|  |  |  |
| --- | --- | --- |
| **Unigrb** | Univerzitet u Nišu  ELEKTRONSKI FAKULTET | **logo_1960_4** |

**High Availability rešenja kod Oracle baze podataka**

SEMINARSKI RAD

|  |  |
| --- | --- |
| Mentor: | Student: |
|  |  |
| Prof.dr Aleksandar Stanimirović | Teodora Sekulić 1644 |

Niš, jun 2024.god.

**Sadržaj**

[1. Uvod 3](#_Toc170205668)

[2. Visoka dostupnost 4](#_Toc170205669)

[2.1 Važnost visoke dostupnosti 5](#_Toc170205670)

[2.2 Troškovi vremena zastoja 5](#_Toc170205671)

[2.3 Uzroci vremena zastoja 6](#_Toc170205672)

[2.4 Inženjering haosa 9](#_Toc170205673)

[2.5 Plan implementacije Maximum Availability Architecture (MAA) 9](#_Toc170205674)

[3. Visoka dostupnost i zaštita podataka – Od zahteva do arhitekture 10](#_Toc170205675)

[3.1 Zahtevi visoke dostupnosti 10](#_Toc170205676)

[3.2 Metodologija za dokumentovanje zahteva visoke dostupnosti 11](#_Toc170205677)

[3.3 Mapiranje zahteva na arhitekture 14](#_Toc170205678)

[4. Rešenja visoke dostupnosti 18](#_Toc170205679)

[4.1 Oracle Data Guard 18](#_Toc170205680)

[4.2 Oracle GoldenGate 20](#_Toc170205681)

[4.3 Recovery Manager 22](#_Toc170205682)

[4.4 Oracle Real Application Clusters i Oracle Clusterware 23](#_Toc170205683)

[5. Najbolje prakse Oracle Data Guard-a 25](#_Toc170205684)

[5.1 Planiranje implementacije Oracle Data Guard-a 25](#_Toc170205685)

[5.2 Konfigurisanje i implementacija Oracle Data Guard-a 28](#_Toc170205686)

[5.3 Optimizacija i rešavanje problema u Oracle Data Guard-u 39](#_Toc170205687)

[6. Zaključak 41](#_Toc170205688)

[Literatura 42](#_Toc170205689)

# **Uvod**

U današnjem svetu koji se sve više oslanja na digitalne tehnologije, visoka dostupnost postaje ključni faktor za održavanje kontinuiteta poslovanja i sigurnosti podataka. Svaki prekid rada informacionih sistema može rezultirati gubitkom prihoda, reputacije i poverenja korisnika. Zbog toga, kompanije ulažu znatne resurse u implementaciju rešenja koja obezbeđuju visoku dostupnost i zaštitu podataka.

Oracle, kao jedan od vodećih provajdera baza podataka, nudi niz rešenja koja omogućavaju neprekidan rad sistema i zaštitu podataka u slučajevima neočekivanih incidenata. Ova rešenja obuhvataju različite tehnologije i pristupe koji zajedno formiraju robustan okvir za visoku dostupnost.

Ovaj seminarski rad se fokusira na istraživanje i analizu High Availability (HA) rešenja u Oracle bazama podataka. Prvi deo rada objašnjava značaj dostupnosti i analizira troškove i uzroke zastoja, kao i metodologije poput inženjeringa haosa koje se koriste za testiranje otpornosti sistema. Drugi deo rada razmatra kako se zahtevi za visoku dostupnost definišu i dokumentuju, kao i proces mapiranja tih zahteva na konkretne arhitekture.

Treći deo rada predstavlja konkretna Oracle rešenja za visoku dostupnost, uključujući Oracle Data Guard, Oracle GoldenGate, Recovery Manager, te Oracle Real Application Clusters (RAC) i Oracle Clusterware. Kroz detaljan pregled ovih tehnologija, ističu se njihove prednosti, načini implementacije i ključne karakteristike koje doprinose postizanju visoke dostupnosti.

Na kraju, rad pruža najbolje prakse za implementaciju Oracle Data Guard-a, uključujući planiranje, konfiguraciju, optimizaciju i rešavanje problema.

# **Visoka dostupnost**

Dostupnost je stepen do kojeg je aplikacija i usluga baze podataka dostupna.

Dostupnost se meri percepcijom korisnika aplikacije. Korisnici doživljavaju frustraciju kada njihovi podaci nisu dostupni ili kada računski sistem ne radi kako se očekuje, i oni ne razumeju niti žele da razlikuju kompleksne komponente celokupnog rešenja. Neuspeh u performansama zbog većeg broja korisnika nego što se očekivalo stvara isti prekid kao i kvar kritičnih komponenti u arhitekturi. Ako korisnik ne može da pristupi aplikaciji ili usluzi baze podataka, kaže se da je sistem nedostupan. Generalno, pojam "*vreme zastoja*" (downtime) se koristi za označavanje perioda kada je sistem nedostupan.

Korisnici koji očekuju da njihovi sistemi budu stalno dostupni, zahtevaju visoku dostupnost. Sistem koji je visoko dostupan je dizajniran da pruži neprekidne računarske usluge tokom ključnih vremenskih perioda, tokom većine sati u danu i većine dana u nedelji tokom cele godine; ovo merenje se često prikazuje kao 24x365. Takvim sistemima je takođe potrebno rešenje visoke dostupnosti za planirane operacije održavanja, kao što su nadogradnja hardverskih ili softverskih komponenti.

Pouzdanost, mogućnost oporavka, pravovremeno otkrivanje grešaka i neprekidne operacije su osnovne karakteristike rešenja visoke dostupnosti:

* **Pouzdanost**: Pouzdan hardver je jedna komponenta rešenja visoke dostupnosti. Pouzdan softver—uključujući bazu podataka, veb servere i aplikacije—je jednako kritičan za implementaciju rešenja visoke dostupnosti. Povezana karakteristika je otpornost. Na primer, jeftin hardver, u kombinaciji sa softverom kao što je Oracle Real Application Clusters (Oracle RAC), može se koristiti za implementaciju veoma pouzdanog sistema. Otpornost Oracle RAC baze podataka omogućava nastavak obrade čak i ako pojedini serveri zakažu.
* **Mogućnost oporavka**: Iako može postojati mnogo načina za oporavak od kvara, važno je odrediti koje vrste kvarova se mogu dogoditi u vašem okruženju visoke dostupnosti i kako se brzo oporaviti od tih kvarova kako bi se zadovoljili poslovni zahtevi. Na primer, ako se kritična tabela slučajno izbriše iz baze podataka, koje mere treba preduzeti za njen oporavak? Da li arhitektura omogućava oporavak u vremenu specificiranom u ugovoru o nivou usluge (SLA)?
* **Pravovremeno otkrivanje grešaka**: Ako komponenta u arhitekturi zakaže, brzo otkrivanje je od suštinskog značaja za oporavak od neočekivanog kvara. Iako je moguće brzo se oporaviti od prekida, ako otkrivanje problema traje dodatnih 90 minuta, SLA možda neće biti ispunjen. Praćenje stanja okruženja zahteva pouzdan softver za brzo pregledanje i mogućnost obaveštavanja administratora baze podataka o problemu.
* **Neprekidne operacije**: Pružanje neprekidnog pristupa podacima je od suštinskog značaja kada je vrlo malo ili nimalo vremena zastoja prihvatljivo za izvođenje aktivnosti održavanja. Aktivnosti, kao što je premeštanje tabele na drugu lokaciju u bazi podataka ili čak dodavanje CPU-a hardveru, trebaju biti transparentne za korisnika u arhitekturi visoke dostupnosti.

Viša dostupnost bi trebala imati sledeće karakteristike:

* Tolerisanje kvarova tako da se obrada nastavlja sa minimalnim ili bez prekida
* Biti transparentan za promene u sistemu, podacima ili aplikacijama
* Pružanje ugrađenih preventivnih mera
* Aktivno praćenje i brzo otkrivanje kvarova
* Brza mogućnost oporavka
* Automatizacija otkrivanja i operacija oporavka
* Zaštita podataka kako bi se minimizirali ili sprečili gubici i korupcija podataka
* Implementacija najboljih operativnih praksi za upravljanje okruženjem
* Postizanje ciljeva postavljenih u SLA-ovima (na primer, ciljevi vremena oporavka (RTO) i ciljevi tačke oporavka (RPO)) uz najniže moguće ukupne troškove vlasništva.

## **Važnost visoke dostupnosti**

Važnost visoke dostupnosti varira među aplikacijama. Baze podataka i internet su omogućili globalnu saradnju i deljenje informacija proširivanjem dometa aplikacija baza podataka unutar organizacija i zajednica.

Ovaj domet naglašava važnost visoke dostupnosti u rešenjima za upravljanje podacima. I male firme i globalna preduzeća imaju korisnike širom sveta koji zahtevaju pristup podacima 24 sata dnevno. Bez ovog pristupa podacima, operacije mogu stati, a prihodi biti izgubljeni. Korisnici sada zahtevaju ugovore o nivou usluge (SLA) od svojih odeljenja za informacione tehnologije (IT) i dobavljača rešenja, što odražava sve veću zavisnost od ovih rešenja. Sve više se dostupnost meri u dolarima, evrima i jenima, a ne samo u vremenu i pogodnostima.

Preduzeća koriste svoju IT infrastrukturu kako bi obezbedila konkurentsku prednost, povećala produktivnost i omogućila korisnicima da donose brže i informisanije odluke. Međutim, sa ovim prednostima dolazi i sve veća zavisnost od te infrastrukture. Ako kritična aplikacija postane nedostupna, poslovanje može biti ugroženo. Preduzeće može izgubiti prihode, pretrpeti kazne i dobiti loš publicitet koji može imati trajan efekat na kupce i cenu akcija kompanije.

Važno je ispitati faktore koji određuju kako su vaši podaci zaštićeni i maksimalno povećati dostupnost korisnicima.

## **Troškovi vremena zastoja**

Potreba za obezbeđivanjem sve većih nivoa dostupnosti nastavlja da ubrzano raste kako preduzeća rekonstruišu svoja rešenja kako bi stekla konkurentsku prednost. Najčešće, ova nova rešenja se oslanjaju na trenutan pristup kritičnim poslovnim podacima.

Kada podaci nisu dostupni, operacija može prestati da funkcioniše. Vreme zastoja može dovesti do gubitka produktivnosti, gubitka prihoda, oštećenih odnosa sa korisnicima, loše reputacije i sudskih sporova.

Nije uvek jednostavno odrediti direktni trošak vremena zastoja. Besni korisnici, neaktivni zaposleni i loša reputacija sve su skupe posledice, ali se ne mere direktno u valuti. S druge strane, gubici prihoda i pravne kazne koje nastaju jer se ne ispunjavaju ciljevi u SLA-u lako se mogu kvantifikovati. Troškovi vremena zastoja mogu brzo rasti u industrijama koje zavise od svojih rešenja za pružanje usluga.

Drugi faktori koje treba uzeti u obzir u troškovima vremena zastoja su:

* Maksimalno podnošljiva dužina jednog nepredviđenog prekida

Ako događaj traje manje od 30 sekundi, može izazvati vrlo malo uticaja i možda jedva da bude primetan korisnicima. Sa rastom trajanja prekida, efekat može eksponencijalno rasti i negativno uticati na poslovanje.

* Maksimalna učestalost dozvoljenih incidenata

Česti prekidi, čak i ako su kratkog trajanja, mogu slično ometati poslovne operacije.

Prilikom dizajniranja rešenja, važno je prepoznati pravi trošak vremena zastoja kako bi se razumelo kako poslovanje može imati koristi od poboljšanja dostupnosti.

Oracle pruža širok spektar rešenja visoke dostupnosti prilagođenih svakoj organizaciji bez obzira na veličinu. Male radne grupe i globalna preduzeća mogu proširiti doseg svojih kritičnih poslovnih aplikacija. Zahvaljujući Oracle-u i internetu, aplikacije i podaci su pouzdano dostupni svuda i u svakom trenutku.

## **Uzroci vremena zastoja**

Jedan od izazova u dizajniranju rešenja visoke dostupnosti jeste razmatranje i rešavanje svih mogućih uzroka vremena zastoja.

Važno je razmotriti uzroke kako nepredviđenog tako i planiranog vremena zastoja prilikom dizajniranja otpornih IT infrastruktura koje su tolerantne na greške. Planirano vreme zastoja može biti jednako ometajuće za operacije kao i nepredviđeno vreme zastoja, pogotovo u globalnim preduzećima koja podržavaju korisnike u više vremenskih zona.

Sledeća tabela 2.1 opisuje vrste nepredviđenih prekida i daje primere svake vrste.

|  |  |  |
| --- | --- | --- |
| **Tip** | **Opis** | **Primer** |
| Kvar sajta | Kvar sajta može uticati na sve procese u centru podataka ili na podskup aplikacija koje podržava centar podataka.  Definicija sajta varira u zavisnosti od konteksta lokalnih (on-premises) sistema i oblaka.   * Kvar sajta - kvar celog regionalnog sistema * Centar podataka - lokacija celog centra podataka * Domen dostupnosti - izolovani podatkovni centar unutar regiona sa mogućnošću postojanja drugih domena dostupnosti * Zona greške - izolovani set sistemskih resursa unutar domena dostupnosti ili podatkovnog centra   Obično, svaki sajt, podatkovni centar, domen dostupnosti i zona greške ima svoj skup izolovanog hardvera, DB računara, mreže, skladišta i napajanja. | * Produženi prekid napajanja na nivou celog sajta * Prekid mreže na nivou celog sajta * Prirodna katastrofa koja čini podatkovni centar neupotrebljivim * Teroristički ili zlonamerni napad na operacije ili sajt |
| Kvar na nivou klastera | Čitav klaster koji hostuje Oracle RAC bazu podataka je nedostupan ili doživljava kvar. To uključuje:   * Kvarove čvorova u klasteru * Kvar bilo koje druge komponente koji rezultira nedostupnošću klastera i nedostupnošću Oracle baze podataka i instanci na sajtu | * Poslednji preostali čvor na Oracle RAC klasteru doživljava kvar i čvor ili baza podataka ne može biti ponovo pokrenuti. * Obe redundantne veze između klastera dožive kvar ili kvar Clusterware-a. * Korupcija baze podataka toliko teška da nije moguće održavati kontinuitet na trenutnom serveru baze podataka. * Kvar Clusterware-a i hardversko-softverski defekti sprečavaju dostupnost ili stabilnost. |
| Kvar računara | Do prekida zbog kvara na računaru dolazi kada sistem na kojem se izvršava baza podataka postane nedostupan zbog kvara ili više nije dostupan. Kada se koristi Oracle RAC baza podataka, kvar na računaru predstavlja podskup sistema (zadržavajući potpuni pristup podacima). | * Kvar hardvera sistema baze podataka * Kvar operativnog sistema * Kvar Oracle instance |
| Kvar mreže | Prekid usled kvara na mreži nastaje kada se mrežni uređaj zaustavi ili smanji saobraćaj na mreži i komunikaciju između vaše aplikacije i baze podataka, baze podataka i skladišta ili bilo kog sistema do sistema koji je ključan za obradu vaših aplikacija. | * Kvar mrežnog prekidača * Kvar mrežnog interfejsa * Kvar mrežnog kabla |
| Kvar skladišta | Prekid usled kvara skladišta nastaje kada skladište koje sadrži neke ili sve sadržaje baze podataka postane nedostupno jer je isključeno ili više nije dostupno. | * Kvar diska ili fleš drajva * Kvar kontrolera diska * Kvar niza skladišta |
| Korupcija podataka | Korumpirani blok je blok koji je promenjen tako da se razlikuje od onoga što Oracle baza podataka očekuje da nađe. Korupcije blokova mogu se kategorisati kao fizičke ili logičke:   * U slučaju fizičke korupcije bloka, koja se naziva i medijska korupcija, baza podataka uopšte ne prepoznaje blok; kontrolni zbir nije validan ili blok sadrži sve nule. Primer sofisticiranije korupcije bloka je kada zaglavlje i podnožje bloka se ne podudaraju. * U slučaju logičke korupcije bloka, sadržaj bloka je fizički ispravan i prolazi provere fizičkog bloka; međutim, blok može biti logički nesaglasan. Primeri logičke korupcije bloka uključuju neispravan tip bloka, neispravne podatke ili broj sekvenca ponovnog bloka, korupciju dela reda ili unosa indeksa ili korupciju podataka u rečniku podataka.   Korupcije blokova takođe mogu biti podeljene na međubloknu (interblock) korupciju i unutarbloknu (intrablock) korupciju:   * U slučaju unutarblokne korupcije, korupcija se dešava u samom bloku i može biti fizička ili logička korupcija bloka. * U slučaju međublokne korupcije, korupcija se dešava između blokova i može biti samo logička korupcija bloka.   Prekid uzrokovan korupcijom podataka nastaje kada hardverska, softverska ili mrežna komponenta uzrokuje čitanje ili pisanje korumpiranih podataka. Uticaj na nivo usluge (SLA) zbog prekida uzrokovane korupcijom podataka može varirati, od male delova aplikacije ili baze podataka (samo do jednog bloka baze podataka) do velikih delova aplikacije ili baze podataka (što ih čini suštinski neupotrebljivim). | * Kvar operativnog sistema ili upravljačkog programa skladišnog uređaja * Neispravan host bus adapter * Kvar kontrolera diska * Greška u upravljaču zapremina koja uzrokuje loše čitanje ili pisanje na disku * Softverski ili hardverski defekti |
| Greška korisnika | Prekid usled greške korisnika nastaje kada se izvrše nehotične ili druge akcije koje dovode do toga da podaci u bazi podataka postanu netačni ili neupotrebljivi. Uticaj na nivo usluge (SLA) zbog prekida uzrokovanog greškom korisnika može značajno varirati, zavisno od količine i kritične prirode pogođenih podataka | * Brisanje datoteka (na nivou sistema datoteka) * Brisanje objekta baze podataka * Nehotične promene podataka * Zlonamjerne promene podataka |

