

Implementasi Oracle Data Guard dengan Metode Switchover dan Failover di PT. Prima Integrasi Network

Ali Iskandar¹, Devi Yunita²

¹ Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Pamulang

² Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Pamulang

¹aliiskann@gmail.com, ²dosen00846@unpam.ac.id

Info Artikel

Riwayat Artikel:

Received December 03, 2025

Revised December 10, 2025

Accepted December 12, 2025

Abstract – In the era of digital transformation, data has become a highly vital strategic asset for organizational sustainability. PT. Prima Integrasi Network, as an information technology company, heavily relies on reporting applications to support business processes and operational decision-making. However, the current database infrastructure lacks real-time data replication mechanisms, making it vulnerable to various risks such as hardware failures, natural disasters, and human errors that can cause prolonged service disruptions and significant data loss. This research aims to implement Oracle Data Guard as a High Availability and Disaster Recovery solution to ensure data security and availability for the reporting application. The implementation utilizes Oracle Database version 19c Enterprise Edition with Physical Standby Database configuration and Maximum Availability protection mode, specifically analyzing the effectiveness of two main mechanisms: Switchover for planned database role transitions and Failover for automatic recovery during critical failures. The research methodology includes literature review, observation of existing database infrastructure, interviews with Database Administrators and IT Managers, and comprehensive testing of both mechanisms. Results demonstrate that Oracle Data Guard implementation successfully enhances system availability by minimizing Recovery Time Objective (RTO) and Recovery Point Objective (RPO). Switchover can be executed in 3 minutes 39 seconds without data loss, while Failover requires only 32 seconds with zero RPO, ensuring complete data integrity even during sudden failures.

Keywords: Database Replication; Failover; High Availability; Oracle Data Guard; Switchover.

Corresponding Author:

Ali Iskandar

Email: aliiskann@gmail.com



This is an open access article under the [CC BY 4.0](https://creativecommons.org/licenses/by/4.0/) license.

Abstrak – Di era transformasi digital, data telah menjadi aset strategis yang sangat vital bagi keberlangsungan organisasi. PT. Prima Integrasi Network sebagai perusahaan teknologi informasi sangat bergantung pada aplikasi reporting untuk mendukung proses bisnis dan pengambilan keputusan operasional. Namun, infrastruktur database yang ada saat ini belum memiliki mekanisme replikasi data secara real-time, sehingga rentan terhadap berbagai risiko seperti kegagalan perangkat keras, bencana alam, dan kesalahan manusia yang dapat menyebabkan gangguan layanan berkepanjangan dan kehilangan data yang signifikan. Penelitian ini bertujuan untuk mengimplementasikan Oracle Data Guard sebagai solusi High Availability dan Disaster Recovery guna menjamin keamanan dan ketersediaan data pada aplikasi reporting. Implementasi dilakukan menggunakan Oracle Database versi 19c Enterprise Edition dengan konfigurasi Physical Standby Database dan mode proteksi Maximum Availability, yang secara spesifik menganalisis efektivitas dua mekanisme utama yaitu Switchover untuk perpindahan peran database secara terencana dan Failover untuk pemulihan otomatis ketika terjadi kegagalan kritis. Metodologi penelitian meliputi studi pustaka, observasi infrastruktur, wawancara dengan administrator database dan IT manager, serta pengujian komprehensif terhadap kedua mekanisme. Hasil penelitian menunjukkan bahwa implementasi Oracle Data Guard berhasil meningkatkan ketersediaan sistem secara signifikan dengan meminimalkan RTO dan RPO. Switchover dapat dilakukan dalam waktu 3 menit 39 detik tanpa

kehilangan data, sedangkan Failover hanya memerlukan waktu 32 detik dengan RPO nol, memastikan integritas data lengkap bahkan dalam kondisi kegagalan mendadak.

Kata Kunci: Database Replication; Failover; High Availability; Oracle Data Guard; Switchover

1. PENDAHULUAN

Di era transformasi digital yang berkembang pesat, data telah menjadi aset strategis yang sangat vital bagi keberlangsungan dan pertumbuhan organisasi modern. Perusahaan-perusahaan kini sangat bergantung pada ketersediaan data yang akurat dan real-time untuk mendukung proses bisnis kritis dan pengambilan keputusan operasional yang tepat. PT. Prima Integrasi Network sebagai perusahaan teknologi informasi terkemuka sangat mengandalkan aplikasi reporting sebagai tulang punggung operasional untuk memantau performa proyek, menganalisis tren bisnis, dan menghasilkan laporan manajemen yang komprehensif.

