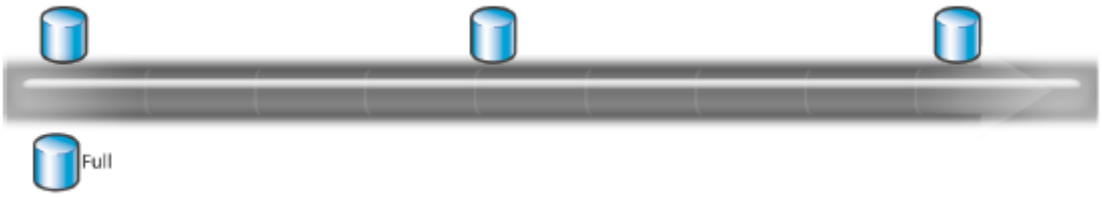
Pri određivanju sigurnosne strategije za izradu i rukovanje sigurnosnom kopijom podataka, jedno od glavnih razmatranja je mjera tolerancije potencijalnog gubitka podataka u slučaju problema. Ako je tolerancija, primjerice 24 sata, tada je dovoljno napraviti jednu potpunu sigurnosnu kopiju izvan radnog vremena organizacije. No, ako je tolerancija na izloženost riziku gubitka podataka znatno niža od toga, potpunoj sigurnosnoj kopiji je potrebno dodati zapis izvršenih promjena.

2.4. Kombinirani tipovi sigurnosnih kopija podataka

Prilikom formiranja strategije za izradu i rukovanje sigurnosnom kopijom podataka, administrator baza podataka uzima u obzir plan povratka podataka organizacije, a na raspolaganju su mu tri osnovne vrste sigurnosne kopije. Kako bi postigao optimalan rezultat, s obzirom na odnos postavljenih poslovnih zahtjeva i pripadajućih troškova, administrator baza podataka mora kombinirati osnovne vrste sigurnosnih kopija. Iz tog kombiniranja proizlaze kombinirani tipovi sigurnosnih kopija podataka. Funkcionalni kombinirani tipovi sigurnosnih kopija podataka su: jednostavna potpuna sigurnosna kopija, kombinacija zapisa izvršenih promjena i potpune sigurnosne kopije (dva načina), kombinacija potpune sigurnosne kopije, diferencijalne sigurnosne kopije i zapisa izvršenih promjena.

2.4.1. Potpuna sigurnosna kopija podataka – jednostavan način

U ovom kombiniranom tipu sigurnosne kopije podataka, administrator baza podataka kombinira više potpunih sigurnosnih kopija podataka. To je najjednostavniji kombinirani tip sigurnosnih kopija podataka jer je oporavak podataka u ovom tipu najjednostavniji. No, to je ujedno tip kojem treba najviše vremena za izradu sigurnosne kopije i nije moguć u većini slučajeva. Osnovni princip izvođenja ovog tipa je periodična izrada potpunih sigurnosnih kopija podataka.



Sl. 2.4.: Raspored izrade kombinacije potpune sigurnosne kopije podataka [5]

Kombinacija više sigurnosnih kopija podataka se koristi u sljedećim slučajevima:

- U razvojnim bazama podataka (engl. *Development databases*) – baze podataka koje se koriste u izradi ili testiranju okruženja, pri čemu si organizacija može priuštiti gubitak dijela radnog vremena
- U razinskim bazama podataka (engl. *Stage databases*) – baze podataka koje se koriste za posredno pohranjivanje podataka prilikom prijenosa između izvora i skladišta podataka

- U bazama podataka koje služe samo za čitanje (engl. *Read only databases)* – baze podataka koje sadrže podatke samo za čitanje, npr. pretplatničke baze podataka u koje se pohranjuju podaci za potrebe izvješćivanja
- U sistemskim bazama podataka (engl. *System databases*) – glavna (izvorna) baza podataka organizacije ili distribucijske baze podataka

2.4.2. Zapis izvršenih promjena i potpuna sigurnosna kopija podataka (engl. *Log & Full Backup*)

Ovaj kombinirani tip sigurnosnih kopija podataka je po principu djelovanja sličan kombinaciji više potpunih sigurnosnih kopija podataka. Razlika je u tome što se izradi zapis izvršenih promjena neposredno prije potpune sigurnosne kopije podataka. Takav pristup ima prednost u kopiranju ne samo podataka, nego i promjena koje su se dogodile od zadnje potpune sigurnosne kopije podataka. Ovaj kombinirani tip sigurnosnih kopija podataka se koristi u organizacijama kojima podaci nisu neprestano potrebni, tj. nisu potrebni izvan radnog vremena.

Sl. 2.5.: Raspored izrade zapisa izvršenih promjena i potpune sigurnosne kopije podataka [5]

Prednosti ovog kombiniranog tipa sigurnosnih kopija podataka su:

1. Ako se podaci i zapisi izvršenih promjena nalaze na odvojenim fizičkim medijima, moguće je, u slučaju oštećenja medija na kojima se nalaze podaci, kopirati zapis izvršenih promjena i ne izgubiti sve podatke.
2. U slučaju kvara programske opreme, ljudske pogreške ili proboja sigurnosti, administrator baza podataka može prvo izraditi zapis izvršenih promjena i povratiti podatke do određene točke u vremenu (posljednje poznato pouzdano stanje), smanjujući količinu izgubljenih podataka.
3. Ako baza podataka sadrži više datoteka i dogodi se kvar na jednoj od njih, moguće je pomoću zapisa izvršenih promjena i posljednje potpune sigurnosne kopije podataka,

povratiti samo oštećenu datoteku i zapis izvršenih transakcija, kako bi se očuvao transakcijski integritet.

4. Zapis izvršenih transakcija u ovom kombiniranom tipu sigurnosnih kopija podataka može biti iskorišten u forenzičkoj analizi – analizi strukturiranih podatka u cilju otkrivanja financijskog kriminala.

2.4.3. Potpuna sigurnosna kopija i zapis izvršenih promjena (engl. *Full & Log Backup*)

U ovom kombiniranom tipu sigurnosnih kopija podataka, administrator baza podataka izrađuje jednu potpunu sigurnosnu kopiju podataka i više zapisa izvršenih promjena između potpunih sigurnosnih kopija podataka. Prednost ovakvog pristupa je smanjenje količine izgubljene informacije u slučaju potpunog oštećenja poslužitelja, jer se zapisi izvršenih promjena mogu češće izrađivati nego potpune sigurnosne kopije podataka. Ovaj kombinirani tip sigurnosnih kopija podataka se koristi u organizacijama kojima podaci nisu neprestano potrebni, kao i obrnuta kombinacija ova dva jednostavna tipa sigurnosnih kopija podataka. No, također se koristi i u organizacijama u kojima su podaci neprestano na raspolaganju, ali moraju biti nepromjenjivi.

Sl. 2.6.: Raspored izrade potpune sigurnosne kopije podataka i zapisa izvršenih promjena [5]

Razlika ovog kombiniranog tipa sigurnosnih kopija podataka u odnosu na prethodni je što izrada zapisa izvršenih promjena nakon izrade potpune sigurnosne kopije podataka zahtjeva oporavak podataka pomoću posljednje potpune sigurnosne kopije podataka i posljednja dva zapisa izvršenih transakcija. To rezultira većom složenošću i dugotrajnijim procesom oporavka podataka, no količina oporavljenih podataka je veća nego u prethodnom kombiniranom tipu sigurnosnih kopija podataka.

2.4.4. Kombinacija svih osnovnih tipova sigurnosnih kopija podataka

Ponekad su podaci, pohranjeni u bazi podataka, toliko vrijedni da je potrebno izrađivati sigurnosnu kopiju podataka vrlo često. No, oslanjanje na kombinaciju potpune sigurnosne kopije podataka i zapisa izvršenih promjena nije izvedivo s obzirom na raspoložive resurse, jer je, u slučaju problema, potrebno povratiti podatke iz svakog zapisa izvršenih promjena od posljednje potpune sigurnosne kopije podataka. U tom slučaju se koristi kombinacija sva tri tipa osnovnih sigurnosnih kopija podataka. U ovoj kombinaciji sigurnosnih kopija podataka, najčešće se izrađuje zapis izvršenih promjena, zatim diferencijalna sigurnosna kopija podataka pa potpuna sigurnosna kopija podataka.