**Tabela 2.1** Uzroci nepredviđenog vremena zastoja

Sledeća tabela 2.2 opisuje vrste planiranih prekida i daje primere svake vrste.

|  |  |  |
| --- | --- | --- |
| **Tip** | **Opis** | **Primer** |
| Promene u softveru | * Planirane periodične promene softvera radi primene manjih popravki za stabilnost i bezbednost * Planirani godišnji ili polugodišnji glavni nadogradnji radi usvajanja novih funkcija i mogućnosti | * Ažuriranja softvera, uključujući bezbednosna ažuriranja operativnog sistema, klaster softvera ili baze podataka * Glavno ažuriranje operativnog sistema, klaster softvera ili baze podataka * Ažuriranje ili nadogradnja aplikativnog softvera |
| Promene u sistemu i bazi podataka | * Planirane promene u sistemu radi zamene oštećenog hardvera * Planirane promene u sistemu radi proširenja ili smanjenja resursa sistema * Planirane promene u bazi podataka radi usvajanja promena parametara * Planirane promene radi migracije na novi hardver ili arhitekturu | * Dodavanje ili uklanjanje procesora ili memorije sa servera * Dodavanje ili uklanjanje čvorova u klasteru * Dodavanje ili uklanjanje diskova ili nizova skladišta * Zamena bilo kojeg jedinjenja koje se može zameniti na terenu (Field Replaceable Unit - FRU) * Promena konfiguracionih parametara * Migracija platforme sistema * Migracija na klaster arhitekturu * Migracija na novi sistem skladišta |
| Promene podataka | Planirane promene podataka u logičkoj strukturi ili fizičkoj organizaciji objekata Oracle baze podataka. Osnovni cilj ovih promena je poboljšanje performansi ili upravljivosti. | * Promene definicija tabela * Dodavanje particionisanja tabela * Kreiranje i ponovno izgradnja indeksa |
| Promene u aplikaciji | Planirane promene u aplikaciji mogu obuhvatiti promene podataka, šemu i programatske promene. Osnovni cilj ovih promena je poboljšanje performansi, upravljivosti i funkcionalnosti. | Ažuriranje aplikacije |

**Tabela 2.2** Uzroci planiranog vremena nedostupnosti

## **Inženjering haosa**

Maksimalna arhitektura dostupnosti (MAA) koristi inženjering haosa tokom svih faza testiranja i razvoja kako bi osigurala da se krajnja dostupnost aplikacija i baza podataka održava ili dostiže optimalne nivoe tokom bilo kog kvara ili događaja održavanja.

*Inženjering haosa* je disciplina eksperimentisanja nad sistemom kako bi se izgradio poverenje u sposobnost sistema da izdrži turbulentne uslove u produkciji. Konkretno, MAA ubacuje različite kvarove i planirane događaje održavanja kako bi se procenio uticaj na aplikacije i baze podataka tokom razvoja, stresnih testova i testnih ciklusa. Kroz te eksperimente, izvode se najbolje prakse, detektuju nedostaci i izvlače naučene lekcije, a stečeno znanje se primenjuje kako bi se evoluirala i unapredila naša MAA rešenja.

## **Plan implementacije Maximum Availability Architecture (MAA)**

Rešenja visoke dostupnosti Oracle-a i zvuk operativnih praksi ključni su za uspešnu implementaciju IT infrastrukture. Međutim, tehnologija sama po sebi nije dovoljna.

Izbor i implementacija arhitekture koja najbolje odgovara vašim zahtevima za dostupnost može biti zastrašujući zadatak. Oracle Maximum Availability Architecture (MAA) pojednostavljuje proces izbora i implementacije arhitekture visoke dostupnosti koja odgovara vašim poslovnim zahtevima uz sledeće razmatranja:

* Obuhvata redundantnost svih komponenti
* Pruža zaštitu i toleranciju od kvarova računara, kvarova skladišta, ljudskih grešaka, korupcije podataka, izgubljenih pisanja, kašnjenja ili usporavanja sistema, i katastrofa na lokacijama
* Oporavlja se od prekida što je brže i transparentnije moguće
* Nudi rešenja za eliminaciju ili smanjenje planiranog vremena nedostupnosti
* Prati dosledno visoke performanse i snažnu sigurnost
* Prati Oracle Engineered System i opcije u oblaku za pojednostavljenje implementacije i upravljanje i postizanje najviše skalabilnosti, performansi i dostupnosti
* Postiže SLA-e uz najniže moguće ukupne troškove svojine
* Primenjuje se na lokalne sisteme, Oracle javni oblak i hibridne arhitekture koje se sastoje od delova na lokaciji i delova u oblaku
* Prilagođava se posebnim zahtevima za Container ili Oracle Multitenant, Oracle Database In-Memory i Oracle Sharding arhitekturama

Za izgradnju, implementaciju i održavanje ovakve arhitekture, potrebno je:

* Analizirati specifične zahteve za visokom dostupnošću, uključujući tehničke i operativne aspekte IT sistema i poslovnih procesa.
* Proceniti različite arhitekture visoke dostupnosti i njihove koristi i opcije.
* Razumeti uticaj dostupnosti za svaku MAA referentnu arhitekturu, ili različite karakteristike visoke dostupnosti, na poslovanje i aplikacije.
* Upoznati se sa Oracle karakteristikama visoke dostupnosti.
* Primena operativnih najboljih praksi za uspešnu implementaciju MAA.
* Implementirati arhitekturu visoke dostupnosti koristeći Oracle MAA resurse, koji pružaju tehničke detalje o različitim Oracle MAA tehnologijama visoke dostupnosti, zajedno sa preporukama najboljih praksi za konfigurisanje i korišćenje takvih tehnologija, kao što su beli papiri o najboljim praksama MAA, studije slučaja korisnika sa dokazima koncepta, snimljeni vebinari, demonstracije i prezentacije.

# **Visoka dostupnost i zaštita podataka – Od zahteva do arhitekture**

U ovom poglavlju će se detaljno razmotriti tema visoke dostupnosti i zaštite podataka u kontekstu Oracle Maximum Availability Architecture. Fokus će biti na razumevanju zahteva visoke dostupnosti, metodologije za dokumentovanje tih zahteva, kao i proces mapiranja specifičnih zahteva na odgovarajuće arhitekture visoke dostupnosti.

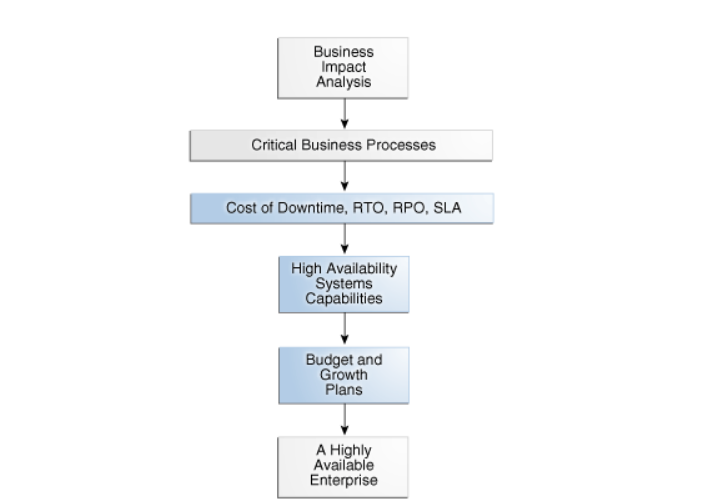
## **Zahtevi visoke dostupnosti**

Svaki napor za dizajn i implementaciju strategije visoke dostupnosti za Oracle bazu podataka počinje izvođenjem detaljne analize poslovnog uticaja kako bi se identifikovale posledice prekida rada i gubitka podataka na preduzeće, bilo da su uzrokovani neplaniranim ili planiranim prekidima.

Termin "*poslovni uticaj*" je namenjen da bude neutralan prema tome da li je preduzeće komercijalni poduhvat, vladina agencija ili neprofitna organizacija. U svim slučajevima, gubitak podataka i prekid rada mogu ozbiljno uticati na sposobnost bilo kojeg preduzeća da obavlja svoje funkcije. Implementacija visoke dostupnosti može uključivati kritične zadatke kao što su:

* Penzionisanje zastarelih sistema
* Investiranje u sposobnije i robusnije sisteme i objekte
* Redizajn ukupne IT arhitekture i operacija kako bi se prilagodili ovom modelu visoke dostupnosti
* Modifikacija postojećih aplikacija kako bi se u potpunosti iskoristile infrastrukture visoke dostupnosti
* Redizajn poslovnih procesa
* Zapošljavanje i obuka osoblja
* Premeštanje delova ili cele aplikacije ili baze podataka u Oracle Public Cloud
* Balansiranje pravog nivoa konsolidacije, fleksibilnosti i izolacije
* Razumevanje mogućnosti i ograničenja postojećeg sistema i mrežne infrastrukture

Kombinovanjem poslovne analize sa razumevanjem nivoa investicija potrebnih za implementaciju različitih rešenja visoke dostupnosti, moguće je razviti arhitekturu visoke dostupnosti koja postiže i poslovne i tehničke ciljeve.



**Slika 3.1** Planiranje i implementacija visoko dostupnog preduzeća

## **Metodologija za dokumentovanje zahteva visoke dostupnosti**

Elementi ovog analitičkog okvira su:

1. **Analiza poslovnog uticaja**

Analiza poslovnog uticaja kategorizuje poslovne procese na osnovu težine uticaja IT prekida.

Rigorozna analiza poslovnog uticaja:

* Identifikuje ključne poslovne procese u organizaciji
* Izračunava kvantitativni rizik od gubitka za neplanirane i planirane IT prekide koji utiču na svaki od ovih poslovnih procesa
* Ocrtava efekte ovih prekida
* Uključuje bitne poslovne funkcije, ljude i sistemske resurse, državne propise i unutrašnje i spoljašnje poslovne zavisnosti
* Zasniva se na objektivnim i subjektivnim podacima prikupljenim iz intervjua sa stručnim i iskusnim osobljem
* Pregledava istorije poslovne prakse, finansijske izveštaje, IT sisteme logove i slično

Na primer, razmotrite proizvođača poluprovodnika sa fabrikama čipova smeštenim širom sveta. Proizvodnja poluprovodnika je izuzetno konkurentan posao koji zahteva ogromne finansijske investicije koje se amortizuju kroz velike proizvodne količine. Aplikacije za ljudske resurse koje koristi administracija fabrike verovatno neće biti smatrane kao kritične aplikacije koje kontrolišu proces proizvodnje u fabrici. Neuspeh aplikacija koje podržavaju proizvodnju utiče na nivoe proizvodnje i ima direktan uticaj na finansijske rezultate kompanije.

Kao drugi primer, interni sistem za upravljanje znanjem verovatno će biti smatran kao misija kritičan za firmu za savetovanje u oblasti menadžmenta, jer poslovanje kompanije fokusirane na klijente zavisi od pristupa unutrašnjim istraživanjima za njene konsultante i radnike sa znanjem. Trošak prekida rada takvog sistema je izuzetno visok za ovo poslovanje.

Slično, e-trgovinska kompanija u velikoj meri zavisi od korisničkog saobraćaja na svom vebsajtu za generisanje prihoda. Svaki prekid u usluzi i gubitak dostupnosti može umanjiti korisničko iskustvo i odvesti kupce konkurenciji. Stoga, kompanija mora osigurati da postojeća infrastruktura može da se skalira i nosi sa naglim porastom korisničkog saobraćaja. Ponekad, to nije moguće koristiti hardver na lokaciji i prelaskom na cloud kompanija može osigurati da njihovi sistemi uvek ostanu operativni.

1. **Trošak prekida rada**

Kompletna analiza poslovnog uticaja pruža uvid potreban za kvantifikovanje troškova neplaniranog i planiranog prekida rada.

Razumevanje ovog troška je ključno jer pomaže u prioritetizaciji vaših investicija u visoku dostupnost i direktno utiče na tehnologije visoke dostupnosti koje birate kako biste minimizirali rizik od prekida rada.

Različiti izveštaji su objavljeni, dokumentujući troškove prekida rada u različitim industrijama. Primeri uključuju troškove koji se kreću od milion dolara za svaki sat rada brokerskih operacija i prodaje kreditnih kartica, do desetina hiljada dolara za svaki sat rada usluga dostave paketa.

Ovi brojevi su zapanjujući. Internet i Cloud mogu direktno povezati poslovanje sa milionima kupaca. Prekid rada aplikacija može poremetiti ovu vezu, odsečući preduzeće od njegovih kupaca. Pored izgubljenog prihoda, prekid rada može negativno uticati na odnose sa kupcima, konkurentske prednosti, zakonske obaveze, reputaciju u industriji i poverenje akcionara.

1. **Cilj vremena oporavka (RTO)**

Analiza poslovnog uticaja određuje vašu toleranciju prema prekidu rada, poznatu i kao cilj vremena oporavka (RTO).

RTO je definisan kao maksimalno vreme koje IT-bazirani poslovni proces može biti van funkcije pre nego što organizacija počne da trpi neprihvatljive posledice (finansijski gubici, nezadovoljstvo kupaca, reputacija, i tako dalje). RTO pokazuje toleranciju prema prekidu rada poslovnog procesa ili organizacije uopšte.

Zahtevi za RTO su vođeni kritičnom prirodom poslovanja. Stoga, za sistem koji upravlja berzom, RTO je nula ili blizu nule.

Organizacija će verovatno imati različite zahteve za RTO za različite poslovne procese. Za vebsajt za e-trgovinu sa velikim obimom prometa, gde se očekuju brzi odgovori i gde su troškovi prelaska kupaca vrlo niski, veb-bazirani sistem za interakciju sa kupcima koji podstiče prodaju e-trgovine verovatno će imati RTO od nula ili blizu nule. Međutim, RTO sistema koji podržavaju pozadinske operacije, kao što su isporuka i naplata, može biti viši. Ako su ovi pozadinski sistemi van funkcije, preduzeće može privremeno pribegnuti ručnim operacijama bez značajnog vidljivog uticaja.

Neke organizacije imaju različite RTO-ove na osnovu verovatnoće kvarova. Jednostavna klasifikacija su lokalni kvarovi (kao što su pojedinačni računski resursi baze podataka, disk/flash, mrežni kvar) u odnosu na katastrofe (kao što su potpuni kvar klastera, baze podataka, korupcija podataka ili kvar lokacije). Tipično, poslovno-kritični kupci imaju RTO manji od 1 minut za lokalne kvarove, a mogu imati viši RTO manji od 1 sat za katastrofe. Za kritične aplikacije, RTO-ovi mogu zaista biti isti za sve neplanirane prekide.

1. **Cilj tačke oporavka (RPO)**

Analiza poslovnog uticaja takođe određuje vašu toleranciju prema gubitku podataka, poznatu kao cilj tačke oporavka (RPO).

RPO je maksimalna količina podataka koju IT-bazirani poslovni proces može izgubiti bez štete po organizaciju. RPO meri toleranciju poslovnog procesa ili organizacije prema gubitku podataka uopšte. Ovaj gubitak podataka se često meri u vremenskim jedinicama, na primer, nula, sekunde, sati ili dani gubitka podataka.

Berza na kojoj se transakcije u vrednosti od miliona dolara dešavaju svakog minuta ne može sebi priuštiti gubitak bilo kakvih podataka. Stoga, njen RPO mora biti nula. Veb-bazirani prodajni sistem u primeru e-trgovine ne zahteva RPO od nula, iako je nizak RPO ključan za zadovoljstvo kupaca. Međutim, njegov pozadinski sistem za ažuriranje robe i inventara može imati viši RPO jer izgubljeni podaci mogu biti ponovo uneseni.