Namun demikian, infrastruktur database yang ada saat ini belum memiliki mekanisme replikasi data secara real-time dan sistem disaster recovery yang memadai. Kondisi ini menciptakan single point of failure yang sangat berbahaya, dimana kegagalan pada satu komponen dapat menyebabkan gangguan layanan secara menyeluruh. Sistem saat ini rentan terhadap berbagai risiko seperti kegagalan perangkat keras (hardware failure), bencana alam, serangan siber, kesalahan manusia dalam pengelolaan sistem, dan korupsi data yang dapat menyebabkan gangguan layanan berkepanjangan serta kehilangan data yang sangat signifikan.

Penelitian ini bertujuan untuk mengimplementasikan Oracle Data Guard sebagai solusi High Availability dan Disaster Recovery yang komprehensif guna menjamin keamanan dan ketersediaan data pada aplikasi reporting di PT. Prima Integrasi Network. Oracle Data Guard merupakan teknologi yang menyediakan kemampuan replikasi data real-time, monitoring otomatis yang terintegrasi, dan mekanisme pemulihan yang cepat dan reliable melalui dua metode utama yaitu Switchover untuk perpindahan peran database secara terencana dan terkontrol, serta Failover untuk pemulihan otomatis ketika terjadi kegagalan kritis pada primary database.

Implementasi ini menggunakan Oracle Database versi 19c Enterprise Edition dengan konfigurasi Physical Standby Database dan mode proteksi Maximum Availability yang memberikan keseimbangan optimal antara performa sistem dan proteksi data. Penelitian ini mencakup analisis mendalam terhadap efektivitas kedua mekanisme tersebut dalam menjaga kontinuitas layanan, meminimalkan downtime operasional, memastikan integritas data perusahaan, serta memberikan jaminan keamanan data yang berlapis.

Kontribusi utama penelitian ini meliputi: (1) pengukuran kuantitatif yang detail terhadap Recovery Time Objective (RTO) dan Recovery Point Objective (RPO) untuk kedua mekanisme; (2) analisis komparatif antara Switchover dan Failover dalam berbagai skenario kegagalan; (3) dokumentasi best practices untuk implementasi Oracle Data Guard di lingkungan enterprise; dan (4) evaluasi dampak implementasi terhadap ketersediaan sistem dan keamanan data organisasi.

2. PENELITIAN YANG TERKAIT

Beberapa penelitian terdahulu telah membahas implementasi Oracle Data Guard dalam berbagai konteks organisasi dan industri. Efendi dan Mansuri (2023) [3] melakukan penelitian tentang disaster recovery dengan standby database pada PT. Sigma Solusi Integrasi yang berhasil meningkatkan ketersediaan data secara signifikan dan mengurangi risiko kehilangan data akibat gangguan sistem. Penelitian tersebut membuktikan efektivitas standby database dalam menjaga kontinuitas bisnis, namun tidak mengukur secara spesifik waktu pemulihan dan tidak membedakan antara mekanisme switchover dan failover.

Krisancoyo (2013) [5] melakukan perancangan dan implementasi Maximum Availability menggunakan teknologi Oracle Data Guard pada sistem pencatatan jemaat Gereja Bethany Salatiga yang terbukti efektif dalam meningkatkan keamanan dan ketersediaan data pada sistem pencatatan gereja.

Penelitian ini menunjukkan bahwa Oracle Data Guard dapat diimplementasikan bahkan pada organisasi skala menengah, namun tidak mengeksplorasi mekanisme switchover dan failover secara mendalam serta tidak menyediakan pengukuran RTO dan RPO yang kuantitatif.

Andreansyah (2023) [1] meneliti perlindungan data tingkat tinggi pada aplikasi P2APST PLN melalui disaster recovery center menggunakan Oracle Data Guard di kota Bandung. Penelitian ini fokus pada aspek perlindungan data dan kontinuitas layanan di sektor utilitas publik, namun tidak memberikan analisis mendalam terhadap performa switchover dan failover serta data kuantitatif mengenai waktu pemulihan sistem.

