DISASTER RECOVERY DENGAN STANDBY DATABASE PADA PT. SIGMA SOLUSI INTEGRASI

I Made Rothman Nova Efendi [1)], Mansuri [2)]
Fakultas Ilmu Komputer Universitas Borobudur
Jalan raya kalimalang no.1 Jakarta Timur 13620
Email: imade@borobudur.ac.id [1)], mansuri@borobudur.ac.id [2)]

Abstract

The purpose of this research is to design standby database system at PT. Sigma Integration Solutions. The method used in this research is Recovery Time Objective (RTO) and Recovery Point Objective (RPO). The design method is done by designing a standby database using physical standby database, real-time apply method, and maximum availability data protection type that supports the fast-start failover switch role. The results of this research is the implementation of disaster recovery that serves to handle the threat of loss due to system disruption.

Keyword: Disaster, Recovery, Standby, Database, Primary, Secondary

Abstrak

Tujuan dari penelitian ini adalah merancang sistem *standby database* pada PT. Sigma Solusi Integrasi. Metode yang digunakan dalam penelitian ini adalah *Recovery Time Objektive* (RTO) dan *Recovery Point Objective* (RPO). Metode perancangan dilakukan dengan merancang sebuah standby database yang menggunakan *physical standby database*, metode *real-time apply*, dan tipe proteksi data maximum availability yang mendukung role transition *fast-start failover*. Hasil penelitian ini merupakan implementasi *disaster recovery* yang berfungsi menangani ancaman kerugian akibat gangguan sistem.

Keyword: Disaster, Recovery, Standby, Database, Primary, Secondary

1. PENDAHULUAN

1.1. Latar Belakang

Kebutuhan akan sistem database yang semakin meningkat menjadikan data menjadi aset yang bernilai tinggi. Dengan demikian penting untuk menjaga data agar tetap ada kapan saja dibutuhkan. Akan tetapi resiko terjadinya kerusakan (*failure*) pada *database* yang mengakibatkan data tidak dapat diakses atau bahkan mengakibatkan data loss dapat terjadi setiap saat. Gangguan tersebut dapat berupa *maintenance*, kerusakan *database*, kerusakan media dan *data corruption. Database* juga dapat rusak akibat adanya bencana alam seperti kebakaran, gempa bumi dan banjir.

Banyaknya organisasi atau devisi informasi mulai memikirkan cara menangani masalah yang timbul akibat sistem yang mengalamai penghentian (*downtime*), karena akan menimbulkan kerugian yang tinggi, mengganggu aktivitas bisnis yang sedang berjalan, dan ketersediaan data yang memadai. Meskipun banya cara yang dipakai untuk mengatasi masalah yang timbul akibat system yang mengalami penghentian. Kebanyakan paa Manager IT menyetujui bahwa system yang mengalami penghentian tidak dapat diterima

dengan kegiatan bisnis yang ada sekarang ini. Pihak perusahaan menginginkan sistemnya dapat dipakai dan berjalan tanpa sedikitpun gangguan selama 24 jam setiap hari.
Sistem yang mengalami penghentian (*downtime*), baik yang direnacanakan maupun tidak direnanakan, sama halnya seperti kehilangan kesempatan dan dapat meningkatkan biaya operasional. *Standby Database* berfungsi untuk memberikan perlindungan kepada data perusahaan terhadap kegagalan, bencana, kesalahan oleh user, dan data yang korup. *Standby Database* dapat ditempatkan pada daerah yang aman dari bencana dan berada pada jarak yang jauh dari pusat (*primary database*). Jika *primary database* tidak bisa dipakai karena suatu sebab, baik yang direnacanakan atau tidak direnacanakan, maka *standby database* akan diubah menjadi *primary database* (sebagai *production database*) dan hal ini akan mengurangi waktu penghentian (*downtime*) serta membantu mencegah kehilangan data.
Adapun teknik penyelamatan data yang sering dilakukan, yaitu *backup data*. *Backup data* adalah teknik menyalin data ke dalam media lain. Dalam penelitian ini berarti data yang berada pada *primary database* (utama) disalin ke dalam *secondary database* (cadangan). Jika *primary database* mengalami kerusakan maka data tetap aman di dalam secondary database. Dan *secondary database* akan mengembalikan (*restore*) data apabila primary database sudah siap untuk digunakan kembali. Namun demikian hal ini belum dapat menjadi solusi terbaik. Karena backup tidak menggantikan kinerja *primary database* secara langsung yang mengakibatkan data tidak dapat diakses sampai *maintenance* pada sistem *primary database* tersebut berakhir.