RPO od nula može biti izazovan za katastrofe, ali se može postići uz različite Oracle tehnologije koje štite vašu bazu podataka, posebno Zero Data Loss Recovery Appliance (uređaj za oporavak bez gubitka podataka).

1. **Cilj upravljivosti**

Cilj upravljivosti je subjektivniji od RPO-a ili RTO-a. Potrebno je napraviti objektivnu procenu veština, resursa za upravljanje i dostupnih alata u organizaciji, kao i stepen do kojeg organizacija može uspešno upravljati svim elementima arhitekture visoke dostupnosti.

Baš kao što RPO i RTO mere toleranciju organizacije prema prekidu rada i gubitku podataka, cilj upravljivosti meri toleranciju organizacije prema kompleksnosti u IT okruženju. Kada je manja kompleksnost zahteva, preferiraju se jednostavnije metode postizanja visoke dostupnosti u odnosu na metode koje mogu biti kompleksnije za upravljanje, čak i ako bi ove druge mogle ostvariti agresivnije ciljeve RTO-a i RPO-a. Razumevanje ciljeva upravljivosti pomaže organizacijama da razlikuju između onoga što je moguće i onoga što je praktično za implementaciju.

Premeštanjem Oracle baza podataka u Oracle Cloud može se značajno smanjiti trošak upravljivosti i kompleksnost, jer Oracle Cloud omogućava izbor između različitih arhitektura maksimalne dostupnosti sa ugrađenim konfiguracijama i operacijama životnog ciklusa. Sa Autonomous Database Cloud, operacije životnog ciklusa baze podataka kao što su rezervno kopiranje i vraćanje, ažuriranje softvera i ključne operacije popravke su automatske.

1. **Ukupni trošak vlasništva i povraćaj investicije (TCO i ROI)**

Razumevanje ukupnog troška vlasništva (TCO) i ciljeva povrata investicije (ROI) su ključni za izbor arhitekture visoke dostupnosti koja takođe postiže poslovne ciljeve vaše organizacije.

TCO obuhvata sve troškove (kao što su nabavka, implementacija, sistemi, mreže, objekti, osoblje, obuka i podrška) tokom korisnog veka vašeg izabranog rešenja visoke dostupnosti. Slično tome, proračun ROI-a obuhvata sve finansijske koristi koje se ostvaruju za određenu arhitekturu visoke dostupnosti.

Na primer, razmotrite arhitekturu visoke dostupnosti u kojoj IT sistemi i skladišta na udaljenom rezervnom mestu ostaju neaktivni, bez drugih poslovnih upotreba koje bi mogle biti podržane tim rezervnim sistemima. Jedini povrat investicije za rezervno mesto su troškovi povezani sa izbegnutim prekidima rada u scenariju prelaska na rezervnu opciju. Ovo se može napraviti kontrast sa drugom arhitekturom visoke dostupnosti koja omogućava da se IT sistemi i skladišta na rezervnom mestu koriste produktivno dok su u rezervnoj ulozi (na primer, za izveštaje ili za preusmeravanje opterećenja korisničkih upita ili distribuciju opterećenja čitanja i pisanja sa primarnog sistema). Povrat investicije takve arhitekture obuhvata kako troškove izbegnutih prekida rada, tako i finansijske koristi koje proističu iz njihove produktivne upotrebe, dok istovremeno obezbeđuje visoku dostupnost i zaštitu podataka.

Preduzeća takođe mogu smanjiti TCO za rastuće potrebe infrastrukture prebacivanjem opterećenja u oblak umesto ulaganja u izgradnju novog centra podataka. Glavna ekonomska privlačnost je pretvaranje kapitalnih rashoda u operativne rashode i generisanje većeg ROI-a.

## **Mapiranje zahteva na arhitekture**

Analiza poslovnog uticaja pomoći će da dokumentujete ono što već znate. Rezultat analize poslovnog uticaja pruža uvid koji je potreban da grupišete baze podataka sa sličnim ciljevima RTO-a i RPO-a zajedno.

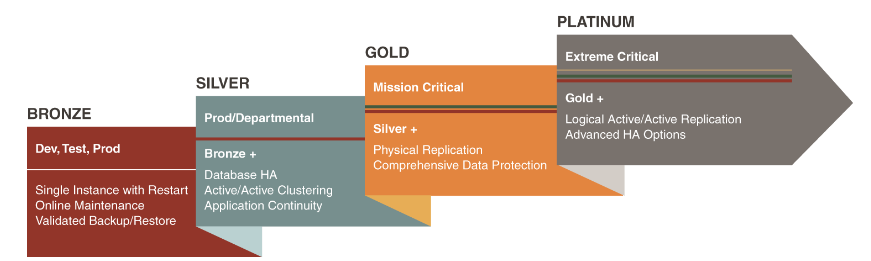
Različite aplikacije, i baze podataka koje ih podržavaju, predstavljaju različite stepene značaja za preduzeće. Visok nivo investicija u infrastrukturu visoke dostupnosti možda nema smisla za aplikaciju koja, ako je nedostupna, ne bi imala odmah vidljiv uticaj na preduzeće.

Grupe baza podataka sa sličnim ciljevima RTO-a i RPO-a mogu se mapirati na kontrolisan skup referentnih arhitektura visoke dostupnosti koje najviše odgovaraju zahtevanim nivoima usluga. Treba imati na umu da u slučaju da postoje zavisnosti između baza podataka, one se grupišu sa bazom podataka koja ima najstrožiji zahtev za visokom dostupnošću.

**Reference arhitekture Oracle MAA**

Oracle MAA najbolje prakse definišu referentne arhitekture visoke dostupnosti koje adresiraju kompletni spektar dostupnosti i zaštite podataka potrebnih za preduzeća svih veličina i linija poslovanja.

Platinum, Gold, Silver i Bronze MAA referentne arhitekture, ili nivoi, primenjive su na on-premises, privatne i javne konfiguracije u oblaku, kao i na hibridni oblak. One pružaju nivoe usluga opisane na sledećoj slici (slika 3.2).



**Slika 3.2** Reference arhitekture Oracle MAA

Svaki nivo koristi različitu Oracle MAA referentnu arhitekturu kako bi implementirao optimalni set Oracle sposobnosti visoke dostupnosti koji pouzdano ostvaruju određeni nivo usluge uz najniže troškove i kompleksnost. Nivoi eksplicitno adresiraju sve vrste neplaniranih prekida, uključujući korupciju podataka, kvar komponenti, prekide sistema i lokacija, kao i planirane prekide zbog održavanja, migracija ili drugih svrha.

Kontejnerske baze podataka (CDB) koje koriste Oracle Multitenant mogu postojati u bilo kom nivou, od Bronze do Platinum, pružajući veću gustinu konsolidacije i niži TCO. Tipično, gustina konsolidacije je veća sa Bronze i Silver nivoima, dok nema ili je minimalna konsolidacija pri implementaciji Platinum nivoa.

Oracle Database In-Memory takođe može biti iskorišćen u bilo kom od MAA nivoa. Zbog toga što je In-Memory kolonski skladište integrisano u Oracle bazu podataka, svi benefiti visoke dostupnosti koji dolaze iz MAA nivoa se nasleđuju prilikom implementacije Oracle Database In-Memory.

Oracle Engineered Systems takođe mogu postojati u bilo kom od nivoa. Integracija Zero Data Loss Recovery Appliance (Recovery Appliance) kao rešenja za rezervno kopiranje i oporavak Oracle baze podataka za celokupni data centar smanjuje RPO i RTO prilikom vraćanja sa rezervnih kopija. Iskorišćavanje Oracle Exadata Database Machine kao platforme za bazu podataka u Oracle MAA referentnim arhitekturama pruža najbolje rešenje za platformu baze podataka sa najnižim RTO i "brownout", zajedno sa dodatnim Exadata MAA kvalitetom usluge.

**Bronzana referentna arhitektura**

Bronzani nivo je prikladan za baze podataka gde je jednostavno ponovno pokretanje neispravnog komponenta (na primer, listenera, instanci baze podataka ili same baze podataka) ili vraćanje sa rezervne kopije "*dovoljno za visoku dostupnost i oporavak u slučaju katastrofe*".

Bronzana referentna arhitektura se zasniva na jednoj instanci Oracle baze podataka koja koristi Oracle MAA najbolje prakse koje implementiraju brojne sposobnosti za zaštitu podataka i visoku dostupnost, koje su uključene u svaku licencu Oracle Enterprise Edition. Oracle-optimizovani rezervni kopiranja korišćenjem Oracle Recovery Manager (RMAN) pružaju zaštitu podataka i koriste se za obnovu dostupnosti u slučaju prekida koji sprečava ponovno pokretanje baze podataka. Branzana arhitektura takođe koristi redundantnu sistemsku infrastrukturu poboljšanu Oracle tehnologijama kao što su Oracle Restart, Recovery Manager (RMAN), Zero Data Loss Recovery Appliance, Flashback tehnologije, Online Redefinition, Online Patching, Automatic Storage Management (ASM), Oracle Multitenant i još mnogo toga.

**Srebrna referentna arhitektura**

Srebrni nivo pruža dodatni nivo visoke dostupnosti za baze podataka koje zahtevaju minimalan ili nulti prekid rada u slučaju kvara instance baze podataka ili servera, kao i tokom većine planiranih događaja održavanja, kao što su ažuriranja hardvera i softvera.

Srebrna referentna arhitektura dodaje bogat set korporativnih mogućnosti i beneficija, uključujući tehnologiju klasterizacije korišćenjem Oracle RAC ili Oracle RAC One Node. Takođe, Application Continuity omogućava pouzdanu reprodukciju transakcija u toku, što maskira prekide korisnicima i pojednostavljuje prebacivanje aplikacija.

**Zlatna referentna arhitektura**

Zlatni nivo značajno podiže uloge za poslovno kritične aplikacije koje ne mogu tolerisati visoke RTO i RPO za bilo kakve katastrofe poput kvarova baze podataka, klastera, korupcija ili prekida na lokaciji. Dodatno, glavna ažuriranja baze podataka ili migracije lokacija mogu se obaviti u sekundama.

Zlatni nivo takođe smanjuje troškove i poboljšava povrat investicije tako što aktivno koristi sve replike u svakom trenutku.

Zlatna referentna arhitektura dodaje tehnologije replikacije baze podataka, Oracle Data Guard i Oracle Active Data Guard, koje sinhronizuju jednu ili više replika produkcijske baze podataka radi pružanja zaštite podataka u realnom vremenu i dostupnosti. Replikacija baze podataka značajno unapređuje visoku dostupnost i zaštitu podataka (zaštita od korupcije) izvan mogućnosti koje pružaju tehnologije replikacije skladišta. Oracle Active Data Guard Far Sync se koristi za zaštitu bez gubitka podataka na bilo kojoj udaljenosti.

**Platinska referentna arhitektura**

Platinski nivo uvodi nekoliko novih sposobnosti Oracle baze podataka, uključujući Oracle GoldenGate za ažuriranja i migracije bez prekida rada.

Edition Based Redefinition omogućava razvojenim timovima da dizajniraju aplikacije za ažuriranja bez prekida rada. Takođe, moguće je dizajnirati aplikacije za Oracle Sharding, što pruža ekstremnu dostupnost distribuiranjem podskupova baze podataka u visoko dostupne fragmente, dok aplikacija može pristupiti celoj bazi podataka kao jednoj logičkoj bazi.

Svaka od ovih tehnologija zahteva dodatne napore za implementaciju, ali pružaju značajnu vrednost za najkritičnije aplikacije gde prekid rada nije opcija.

**Atributi visoke dostupnosti i zaštite podataka po nivou**

Svaka MAA referentna arhitektura pruža poznate i testirane nivoe vremena nedostupnosti i zaštite podataka.

Sledeća tabela 3.1 sumira atribute visoke dostupnosti i zaštite podataka inherentne svakoj arhitekturi. Svaka arhitektura uključuje sve mogućnosti prethodne arhitekture i nadograđuje je kako bi se nosila sa proširenim setom prekida. Različite komponente uključene i nivoi usluga postignuti svakom arhitekturom opisani su u drugim temama.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **MAA referentna arhitektura** | **Nepredviđeni prekidi (lokalna lokacija)** | **Planirano održavanje** | **Zaštita podataka** | **Nepopravljivi lokalni prekidi i oporavak od katastrofe** |
| Bronzana arhitektura | Jedna instanca, automatsko ponovno pokretanje za oporavljive kvarove instance i servera. Redundancija za sistemsku infrastrukturu tako da kvarovi pojedinačnih komponenti poput diska, fleša i mreže ne bi trebalo da rezultuju u prekidu rada. | Neki resursi su dostupni online, većina je van mreže. | Osnovna validacija u toku rada kombinovana sa ručnim proverama. | Obnova iz rezervne kopije, potencijalni gubitak podataka generisanih od poslednje rezervne kopije. Korišćenje Zero Data Loss Recovery Appliance smanjuje potencijalni gubitak podataka na nulu ili blizu nule. |
| Srebrna arhitektura | Visoka dostupnost sa automatskim prebacivanjem za kvarove instance i servera | Većina se vrši tokom izvođenja, nešto je dostupno online, a malo van mreže | Osnovna validacija u toku rada kombinovana sa ručnim proverama | Obnova iz rezervne kopije, potencijalni gubitak podataka generisanih od poslednje rezervne kopije. Korišćenje Zero Data Loss Recovery Appliance smanjuje potencijalni gubitak podataka na nulu ili blizu nule. Transakcije u toku su sačuvane uz Application Continuity. |
| Zlatna arhitektura | Kompletna visoka dostupnost i oporavak od katastrofe | Sve se vrši tokom izvođenja ili je online | Kompletna validacija u toku rada kombinovana sa ručnim proverama | Prebacivanje u realnom vremenu, nula ili minimalan gubitak podataka |
| Platinska arhitektura | Nema prekida aplikacije za aplikacije spremne za Platinum | Nema prekida aplikacije | Kompletna validacija u toku rada kombinovana sa ručnim proverama | Nema prekida aplikacije za aplikacije spremne za Platinum, sa nula gubitkom podataka. Oracle RAC, Oracle Active Data Guard i Oracle GoldenGate se međusobno dopunjuju pružajući širok spektar rešenja za postizanje nultog prekida usluge baze podataka za nepredviđene prekide. Alternativno, koristite Oracle Sharding za zaštitu od prekida na lokaciji, jer uticaj na aplikaciju postoji samo na fragmentima u neispravnoj lokaciji umesto na celokupnoj bazi podataka. Svaki fragment može biti konfigurisan sa prebacivanjem u realnom vremenu, nula ili blizu nule gubitkom podataka ili bez prekida aplikacije za aplikacije spremne za Platinum. Transakcije u toku su sačuvane, sa nultim gubitkom podataka. |

**Tabela 3.1** Atributi visoke dostupnosti i zaštite podataka po MAA referentnoj arhitekturi

# **Rešenja visoke dostupnosti**

U ovom poglavlju biće predstavljena glavna rešenja koja Oracle nudi za postizanje visoke dostupnosti. Svako od ovih rešenja igra ključnu ulogu u obezbeđivanju neprekidnog rada sistema i zaštiti podataka. Biće istraženi Oracle Data Guard, Oracle GoldenGate, Recovery Manager, te Oracle Real Application Clusters (RAC) i Oracle Clusterware.

## **Oracle Data Guard**

Oracle Data Guard obezbeđuje visoku dostupnost, zaštitu podataka i oporavak od katastrofe za podatke preduzeća.

Data Guard pruža sveobuhvatan skup usluga koje kreiraju, održavaju, upravljaju i nadgledaju jednu ili više rezervnih baza podataka kako bi omogućile Oracle bazama podataka da prežive prekide svake vrste, uključujući prirodne katastrofe i korupciju podataka. Rezervna baza podataka u Data Guard-u je tačna replika produkcijske baze podataka i može se transparentno koristiti u kombinaciji sa tradicionalnim tehnikama rezervne kopije, vraćanja podataka, flashback-a i klaster tehnika kako bi se pružio najviši mogući nivo zaštite podataka, dostupnosti podataka i oporavka od katastrofe. Data Guard je uključen u Oracle Enterprise Edition.

Data Guard konfiguracija se sastoji od jedne primarne baze podataka i jedne ili više rezervnih baza podataka. Primarna baza podataka može biti ili jedna instanca Oracle baza podataka ili Oracle RAC baza podataka. Slično primarnoj bazi podataka, rezervna baza podataka može biti ili jedna instanca Oracle baza podataka ili Oracle RAC baza podataka. Koristeći rezervnu kopiju primarne baze podataka, možete kreirati do 30 rezervnih baza podataka koje direktno primaju redo zapise iz primarne baze podataka. Opciono možete koristiti kaskadiranu rezervnu bazu podataka da biste kreirali Data Guard konfiguracije gde primarna baza podataka šalje redo zapise ka jednoj udaljenoj destinaciji, a ta destinacija dalje šalje redo zapise ka više rezervnih baza podataka. Ovo omogućava primarnoj bazi podataka da efikasno sinhronizuje mnogo više od 30 rezervnih baza podataka ako je potrebno.