Wibowo et al. (2007) [12] menganalisis dan mengimplementasikan standby database dengan Oracle pada perusahaan jasa komunikasi yang berhasil mengurangi downtime hingga rata-rata 2-3 menit saat terjadi kegagalan sistem. Penelitian ini menunjukkan efektivitas standby database dalam menangani berbagai kondisi kegagalan, namun belum menganalisis perbedaan antara switchover dan failover serta tidak mengimplementasikan mode Maximum Availability yang lebih advance.

Oloruntoba (2024) [7] membahas business continuity dalam sistem database dan peran Data Guard dengan mengeksplorasi keunggulan komparatif dan best practices dalam implementasi Data Guard untuk kelangsungan bisnis. Penelitian ini memberikan framework teoritis yang komprehensif untuk business continuity, namun bersifat konseptual dan belum ada implementasi praktis dengan pengukuran metrik spesifik seperti RTO dan RPO.

Martin (2024) [13] melakukan penelitian tentang peningkatan strategi disaster recovery dan failover dalam Oracle Cloud Databases, yang memberikan perspektif modern tentang implementasi Data Guard dalam lingkungan cloud computing. Stephen dan Ade (2023) [14] membahas strategi backup data dalam disaster recovery untuk memastikan minimal downtime, yang melengkapi pemahaman tentang berbagai pendekatan dalam menjaga ketersediaan data.

Berdasarkan tinjauan literatur tersebut, teridentifikasi research gap yang signifikan dimana penelitian-penelitian sebelumnya belum memberikan analisis kuantitatif yang detail mengenai perbandingan efektivitas switchover dan failover, pengukuran RTO dan RPO yang spesifik, serta implementasi praktis dalam konteks aplikasi reporting enterprise. Penelitian ini akan berkontribusi dengan secara spesifik mengukur dan membandingkan efektivitas kedua mekanisme tersebut dalam menjaga ketersediaan aplikasi reporting di PT. Prima Integrasi Network, termasuk memberikan data empiris lengkap tentang waktu pemulihan, tingkat kehilangan data, dan dampak terhadap operasional bisnis yang belum banyak dibahas pada penelitian-penelitian sebelumnya.

3. METODE PENELITIAN

A. Desain Penelitian

Penelitian ini menggunakan pendekatan Research and Development (R&D) dengan metode eksperimental untuk mengimplementasikan dan menguji Oracle Data Guard dalam lingkungan produksi PT. Prima Integrasi Network. Desain penelitian mencakup tiga fase utama: fase persiapan dan analisis kebutuhan, fase implementasi dan konfigurasi sistem, serta fase pengujian dan evaluasi hasil.

B. Metode Pengumpulan Data

Metodologi pengumpulan data dalam penelitian ini meliputi beberapa teknik komprehensif:

1. **Studi Pustaka** - Mengkaji literatur ilmiah, dokumentasi Oracle resmi, white papers, dan jurnal internasional mengenai high availability, disaster recovery, dan implementasi Oracle Data Guard untuk membangun fondasi teoritis yang kuat.
2. **Observasi Infrastruktur** - Melakukan pengamatan langsung dan analisis mendalam terhadap infrastruktur database yang berjalan saat ini, mengidentifikasi potensi kelemahan, menganalisis pola traffic database, dan mengevaluasi kapasitas sistem existing.

3. **Wawancara Terstruktur** - Melakukan wawancara mendalam dengan Database Administrator (DBA), IT Manager, dan stakeholder kunci untuk memahami kebutuhan bisnis, requirements operasional, dan ekspektasi terhadap sistem high availability.
4. **Pengujian Eksperimental** - Melakukan serangkaian pengujian komprehensif terhadap mekanisme Switchover dan Failover dalam berbagai skenario kegagalan sistem yang disimulasikan secara controlled.

C. Tahapan Implementasi

Implementasi Oracle Data Guard dilakukan melalui tahapan sistematis sebagai berikut:

5. **Persiapan Infrastruktur** - Mempersiapkan dua server dengan spesifikasi identik untuk primary dan standby database, termasuk instalasi Oracle Linux 8, konfigurasi network connectivity, dan setup storage yang adequate.
6. **Instalasi Oracle Database 19c** - Menginstall Oracle Database 19c Enterprise Edition pada kedua server (primary dan standby) dengan konfigurasi parameter yang optimal untuk high availability environment.
7. **Aktivasi Mode Archivelog** - Mengaktifkan mode archivelog pada primary database untuk memungkinkan replikasi redo log secara continuous ke standby database, yang merupakan prerequisite untuk Data Guard.
8. **Konfigurasi Parameter Data Guard** - Mengkonfigurasi parameter spesifik Data Guard pada primary dan standby database, termasuk LOG_ARCHIVE_CONFIG, LOG_ARCHIVE_DEST_n, FAL_SERVER, dan parameter lainnya yang critical untuk replikasi.
9. **Pembuatan Standby Database** - Menggunakan RMAN Duplicate untuk membuat physical standby database dari primary database dengan memastikan sinkronisasi data yang perfect dan konfigurasi yang konsisten.
10. **Setup Data Guard Broker** - Mengaktifkan dan mengkonfigurasi Data Guard Broker untuk otomatisasi management, simplified administration, dan centralized monitoring dari seluruh konfigurasi Data Guard.
11. **Implementasi Maximum Availability Mode** - Mengkonfigurasi protection mode Maximum Availability yang menjamin zero data loss dengan memastikan redo data telah dikirim ke standby sebelum transaksi di-commit pada primary.
12. **Testing dan Validasi** - Melakukan pengujian komprehensif terhadap mekanisme Switchover dan Failover dalam berbagai skenario, termasuk pengukuran waktu pemulihan dan verifikasi integritas data.

D. Metrik Evaluasi

Evaluasi efektivitas implementasi menggunakan beberapa metrik kunci: (1) Recovery Time Objective (RTO) - waktu maksimum yang dapat ditoleransi untuk pemulihan sistem; (2) Recovery Point Objective (RPO) - jumlah maksimum data yang dapat hilang yang masih dapat diterima; (3) Apply Lag - waktu delay antara primary dan standby database; (4) Transport Lag - waktu yang diperlukan untuk transfer redo log; dan (5) Uptime Percentage - persentase waktu sistem tersedia untuk operasional.

Pengujian dilakukan dengan mensimulasikan berbagai skenario kegagalan sistem yang realistis dan mengukur waktu pemulihan (RTO) serta kehilangan data (RPO) untuk setiap mekanisme. Data dikumpulkan melalui log system Oracle, monitoring tools seperti Data Guard Broker, dan observasi langsung terhadap performa sistem selama masa pengujian.

4. HASIL DAN PEMBAHASAN

A. Hasil Implementasi Infrastruktur

Implementasi Oracle Data Guard telah berhasil dilakukan dengan konfigurasi Physical Standby Database menggunakan Oracle Database 19c Enterprise Edition. Infrastruktur yang dibangun terdiri dari dua server database yang terletak di lokasi berbeda untuk memastikan proteksi terhadap bencana. Primary database terletak di data center utama perusahaan, sementara standby database ditempatkan di bencana recovery site yang berjarak sekitar 25 kilometer dari lokasi utama.

Konfigurasi sistem menggunakan mode proteksi Maximum Availability yang memberikan jaminan zero data loss dengan mempertahankan performa yang optimal. Dalam mode ini, transaksi pada primary database hanya akan di-commit setelah redo data berhasil dikirim dan diterima oleh standby database. Hal ini memastikan bahwa tidak ada data yang hilang bahkan dalam kondisi kegagalan mendadak pada primary database.

B. Analisis Performa Switchover

Pengujian mekanisme Switchover dilakukan sebanyak 10 kali dalam kondisi yang berbeda-beda untuk mendapatkan data yang reliable. Switchover merupakan perpindahan peran database yang terencana dan terkontrol, dimana primary database berubah menjadi standby dan sebaliknya. Hasil pengujian menunjukkan bahwa proses Switchover dapat diselesaikan dengan rata-rata waktu 3 menit 39 detik (219 detik) tanpa kehilangan data sama sekali.

Tahapan Switchover meliputi: (1) Verifikasi readiness dari kedua database (15-20 detik); (2) Flush dan close redo log pada primary (20-25 detik); (3) Transfer final redo data ke standby (30-40 detik); (4) Apply remaining redo pada standby (40-50 detik); (5) Konversi standby menjadi primary dan sebaliknya (60-80 detik); (6) Open database dalam mode baru (30-40 detik); dan (7) Verifikasi final dan restart services (20-30 detik).

Keuntungan utama Switchover adalah prosesnya yang controlled dan predictable, memungkinkan dilakukan maintenance terencana tanpa risiko data loss. Downtime yang terjadi hanya 3-4 menit, yang sangat acceptable untuk maintenance window. RPO untuk Switchover adalah nol karena semua transaksi yang sudah di-commit dipastikan telah direplikasi sebelum proses switchover dimulai.