Sl. 2.7.: Raspored izrade kombinacije potpune sigurnosne kopije, diferencijalne sigurnosne kopije i zapisa izvršenih promjena [5]

Količina potpunih sigurnosnih kopija podataka se pokušava minimalizirati, no pri tome veličina diferencijalnih sigurnosnih kopija ne smije nadmašiti zadano ograničenje. Diferencijalna sigurnosna kopija se izrađuje onoliko puta koliko je potrebno da se minimalizira vrijeme oporavka podataka iz zapisa izvršenih promjena. Zapis izvršenih promjena se izrađuje do te mjere koliko je potrebno da bi se smanjila izloženost gubitku podataka. Prema [5], odnos učestalosti izrade osnovna tri tipa sigurnosnih kopija podataka pokazuju sljedeći primjeri implementacije ovog kombiniranog tipa sigurnosnih kopija:

1) Potpuna sigurnosna kopija svaki mjesec, diferencijalna sigurnosna kopija svaku noć, zapis izvršenih promjena svaka dva sata.
2) Potpuna sigurnosna kopija svaki tjedan, diferencijalna sigurnosna kopija svakih šest sati, zapis izvršenih promjena svakih 15 minuta.

3. STRATEGIJE IZRADE SIGURNOSNIH KOPIJA PODATAKA

3.1. Kategorije sigurnosnih kopija podataka

Sigurnosne kopije podataka se ne moraju uvijek vršiti nad bazom podataka neke organizacije. Cilj izrade sigurnosne kopije podataka je sačuvati podatke organizacije u slučaju problema te omogućiti oporavak podataka. Ukoliko je potrebno povratiti samo određene podatke, oporavak svih podataka baze podataka predstavljao bi neefikasno trošenje resursa, što bi rezultiralo ekonomskim smanjenjem dobiti organizacije.

Upravo zato, jedna od osnovnih zadaća administratora baza podataka je osmisliti strategiju izrade sigurnosnih kopija podataka. Prema [6], s obzirom na strukturu podataka koja se kopira, sigurnosne kopije podataka se dijele na tri kategorije:

1) Sigurnosne kopije baza podataka (engl. *Database backups*)
2) Zapis izvršenih transakcija (engl. *Transaction log backups*)
3) Sigurnosne kopije datoteka (engl. *File backups*).

Kombinirajući osnovne i kombinirane tipove sigurnosnih kopija podataka unutar tri osnovne kategorije sigurnosnih kopija podataka, administrator baza podataka formira strategije izrade sigurnosnih kopija podataka. Samo određene kombinacije tipova i kategorija sigurnosnih pohrana podataka su funkcionalne i one čine osnovnu podjelu strategija izrade sigurnosnih kopija podataka.

3.2. Sigurnosne kopije baza podataka

Jedna od tri kategorije sigurnosnih kopija podataka je sigurnosna kopija baze podataka. Prema [1], baza podataka je organizirano skladište podataka u kojem su podaci dostupni preko imenovanih podatkovnih elemenata (npr., polja, zapisi, datoteke). Funkcionalne sigurnosne kopije baza podataka su potpuna sigurnosna kopija baze podataka i diferencijalna sigurnosna kopija baze podataka. Potpuna sigurnosna kopija baze podataka sadrži cijelu bazu podatka u trenutku kad je izvršena. Diferencijalna sigurnosna kopija baze podataka sadrži samo promjene načinjene u bazi podataka od posljednje potpune sigurnosne kopije baze podataka.

3.2.1. Potpuna sigurnosna kopija baze podataka

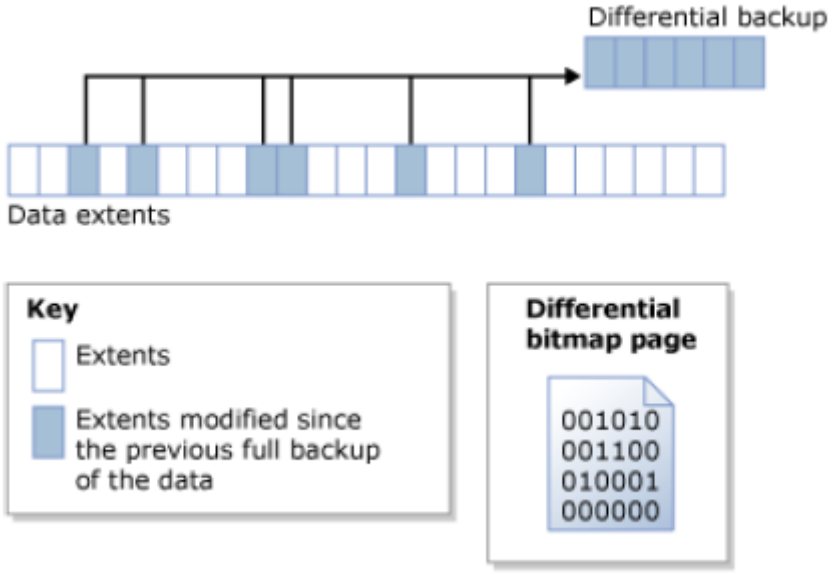
Potpuna sigurnosna kopija baze podataka kopira cijelu bazu podataka. Prema [6], potpuna sigurnosna kopija baze podataka je arhiva baze podataka, koja sadrži: kopiju baze podataka u trenutku kada se izvrši, sve korisničke objekte i podatke, sistemske informacije važne za bazu podataka, dio zapisa izvršenih transakcija. Dio zapisa izvršenih transakcija je važan zbog toga što je, uz potpunu sigurnosnu kopiju baze podataka, potreban kako bi se cjelovita baza podatka povratila u slučaju problema.

Prema [6], potpuna sigurnosna kopija baze podataka se izvršava u sljedećim slučajevima:

1) Kada je potreban potpuni oporavak baze podataka
2) Prilikom postavljanja razvojnog projekta u proizvodnju
3) Prilikom osvježavanja sustava procjene kvalitete s novim proizvodnim podacima za uporabu u testiranju novih procesa ili promjena u procesima

3.2.2. Diferencijalna sigurnosna kopija baze podataka

Diferencijalna sigurnosna kopija baze podataka je kopija svake stranice baze podataka koja se promijenila od posljednje potpune sigurnosne kopije baze podataka. To znači da veličina diferencijalne sigurnosne kopije ovisi o količini podataka koji su se promijenili od posljednje potpune sigurnosne kopije. Što je posljednja potpuna sigurnosna kopija starija, diferencijalna sigurnosna kopija će biti veća.



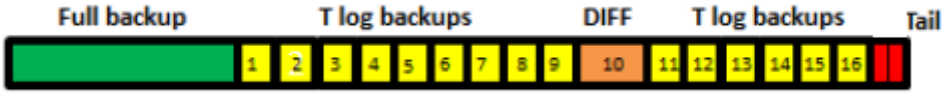
Sl. 3.1.: Princip izrade diferencijalne sigurnosne kopije baze podataka [3]

Slika 3.1. prikazuje princip izrade diferencijalne sigurnosne kopije baze podataka. Prikazano je 24 podatkovna polja, od kojih su šest označeni kao promijenjeni od posljednje potpune sigurnosne kopije baze podataka. Izrada diferencijalne sigurnosne kopije baze podataka oslanja se na stranicu polja bitova (engl. *bitmap page*) koja sadrži jedan bit za svako podatkovno polje. Za svako podatkovno polje koje je promijenjeno od posljednje potpune sigurnosne kopije baze podataka, pripadni bit se postavlja na vrijednost jedan u stranici polja bitova. Diferencijalna sigurnosna kopija baze podataka se sastoji samo od podatkovnih polja za koja su pripadni bitovi u stranici polja bitova postavljeni na vrijednost jedan.

Izrada diferencijalne sigurnosne kopije baze podataka može biti vrlo brza u odnosu na izradu potpune sigurnosne kopije baze podataka. Međutim, prije oporavka podataka iz diferencijalne sigurnosne kopije baze podataka, potrebno je povratiti podatke iz posljednje potpune sigurnosne kopije baze podataka. Kako veličina diferencijalne sigurnosne kopije baze podatka raste prilikom svakog sljedeće izrade, ona na taj način gubi prednosti u odnosu na potpunu sigurnosnu kopiju baze podataka, a to su brži oporavak podataka i manje iskorištenje resursa. Stoga je potrebno periodično izrađivati potpune sigurnosne kopije baze podataka, u zadanim intervalima, kako bi se uspostavila nova diferencijalna sigurnosna kopija baze podataka s karakterističnim prednostima u odnosu na potpunu sigurnosnu kopiju baze podataka.

Sl. 3.2.: Lanac sigurnosnih kopija baze podataka [6]

Prema [6], primarni razlog zašto administratori baza podataka izrađuju diferencijalnu sigurnosnu kopiju baza podataka je što na taj način, smanjuju broj zapisa izvršenih promjena koji bi se morali povratiti u slučaju problema. Slika 3.2. pokazuje lanac sigurnosnih kopija baza podataka koje bi se morale povratiti u slučaju kada se organizacijska strategija izrade sigurnosnih kopija baza podataka sastoji od: noćne potpune sigurnosne kopije u 02:00 sati i zapisnika izvršenih promjena svaki idući sat. Ako se problem dogodi u 18:15 sati, potrebno je povratiti 17 sigurnosnih kopija (16 zapisa izvršenih promjena i jednu potpunu sigurnosnu kopiju) i zapis izvršenih promjena koje nisu kopirane (engl. *tail log backup*).