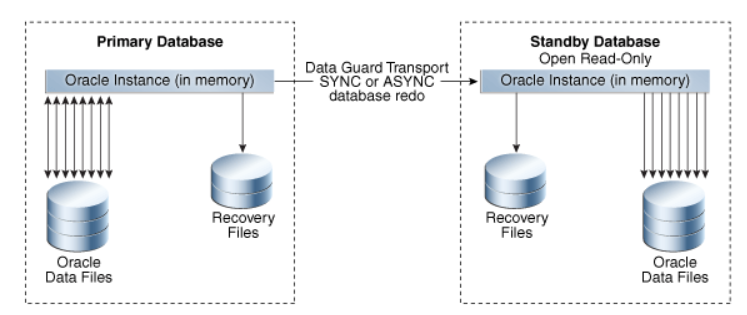
Benefiti korišćenja Data Guard-a:

* **Kontinuirana Oracle-verifikacija**: Sve promene su proverene Oracle-verifikacijom pre nego što se primene na standby bazu, što izoluje standby bazu i sprečava da bude pogođena greškama podataka sa primarnog sistema.
* **Transparentna operacija**: Nema ograničenja u korišćenju Data Guard fizičkog standby-a za zaštitu podataka. Redo primena podržava sve tipove podataka i skladišta, sve DDL operacije i sve aplikacije, garantujući konzistentnost podataka između primarne i standby baze.
* **Najbolja performansa**: Brz prenos redo zapisa za optimalan cilj oporavka, brza primena za najbolje ciljeve vremena oporavka. Višestruka primena redo zapisa omogućava skaliranje Oracle RAC-a za redo primenu, eliminisajući uska grla jednog serverskog sistema baze podataka.
* **Brzo preusmeravanje na standby bazu**: Omogućava brzo prebacivanje na standby bazu kako bi se održala dostupnost u slučaju neuspeha primarne baze. Preusmeravanje može biti ručno ili automatsko, u zavisnosti od konfiguracije Data Guard-a.
* **Integrisani okvir za obaveštavanje klijenata**: Omogućava aplikacijskim klijentima da se povežu sa novom primarnom bazom podataka nakon što dođe do preusmeravanja.

**Oracle Active Data Guard**

Oracle Active Data Guard je Oracle-ovo strateško rešenje za zaštitu podataka u realnom vremenu i oporavak od katastrofa za Oracle bazu podataka korišćenjem procesa fizičke replikacije.

Oracle Active Data Guard takođe pruža visoku povratnu vrednost na ulaganje u sisteme za oporavak od katastrofa omogućavajući da rezervna baza podataka bude otvorena za čitanje dok primenjuje promene primljene od primarne baze podataka. Oracle Active Data Guard je posebno licenciran proizvod koji pruža napredne funkcije koje značajno proširuju mogućnosti Data Guard-a uključenih u Oracle Enterprise Edition.



**Slika 4.1** Oracle Active Data Guard arhitektura

Oracle Active Data Guard omogućava administratorima da poboljšaju performanse prebacivanjem obrade sa primarne baze podataka na fizičku rezervnu bazu podataka koja je otvorena samo za čitanje dok primenjuje ažuriranja primljena od primarne baze podataka. Mogućnosti prebacivanja Oracle Active Data Guard uključuju izveštavanje samo za čitanje i ad-hoc upite (uključujući DML na globalnim privremenim tabelama i jedinstvene globalne ili sesijske sekvence), ekstrakciju podataka, brze inkrementalne bekape, kompresiju prenosa redo logova, efikasno opsluživanje više udaljenih destinacija i mogućnost proširenja zaštite bez gubitka podataka na udaljenu rezervnu bazu podataka bez uticaja na performanse primarne baze podataka. Oracle Active Data Guard takođe povećava visoku dostupnost automatskim popravkom blokova i omogućava automatizaciju nadogradnji sa visokom dostupnošću.

## **Oracle GoldenGate**

Oracle GoldenGate je Oracle-ovo strateško rešenje za logičku replikaciju podataka, koje omogućava distribuciju podataka u realnom vremenu i integraciju podataka.

Oracle GoldenGate nudi platformu za promenu podataka zasnovanu na logovima, koja omogućava uhvatanje, rutiranje, transformaciju i isporuku transakcionih podataka između heterogenih baza podataka u realnom vremenu.

Za razliku od rešenja za replikaciju drugih proizvođača, Oracle GoldenGate je bliže integrisan sa Oracle bazom podataka, istovremeno pružajući otvorenu, modularnu arhitekturu idealnu za replikaciju između heterogenih sistema za upravljanje bazama podataka. Ova kombinacija karakteristika eliminiše kompromise i čini Oracle GoldenGate preferiranim rešenjem za logičku replikaciju koje zadovoljava zahteve koji obuhvataju Oracle bazu podataka i nerešene baze podataka drugih proizvođača.

Tipično okruženje uključuje procese uhvatanja, pumpiranja i isporuke. Svaki od ovih procesa može se izvoditi na većini popularnih operativnih sistema i baza podataka, uključujući Oracle bazu podataka. Svi ili deo podataka može biti replikovan, a podaci unutar ovih procesa mogu se manipulisati ne samo za heterogene okruženja već i za različite šeme baza podataka, nazive tabela ili strukture tabela. Oracle GoldenGate takođe podržava bidirekcionalnu replikaciju sa unapred konfigurisanim handlerima za otkrivanje i rešavanje sukoba podataka.

Logička replikacija pomoću Oracle GoldenGate omogućava da sve baze podataka u Oracle GoldenGate konfiguraciji, kako izvorišne tako i ciljne baze podataka, budu otvorene za čitanje i pisanje. Ovo ga čini ključnim komponentom MAA za rešavanje širokog spektra izazova visoke dostupnosti, kao što su održavanje bez zastoja, migracija između platformi i kontinuirana dostupnost podataka, specifično:

* **Održavanje bez zastoja ili sa minimalnim zastojem**. Oracle GoldenGate omogućava veću fleksibilnost od mogućnosti koje pruža Data Guard. Oracle GoldenGate izvorne i ciljne baze podataka mogu imati različitu fizičku i logičku strukturu, mogu se nalaziti na različitom hardveru i arhitekturi operativnog sistema, mogu obuhvatiti velike razlike u izdanjima Oracle baze podataka (na primer, od 12.2 do 19c), ili biti mešavina Oracle i drugih sistema. Ovo omogućava modernizaciju 24x7 servera i implementaciju novih Oracle funkcionalnosti bez uticaja na dostupnost baza podataka. Održavanje se prvo izvodi na ciljnoj bazi podataka dok proizvodnja radi na izvorišnoj. Nakon što se održavanje završi, proizvodnja može biti prebačena na izvorišnu bazu podataka odjednom, slično kao kod Data Guard prebacivanja. Opciono, bidirekcionalna replikacija može se koristiti za postepeno premeštanje korisnika na novi sistem kako bi se stvorio utisak minimalnog zastoja. U oba slučaja, Oracle GoldenGate replikacija može biti omogućena u obrnutom smeru kako bi se tokom tranzicionog perioda originalna izvorišna baza podataka održavala sinhronizovanom, što omogućava jednostavno izvršavanje planiranog povratka na prethodnu verziju uz minimalan zastoj i bez gubitka podataka.
* **Migracija sa minimalnim zastojem ili bez zastoja kada rešenje Data Guard nije primenljivo**. Migracije platforme ili baze podataka mogu se izvoditi koristeći Oracle GoldenGate kao metod sinhronizacije podataka između starih i novih sistema. Nakon što je baza podataka instancirana na drugom serveru, Oracle GoldenGate je podešen da replikuje promene iz produkcione baze podataka. Može se kreirati garantovana tačka povratka na migriranoj bazi podataka tako da nakon testiranja korisnika baza podataka može biti vraćena koristeći flash back opciju, a Oracle GoldenGate može primeniti sve preostale promene podataka iz produkcione baze podataka pre nego što korisnici aplikacije budu prebačeni na novu bazu podataka, slično kao kod snapshot standby baze podataka. Ako je potrebno, može se konfigurisati i bidirekcionalna replikacija iz migrirane baze podataka nazad u produkcioni sistem za slučaj povratka na prethodno stanje.
* **Nadogradnje aplikacija sa minimalnim ili bez zastoja**. Nadogradnje aplikacija koje modifikuju objekte baze podataka na pozadini obično rezultiraju značajnim planiranim zastojem tokom izvršenja održavanja. Oracle GoldenGate replikacija omogućava transformaciju podataka koja mapira objekte baze podataka koje koristi prethodna verzija aplikacije na objekte modifikovane novom verzijom aplikacije. Ovo omogućava da se održavanje baze podataka izvodi na posebnoj kopiji produkcione baze podataka bez uticaja na dostupnost aplikacije. Nakon što se održavanje završi i Oracle GoldenGate sinhronizuje stare i nove verzije, korisnici mogu biti prebačeni na novu verziju aplikacije.
* **Pristup čitanja i pisanja replika baze podataka dok se sinhronizuje sa izvornom bazom podataka**. Ovo se najčešće koristi za prebacivanje izveštavanja na kopiju produkcione baze podataka kada aplikacija za izveštavanje zahteva vezu za čitanje i pisanje sa bazom podataka kako bi funkcionisala. Ovo je takođe relevantno za okruženja oporavka od katastrofe gde priroda tehnologije korišćene za aplikacioni sloj zahteva aktivnu vezu za čitanje i pisanje sa DR bazom podataka kako bi se ispunili ciljevi vremena oporavka.
* **Aktivna-aktivna replikacija**. Oracle GoldenGate podržava aktivno-aktivnu višesmernu konfiguraciju, gde postoji dve ili više sistema sa identičnim skupovima podataka koji mogu biti promenjeni od strane korisnika aplikacije na bilo kom sistemu. Oracle GoldenGate replikuje promene transakcionih podataka sa svake baze podataka na druge kako bi se održali svi skupovi podataka ažurnim.
* **Bez prekida prelaska između čvorova Oracle Real Application Clusters (RAC) u slučaju pada instance baze podataka ili tokom primenjivih operacija održavanja**. Ova sposobnost obezbeđuje visoku dostupnost uz Oracle GoldenGate, i moguće je zakrpiti i nadograditi softver Oracle GoldenGate na jednom ili više čvorova u klasteru Oracle RAC bez uticaja na čvor gde je Oracle GoldenGate trenutno pokrenut. Zatim, u unapred određeno vreme, Oracle GoldenGate se može prebaciti na jedan od nadograđenih čvorova. Prebacivanje se vrši bez ponovnog konfigurisanja Oracle GoldenGate jer se informacije o konfiguraciji dele širom Oracle RAC klastera.

## **Recovery Manager**

Recovery Manager (RMAN) pruža sveobuhvatnu osnovu za efikasno bekapovanje i oporavak baze podataka. RMAN eliminiše operativnu kompleksnost dok istovremeno pruža izuzetne performanse i dostupnost baze podataka.

RMAN određuje najefikasniju metodu za izvođenje zahtevanog bekapovanja, obnove ili operacije oporavka, a zatim šalje te operacije serveru Oracle Database-a na procesiranje. RMAN i server automatski identifikuju modifikacije strukture baze podataka i dinamički prilagođavaju potrebne operacije kako bi se prilagodile promenama.

RMAN je standardni interfejs za bekapovanje i obnavljanje sa Recovery Appliance, lokalnog diska (ZFS skladišta), trake i skladišta u oblaku.

RMAN (Recovery Manager) pruža sledeće benefite:

* Podrška za Oracle Sharding omogućava upotrebu RMAN-a za svaku nezavisnu bazu podataka (shard).
* Mogućnost rada sa retkim bazama podataka, što omogućava bekapovanje i obnavljanje na retkim setovima podataka ili kopijama slika.
* Popravka stanja na standby bazi podataka preko mreže za operacije koje nisu evidentirane u dnevnicima.
* Poboljšana funkcionalnost RMAN DUPLICATE za kreiranje Far Sync stanica iz primarne baze i backupa.
* Podrška za enkriptovane backupove bazirane na novoj komandi SET, omogućava kloniranje bez prekida.
* Mogućnost cross-platform bekapovanja i obnavljanja preko mreže.
* Omogućeno obnavljanje preko mreže direktno između baza podataka.
* Jednostavno obnavljanje tabela pomoću komande RECOVER TABLE.
* Podrška za Oracle Multitenant, uključujući bekapovanje i oporavak pojedinačnih pluggable baza podataka.
* Automatsko prebacivanje kanala tokom operacija bekapovanja i obnavljanja.
* Automatsko prebacivanje na prethodni bekap ukoliko se tokom obnavljanja otkrije da je bekap nedostajući ili oštećen.
* Automatsko kreiranje novih fajlova baza podataka i privremenih fajlova tokom oporavka.
* Automatski oporavak preko tačke u prošlosti, omogućava oporavak kroz resetovanje dnevnika.
* Block media recovery, omogućava popravku oštećenih blokova dok su data fajlovi online.
* Brzi inkrementalni bekapovi pomoću praćenja promena blokova.
* Brze operacije bekapovanja i obnavljanja sa intrafile i interfile paralelizmom.
* Poboljšana sigurnost sa virtuelnim privatnim katalogom za oporavak.
* Spajanje inkrementalnih bekapova u image kopije, pružajući ažuriranu sposobnost oporavka.
* Optimizovano bekapovanje i obnavljanje samo neophodnih fajlova.
* Politika zadržavanja za osiguravanje relevantnih bekapova.
* Mogućnost nastavka operacija bekapovanja i obnavljanja u slučaju neuspeha.
* Automatsko bekapovanje kontrolnog fajla i server parametarskog fajla, osiguravajući dostupnost metapodataka bekapovanja u slučaju strukturnih promena baze podataka, medijskih grešaka i katastrofa.
* Jednostavno ponovno instanciranje nove baze podataka iz postojećeg bekapa ili direktno iz produkcione baze podataka koristeći funkciju DUPLICATE.

## **Oracle Real Application Clusters i Oracle Clusterware**

Oracle RAC i Oracle Clusterware omogućavaju Oracle bazi podataka da pokreće bilo koju unapred pripremljenu ili prilagođenu aplikaciju na skupu servera u klasteru.

Ova mogućnost pruža najviši nivo dostupnosti i najfleksibilniju skalabilnost. Ako jedan server u klasteru zakaže, Oracle baza podataka nastavlja sa radom na preostalim serverima. Kada je potrebna dodatna procesorska snaga, moguće je dodati još jedan server bez prekidanja pristupa podacima.

Oracle RAC omogućava više instanci koje su povezane međusobno da dele pristup Oracle bazi podataka. U Oracle RAC okruženju, Oracle baza podataka radi na dva ili više sistema u klasteru dok istovremeno pristupa jednoj zajedničkoj bazi podataka. Rezultat je jedinstven sistem baza podataka koji se proteže na više hardverskih sistema, omogućavajući Oracle RAC-u da obezbedi visoku dostupnost i redundanciju tokom kvarova u klasteru. Oracle RAC podržava sve tipove sistema, od sistema za čitanje podataka (read-only) kao što su skladišta podataka, do sistema za intenzivnu obradu transakcija (OLTP).

Oracle Clusterware je softver koji, kada se instalira na serverima sa istim operativnim sistemom, omogućava da se serveri povežu i funkcionišu kao jedan server, te upravlja dostupnošću korisničkih aplikacija i Oracle baza podataka. Oracle Clusterware takođe pruža sve funkcije potrebne za upravljanje klasterom, uključujući članstvo čvorova, grupne servise, globalno upravljanje resursima i funkcije visoke dostupnosti:

* Za visoku dostupnost, moguće je staviti Oracle baze podataka (single-instance ili Oracle RAC baze podataka) i korisničke aplikacije (Oracle i ne-Oracle) pod upravljanje i zaštitu Oracle Clusterware-a, tako da se baze podataka i aplikacije ponovo pokreću kada proces zakaže ili da dođe do prebacivanja na drugi čvor nakon kvara čvora.
* Za upravljanje klasterom, Oracle Clusterware prikazuje više nezavisnih servera kao jednu virtuelnu sliku sistema ili jedan virtuelni server. Ovaj jedinstveni virtuelni server se održava kroz ceo klaster za sve upravljačke operacije, omogućavajući administratorima da izvršavaju instalacije, konfiguracije, bekapove, nadogradnje i funkcije praćenja. Oracle Clusterware automatski distribuira obradu ovih upravljačkih funkcija na odgovarajuće čvorove u klasteru.