C. Analisis Performa Failover

Pengujian mekanisme Failover disimulasikan dengan mematikan primary database secara mendadak untuk meniru kondisi kegagalan kritis seperti hardware failure atau bencana. Hasil pengujian menunjukkan bahwa Failover dapat diselesaikan dalam waktu rata-rata 32 detik dengan RPO (Recovery Point Objective) nol, yang berarti tidak ada data yang hilang bahkan dalam kondisi kegagalan yang tidak terencana.

Proses Failover yang cepat ini dimungkinkan karena: (1) Standby database sudah dalam kondisi synchronized dan ready; (2) Mode Maximum Availability memastikan semua committed transaction sudah ada di standby; (3) Data Guard Broker melakukan automatic failover orchestration; dan (4) Konfigurasi Fast-Start Failover (FSFO) yang telah diaktifkan memungkinkan automatic role transition tanpa intervensi manual.

Tahapan Failover meliputi: (1) Detection of primary failure oleh Observer (5-8 detik); (2) Automatic failover decision making (2-3 detik); (3) Apply remaining redo data pada standby (8-10 detik); (4) Konversi standby menjadi primary (10-12 detik); (5) Open database untuk aplikasi (5-7 detik). Total waktu dari failure detection hingga database ready adalah sekitar 30-40 detik.

D. Perbandingan Switchover vs Failover

Tabel I menunjukkan perbandingan komprehensif antara mekanisme Switchover dan Failover:

Tabel 1. 1 Perbandingan Switchover dan Failover

Aspek	Switchover	Failover
Waktu Pemulihan (RTO)	3 menit 39 detik	32 detik
Data Loss (RPO)	Zero (0 detik)	Zero (0 detik)
Tipe Operasi	Terencana	Emergency
Intervensi Manual	Ya (DBA initiated)	Tidak (Automatic)
Bidirectional	Ya (reversible)	Tidak (one-way)
Use Case	Maintenance, upgrade	Hardware failure, disaster

E. Analisis Keamanan Data

Implementasi Oracle Data Guard memberikan proteksi keamanan data yang berlapis (layered protection). Pertama, mekanisme replikasi real-time memastikan bahwa setiap perubahan data pada primary database segera direplikasi ke standby database, sehingga meminimalkan risiko kehilangan data sensitif perusahaan. Dengan apply lag di bawah 5 detik, sistem mampu mempertahankan konsistensi data dengan sangat baik.

Kedua, sistem keamanan yang terintegrasi mencakup validasi log transaksi secara otomatis untuk mendeteksi dan mencegah korupsi data. Data Guard melakukan continuous validation terhadap redo stream untuk memastikan integritas data. Ketiga, enkripsi transmisi data antara primary dan standby database melindungi data dari ancaman intersepsi selama proses replikasi melalui jaringan.

Keempat, setiap operasi administratif dicatat dalam audit log dengan informasi timestamp, identitas pengguna, dan detail aktivitas, sehingga mendukung compliance terhadap regulasi keamanan data dan memudahkan forensik digital jika diperlukan. Kelima, fitur monitoring real-time memberikan visibilitas penuh terhadap status replikasi, gap analysis, dan potensi ancaman keamanan, sehingga administrator dapat segera mengambil tindakan preventif sebelum terjadi insiden yang mengancam keamanan data.

F. Dampak terhadap Ketersediaan Sistem

Implementasi Oracle Data Guard telah meningkatkan ketersediaan sistem secara dramatis. Sebelum implementasi, sistem memiliki Single Point of Failure dimana kegagalan pada satu komponen dapat menyebabkan downtime berkepanjangan. Setelah implementasi, sistem kini memiliki redundansi geografis dengan primary dan standby database di lokasi terpisah, sehingga mampu bertahan terhadap bencana di salah satu lokasi.

Uptime sistem meningkat dari sekitar 99.5% menjadi 99.95%, yang berarti pengurangan downtime dari sekitar 43.8 jam per tahun menjadi hanya 4.38 jam per tahun. Peningkatan ini sangat signifikan untuk business continuity perusahaan. Aplikasi reporting yang sebelumnya sering mengalami gangguan kini dapat beroperasi secara kontinyu dengan availability yang sangat tinggi.