1.2. Rumusan Masalah
Dari uraian di atas maka rumusan masalah dalam penelitian ini adalah:
1. Bagaimana mengitegrasikan *primary database* dengan *standby database*
2. Menjamin ketersediaan data disaat terjadi bencana yang tidak direnanakan pada server primary.
3. Melakukan pemulihan terhadap kerusakan data karena *downtime*.
4. Mengembalikan data yang rusak atau hilang
5. Manajemen sistem dapat dilakukan (secara local maupun dari jarak jauh) dengan mudah dan terdesentralisasi.
6. Bagaimana membangun *standby database* agar selalu *up-to-date* dan sinkron dengan *primary database*.

1.3. Batasan Masalah
Adapun batasan masalah dalam penelitian ini adalah:
1. Server yang berjalan 24 jam memerlukan system backup dengan downtime rate yang sekecil mungkin.
2. Instalasi *primary database* serta *standby database* pada computer dengan system operasi *Oracle Enterprice Linuz Release 5*.
3. Database yang digunakan adalah *Oracle Database 11g. R2*.
4. Mode proteksi data menggunakan *maximum abailability*.

1.4. Tujuan Penelitian
Tujuan penelitian ini adalah membuat standby database yang mampu melakukan backup data secara realtime pada lingkungan *DBMS Oracle* dan menggantikan *primary database* pada saat *primary database* mengalami kerusakan (*failure*) serta menguji waktu respon dan throughput pada proses replikasi dari *primary database server* ke *standby database server* yang diharapkan mampu mengatasi kehilangan data jika terjadi gangguan seperti bencana alam, kerusakan database dan kerusakan media.

1.5. Manfaat Penelitian
Adapun manfaat yang didapat dari penelitian ini adalah:
1. Meminimalkan dampak negative yang dapat merugikan dari gangguan pada *database server* dan *storage server* terhadap proses bisnis suatu perusahaan.
2. Memelihara stabilitas proses bisnis dan integrasi data selama proses *recovery server* utama database.
3. Mencegah terjadinya kehilangan data yang belum dibacup pada saat *database server* dan *storage server* perusahaan mengalami perusahaan secara fisik.

2. TINJAUAN PUSTAKA
2.1. Pengertian Implementasi

Implementasi berasal dari bahasa Inggris yaitu to implement yang berarti mengimplementasikan. Implementasi merupakan penyediaan sarana untuk melaksanakan sesuatu yang menimbulkan dampak atau akibat terhadap sesuatu.

Sesuatu tersebut dilakukan untuk menimbulkan dampak atau akibat itu dapat berupa undang-undang, peraturan pemerintah, keputusan peradilan dan kebijakan yang dibuat oleh lembaga-lembaga pemerintah dalam kehidupan kenegaraan

Implementasi menurut para ahli

Pendapat Cleaves yang dikutip (dalam Wahab 2008;187), yang secara tegas menyebutkan bahwa: Implementasi itu mencakup "Proses bergerak menuju tujuan kebijakan dengan cara langkah administratif dan politik". Keberhasilan atau kegagalan implementasi sebagai demikian dapat dievaluasi dari sudut kemampuannya secara nyata dalam meneruskan atau mengoperasionalkan program-program yang telah dirancang sebelumya.