Oracle Clusterware je zahtev za korišćenje Oracle RAC-a. Oracle Clusterware je jedini clusterware koji vam je potreban za većinu platformi na kojima Oracle RAC radi. Iako Oracle baza podataka nastavlja da podržava proizvode trećih strana za klastere na određenim platformama, korišćenje Oracle Clusterware-a pruža sledeće glavne prednosti:

* Eliminisanje vlasničkog softvera za klastere
* Korišćenje integrisanog softverskog paketa od Oracle-a koji pruža upravljanje diskovima sa lokalnim ili udaljenim Oracle Automatic Storage Management (Oracle Flex ASM) do upravljanja podacima sa Oracle bazom podataka i Oracle RAC-om
* Može biti konfigurisano u velike klastere, nazvane Oracle Flex Cluster.

Pored toga, funkcije Oracle baze podataka, kao što su Oracle servisi, koriste osnovne mehanizme Oracle Clusterware-a da bi pružile svoje mogućnosti.

Oracle Clusterware zahteva dva komponenta za klaster: glasajući disk (voting disk) za beleženje informacija o članstvu čvorova i Oracle Cluster Registry (OCR) za beleženje informacija o konfiguraciji klastera. Glasajući disk i OCR moraju biti smešteni na deljenom skladištu. Oracle Clusterware zahteva da svaki čvor bude povezan na privatnu mrežu preko privatnog interkonekta.

**Prednosti korišćenja Oracle Clusterware-a**

Oracle Clusterware pruža sledeće prednosti:

* Toleriše i brzo se oporavlja od kvarova računara i instanci.
* Pojednostavljuje upravljanje i podršku korišćenjem Oracle Clusterware-a zajedno sa Oracle bazom podataka. Korišćenjem manjeg broja dobavljača i kompletnog Oracle paketa postižete bolju integraciju u poređenju sa korišćenjem klastera trećih strana.
* Izvodi nadogradnje sistema i hardverske promene bez prekida rada (rolling upgrades). Na primer, možete primeniti nadogradnje Oracle Clusterware-a, patch setove i privremene zakrpe na način koji ne zahteva prekid rada.
* Kada nadogradite na Oracle Database 12c, Oracle Clusterware i Oracle ASM binarne datoteke se instaliraju kao jedinstvena binarna datoteka pod nazivom Oracle Grid Infrastructure. Možete nadograditi Oracle Clusterware bez prekida rada sa verzija Oracle Clusterware 10g i Oracle Clusterware 11g; međutim, Oracle ASM možete nadograditi bez prekida rada samo sa Oracle Database 11g release 1 (11.1).
* Automatski ponovo pokreće neuspele Oracle procese.
* Automatski upravlja virtuelnom IP (VIP) adresom. Kada čvor zakaže, VIP adresa tog čvora se prebacuje na drugi čvor na kojem VIP adresa može prihvatiti veze.
* Automatski ponovo pokreće resurse sa neuspelih čvorova na preostalim čvorovima.

**Prednosti korišćenja Oracle Real Application Clusters i Oracle Clusterware**

Zajedno, Oracle RAC i Oracle Clusterware pružaju sve prednosti Oracle Clusterware-a plus sledeće dodatne prednosti:

* Pruža bolju integraciju i podršku Oracle baze podataka korišćenjem kompletnog Oracle softverskog paketa u poređenju sa korišćenjem klastera trećih strana.
* Automatski premešta Oracle uslugu. Pored toga, kada izvedete dodatnu brzu obaveštenje aplikacija (FAN) i konfiguraciju klijenata, distribuirate FAN događaje tako da aplikacije mogu odmah reagovati kako bi postigle brzo, automatsko i inteligentno povezivanje i prebacivanje na drugi čvor.
* Brzo otkriva kvarove veze i automatski uklanja prekinute veze za bilo koju Java aplikaciju koristeći Oracle Universal Connection Pool (Oracle UCP) Fast Connection Failover i FAN događaje.
* Balansira radne zahteve koristeći Oracle UCP balansiranje opterećenja u toku izvršenja.
* Koristi balansiranje opterećenja u toku izvršenja sa Oracle UCP, Oracle Call Interface (OCI) i Oracle Data Provider za .NET (ODP.NET).
* Distribuira rad preko svih dostupnih instanci koristeći savetnik za balansiranje opterećenja.
* Možete konfigurisati bazu podataka tako da je Oracle Clusterware svestan CPU zahteva i ograničenja za datu bazu podataka. Oracle Clusterware koristi ove informacije da postavi resurs baze podataka samo na servere koji imaju dovoljan broj CPU-ova, količinu memorije ili oboje.
* Omogućava fleksibilnost povećanja procesne snage korišćenjem jeftinog hardvera bez zastoja ili promena aplikacije.
* Pruža sveobuhvatnu mogućnost upravljanja integrisanjem funkcija baze podataka i klastera.
* Pruža skalabilnost preko instanci baze podataka.
* Implementira brzo prebacivanje veza za nepovezane veze.

# **Najbolje prakse Oracle Data Guard-a**

Dodavanjem fizičke rezervne baze podataka sa Oracle Active Data Guard, Silver MAA referentna arhitektura se unapređuje na Gold MAA referentnu arhitekturu. Implementacija najboljih praksi Oracle Data Guard-a omogućava postizanje minimalnog vremena zastoja i potencijalno nultog gubitka podataka tokom svih neplaniranih prekida.

Oracle Active Data Guard ima ključnu ulogu u obezbeđivanju visoke dostupnosti i sveobuhvatne zaštite podataka, što je i očekivano od Gold MAA referentne arhitekture. Gold referentna arhitektura, koja obuhvata primarnu Oracle RAC bazu podataka i Oracle RAC rezervne sisteme sa Oracle Active Data Guard-om, zajedno sa MAA konfiguracijom i operacijama životnog ciklusa, pruža sveobuhvatan skup usluga za kreiranje, održavanje, upravljanje i praćenje jedne ili više rezervnih baza podataka. Oracle Active Data Guard štiti podatke tokom svih vrsta planiranog održavanja, kao što su softverska ažuriranja i velike nadogradnje baza podataka, kao i tokom neplaniranih prekida, uključujući kvarove baza podataka, prekide rada na lokaciji, prirodne katastrofe i oštećenja podataka.

Cilj najboljih praksi Oracle Data Guard-a je omogućavanje implementacije testiranih i dokazanih MAA najboljih praksi, kako bi se osigurala uspešna i stabilna implementacija Data Guard-a. Sledeći koraci vode kroz Oracle MAA najbolje prakse za planiranje, implementaciju i održavanje ove vrste arhitekture:

1. Planiranje Oracle Data Guard arhitekture, uzimajući u obzir različite faktore kao što su aplikacija, mreža i drugi relevantni elementi.
2. Konfiguracija i implementacija Data Guard-a prema Oracle MAA najboljim praksama.
3. Optimizacija i rešavanje problema sa Data Guard implementacijom.

## **Planiranje implementacije Oracle Data Guard-a**

Treba analizirati specifične zahteve, uključujući tehničke i operativne aspekte IT sistema i poslovnih procesa, razumeti uticaj dostupnosti za opcije arhitekture Oracle Data Guard-a i razmisliti o uticaju aplikacije i mreže.

**Arhitekture Oracle Data Guard-a**

Gold MAA referentna arhitektura pruža četiri arhitektonska obrasca, koristeći Oracle Active Data Guard radi eliminacije tačke pojedinačnog otkaza. Obrasci variraju od jedne udaljene aktivne rezervne sa brzim startom prebacivanja i HA posmatračem, do uključivanja daleko sinhronizovanih instanci, višestrukih rezervnih sistema i farmi za čitanje.

**Razmatranja aplikacija za implementaciju Oracle Data Guard-a**

Kao deo planiranja implementacije Oracle Data Guard-a, razmotriti potrebne resurse i zahteve za dostupnost aplikacija u scenariju prebacivanja na rezervni sistem.

Takođe je bitno odabrati između ***potpunog prebacivanja lokacije*** i ***bezbednog prebacivanja veze*** u skladu sa poslovnim i aplikativnim zahtevima.

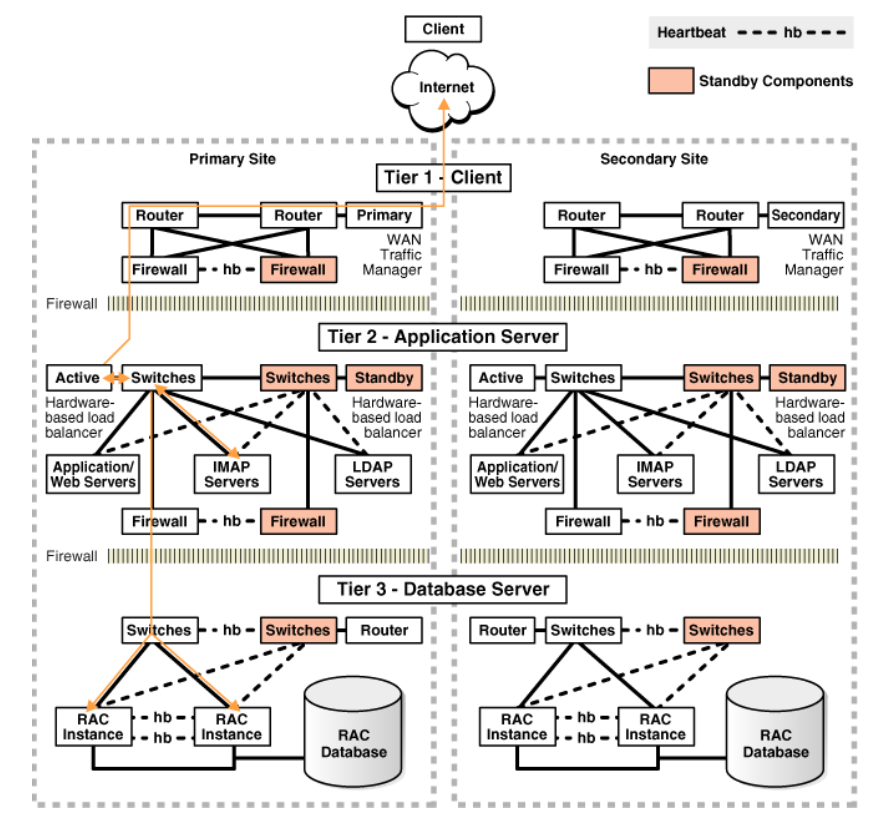
Prvi korak je procena koja opcija prebacivanja najbolje odgovara vašim poslovnim i aplikativnim zahtevima kada vaša primarna baza podataka ili primarna lokacija postanu nedostupni ili izgubljeni usled katastrofe.

**Najbolje prakse za potpuno prebacivanje lokacije**

Potpuno prebacivanje lokacije znači da se cela lokacija prebacuje na drugu lokaciju sa novim setom aplikativnih slojeva i novom primarnom bazom podataka.

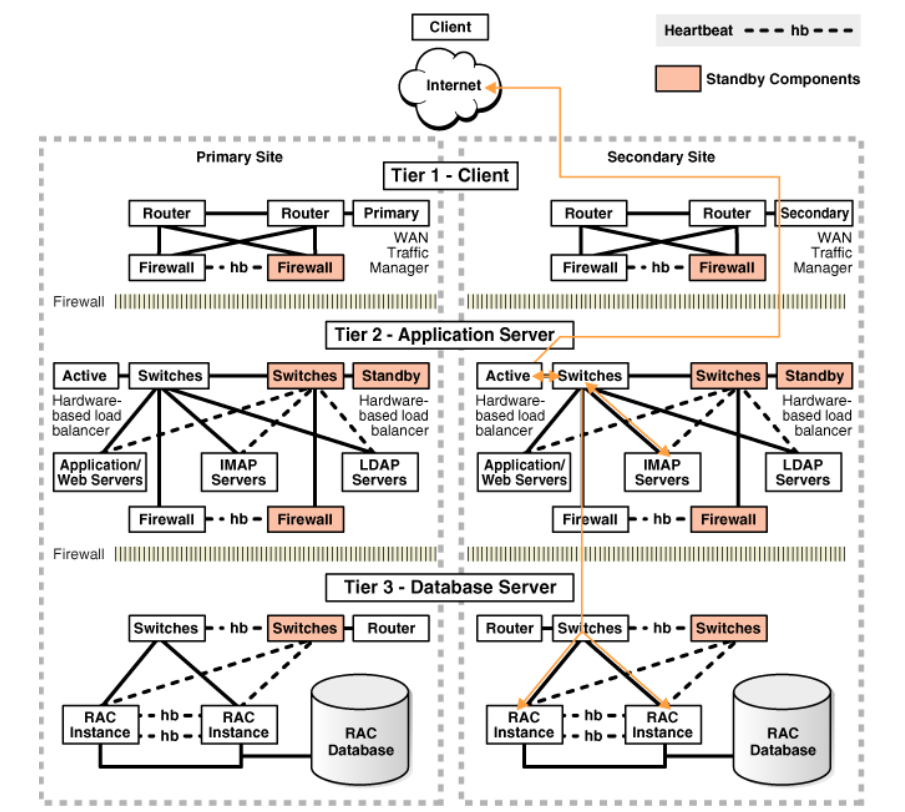
Potpuni pad lokacije rezultira nedostupnošću i aplikativnih i baza podataka. Da bi se održala dostupnost, korisnici aplikacija moraju biti preusmereni na sekundarnu lokaciju koja sadrži redundantan aplikativni sloj i sinhronizovanu kopiju produkcijske baze podataka.

Razmotriti dva prikaza ispod. Prvi prikaz (slika 5.1) pokazuje mrežne rute pre prebacivanja. Zahtevi klijenata ili aplikacija ulaze na primarnu lokaciju na nivou klijentskog sloja i rutiraju se ka aplikativnom serveru i serveru baze podataka na primarnoj lokaciji.



**Slika 5.1** Mrežne rute pre prebacivanja lokacije

Druga slika (slika 5.2), ilustruje mrežne rute nakon potpunog prebacivanja lokacije. Zahtevi klijenata ili aplikacija ulaze na sekundarnu lokaciju na nivou klijentskog sloja i prate isti put na sekundarnoj lokaciji koji su pratili na primarnoj lokaciji.



**Slika 5.2** Mrežne rute nakon prebacivanja lokacije

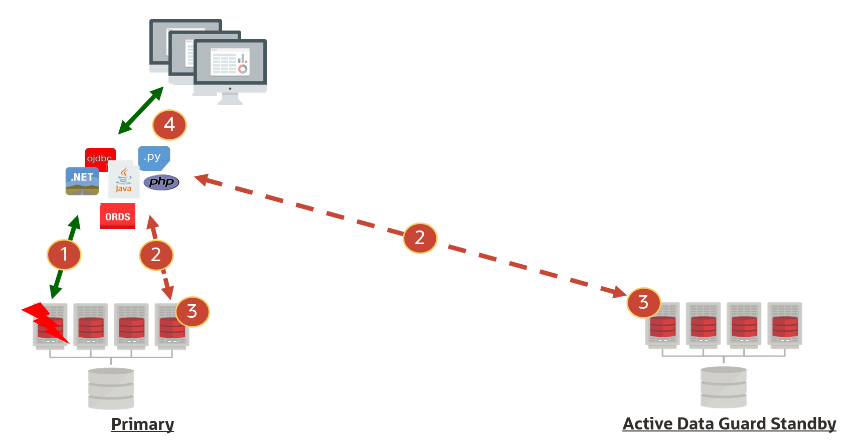
MAA najbolja praksa je održavanje aktivnog aplikativnog sloja na rezervnoj lokaciji kako bi se izbeglo vreme pokretanja, i korišćenje Oracle Data Guard-a za održavanje sinhronizovane kopije produkcijske baze podataka. Prilikom neuspeha lokacije, WAN upravljač saobraćajem se koristi za izvršavanje DNS preusmeravanja (ručno ili automatski) radi preusmeravanja svih korisnika na aplikativni sloj na rezervnoj lokaciji, dok se Data Guard prebacivanjem prelazi rezervna baza podataka u primarnu produkcijsku ulogu.

Koristi se Oracle Active Data Guard Fast-Start Failover za automatizaciju prebacivanja baze podataka. Prebacivanje aplikacionih servera i ostalih delova aplikacije može biti automatizovano i koordinisano korišćenjem Oracle Site Guard-a. Oracle Site Guard orkestrira i automatizuje sve operacije, kao što su pokretanje aplikacionih servera na sekundarnoj lokaciji, resinhronizacija meta podataka koji nisu baza podataka dok se Data Guard automatski prebacuje.

**Konfigurisanje bezbednog prebacivanja veze**

Automatizacija bezbednog prebacivanja klijenata u Oracle Data Guard konfiguraciji uključuje premestanje usluga baze podataka na novu primarnu bazu podataka kao deo Data Guard prebacivanja, obaveštavanje klijenata o nastalom prekidu kako bi se prekinulo čekanje na TCP timeout, i preusmeravanje klijenata ka novoj primarnoj bazi podataka.