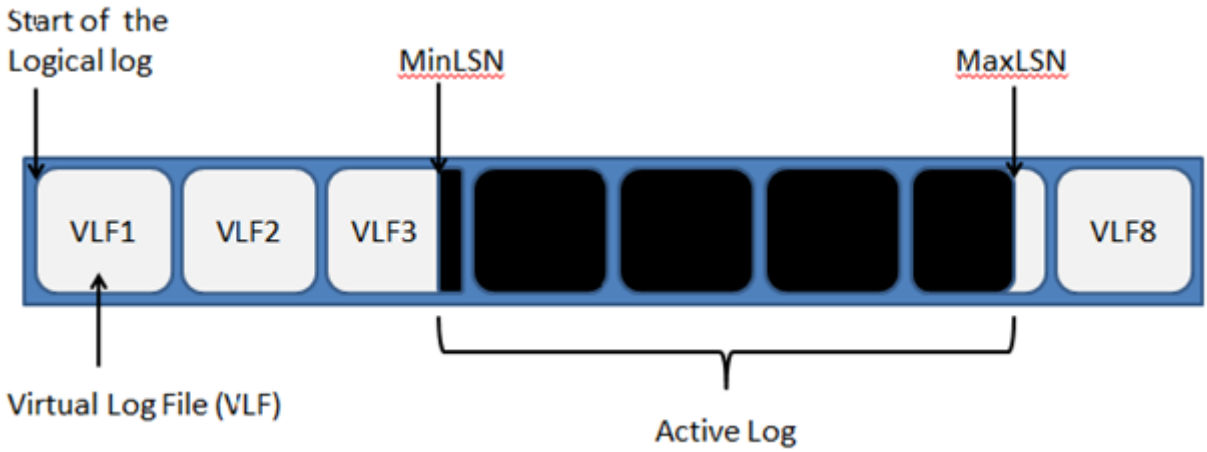
Sl. 3.3.: Modificirani lanac sigurnosnih kopija baze podataka [6]

Broj sigurnosnih kopija koje je potrebno povratiti u slučaju problema, poželjno je svesti na minimum, jer što je veći broj sigurnosnih kopija, veća je vjerojatnost da je jedna od tih kopija neupotrebljiva. Slika 3.3. pokazuje istu organizacijsku strategiju kao i slika 3.2., s time da je u 12:00 sati svakoga dana uvedena diferencijalna sigurnosna kopija baze podataka. Na taj način je potrebno povratiti samo osam sigurnosnih kopija (jedna potpuna sigurnosna kopija, jedna diferencijalna sigurnosna kopija i šest zapisa izvršenih promjena) i zapis izvršenih promjena koje nisu kopirane.

3.3. Zapis izvršenih transakcija

Zapis izvršenih transakcija podrazumijeva pohranu zapisa transakcija koje su se izvršile od posljednje izrade potpune sigurnosne kopije baze podataka. Stoga je potrebno izraditi barem jednu potpunu sigurnosnu kopiju baze podataka kako bi bilo moguće izraditi zapis izvršenih transakcija. Svaki zapis izvršenih transakcija sadrži detalje specifičnih promjena koje se odnose na kreiranje i izmjenu objekata (engl. *Data definition language*), kao i na svaku izmjenu podataka (engl. *Data modification language*).

Zapisi izvršenih transakcija se zapisuju slijedno, za razliku od podataka koji se kopiraju na neodređen, nasumičan način. Zbog takvog načina zapisivanja, u slučaju oporavka podataka, moguće je povratiti operacije nad podacima ili objektima, istim redoslijedom kao što su se i izvršile. Redoslijed obavljanja transakcija je bitan kao i sama funkcija transakcije, jer različiti redoslijedi istih transakcija mogu dati različite rezultate. Na taj način, moguće je povratiti bazu podataka u točno određeno poželjno stanje, pod uvjetom da su podaci očuvani.



Sl. 3.4.: Unutarnja struktura zapisa izvršenih transakcija [6]

Svaki pojedinačni zapis u zapisu izvršenih transakcija je označen slijednim brojem zapisa (engl. *Log Sequence Number*). Prvi pojedinačni zapis označava početak, a posljednji dodani pojedinačni zapis označava kraj zapisa izvršenih transakcija. Prema slici 3.4., vidljivo je kako su pojedinačni zapisi povezani u lanac s pokazivačima na prethodnu i sljedeću transakciju. Također, na slici 3.4., zapisi izvršenih transakcija su podijeljeni u osam sekcija zvanih virtualne datoteke zapisa (engl. *virtual log files*) i označen je aktivni dio zapisa (engl. *active log*). Virtualna

datoteka zapisa može biti ili aktivna, ako sadrži jedan dio aktivnog zapisa, ili neaktivna ako ne sadrži dio aktivnog zapisa.

Bilo koji zapis koji je povezan uz trenutno otvorenu transakciju i potreban je za trenutni oporavak podataka, dio je aktivnog zapisa. Najmanji slijedni broj aktivnog zapisa označava najstariji pojedinačni zapis koji je potreban za uspješan povratak baze podataka u stanje u kojem se odvija transakcija koja je povezana uz aktivni zapis. Najveći slijedni broj aktivnog zapisa označava njegov kraj.

Primarni razlog za izradu zapisa izvršenih transakcija je očuvanje transakcija koje su se dogodile od posljednje potpune sigurnosne kopije baze podataka, kako bi se pomoću tih transakcija baza podataka mogla dovesti u prijašnje stabilno stanje. Međutim, zapisi izvršenih transakcija mogu biti korisni u smanjivanju vremena potrebnog za premještanje podataka s jednog poslužitelja na drugi (engl. *database migrations*) i za dostavljanje izvješća od proizvodnog okružja, pomoću dostave zapisa (engl. *log shipping*). Dostava zapisa funkcionira tako da, prilikom premještanja podataka s jednog poslužitelja na drugi, dovoljno je samo kopirati trenutne podatke sa izvornog poslužitelja na odredišni i odredišnom poslužitelju dostaviti zapis izvršenih transakcija, pomoću kojeg može povratiti bazu podataka u željeno stanje.

3.4. Sigurnosne kopije datoteka

Sigurnosne kopije datoteka se koriste kada je baza podataka toliko velika da je utrošak resursa na izradu sigurnosne kopije baze podataka veći od količine raspoloživih resursa. Pri tome se ne računa utrošak resursa na temeljnu sigurnosnu kopiju baze podataka. U tom slučaju, sigurnosne kopije podataka se ne izrađuju nad cijelom bazom podataka, nego nad nekim njenim određenim dijelovima. Sigurnosne kopije datoteka ne kopiraju bazu podataka, nego jednu ili više datoteka koje su dio baze podataka.

Ova strategija sigurnosne kopije podataka se može koristiti u svrhu ubrzanja procesa oporavka podataka, u slučaju kada se ošteti medij na kojem je pohranjen samo dio baze podataka. Tada nema potrebe za oporavkom svih podataka, pošto svi podaci nisu izgubljeni, nego samo oni pohranjeni na oštećenom mediju. Osnovni zahtjev prilikom izrade sigurnosne kopije datoteka je da podaci sadržani u toj kopiji mogu biti dostupni samo za čitanje ili se takva sigurnosna kopija mora koristiti u kombinaciji sa zapisom izvršenih transakcija kako bi se očuvao transakcijski integritet baze podataka. Razlog tomu je što sigurnosne kopije datoteka ne kopiraju zapis izvršenih transakcija.

Funkcionalne sigurnosne kopije datoteka su : potpuna sigurnosna kopija datoteka (engl. *Full file backup*), diferencijalna sigurnosna kopija datoteka (engl. *Differential file backup*), djelomična sigurnosna kopija datoteka (engl. *Partial backup*) i djelomična diferencijalna sigurnosna kopija datoteka (engl. *Differential partial backup*).

3.4.1. Potpuna sigurnosna kopija datoteka

Potpuna sigurnosna kopija datoteka kopira sve podatke i objekte u naznačenoj datoteci ili grupi datoteka. Kombinacija svih potpunih sigurnosnih kopija datoteka sa svim zapisima izvršenih promjena je ekvivalentna potpunoj sigurnosnoj kopiji baze podataka. Broj potpunih sigurnosnih kopija datoteka ovisi o veličini baze podataka, broju datoteka i rasporedu izrade sigurnosnih kopija datoteka.