Dari aspek performa aplikasi, tidak terdeteksi penurunan performa yang signifikan setelah implementasi Data Guard. Overhead replikasi sangat minimal karena menggunakan metode asynchronous redo transport untuk mode Maximum Availability. Latency aplikasi tetap stabil dan bahkan sedikit membaik karena sistem sekarang lebih reliable dan tidak mengalami interupsi mendadak.

G. Tantangan dan Solusi

Beberapa tantangan ditemui selama implementasi. Pertama, kompleksitas konfigurasi initial setup memerlukan pemahaman mendalam tentang arsitektur Oracle Database dan networking. Solusinya adalah melakukan training intensif untuk tim DBA dan mengikuti best practices dari Oracle documentation serta berkonsultasi dengan Oracle support.

Kedua, network connectivity antara primary dan standby site harus stabil dan memiliki bandwidth yang adequate. Solusinya adalah melakukan upgrade koneksi network dengan dedicated line dan implementasi redundant network path untuk memastikan availability jalur replikasi.

Ketiga, koordinasi dengan aplikasi team untuk memastikan connection failover yang smooth. Solusinya adalah mengimplementasikan connection pooling dan automatic retry logic pada aplikasi layer, serta menggunakan Service Name yang dapat otomatis redirect ke database yang aktif setelah role transition.

5. KESIMPULAN

Implementasi Oracle Data Guard dengan metode switchover dan failover pada aplikasi reporting di PT. Prima Integrasi Network telah berhasil meningkatkan ketersediaan dan keamanan data secara signifikan. Melalui tahapan konfigurasi, deployment, dan pengujian yang sistematis, sistem kini mampu menghindari single point of failure dengan adanya replikasi data real-time antara primary dan standby database yang terletak di lokasi geografis berbeda.

Mekanisme switchover dan failover terbukti sangat efektif dalam menjaga kontinuitas layanan aplikasi dengan tingkat keamanan data yang terjamin. Hasil pengujian menunjukkan bahwa proses switchover dapat dilakukan dalam waktu 3 menit 39 detik tanpa kehilangan data sama sekali, sedangkan failover hanya memerlukan waktu 32 detik dengan RPO (Recovery Point Objective) nol. Kedua mekanisme tersebut memastikan integritas data terjaga sepenuhnya selama proses transisi, dengan audit trail yang mencatat setiap aktivitas untuk keperluan compliance dan investigasi.

Oracle Data Guard dengan mode proteksi Maximum Availability memberikan keseimbangan optimal antara perlindungan data, keamanan informasi, dan kinerja sistem. Dengan apply lag di bawah 5 detik, sistem mampu mempertahankan konsistensi data dan mendukung kebutuhan bisnis yang memerlukan akses data secara real-time tanpa mengorbankan aspek keamanan. Mode Maximum Availability secara khusus dirancang untuk mencegah kehilangan data dengan memastikan bahwa transaksi pada primary database hanya dianggap berhasil (committed) setelah redo log berhasil dikirim ke standby database.

Penggunaan Data Guard Broker mempermudah manajemen dan pemantauan konfigurasi Oracle Data Guard sekaligus memperkuat aspek keamanan operasional. Antarmuka terpusat yang disediakan oleh DGMGRL memungkinkan administrator untuk melakukan operasi switchover, failover, dan validasi konfigurasi dengan lebih efisien sambil mempertahankan kontrol keamanan yang ketat. Fitur monitoring real-time memberikan visibilitas penuh terhadap status replikasi, gap analysis, dan potensi ancaman keamanan.

Penelitian ini telah memenuhi tujuan yang ditetapkan dengan memberikan solusi high availability dan disaster recovery yang andal dengan proteksi keamanan berlapis yang mencakup pencegahan kehilangan data, deteksi korupsi data, enkripsi transmisi, dan audit trail yang komprehensif. Implementasi ini berhasil mengurangi risiko keamanan data dari nilai tinggi menjadi nilai yang dapat ditoleransi melalui redundansi geografis dan mekanisme failover otomatis.

Rekomendasi untuk Pengembangan Lebih Lanjut:

1. Pertimbangkan upgrade ke Oracle Active Data Guard untuk memanfaatkan standby database untuk keperluan read-only reporting, sehingga mengurangi beban pada primary database sekaligus mengoptimalkan penggunaan sumber daya infrastruktur.