Na sledećoj slici (slika 5.3), zahtev za bazom podataka se prekida zbog prekida u radu ili timeout-a (1), nakon čega se sesija ponovo uspostavlja sa Oracle RAC klasterom (2) (ili rezervnom bazom) (2), zahtev za bazom podataka se automatski ponovo izvršava na alternativnom čvoru (3), i rezultat zahteva se vraća korisniku (4).



**Slika 5.3** Bezbedno prebacivanje veze

**Procena i optimizacija performansi mreže**

Oracle Data Guard se oslanja na osnovnu mrežu kako bi slao redo logove sa primarne baze podataka ka rezervnim bazama podataka. Osiguravanje da je mreža zdrava i sposobna da podrži vrhunske stope generisanja redo logova pomaže u izbegavanju budućih transportnih zastoja.

Transportni zastoj nastaje kada primarna baza podataka nije u mogućnosti da isporuči redo logove rezervnoj bazi brže od stope generisanja redo logova na primarnoj instanci. Transportni zastoj može dovesti do potencijalnog gubitka podataka u slučaju kvara primarne baze podataka.

Procena mreže se sastoji od evaluacije:

* Pouzdanosti mreže
* Propusnosti mreže za podršku vrhunskih stopa generisanja redo logova

## **Konfigurisanje i implementacija Oracle Data Guard-a**

Sledeće poglavlje opisuju Oracle MAA najbolje prakse za postavljanje Oracle Data Guard konfiguracije.

**Primena najboljih praksi za konfiguraciju Oracle baze podataka**

Pre nego što se implementiraju najbolje prakse za Oracle Data Guard, neophodno je primeniti najbolje prakse za konfiguraciju Oracle baze podataka.

Najbolje prakse za konfiguraciju Oracle Data Guard-a predstavljaju dopunu opštim najboljim praksama za konfiguraciju Oracle baze podataka i doprineće postizanju očekivanih nivoa usluga u skladu sa MAA Gold referentnom arhitekturom. Pretpostavlja se da sve najbolje prakse za konfiguraciju baze podataka treba primeniti u Data Guard konfiguraciji, a da preporuke za Data Guard, koje su ovde navedene, zamenjuju opšte preporuke za bazu podataka u slučaju konflikta.

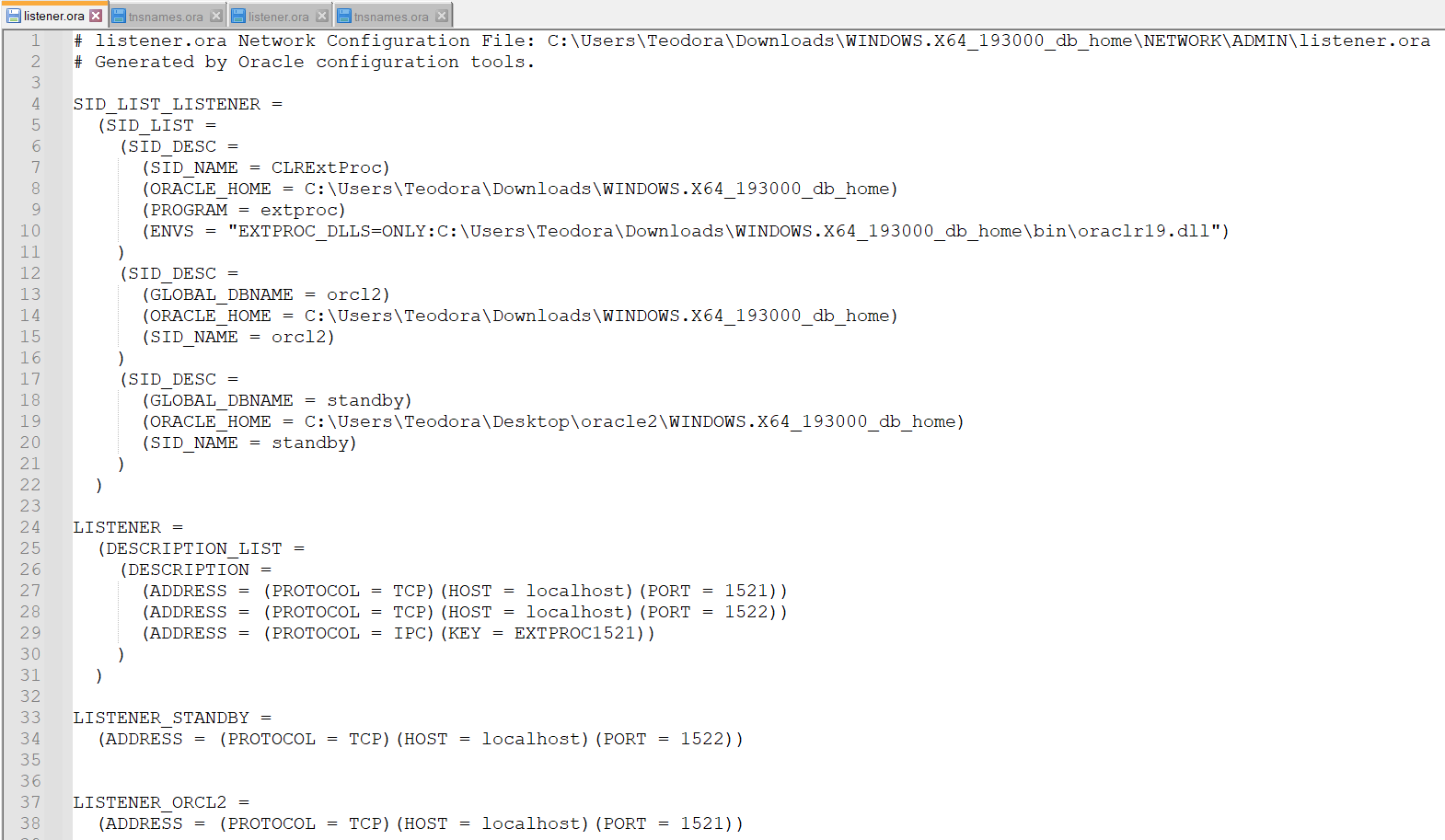
**Korišćenje Recovery Manager-a za kreiranje rezervnih baza podataka**

Postoji nekoliko metoda koje se mogu koristiti za kreiranje Oracle Data Guard rezervne baze podataka, ali zbog svoje jednostavnosti, Oracle MAA preporučuje pristup kreiranju fizičke rezervne baze podataka korišćenjem RMAN RESTORE ... FROM SERVICE klauzule.

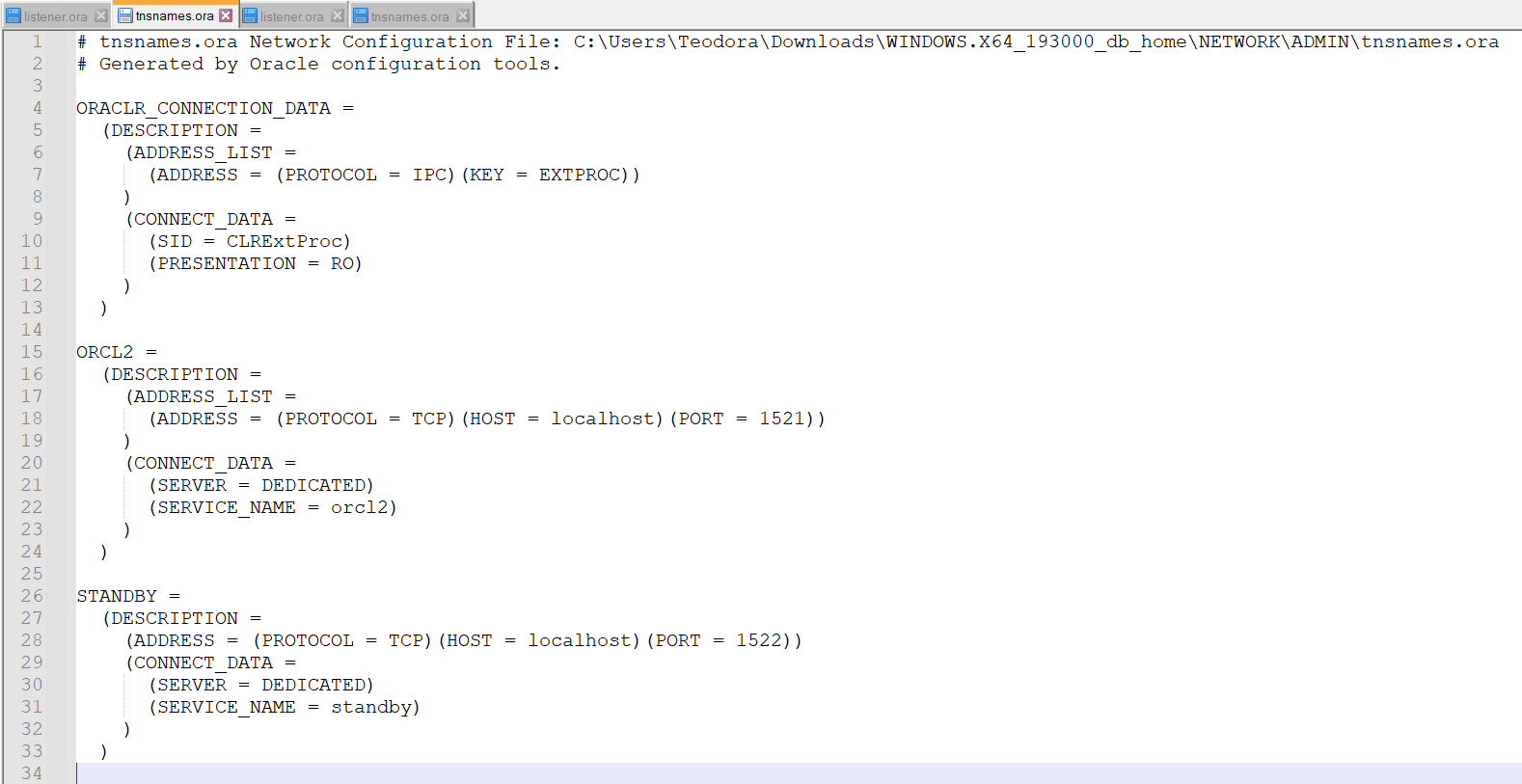
**Primer 5.1 Konfiguracija Oracle Data Guard-a (ručna konfiguracija)**

* **Konfigurisanje Oracle Net Services za komunikaciju između servera**

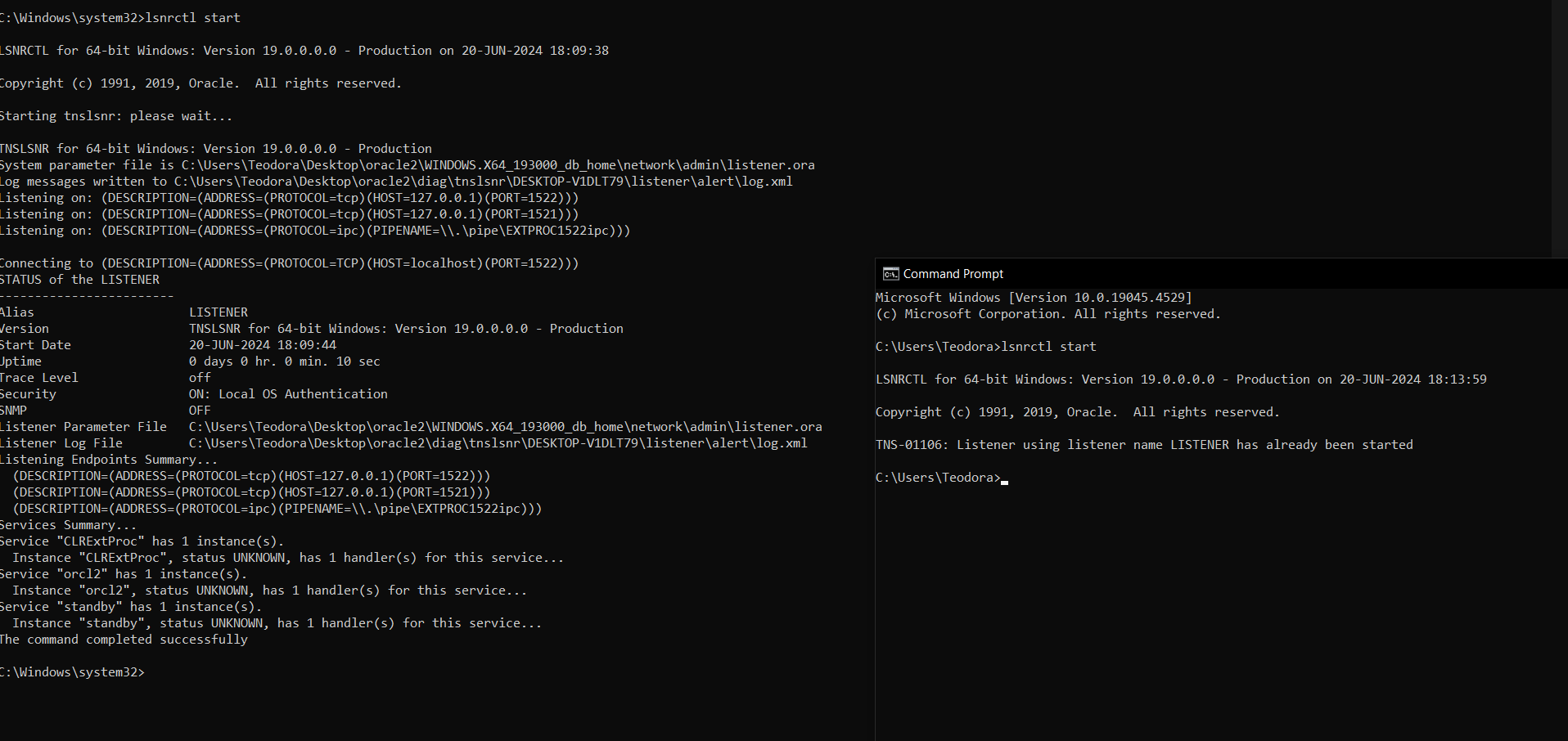
U „listener.ora" fajlu definišemo informacije o slušaču (listeneru) koji služi za osluškivanje dolaznih mrežnih zahteva za povezivanje sa Oracle bazom podataka. Ovde definišemo na kojoj IP adresi i portu će slušač osluškivati zahteve.



U „tnsnames.ora“ fajlu definišemo nazive (service name) i mrežne adrese (adresa servera, port) za Oracle baze podataka kojima želimo da pristupimo. Ovde se definiše kako klijentske aplikacije, kao što je SQL\*Plus, mogu pronaći bazu podataka preko Oracle Net Services.

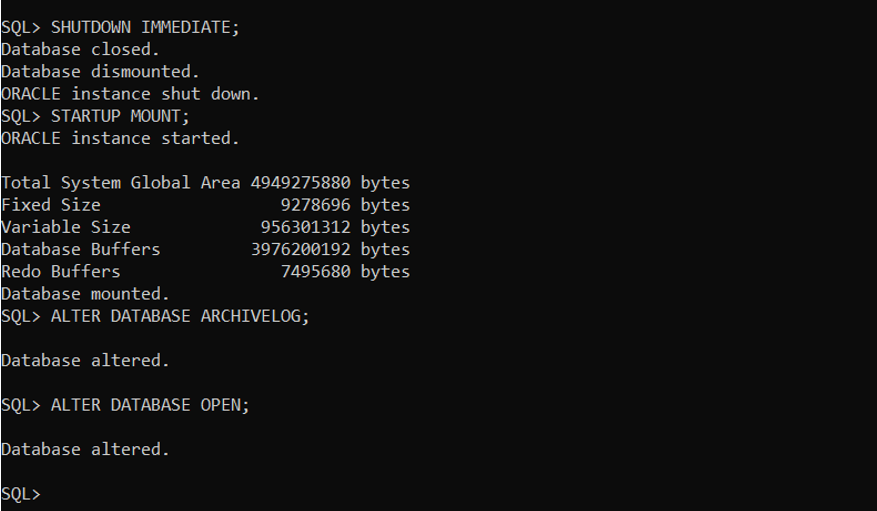


Kada pokrenemo Oracle listener, on počinje da osluškuje na definisanim mrežnim adresama i portovima iz „listener.ora“ fajla.

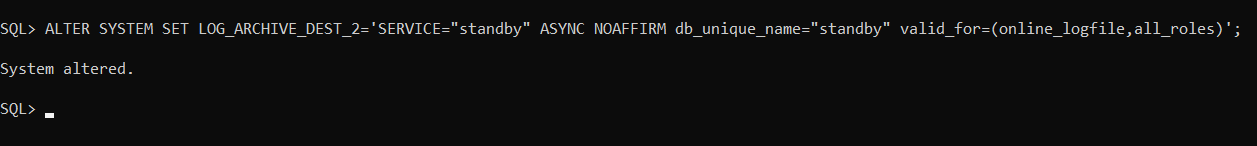


* **Primarna baza podataka**

Povezivanje sa primarnom bazom i omogućavanje arhiviranja redo logova (ARCHIVELOG mode). ARCHIVELOG mod omogućava arhiviranje redo logova, što je neophodno za slanje i primanje promena između primarne i sekundarne baze.