Prema [3], potpune sigurnosne kopije datoteka pružaju sljedeće prednosti u odnosu na potpune sigurnosne kopije baze podataka:

- Korištenje potpunih sigurnosnih kopija datoteka može povećati brzinu oporavka dopuštajući oporavak samo oštećenih datoteka, bez potrebe za oporavkom cijele baze podataka
- Korištenje potpunih sigurnosnih kopija datoteka povećava fleksibilnost u sastavljanju rasporeda strategije izrade sigurnosnih kopija i u rukovanju s medijima za pohranu podataka

Nedostaci potpune sigurnosne kopije datoteka u odnosu na potpunu sigurnosnu kopiju baze podataka su:

- Dodatna administrativna složenost u procesima održavanja i praćenja kompletnog seta sigurnosnih kopija, koja može nadmašiti potrebe za resursima potpune sigurnosne kopije baze podataka
- Oštećenje jednog fizičkog medija može učiniti cijelu bazu podataka nepopravljivom ukoliko datoteka na oštećenom mediju nije sigurnosno kopirana

Samo jedna potpuna sigurnosna kopija datoteke se može izrađivati u nekom trenutku. Moguće je napraviti sigurnosnu kopiju grupe datoteka (engl. *filegroup*), ali takvoj sigurnosnoj kopiji je potrebno više vremena za oporavak podataka i više vremena za pronalaženje točno određene datoteke. Princip izrade potpune sigurnosne kopije datoteke i grupe datoteka je jednak.

3.4.2. Diferencijalna sigurnosna kopija datoteka

Diferencijalna sigurnosna kopija datoteka kopira samo one stranice baze podataka u specificiranim datotekama za kopiranje, koje su promijenjene od posljednje potpune sigurnosne kopije datoteka. Kao i u kategoriji baza podataka, diferencijalna sigurnosna kopija datoteka može smanjiti broj zapisa izvršenih promjena nad datotekama, koje su potrebne prilikom oporavka tih datoteka. Koristi se kao dio strategije za izradu sigurnosnih kopija datoteka, jer zahtjeva mnogo manje vremena za obradu nego potpuna sigurnosna kopija datoteka i također zauzima manje resursa.

U odnosu na diferencijalnu sigurnosnu kopiju baze podataka, prednost diferencijalne sigurnosne kopije datoteka je kraće vrijeme izvođenja i mogućnost kopiranja promjena u točno određenim datotekama. Također, ako je broj datoteka koje se kopiraju manji od ukupnog broja datoteka baze podataka, diferencijalna sigurnosna kopija datoteka će zauzimati manje resursa nego

diferencijalna sigurnosna kopija baze podataka. Ukoliko se dogodi oštećenje jednog dijela baze podataka, pomoću diferencijalne sigurnosne kopije datoteka, moguće je povratiti samo podatke sa oštećenih datoteka, zajedno s njihovim promjenama koje su se dogodile od posljednje izrade potpune sigurnosne kopije datoteka.

3.4.3. Djelomična sigurnosna kopija datoteka

Djelomična sigurnosna kopija datoteka je slična potpunoj i diferencijalnoj sigurnosnoj kopiji datoteka jer omogućuje kopiranje dijela baze podataka, bez potrebe za kopiranjem cijele baze podataka. Međutim, dok potpuna i diferencijalna sigurnosna kopija omogućuju kopiranje određenih i individualnih datoteka, djelomična sigurnosna kopija datoteka je samo kopija primarne grupe datoteka i svih datoteka za čitanje i pisanje, izostavljajući one datoteke koje služe samo za čitanje. To znači da je djelomična sigurnosna kopija datoteka značajna samo za baze podataka koje sadrže datoteke koje se mogu samo čitati. U protivnom, djelomična sigurnosna kopija datoteka sadrži jednak broj podataka i objekata baze podataka, kao i potpuna sigurnosna kopija baze podataka.

Isti rezultat izvođenja djelomične sigurnosne kopije datoteka se može ostvariti izradom odvojenih potpunih sigurnosnih kopija datoteka za svaku datoteku koja se može čitati i pisati. Međutim, prilikom izvođenja potpunih sigurnosnih kopija datoteka, potrebno je izraditi i zapise izvršenih transakcija, pa to može predstavljati nepotrebnu dodatnu složenost. U slučaju izrade djelomične sigurnosne kopije datoteka, zapis izvršenih transakcija je potreban samo ako je potreban oporavak baze podataka u točno određeno prijašnje stanje.

3.4.4. Diferencijalna djelomična sigurnosna kopija datoteka

Diferencijalna djelomična sigurnosna kopija datoteka je diferencijalna sigurnosna kopija datoteka, čija je temeljna sigurnosna kopija podataka djelomična sigurnosna kopija datoteka. Diferencijalne sigurnosne kopije svake kategorije se mogu izvršavati tek nakon što postoji temeljna sigurnosna kopija podataka te kategorije. Za razliku od ostalih strategija, gdje je temeljna sigurnosna kopija uvijek potpuna sigurnosna kopija određene kategorije, u ovoj strategiji to je djelomična sigurnosna kopija datoteka.

Princip izrade diferencijalne djelomične sigurnosne kopije datoteka je jednak kao i kod diferencijalne kopije datoteka. No, kopiranje se vrši samo nad datotekama baze podataka koje se mogu čitati i pisati, ne i nad datotekama koje služe samo za čitanje. Diferencijalna djelomična sigurnosna kopija datoteka i djelomična sigurnosna kopija datoteka koriste se u bazama podataka koje sadrže velik broj datoteka koje se mogu samo čitati. Odluka o izradi potpune ili djelomične sigurnosne kopije datoteka, nad takvim bazama podataka, predstavlja razliku u upotrebi tih dviju strategija za izradu sigurnosnih kopija podataka.

4. IZRADA VLASTITOG RUKOVODSTVA SIGURNOSNIM KOPIJAMA

4.1. Koraci izrade vlastitog rukovodstva sigurnosnim kopijama

Jedna od ključnih zadaća administratora baza podataka je pripremiti uvjete u organizaciji koji bi omogućili efikasno djelovanje u slučaju potencijalnog problema. Kako bi temeljito pripremio takve uvjete u organizaciji, administrator baza podataka mora izvršiti točno određene procedure, u određenom redoslijedu. Prema [7], popis procedura koje administrator baza podataka mora izvršiti je sljedeći:

1. Razvijanje strategije za izradu sigurnosnih kopija
2. Redovito upravljanje sigurnosnim kopijama
3. Izvršavanje periodičnih testiranja povratka baze podataka
4. Sklapanje ugovora o razini usluge, koju mora izvršiti, s rukovodstvom organizacije
5. Izrada plana povratka podataka
6. Nadograđivanje svojeg znanja o bazama podataka i sigurnosnim kopijama

Prve dvije procedure koje administrator baza podataka mora izvršiti, čine jedinstven posao, koji se naziva rukovodstvo sigurnosnim kopijama (engl. *Backup management*). Razvijanje strategije za izradu sigurnosnih kopija uključuje sljedeće korake:

- Odabir podataka koji trebaju biti sigurnosno kopirani
- Izabrati odgovarajući tip sigurnosne kopije
- Odabir kategorije sigurnosne kopije
- Izrada rasporeda izrade sigurnosnih kopija
- Odabir mjesta spremanja sigurnosnih kopija
- Odabir tolerancije na gubitak podataka

Nakon što izradi odgovarajuću strategiju za izradu sigurnosnih kopija, administrator baza podataka mora redovito upravljati izrađenim sigurnosnim kopijama. Rukovanje sigurnosnim kopijama podrazumijeva sljedeće korake:

- Automatizacija izrade sigurnosnih kopija po zakazanom rasporedu

- Uspostavljanje nadzornog programa koji obavještava administratora baza podataka o neuspješnim izradama sigurnosnih kopija
- Periodično izvršavanja zapisa izvršenih promjena
- Uklanjanje nepotrebnih sigurnosnih kopija
- Potvrđivanje i verifikacija izrađenih sigurnosnih kopija
- Arhiviranje izrađenih sigurnosnih kopija

Izrada rukovodstva sigurnosnim kopijama moguća je pomoću različitih tehnologija i programa dizajniranih za tu specifičnu primjenu. No, ukoliko administrator baza podataka, osim rukovođenja bazom podataka, ima i drugih poslova vezanih uz bazu podataka, efikasnije je izraditi rukovodstvo sigurnosnim kopijama u istom okružju. Ti poslovi mogu biti izrada baze podataka, konfiguriranje, upravljanje, pristupanje i manipuliranje podacima u bazi podataka i kreiranje objekata u bazi podataka. Jedna od najpoznatijih tehnologija koje se primjenjuje za izradu tih poslova je *SQL Server Management Studio* okruženje.

4.2. Izrada vlastitog rukovodstva sigurnosnim kopijama koristeći *SQL Server Management Studio*

Prema [8], *SQL Server Management Studio* je integrirano okruženje za pristupanje, konfiguriranje, upravljanje, vođenje i razvijanje svih komponenata *SQL* poslužitelja i *SQL* baza podataka. Okruženje sadrži i urednike skripta i grafičke alate koji rade s objektima i značajkama poslužitelja. Centralna značajka je istraživač objekata (engl. *Object explorer*) koji omogućuje korisniku pretraživanje, pregledavanje i odabir bilo kojeg objekta unutar servera.