2. Implementasikan sistem pemantauan otomatis yang dilengkapi dengan notifikasi real-time untuk mendeteksi gangguan seperti apply lag, kegagalan replikasi, atau perubahan status database menggunakan Oracle Enterprise Manager atau solusi monitoring lainnya.
3. Tingkatkan kapasitas dan redundansi jaringan antara primary dan standby site melalui implementasi multipath networking atau dedicated VLAN untuk mengurangi risiko gangguan akibat masalah jaringan.
4. Susun dokumen Standard Operating Procedure (SOP) yang lengkap mengenai tata kelola Oracle Data Guard, termasuk prosedur switchover, failover, pemulihan database, dan pelatihan rutin bagi tim IT.
5. Lakukan pengujian switchover dan failover secara berkala (minimal setiap 6 bulan) serta simulasi disaster recovery untuk memvalidasi efektivitas rencana pemulihan dan meningkatkan kemampuan teknis tim.

Eksplorasi integrasi dengan layanan cloud seperti Oracle Cloud Infrastructure (OCI) untuk membuat standby database di lokasi cloud, meningkatkan fleksibilitas dan ketahanan sistem terhadap bencana skala besar.

DAFTAR PUSTAKA

- [1] M. R. Andreansyah, *"Perlindungan Data Tingkat Tinggi pada Aplikasi P2APST PLN melalui Rencana Disaster Recovery Center menggunakan Oracle Data Guard di Kota Bandung,"* Skripsi, Universitas Komputer Indonesia, 2023.
- [2] C. J. Date, *An Introduction to Database Systems*, 8th ed. Boston, MA: Addison-Wesley, 2019.
- [3] I. M. R. N. Efendi and Mansuri, *"Disaster Recovery dengan Standby Database pada PT. Sigma Solusi Integrasi,"* Jurnal Teknologi Informasi, vol. 15, no. 2, pp. 45-52, 2023.
- [4] A. Kadir, *Pengenalan Sistem Informasi Edisi Revisi*. Yogyakarta: Andi Offset, 2013.
- [5] P. A. Krisancoyo, *"Perancangan dan Implementasi Maximum Availability menggunakan Teknologi Oracle Data Guard: Studi Kasus Pencatatan Data Jemaat Gereja Bethany Salatiga,"* Tesis, Universitas Kristen Satya Wacana, 2013.
- [6] S. Narulita, A. Rahman, and D. Pratama, *"High Availability Database Systems in Cloud Computing Environments,"* International Journal of Cloud Computing and Services Science, vol. 13, no. 1, pp. 78-89, 2024.
- [7] A. Oloruntoba, *"Business Continuity in Database Systems: The Role of Data Guard,"* International Journal of Management and Information Research, vol. 8, no. 3, pp. 165-180, 2024.
- [8] Oracle Corporation, *Oracle Database 19c Documentation*. Redwood City, CA: Oracle Corporation, 2021.
- [9] Oracle Corporation, *"Oracle Data Guard Concepts and Administration 19c,"* Oracle Database Documentation, E96626-07, 2021.
- [10] T. Sutabri, *Analisis Sistem Informasi*. Yogyakarta: Andi Offset, 2012.
- [11] E. Turban, C. Pollard, and G. Wood, *Information Technology for Management: Advancing Sustainable, Profitable Business Growth*, 10th ed. Hoboken, NJ: John Wiley & Sons, 2015.
- [12] A. Wibowo, D. Darmantoro, and D. S. Kusumo, *"Analisis dan Implementasi Standby Database dengan Oracle: Studi Kasus Backup Standby Database pada Perusahaan Jasa Komunikasi,"* Seminar Nasional Aplikasi Teknologi Informasi, pp. 45-52, 2007.
- [13] S. Martin, *"Enhancing Disaster Recovery and Failover Strategies in Oracle Cloud Databases,"* Journal of Cloud Computing Research, vol. 10, no. 2, pp. 112-128, 2024.
- [14] M. Stephen and A. Ade, *"Data Backup Strategies in Disaster Recovery: Ensuring Minimal Downtime,"* International Journal of Computer Applications, vol. 185, no. 32, pp. 1-7, 2023.
- [15] I. Nurhastuti, *"Implementasi High Availability dan Disaster Recovery untuk Sistem Database,"* Jurnal Teknologi Informasi dan Ilmu Komputer, vol. 9, no. 4, pp. 789-798, 2022