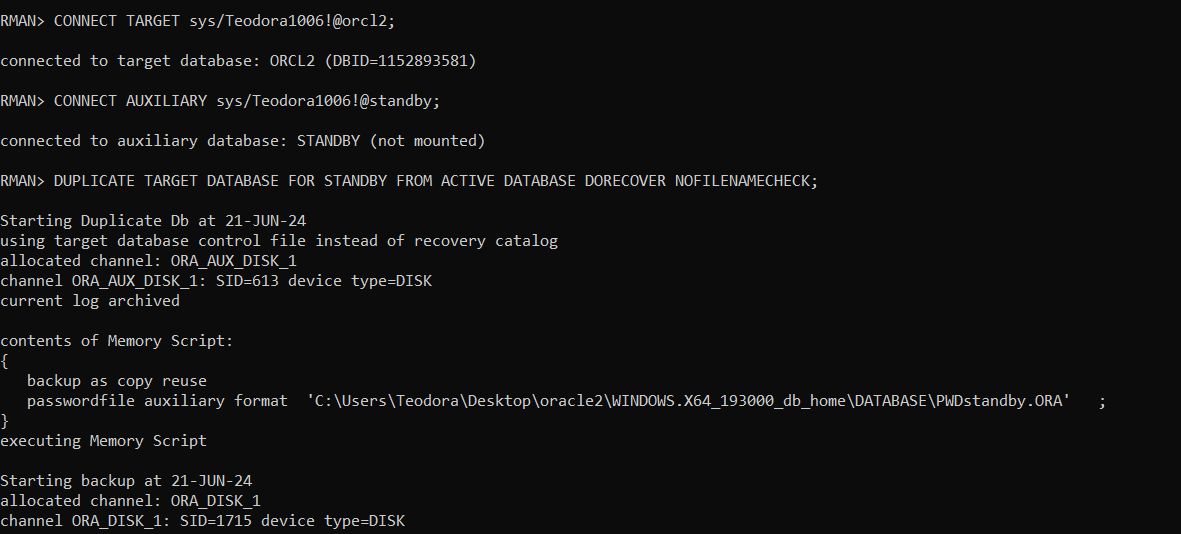
Konfiguracija specifičnih parametara u spfile datoteci je neophodna da bi se primarna baza pravilno sinhronizovala sa standby bazom.



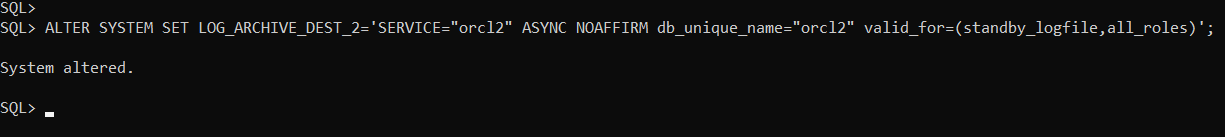


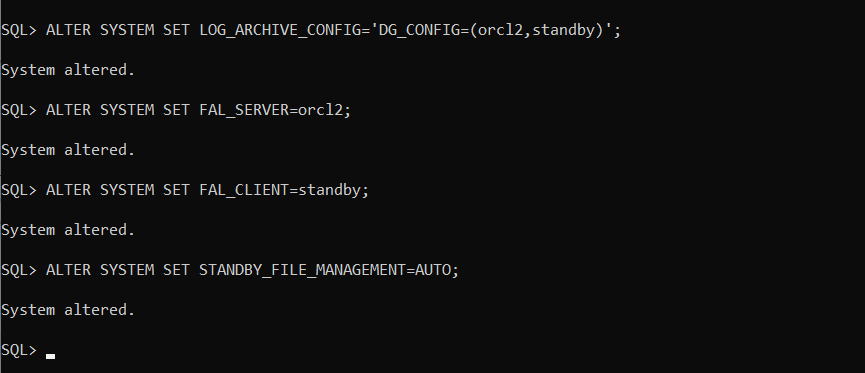
* **Kreiranje standby baze na osnovu postojeće primarne baze**

RMAN funkcija DUPLICATE omogućava kopiranje ili dupliranje baze podataka iz primarne (aktivne) baze u sekundarnu (rezervnu) bazu podataka. Kroz proces dupliranja, RMAN se povezuje s primarnom bazom kao izvorom podataka (TARGET), dok se takođe povezuje i sa sekundarnom bazom kao destinacijom (AUXILIARY). Ovaj postupak osigurava da se podaci sigurno kopiraju i repliciraju između ta dva okruženja.



Postavljanje relevantnih parametara u spfile datoteci standby baze. Ovi parametri su neophodni za pravilno konfigurisanje i sinhronizaciju sa primarnom bazom.





Nakon ovoga sledi konfiguracija Data Guard Broker-a, što će biti obrađeno u nastavku.

**Korišćenje Oracle Data Guard Broker sa Oracle Data Guard-om**

Korišćenje Oracle Data Guard broker-a za kreiranje, upravljanje i praćenje Oracle Data Guard konfiguracije.

Moguće je obavljati sve operacije upravljanja Data Guard-om lokalno ili daljinski koristeći brokerske interfejse: stranice za upravljanje Data Guard-om u Oracle Enterprise Manager-u, koji je grafički korisnički interfejs brokera, i Data Guard komandno-linijski interfejs, poznat kao DGMGRL.

Brokerski interfejsi poboljšavaju upotrebljivost, centralizuju upravljanje i praćenje Data Guard konfiguracije. Dostupan kao funkcija Oracle Database Enterprise Edition i Personal Edition, broker je takođe integrisan sa Oracle Database-om, Oracle Enterprise Manager-om i Oracle Cloud Control Plane-om.

**Primer instalacije i konfiguracije brokera**

Prethodni uslovi:

* Primarna baza podataka, rezervna baza podataka i posmatrači smešteni su na odvojenim serverima i hardverskim resursima radi izolacije grešaka.
* Sve primarne i rezervne baze podataka moraju koristiti SPFILE.
* Postaviti inicijalni parametar DG\_BROKER\_START na TRUE.
* Ako je neka od baza podataka u konfiguraciji Oracle RAC, neophodno je da se inicijalni parametri DG\_BROKER\_CONFIG\_FILEn podešavaju tako da pokazuju na iste deljene datoteke za sve instance te baze podataka. Ove deljene datoteke mogu biti smeštene na klaster fajl sistemu, ako su dostupne, na sirovim uređajima ili korišćenjem Oracle Automatic Storage Management.

1. Ukoliko ne postoje, potrebno je kreirati Oracle Net Services aliase koji omogućavaju povezivanje sa primarnom i rezervnom bazom podataka. Ovi aliasi treba da budu prisutni u bazi podataka na svakom domaćinu ili članu Data Guard konfiguracije. Za Oracle RAC konfiguracije, aliasi bi trebalo da se povežu koristeći SCAN naziv.

chicago =

(DESCRIPTION =

(ADDRESS\_LIST =

(ADDRESS=(PROTOCOL= TCP)

(HOST=prmy-scan)(PORT=1521)))

(CONNECT\_DATA =

(SERVER = DEDICATED)

(SERVICE\_NAME = chicago)))

boston =

(DESCRIPTION =

(ADDRESS\_LIST =

(ADDRESS=(PROTOCOL= TCP)

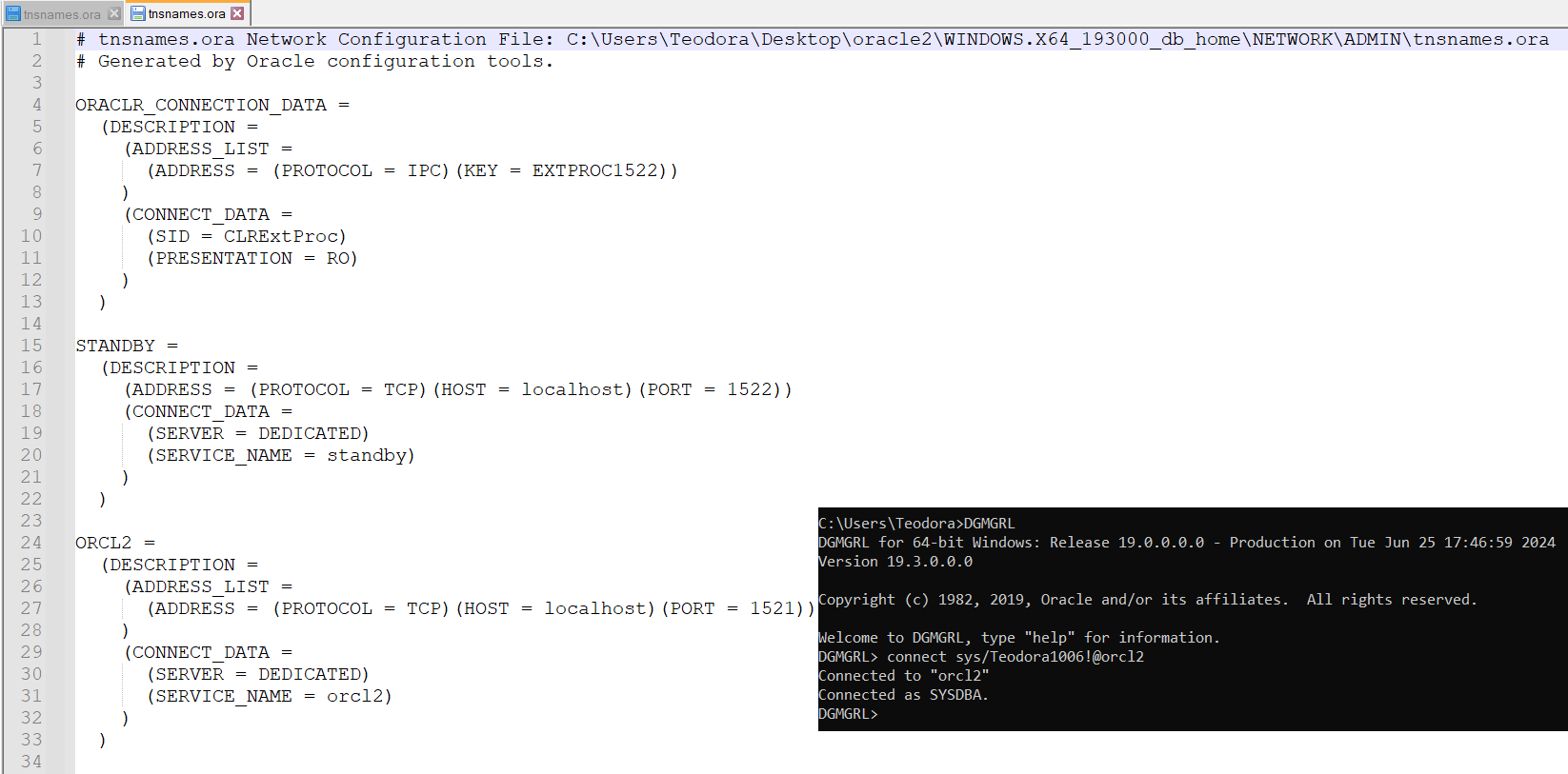
(HOST=stby-scan)(PORT=1521)))

(CONNECT\_DATA =

(SERVER = DEDICATED)

(SERVICE\_NAME = boston)))

**Primer 5.2** orcl2 i standby su aliasi za Oracle baze podataka definirani u „tnsnames.ora“ datoteci. Ovi aliasi omogućuju jednostavan pristup bazama podataka Oracle klijentima putem Oracle Net Services, ključan za upravljanje podacima u raznim scenarijima kao što su visoka dostupnost i otpornost na kvarove.



1. Na primarnom domaćinu, povezati se sa DGMGRL-om i kreirati konfiguraciju.

$ dgmgrl sys

Enter password: password

DGMGRL> create configuration 'dg\_config' as primary database is 'chicago' connect identifier is chicago;

Configuration "dg\_config" created with primary database "chicago"

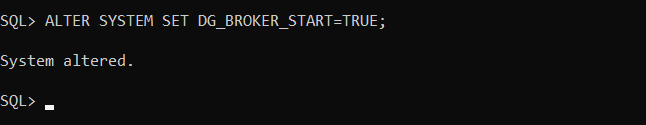
DGMGRL> add database 'boston' as connect identifier is boston;

Database "boston" added

DGMGRL> enable configuration;

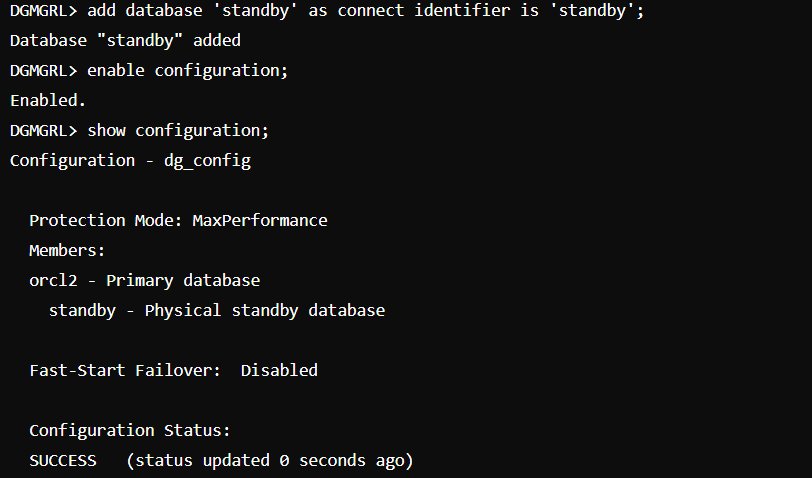
Enabled.

**Primer 5.3** Postavljanjem DG\_BROKER\_START=TRUE omogućuje se Oracle Data Guard broker za upravljanje visokom dostupnošću i zaštitom podataka. U DGMGRL-u je definisana nova konfiguracija 'dg\_config' sa primarnom bazom 'orcl2' i dodata sekundarna baza 'standby'. Nakon aktivacije konfiguracije 'dg\_config' omogućeno je upravljanje Data Guardom, a naredba show configuration prikazuje trenutno postavljenu konfiguraciju, uključujući detalje o primarnoj i sekundarnim bazama podataka.









1. Podrazumevano, broker podešava LOG\_ARCHIVE\_DEST\_n za režim zaštite baze podataka "Maximum Performance". Broker konfiguriše udaljene destinacije arhiviranja sa podrazumevanim vrednostima za asinhroni transport, kao što je prikazano.

log\_archive\_dest\_3=service="boston", ASYNC NOAFFIRM delay=0 optional compression=disable max\_failure=0 reopen=300 db\_unique\_name="boston" net\_timeout=30, valid\_for=(online\_logfile,all\_roles)

**Konfigurisanje režima transporta redo zapisa**

Na svakom članu konfiguracije konfigurišite uslugu transporta redo zapisa postavljanjem svojstva LogXptMode na jedan od sledećih režima.

ASYNC konfiguriše uslugu transporta redo zapisa za ovu rezervnu bazu podataka koristeći ASYNC i NOAFFIRM atribute inicijalnog parametra LOG\_ARCHIVE\_DEST\_n. Ovaj režim, zajedno sa standby redo log fajlovima, omogućava zaštitu podataka sa minimalnim gubitkom podataka koji može biti nekoliko sekundi uz zanemarljiv uticaj na performanse.

FASTSYNC konfiguriše uslugu transporta redo zapisa za ovu rezervnu bazu podataka koristeći SYNC i NOAFFIRM atribute inicijalnog parametra LOG\_ARCHIVE\_DEST\_n. Konfigurišite sinhroni režim transporta redo zapisa sa NOAFFIRM atributom (podrazumevano je AFFIRM) kada koristite režim maksimalne dostupnosti zaštite. Ovo pomaže u minimalizaciji uticaja na performanse sinhronog transporta redo zapisa potvrđivanjem prijema redo zapisa nakon što su uspešno primljeni i verifikovani u memoriji standby, ali pre nego što su zapisi stvarno napisani u standby redo log. Zaštita bez gubitka podataka i dalje je obezbeđena u slučaju kvara primarne baze podataka.

SYNC konfiguriše uslugu transporta redo zapisa za ovu rezervnu bazu podataka koristeći SYNC i AFFIRM atribute inicijalnog parametra LOG\_ARCHIVE\_DEST\_n. Ovaj režim, zajedno sa standby redo log fajlovima, zahteva se za konfiguracije koje rade u režimu maksimalne zaštite ili maksimalne dostupnosti. Ova usluga transporta redo zapisa omogućava zaštitu podataka bez gubitka podataka za primarnu bazu podataka, ali može imati veći uticaj na performanse u slučaju da je latencija između primarne i standby baze visoka (npr. više od 2 ms).