Prvi korak u radu s *SQL Server Management Studio* okruženjem je povezati se na poslužitelj. Za uspostavu rada poslužitelja moguće je instalirati značajke programa *Microsoft SQL Server* i izabrati određeni tip ovjere autentičnosti. U ovom slučaju, izabrana je ovjera autentičnosti preko postojećeg korisničkog računa, operacijskog sustava *Windows*.

Za potrebe izrade vlastitog rukovodstva sigurnosnim kopijama, izrađena je baza podataka u *SQL Server Management Studio* okruženju. Također, samo radi primjera izrade vlastitog rukovodstva, izabrana strategija izrade sigurnosnih kopija je kombinacija potpune sigurnosne kopije baze podataka i zapisa izvršenih promjena. Baza podataka u *SQL Server Management Studio* okruženju se može izraditi na dva načina: koristeći grafičko sučelje okruženja ili pišući skriptu u strukturiranom opisnom jeziku *SQL*. U ovom slučaju izabran je drugi način, čiji je programski kod dan u prilogu P.4.1.

Nakon izrade baze podataka, potrebno ju je popuniti inicijalnim podacima, kako bi bilo moguće izvršiti sigurnosnu kopiju. Baza podataka se popunjava s tri tablice koje sadrže jednostavne poruke i vremensku oznaku koja specificira kada su te poruke ubačene u bazu podataka. Popunjavanje se također izvršava pomoću opisnog jezika *SQL*. Programski kod koji implementira kreiranje tablica, dan je u prilogu P.4.2, a programski kod koji implementira popunjavanje tablica u prilogu P.4.3.

Tablica 4.1.: Primjer popunjene tablice

	Poruka	VremenskaOznaka
1	Ovo je inicijalna poruka za Tablicu1	2016-06-10 14:32:15.3400000
2	Ovo je inicijalna poruka za Tablicu1	2016-06-10 14:32:15.3400000
3	Ovo je inicijalna poruka za Tablicu1	2016-06-10 14:32:15.3400000
4	Ovo je inicijalna poruka za Tablicu1	2016-06-10 14:32:15.3400000
5	Ovo je inicijalna poruka za Tablicu1	2016-06-10 14:32:15.3400000
6	Ovo je inicijalna poruka za Tablicu1	2016-06-10 14:32:15.3570000
7	Ovo je inicijalna poruka za Tablicu1	2016-06-10 14:32:15.3570000
8	Ovo je inicijalna poruka za Tablicu1	2016-06-10 14:32:15.3570000
9	Ovo je inicijalna poruka za Tablicu1	2016-06-10 14:32:15.3570000
10	Ovo je inicijalna poruka za Tablicu1	2016-06-10 14:32:15.3570000

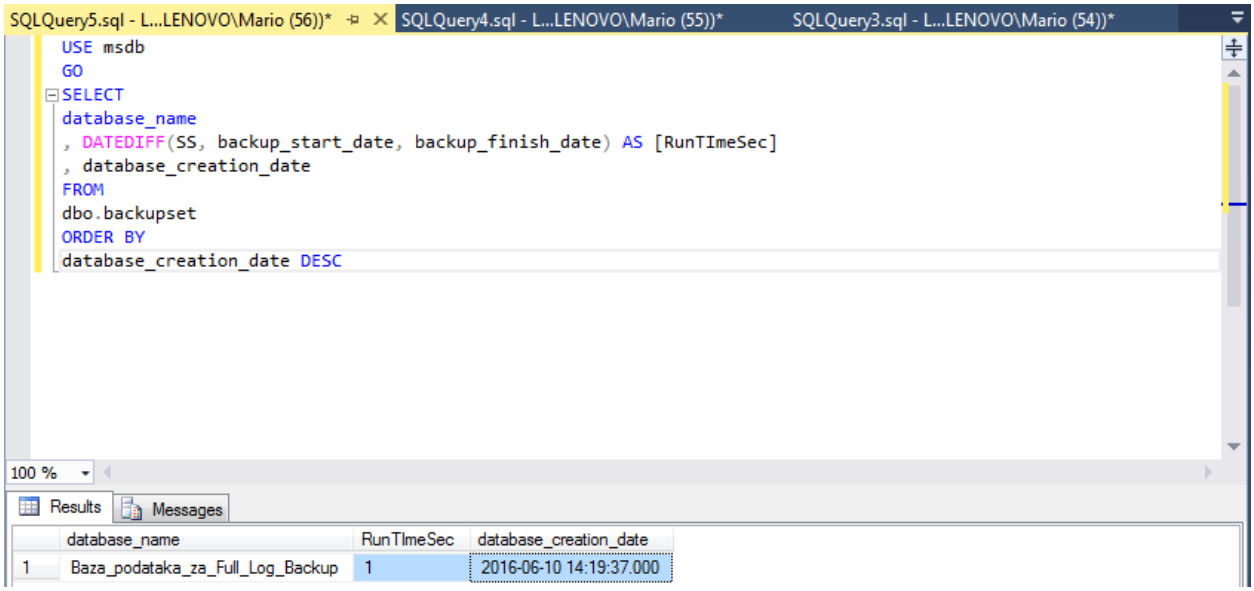
Izabrana strategija za izradu sigurnosnih kopija je izrada potpune sigurnosne kopije baza podataka i zapisa izvršenih promjena. Kako bi se mogao izvršiti zapis izvršenih promjena, potrebno je prvo izraditi potpunu sigurnosnu kopiju baze podataka koja tada predstavlja temeljnu sigurnosnu kopiju podataka. No, prije nego se izvrši potpuna sigurnosna kopija podataka, može se provjeriti kolika bi bila veličina potencijalnog zapisa izvršenih promjena, kako bi se mogla usporediti s veličinom stvarno izvršenog zapisa izvršenih promjena. Ispis veličina zapisa izvršenih promjena za sve postojeće baze podataka se postiže pomoću *DBCC SQLPERF (LOGSPACE)* naredbe.

Tablica 4.2.: Prikaz veličina svih zapisa izvršenih promjena prije izrade potpune sigurnosne kopije baze podataka

	Database Name	Log Size (MB)	Log Space Used (%)	Status
1	master	1,242188	40,8805	0
2	tempdb	0,4921875	63,09524	0
3	model	0,7421875	39,47368	0
4	msdb	2,742188	27,77778	0
5	Baza_podataka_za_Full_Log_Backup	49,99219	0,8477887	0

Potpuna sigurnosna kopija baze podataka izvršava se pomoću niza naredbi u *SQL* opisnom jeziku, koje su prikazane u prilogu P.4.4.

Tablica 4.3.: Primjer uspješno izvršene potpune sigurnosne kopije baze podataka



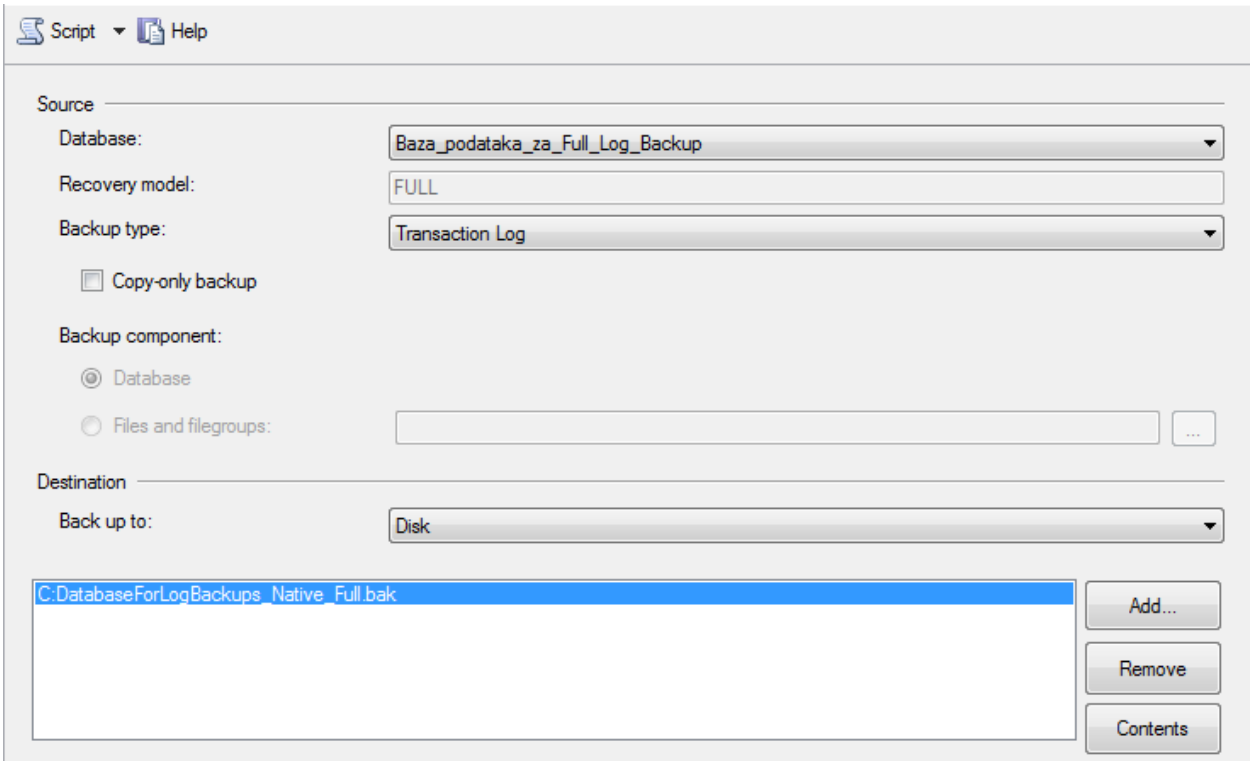
Tablica 4.4.: Prikaz veličina svih zapisa izvršenih promjena nakon izrade potpune sigurnosne kopije baze podataka

	Database Name	Log Size (MB)	Log Space Used (%)	Status
1	master	1,242188	42,13836	0
2	tempdb	0,4921875	63,09524	0
3	model	0,7421875	39,47368	0
4	msdb	2,742188	34,04559	0
5	Baza_podataka_za_Full_Log_Backup	49,99219	0,9239725	0

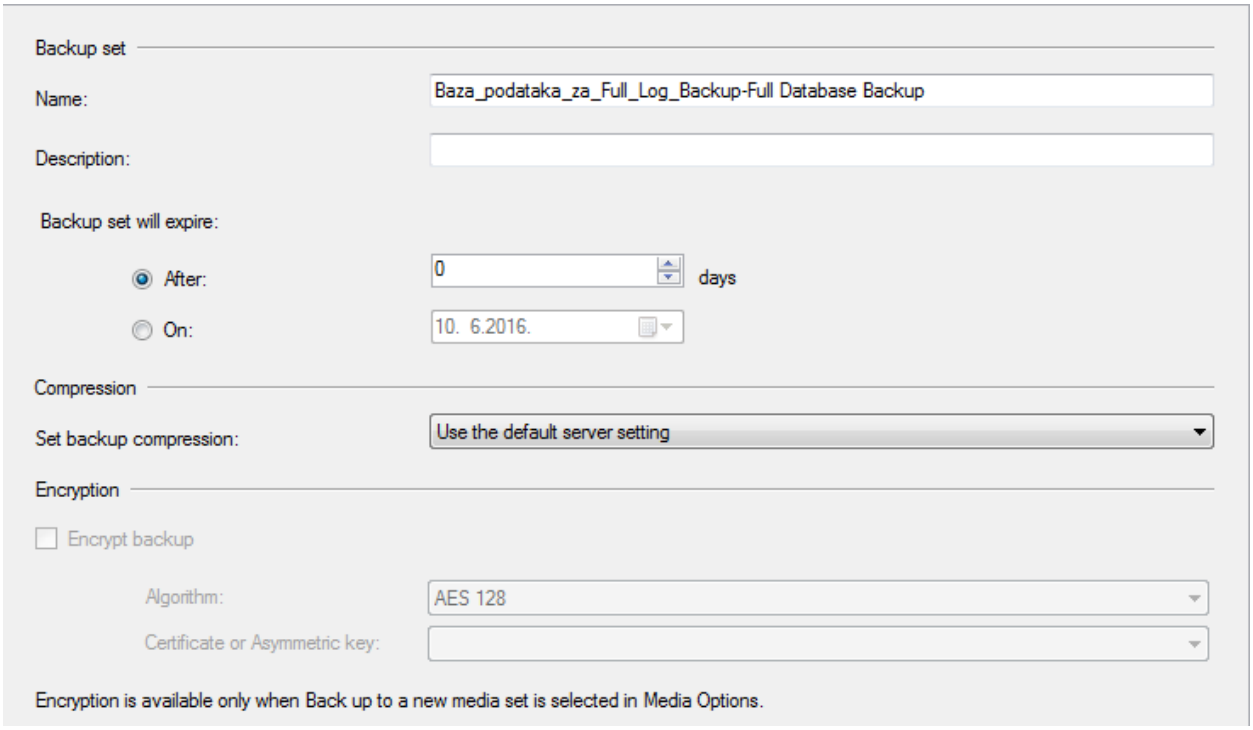
Iz tablice 4.3., može se zaključiti da je potpuna sigurnosna kopija baze podataka uspješno izvršena i to u periodu trajanje od jedne sekunde. Tablice 4.2. i 4.4., pokazuju veličine svih zapisa izvršenih promjena prije i nakon izrade potpune sigurnosne baze podataka. Uspoređujući prikazane podatke, vidljivo je da je veličina zapisa izvršenih promjena nakon izrade potpune sigurnosne kopije veća nego prije izrade potpune sigurnosne kopije baze podataka. Razlog tomu je što zapis izvršenih promjena bilježi izradu potpune sigurnosne kopije baze podataka i sama ta činjenica čini sadržaj zapisa izvršenih promjena. Tek nakon što utvrdi da je potpuna sigurnosna kopija baze podataka izrađena, zapis izvršenih promjena će se moći izraditi.

Nakon što je potpuna sigurnosna kopija baze podataka izvršena, potrebno je izraditi zapis izvršenih promjena. No, kako bi izrada tog zapisa imala smisla, prvo je potrebno izvršiti neke promjene u bazi podataka. To se postiže dodavanjem novih podataka u postojeće tablice, a programski kod implementacije dodavanja novih podataka prikazan je u prilogu P.4.5.

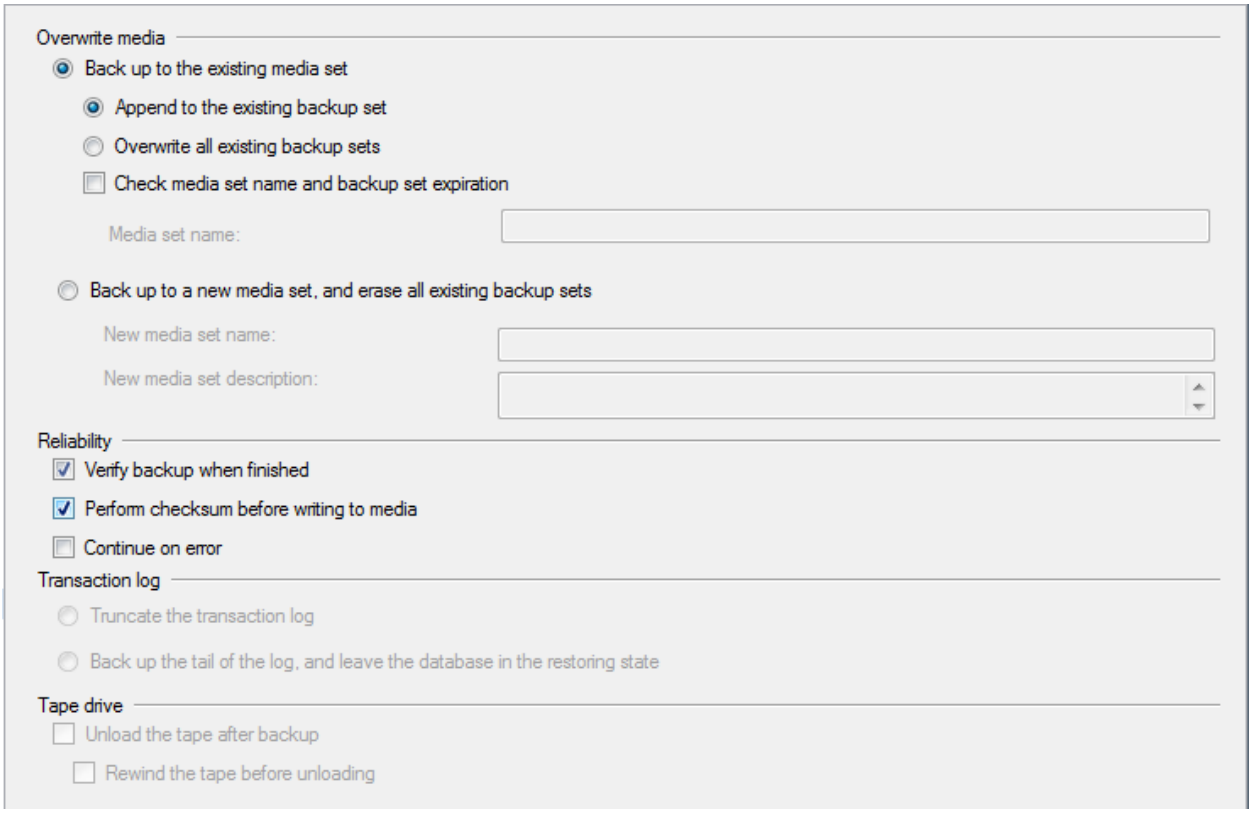
U ovom slučaju, zapis izvršenih promjena će se izraditi koristeći grafičko sučelje *SQL Server Management Studio* okruženja, kako bi se pokazala raznolikost mogućnosti tog okružja. U istraživaču objekata, potrebno je pronaći izrađenu bazu podataka i desnom klikom miša izabrati naredbu *Tasks – Backups*.