Koristite komandu EDIT DATABASE SET PROPERTY kako biste postavili režim transporta u konfiguraciji brokera, kako je prikazano u navedenim primerima.

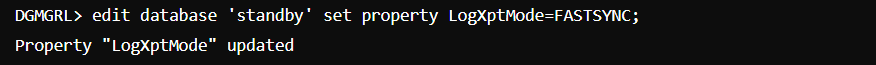
DGMGRL> EDIT DATABASE 'boston' SET PROPERTY LogXptMode=ASYNC;

DGMGRL> EDIT DATABASE 'chicago' SET PROPERTY LogXptMode=FASTSYNC;

DGMGRL> EDIT DATABASE 'SanFran' SET PROPERTY LogXptMode=SYNC;

**Primer 5.4** Konfigurisanje načina replikacije redo log zapisa između primarne i sekundarne baze podataka u Oracle Data Guardu. Postavlja se asinhroni (ASYNC) način replikacije redo log zapisa za primarnu bazu 'orcl2', što omogućuje da se transakcije na primarnoj bazi ne zaustavljaju čekajući potvrdu od sekundarne baze. Za sekundarnu bazu 'standby' postavlja se brzo-sinhronizovani (FASTSYNC) način replikacije, koji kombinuje brzinu asinhronog repliciranja s dodatnim sigurnosnim mehanizmima za zaštitu podataka.





**Konfigurisanje brzog početka greške (Fast Start Failover)**

Brzo pokretanje prekida u radu omogućava automatsko prebacivanje na prethodno odabranu rezervnu bazu podataka u slučaju gubitka primarne baze podataka. Omogućavanje brzog pokretanja prekida u radu je ključno za ispunjenje strogo definisanih zahteva za vreme povratka na rad (RTO) u situacijama kada dođe do kvara primarne baze podataka, klastera ili lokacije.

Ova funkcionalnost omogućava brzo i pouzdano prebacivanje ciljne rezervne baze podataka u ulogu primarne, bez potrebe za ručnim intervencijama. Brzo pokretanje prekida u radu može se implementirati samo u okviru konfiguracije brokera.

U slučaju kada primarna baza podataka ima više rezervnih baza podataka, moguće je definisati više ciljnih meta za brzo pokretanje prekida u radu, koristeći svojstvo FastStartFailoverTarget. Ove mete se nazivaju kandidatima za prekidanje rada. Broker bira metu na osnovu redosleda specificiranog u svojstvu FastStartFailoverTarget. U situaciji kada određena ciljna meta za brzo pokretanje prekida u radu dođe do problema i nije u stanju da preuzme ulogu primarne baze podataka, broker automatski bira drugu ciljnu metu.

Brzo pokretanje prekida u radu može se koristiti u kombinaciji sa svim režimima zaštite. Režimi maksimalne zaštite i maksimalne dostupnosti obezbeđuju automatsko okruženje za prekid u radu u kojem se garantuje očuvanje svih podataka. Režim maksimalne performanse omogućava automatski prekid u radu uz minimalan gubitak podataka, koji je definisan svojstvom FastStartFailoverLagLimit. Ovo svojstvo određuje maksimalni dozvoljeni gubitak podataka u sekundama prilikom automatskog prekida u radu, i koristi se samo kada je omogućeno brzo pokretanje prekida u radu i konfiguracija funkcioniše u režimu maksimalne performanse.

1. Postaviti svojstvo FastStartFailoverThreshold da bi specificirali broj sekundi koje želimo da posmatrač i ciljna rezervna baza podataka čekaju, nakon što detektuju da primarna baza podataka nije dostupna, pre nego što pokrenu prekid u radu, kao što je prikazano u ovom primeru.

DGMGRL> EDIT CONFIGURATION SET PROPERTY FastStartFailoverThreshold = seconds;

Brzo pokretanje prekida u radu se dešava kada posmatrač i rezervna baza podataka izgube kontakt sa proizvodnom bazom podataka na period duži od vrednosti postavljene za FastStartFailoverThreshold, i kada se oba učesnika slože da je stanje konfiguracije sinhronizovano (Maksimalna dostupnost), ili da kašnjenje nije veće od konfigurisane vrednosti FastStartFailoverLagLimit (Maksimalna performansa).

Optimalna vrednost za FastStartFailoverThreshold balansira između brzog prekida u radu (minimalno vreme nedostupnosti) i izbegavanja nepotrebnog pokretanja prekida zbog privremenih mrežnih nepravilnosti ili drugih kratkotrajnih događaja koji nemaju značajan uticaj na dostupnost.

Podrazumevana vrednost za FastStartFailoverThreshold je 30 sekundi.

U sledećoj tabeli 5.1 su prikazana preporučena podešavanja za FastStartFailoverThreshold u različitim scenarijima korišćenja.

|  |  |
| --- | --- |
| **Konfiguracija** | **Minimalno preporučeno podešavanje** |
| Jedna instanca primarne baze podataka, niska latencija i pouzdana mreža | 15 sekundi |
| Jedna instanca primarne baze podataka i mreža sa visokom latencijom preko WAN-a | 30 sekundi |
| Oracle RAC primarna baza podataka | Vreme Oracle RAC ponovnog brojanja + vreme rekonfiguracije + 30 sekundi |

**Tabela 5.1** Minimalno preporučena podešavanja za FastStartFailoverThreshold

**Primer 5.5** Komandom EDIT CONFIGURATION SET PROPERTY FastStartFailoverThreshold = 30 u Oracle Data Guard Manager Command-Line Interface (DGMGRL) postavlja se vreme (u sekundama) koje primarna baza podataka može biti nedostupna pre nego što se automatski pokrene brzi failover na rezervnu (sekundarnu) bazu. U ovom slučaju, vrednost je podešena na 30 sekundi, čime se definiše prag za automatsko prebacivanje na rezervnu bazu u slučaju problema sa primarnom bazom.



1. Odrediti gde će se postaviti posmatrač u topologiji.

U idealnom scenariju, brzo pokretanje prekida u radu se implementira sa primarnom bazom podataka, rezervnom bazom podataka i posmatračem, svaki u svojoj dostupnoj domeni (AD) ili data centru; međutim, podržavaju se i konfiguracije koje koriste samo dve dostupne domene, pa čak i jednu dostupnu domenu. Sledeće su preporuke za postavljanje posmatrača za dva scenarija korišćenja.

Konfiguracija implementacije 1: 2 regiona sa po dve AD u svakom regionu.

* Početni primarni region ima primarnu bazu podataka u AD1, i dva posmatrača visoke dostupnosti (jedan posmatrač u AD2 i drugi posmatrač u AD1)
* Početni rezervni region ima rezervnu bazu podataka u AD1, i dva posmatrača visoke dostupnosti koji se koriste nakon promene uloga (jedan posmatrač u AD2 i drugi posmatrač u AD1)
* Za posmatrača, MAA (Maximum Availability Architecture) preporučuje najmanje 2 ciljne mete posmatrača u istom primarnom regionu, ali u različitim AD-ovima.

Konfiguracija implementacije 2: 2 regiona sa po samo 1 AD u svakom regionu.

* Početni primarni regioni imaju primarnu bazu podataka i dva servera male težine za smeštanje posmatrača.
* Početni rezervni region ima rezervnu bazu podataka i dva servera male težine za smeštanje posmatrača (kada dođe do promene uloga).

1. Konfigurisanje visoke dostupnosti posmatrača.

Možete registrovati do tri posmatrača za praćenje jedne konfiguracije Data Guard brokera. Svaki posmatrač je identifikovan imenom koje zadajete prilikom izdavanja komande START OBSERVER. Takođe, posmatrače možete pokrenuti kao pozadinski proces.

DGMGRL> sys@boston

Enter password: password

DGMGRL> start observer number\_one in background;

Na istom ili drugom hostu možete pokrenuti dodatne posmatrače za visoku dostupnost:

DGMGRL> sys@boston

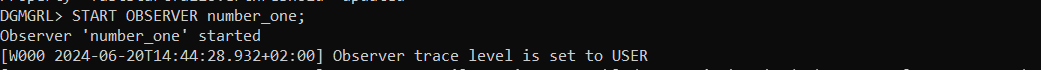
Enter password: password

DGMGRL> start observer number\_two in background;

Samo primarni posmatrač može koordinirati brzo pokretanje prekida u radu sa Data Guard brokerom. Svi ostali registrovani posmatrači se smatraju rezervnim posmatračima.

Ako posmatrač nije pokrenut kao pozadinski proces, on je kontinuirano pokrenuti proces koji se kreira kada se izda komanda START OBSERVER. Stoga, komandna linija na računaru posmatrača neće se vratiti sve dok ne izdate komandu STOP OBSERVER iz druge DGMGRL sesije. Da biste izdali komande i interagirali sa konfiguracijom brokera, morate se povezati koristeći drugu DGMGRL klijentsku sesiju.

**Primer 5.6** Komanda start observer number\_one u DGMGRL (Data Guard Manager) interfejsu pokreće posmatrača sa imenom number\_one. Posmatrač nadgleda stanje primarne baze i, u slučaju da primarna baza postane nedostupna, može automatski prebaciti ulogu primarne baze na jednu od rezervnih baza.



Sada kada je brzo pokretanje prekida u radu pravilno konfigurisano, sledeći uslovi mogu izazvati prekid u radu:

* Kvar baze podataka gde su sve instance baze podataka nedostupne.
* Datoteke podataka su offline zbog I/O grešaka.
* Gubitak mrežne veze između posmatrača i rezervne baze podataka sa proizvodnom bazom podataka, uz potvrdu da je rezervna baza podataka u sinhronizovanom stanju.
* Korisnički konfigurisan uslov.

Opciono, možete specificirati sledeće uslove za koje se može pokrenuti brzo pokretanje prekida u radu. Preporučuje se da ostavite ove korisnički konfigurisane uslove na podrazumevanim vrednostima i da ne aktivirate automatski prekid u radu:

* Datoteka podataka je offline zbog greške pri pisanju.
* Oštećen rečnik.
* Oštećena kontrolna datoteka.
* Nedostupna log datoteka.
* Zaglavljen arhiver.
* ORA-240 (timeout enkju pri kontrolnoj datoteci).

U slučaju da se detektuje jedan od ovih uslova, posmatrač prelazi na rezervnu bazu podataka, dok se primarna baza isključuje, bez obzira na podešavanja za FastStartFailoverPmyShutdown. Važno je napomenuti da za korisnički konfigurisane uslove prag za brzo pokretanje prekida u radu nije primenjen i prekid u radu se odvija odmah.

## **Optimizacija i rešavanje problema u Oracle Data Guard-u**

Kada procesi prenosa redo zapisa, primene redo zapisa ili tranzicije uloga u Oracle Data Guard-u ne ispunjavaju očekivane zahteve, sledeće smernice mogu pomoći u efikasnom optimizovanju i rešavanju problema.

**Pregled optimizacije i rešavanja problema u Oracle Data Guard-u**

Da bi postigli optimalne performanse Oracle Data Guard konfiguracije, važno je primenjivati Oracle Maximum Availability Architecture (MAA) preporučene prakse za praćenje, procenu i optimizaciju performansi.

* Uverite se da su Oracle Database i Oracle Data Guard konfigurisani u skladu sa preporučenim praksama.

Pre nego što započnete sa optimizacijom, pretpostavlja se da su sve relevantne Oracle Database i Data Guard preporučene prakse već implementirane i ispravno funkcionišu. Evaluacija poštovanja ovih praksi je ključna pre nego što započnete bilo kakvo podešavanje.

* Procena i optimizacija usluga prenosa redo zapisa

Oracle Data Guard automatski podešava prenos redo zapisa radi optimizacije performansi. Međutim, ako primetite probleme sa performansama, možete pratiti i optimizovati usluge prenosa redo zapisa.

Asinhroni prenos redo zapisa sa modom zaštite podataka Maximum Performance je podrazumevana konfiguracija u Oracle Data Guard-u. Optimizacija asinhronog prenosa redo zapisa uglavnom se sastoji od osiguravanja da su resursi na primarnoj, rezervnoj i mrežnoj strani dovoljni za obradu radnog opterećenja, kao i praćenje tih resursa kako bi se identifikovala moguća uska grla.

Sinhroni prenos redo zapisa žrtvuje nešto performansi u korist nultog gubitka podataka. Ipak, primenom preporučenih MAA metoda omogućava se praćenje i procena uticaja, uz pravilno raspoređivanje resursa.

* Procena i optimizacija primene redo zapisa

U većini slučajeva, podrazumevane Oracle postavke pružaju zadovoljavajuće performanse za medijski oporavak, pod pretpostavkom da je standby baza uvek ažurirana. Međutim, kako aplikacije i veličina baze podataka rastu, moguće je da će operacije medijskog oporavka imati koristi od dodatne optimizacije kako bi se dalje smanjilo vreme oporavka ili povećala propusna moć primene redo zapisa na standby bazi podataka.

* Procena i optimizacija tranzicija uloga

Efikasno planiranje i implementacija tranzicija uloga u Oracle Data Guard-u i Active Data Guard-u može značajno smanjiti vreme nedostupnosti i obezbediti brzu obnovu okruženja baze podataka uz minimalan uticaj na poslovanje. Testiranja performansi korišćenjem fizičke standby baze podataka i pridržavanje Oracle Maximum Availability Architecture (MAA) preporučenih praksi pokazala su da se procesi prebacivanja i prelaska na standby bazu mogu svesti na svega nekoliko sekundi.

# **Zaključak**

Cilj ovog seminarskog rada je pružiti sveobuhvatan pregled i praktične smernice za postizanje visoke dostupnosti u Oracle bazama podataka, što je od suštinskog značaja za savremeni poslovni svet koji zahteva stalnu dostupnost i zaštitu podataka. U današnjem okruženju, gde je neprekidan pristup informacijama kritičan za poslovanje, implementacija pouzdanih rešenja za visoku dostupnost postaje imperativ.

Ovaj rad predstavlja osnovu za razumevanje ključnih tehnologija i metoda koje Oracle nudi u oblasti visoke dostupnosti. Opisani su alati i tehnologije kao što su Oracle Data Guard, Oracle GoldenGate, Recovery Manager, te Oracle Real Application Clusters (RAC) i Oracle Clusterware, koji zajedno obezbeđuju robustan sistem sposoban da izdrži različite izazove i nepredviđene situacije.

Praktični primeri koji su uključeni u rad dodatno obogaćuju sadržaj i pružaju konkretne uvide u implementaciju i optimizaciju Oracle rešenja. Ovi primeri služe kao vodič IT stručnjacima, pomažući im da primene najbolje prakse u stvarnim situacijama i unaprede pouzdanost svojih sistema.

Međutim, ovo istraživanje je samo početna tačka. Postoji mnogo prostora za dalja unapređenja i dopune, kako u teorijskom, tako i u praktičnom smislu. Tehnologije se neprestano razvijaju, a sa njima i najbolji načini njihove implementacije. Stoga je kontinuirano učenje i prilagođavanje novim alatima i tehnikama neophodno za održavanje visoke dostupnosti.

Postizanje visoke dostupnosti nije jednokratni cilj, već kontinuiran proces koji zahteva stalno prilagođavanje i unapređenje. Ovaj rad je korak u tom smeru, pružajući potrebne informacije i smernice za implementaciju Oracle rešenja koja garantuju visoku dostupnost i sigurnost podataka.

# **Literatura**

1. „High Availability Overview and Best Practices“, Oracle® Database, June 2024

Dostupno: <https://docs.oracle.com/en/database/oracle/oracle-database/21/haovw/oracle-database-high-availability-overview.html>

1. „Oracle Data Guard Best Practices“, Oracle® Database, June 2024

Dostupno: <https://docs.oracle.com/en/database/oracle/oracle-database/21/haovw/oracle-data-guard-best-practices.html>

1. „Introduction to Oracle Data Guard“, Oracle® Data Guard, July 2022

Dostupno: <https://docs.oracle.com/en/database/oracle/oracle-database/21/sbydb/introduction-to-oracle-data-guard-concepts.html>

1. „High Availability“, Oracle® Database, April 2024

Dostupno: <https://docs.oracle.com/en-us/iaas/Content/cloud-adoption-framework/high-availability.htm>

1. „High Availability Architectures“, Oracle® Database

Dostupno: <https://docs.oracle.com/cd/B13789_01/server.101/b10726/architectures.htm>

1. „High Availability Architectures“, Oracle® Database, May 2017

Dostupno: <https://docs.oracle.com/en/database/oracle/oracle-database/12.2/haovw/ha-architectures.html>

1. „Plan High Availability for Databases“, Oracle® Database, August 2023

Dostupno: [https://docs.oracle.com/en/solutions/design-ha/plan-high-availability-databases1.html](https://docs.oracle.com/en/solutions/design-ha/plan-high-availability-databases1.html#GUID-4D125C76-6017-4CAD-BCB1-06930C6882C2)