Sl. 4.1.: Izbornik za odabir tipa sigurnosne kopije podataka



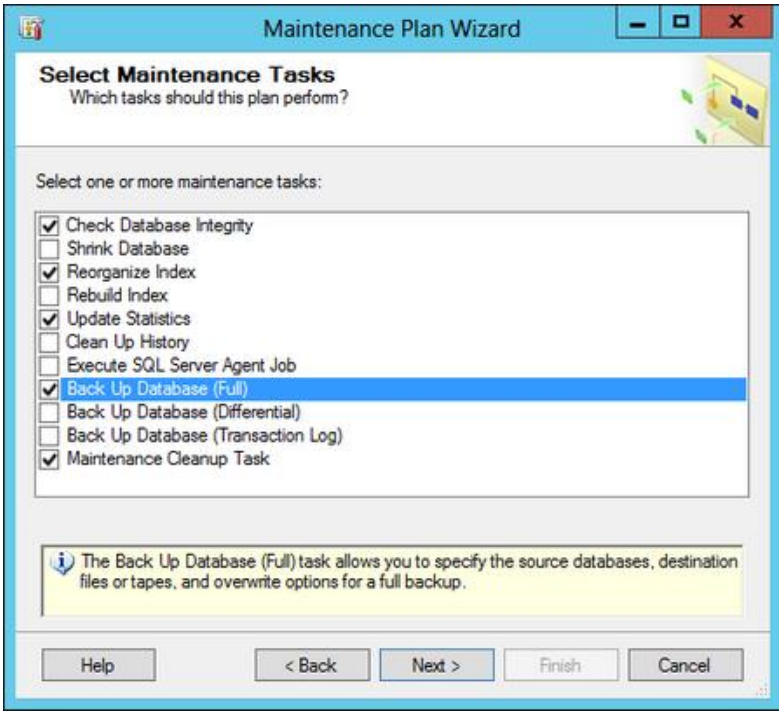
Sl. 4.2.: Izbornik za odabir svojstava sigurnosne kopije podataka



Sl. 4.3.: Izbornik za odabir svojstava medija za pohranu

Na slici 4.1. prikazan je izbornik u kojem se odabir tip sigurnosne kopije koja se izrađuje i on je postavljen na zapis izvršenih promjena. Na slici 4.2. prikazan je izbornik za odabir svojstava sigurnosne kopije podataka. Postavljeno je neograničeno vrijeme trajanja zapisa izvršenih promjena i svojstva kompresije podataka su postavljena na zadana od strane poslužitelja. Na slici 4.3. prikazan je izbornik za odabir svojstava medija na kojem će se pohraniti sigurnosna kopija podataka. Postavljen je medij za pohranu zapisa izvršenih promjena i odabrane su mogućnosti zaštitne provjere zapisa prije pohranjivanja na medij. Veličina zapisa izvršenih promjena se može saznati gledajući svojstva kopije na mjestu gdje je fizički pohranjena. U ovom slučaju to je 85 KB.

Na ovaj način izvršena je izrada potpune sigurnosne kopije baze podataka i zapisa izvršenih promjena. Kako bi strategija bila potpuno izvršena, potrebno je uspostaviti raspored izrade sigurnosnih kopija. U *SQL Server Management Studio* okruženju, to se postiže pomoću grafičkog sučelja. U istraživaču objekata, potrebno je proširiti datoteku *Management*, desnim klikom miša izabrati naredbu *Maintenance Plans – Maintenance Plan Wizard*. Nakon toga, otvara se izbornik prikazan na slici 4.4. u kojem se postavljaju željena svojstva rasporeda izrade sigurnosnih kopija. Nemoguće je unaprijed postaviti strategiju bez poznavanja svojstava baze podataka i načina korištenja podataka. U ovom poglavlju je pokazan samo primjer izrade kombinacije dvaju sigurnosnih kopija podataka.



Sl. 4.4.: Izbornik plana održavanja baze podataka

5. ZAKLJUČAK

U ovom završnom radu, ostvareni su ciljevi zadani u zadatku završnog rada. Prije same obrade strategija za izradu sigurnosnih kopija, objašnjene su teorijske osnove na kojima počiva princip izrade sigurnosnih kopija, kako bi se čitaocu približila pozadina izrade sigurnosnih kopija. Nakon konceptualnog razvrstavanja sigurnosnih kopija u kategorije i tipove, formirane su različite funkcionalne strategije za izradu sigurnosnih kopija. Za svaku formiranu strategiju objašnjen je njen princip izrade te su navedeni prednosti i nedostaci u odnosu na druge strategije. Jedna od formiranih strategija je uklopljena u koncept rukovodstva sigurnosnim kopijama te je praktično ostvarena koristeći jednu od najpopularnijih tehnologija za rukovanje bazama podataka.

Prije iznošenja teorijskih i praktičnih razmatranja vezanih uz znanstvenu granu ovog rada, prikazana je poveznica koncepta izrade sigurnosnih kopija podataka i koncepta poslovanja organizacija. Svaka organizacija zahtjeva administratora baza podataka, koji je odgovaran za osiguravanje stalne operativne funkcionalnosti i učinkovitosti baza podataka organizacije. Dvije osnovne zadaće kojima se to ostvaruje su izrada sigurnosnih kopija podataka i oporavak podataka u slučaju problema. Prije izrade sigurnosnih kopija, potrebno je izraditi plan povratka podataka koji uključuje analizu prijetnji i analizu operativnih i poslovnih zahtjeva organizacije. Kao rezultat usporedbe troškova i učinaka izrade sigurnosnih kopija, formirana su tri osnovna cilja izrade sigurnosnih kopija: povrat izgubljenih podataka, minimalizacija količine izgubljenih podataka i minimalizacija troška oporavaka podataka.

Tri osnovna tipa sigurnosnih kopija podataka su: potpuna sigurnosna kopija podataka, diferencijalna sigurnosna kopija podataka i zapis izvršenih promjena. Potpuna sigurnosna kopija podataka kopira sve podatke iz baze podataka. Diferencijalna sigurnosna kopija kopira samo one podatke koji su izmijenjeni od posljednje izrade potpune sigurnosne kopije. Zapis izvršenih promjena je kopija svih izvršenih operacija nad podacima od posljednje potpune sigurnosne kopije, no ne i kopija samih podataka. Osnovni tipovi sigurnosnih kopija se mogu kombinirati u cilju pronalaženja optimalne strategije za izradu sigurnosnih kopija podataka organizacije. Zaključak je, kako je poželjno kombinirati sva tri osnovna tipa sigurnosnih kopija podataka, kako bi se smanjio broj sigurnosnih kopija koje se moraju povratiti u slučaju problema, a time i vrijeme oporavka podataka.

Sigurnosne kopije podataka se ne moraju uvijek vršiti nad bazom podataka, nego je moguće izraditi kopiju manjih struktura podataka od baze podataka. S obzirom na strukturu podataka koja se kopira, sigurnosne kopije se dijele na tri kategorije: sigurnosne kopije baza podataka, sigurnosne kopije datoteka i zapis izvršenih transakcija. Kombinirajući osnovne tipove i kategorije sigurnosnih kopija podataka, administrator baza podataka može formirati željene strategije za izradu sigurnosnih kopija podataka.

Izrada strategije za izradu sigurnosnih kopija i rukovanje izrađenim kopijama, čini koncept koji se naziva rukovodstvo sigurnosnim kopijama. Jedan od zadataka završnog rada je bio iskoristiti najbolje tehnologije za izradu vlastitog rukovodstva sigurnosnim kopijama. To je ostvareno pomoću *SQL Server Management Studio* okruženja. Iskorištene su dvije mogućnosti izrade sigurnosnih kopija koje to okruženje pruža, a to su grafičko sučelje i pisanje *SQL* skripta. Istaknuta je nemogućnost izrade cjelokupnog rukovodstva sigurnosnim kopijama, jer je potrebno poznavati prirodu podataka koji se kopiraju, tj. njihov način obrade tijekom dužeg vremenskog razdoblja. U *SQL Server Management Studio* okruženju izrađena je kombinacija potpune sigurnosne kopije baze podataka i zapisa izvršenih promjena za bazu podataka kreiranu specifično za tu primjenu. Osim toga, prikazan je način na koji se može napraviti raspored izrade sigurnosnih kopija. Izrada takvog rasporeda upotpunila bi izradu rukovodstva sigurnosnim kopijama, no ta izrada iziskuje poznavanje svrhe same baze podataka i njezin princip korištenja.

LITERATURA

[1] C.S., Mullins, Database Administration: The Complete Guide to Practices and Procedures, Addison Wesley, New Jersey, 2002.

[2] Predložak za sedmu laboratorijsku vježbu iz kolegija Operacijski sustavi, FERIT Osijek

[3] Backup and Restore of SQL Server Databases, Microsoft Corporation, 2012.

[4] L., Ashdown, Oracle Database Backup and Recovery User's Guide, Oracle, 2015.

[5] J., Loria, Best Practices for Backup and Restore in SQL™ Server 2005, Penton Media, 2008.

[6] S., McGehee, SQL Server Backup and Restore, Simple Talk Publishing, Orlando, 2012.

[7] A.N., Akhtar, J., Buchholltz, M., Ryan, K., Setty, Database Backup and Recovery Best Practices, ISACA Journal, 1., 1., str. 14 – 19, 2012.

[8] Use SQL Server Management Studio, Microsoft Corporation, 10. lipnja 2016., https://msdn.microsoft.com/en-us/library/ms174173.aspx

SAŽETAK

U ovom završnom radu obrađuju se strategije izrade sigurnosnih kopija podataka i princip rukovodstva sigurnosnim kopijama podataka. Prikazana su teorijska razmatranja na kojima se temelje spomenuti koncepti. Objašnjena je važnost izrade sigurnosnih kopija podataka za sve organizacije koje koriste neki način pohrane podataka. Pokazan je primjer provedbe analize prijetnji i analize operativnih i poslovnih zahtjeva organizacije te se na temelju rezultata tih analiza formiraju ciljevi izrade sigurnosnih kopija podataka. Postoje tri osnovna tipa sigurnosnih kopija podataka: potpuna sigurnosna kopija podataka, diferencijalna sigurnosna kopija podataka i zapis izvršenih promjena. Također, postoje i tri kategorije sigurnosnih kopija podataka: sigurnosne kopije baza podataka, sigurnosne kopije datoteka i zapisi izvršenih transakcija. Jedna od temeljnih zadaća administratora baza podataka je izraditi strategiju izrade sigurnosnih kopija podataka, kombiniranjem navedenih osnovnih tipova i kategorija sigurnosnih kopija podataka. Pokazan je primjer izrade vlastitog rukovodstva sigurnosnim kopijama koristeći *SQL Server Management Studio* okruženje.

Ključne riječi: baza podataka, oporavak podataka, rukovodstvo sigurnosnim kopijama podataka, sigurnosna kopija podataka

ABSTRACT

The title of the final paper: **Backup management**.

The subject of this final paper is processing of backup strategies and principle of backup management. Before actual processing, some theoretical considerations were pointed out, which are foundation for understanding aforementioned concepts. Firstly, the importance of backup was explained, for various organizations that use some type of data storage. Secondly, examples of carrying out threat analysis and analysis of business and operational requirements were shown. Results of those analyses are used to form backup objectives. There are three basic types of backup: Full, Differential and Log backups. Likewise, there are three broad categories of backup that a Database Administrator can perform: database backups, file backups and transaction log backups. One of the database administrator's main tasks is creating a backup strategy, which is achieved by combining backup types and backup categories. Finally, example of backup management was designed using SQL Server Management Studio environment.

Keywords: backup, backup management, database, recovery

ŽIVOTOPIS

Mario Dudjak je rođen u Našicama 25. ožujka 1995. godine gdje je završio osnovnu školu i prirodoslovno – matematičku gimnaziju. Preddiplomski studij računarstva na Fakultetu elektrotehnike, računarstva i informacijskih tehnologija u Osijeku upisao je 2013. godine. Završni rad pod nazivom *„Backup management“* piše 2016. godine. Nakon završetka treće godine planira upisati diplomski studij Programskog inženjerstva na istom fakultetu.

Tijekom pohađanja srednje i osnovne škole sudjeluje na županijskim natjecanjima iz matematike, fizike i informatike. Najbolji postignuti rezultat je 3. mjesto na županijskom natjecanju iz osnova informatike u kategoriji četvrtih razreda prirodoslovno - matematičkih gimnazija. Također sudjeluje na Hrvatskom otvorenom natjecanju iz informatike (HONI) u trećem i četvrtom razredu srednje škole. Pri završetku srednje škole prima nagradu ravnatelja za postignut odličan uspjeh tijekom srednjoškolskog obrazovanja.

Na prvoj godini fakulteta sudjeluje na međunarodnom natjecanju „IEEE Extreme“. Na drugoj godini fakulteta prima dekanovo priznanje za uspjeh tijekom studija, s prosjekom ocjena 4.88. Također, na drugoj godini fakulteta zaposlen je kao demonstrator na kolegiju Fizika u periodu trajanja od jednog semestra. Na trećoj godini fakulteta sudjeluje na međunarodnom natjecanju studenata elektrotehnike „Elektrijada“ iz informatike. Tijekom sve tri godine preddiplomskog studija prima stipendiju Sveučilišta Josipa Jurja Strossmayera u Osijeku za izvrsnost.

Posjeduje vozačku dozvolu B2 kategorije. Tečno govori engleski jezik (B2) te se služi slovačkim jezikom.

Vrlo dobro poznavanje rada na računalu (Word, Excel, Access, Power Point, Internet Explorer i sl.), te poznavanje sljedećih alata: Matlab, Visual Studio, Xilinx. Poznavanje sljedećih programskih jezika: C, C++, Python.

Potpis:
Mario Dudjak

PRILOZI

Prilog 4.1.

```
USE master;
GO
CREATE DATABASE [Baza_podataka_za_Full_Log_Backup] ON PRIMARY
( NAME = Baza_podataka_za_Full_Log_Backup,
 FILENAME = 'C:\Program Files\Microsoft SQL
Server\MSSQL10.SQLEXPRESS\MSSQL\DATA\mojabaza.mdf',
 SIZE = 512000KB,
 FILEGROWTH = 51200KB )
 LOG ON
( NAME = Baza_podataka_za_Full_Log_Backup_log,
 FILENAME = 'C:\Program Files\Microsoft SQL
Server\MSSQL10.SQLEXPRESS\MSSQL\DATA\mojabazalog.mdf',
 SIZE = 51200KB,
 FILEGROWTH = 51200KB );
GO
ALTER DATABASE [Baza_podataka_za_Full_Log_Backup] SET RECOVERY FULL
GO
```

Prilog 4.2.

```
USE [Baza_podataka_za_Full_Log_Backup]
GO
SET ANSI_NULLS ON
GO
SET QUOTED_IDENTIFIER ON
GO
CREATE TABLE [dbo].[Tablica1]
(
[Poruka] [nvarchar](100) NOT NULL ,
[VremenskaOznaka] [datetime2] NOT NULL
)
ON [PRIMARY]
GO
CREATE TABLE [dbo].[Tablica2]
(
[Poruka] [nvarchar](100) NOT NULL ,
[VremenskaOznaka] [datetime2] NOT NULL
)
ON [PRIMARY]
GO
CREATE TABLE [dbo].[Tablica3]
(
[Poruka] [nvarchar](100) NOT NULL ,
[VremenskaOznaka] [datetime2] NOT NULL
)
ON [PRIMARY]
GO
```

Prilog 4.3.

```
USE [Baza_podataka_za_Full_Log_Backup]
INSERT INTO dbo.Tablica1
VALUES ('Ovo je inicijalna poruka za Tablicu1', GETDATE())
GO 10
INSERT INTO dbo.Tablica2
VALUES ('Ovo je inicijalna poruka za Tablicu2', GETDATE())
GO 10
INSERT INTO dbo.Tablica3
VALUES ('Ovo je inicijalna poruka za Tablicu3', GETDATE())
GO 10
```

Prilog 4.4.

```
USE [master]
GO
BACKUP DATABASE [Baza_podataka_za_Full_Log_Backup]
TO DISK = 'C:DatabaseForLogBackups_Native_Full.bak'
WITH NAME = 'Baza_podataka_za_Full_Log_Backup-Full Database Backup', STATS = 10, INIT
GO
```

Prilog 4.5.

```
	USE [Baza_podataka_za_Full_Log_Backup]
GO
INSERT INTO Tablica1
VALUES ('Drugi set podataka za Tablicu1', GETDATE())
GO 10
INSERT INTO Tablica2
VALUES ('Drugi set podataka za Tablicu2', GETDATE())
GO 10
INSERT INTO Tablica3
VALUES ('Drugi set podataka za Tablicu3', GETDATE())
GO 10
```

ELEKTRONIČKA VERZIJA ZAVRŠNOG RADA