Menurut Mazmanian dan Sebastiar (dalam Wahab, 2008: 68) Implementasi adalah pelaksanaan keputusan kebijakan dasar, biasanya dalam bentuk undang-undang, namun dapat pula berbentuk perintah-perintah atau keputusan-keputusan eksekutif yang penting atau keputusan badan peradilan.

Menurut Van Meter dan Van Horn (dalam Wahab, 2008: 65) Implementasi adalah tindakan-tindakan yang dilakukan baik oleh individu-individu/pejabat-pejabat atau kelompok-kelompok pemerintah atau swasta yang diarahkan pada tercapainya tujuan-tujuan yang telah digariskan dalam keputusan kebijakan.

Menurut Friedrich (dalam Wahab 2008: 3) Kebijakan adalah suatu tindakan yang mengarah pada tujuan yang diusulkan oleh seseorang, kelompok atau pemerintah dalam lingkungan tertentu sehubungan dengan adanya hambatan-hambatan tertentu seraya mencari peluang-peluang untuk mencapai tujuan atau mewujudkan sasaran yang diinginkan.

Secara sederhana implementasi bisa diartikan pelaksanaan atau penerapan. Browne dan Wildavsky (dalam Nurdin dan Usman, 2003:7) mengemukakan bahwa "implementasi adalah perluasan aktivitas yang saling menyesuaikan".

2.2. Disaster

Disaster (bencana) didefinisikan sebagai kejadian yang waktu terjadinya tidak dapat diprediksi dan bersifat sangat merusak. Bencana terjadi dengan frekuensi yang tidak menentu dan akibat yang ditimbulkannya meningkat bagi mereka yang tidak mempersiapkan diri terhadap kemungkinan-kemungkinan timbulnya bencana.

Berbagai bencana yang mungkin terjadi antara lain adalah:

- Bencana alam disebabkan oleh kondisi geografis dan geologis dari lokasi
- Kebakaran disebabkan oleh faktor lingkungan dan pengaturan sistem elektrik yang dapat menyebabkan korsleting
- Kerusakan pada jaringan listrik disebabkan oleh sistem elektrik
- Serangan teroris disebabkan oleh lemahnya keamanan fisik dan non fisik data center
- Sistem atau perangkat yang rusak terkait dengan kesalahan manajemen pengawasan perangkat
- Kesalahan operasional akibat ulah manusia
- Virus misalkan disebabkan oleh kesalahan pemilihan anti-virus yang digunakan

2.3. Disaster Recovery

Disaster recovery adalah proses, kebijakan dan prosedur yang berkaitan dengan persiapan untuk pemulihan (*recovery*) atau kelanjutan pada infrastruktur teknologi yang sangat penting (vital) bagi organisasi setelah bencana yang disebabkan oleh alam maupun manusia. Bencana dapat diklasifikasikan ke dalam dua kategori, yaitu:

1. Yang pertama adalah bencana alam seperti banjir, angin topan, tornado atau gempa bumi. Sementara mencegah bencana alam sangat sulit, memastikan langkah-langkah seperti perencanaan yang baik adalah solusi yang lebih tepat. Langkah-langkah tersebut diharapkan mampu menghindari ataupun mengurangi kerugian akibat bencana (*disaster*).
2. Bencana buatan manusia. Bencana juga dapat terjadi akibat perbuatan manusia. Sebagai contoh kegagalan infrastruktur dan terorisme. Dalam hal ini pengawasan dan

perencanaan juga diharapkan dapat menghindari kerugian.

Menurut (Gregory, 2009) *Disaster Recovery* adalah bagian dari sebuah proses yang lebih besar sebagai perencanaan kelangsungan bisnis dan termasuk di dalamnya perencanaan untuk memulai kembali aplikasi, data, perangkat keras (*hardware*), komunikasi elektronik (*networking*) dan infrastruktur teknologi informasi lainnya. Langkah-langkah kontrol pemulihan (*recovery*) bencana teknologi informasi dapat diklarifikasikan menjadi tiga jenis, yaitu:

1. Langkah preventive, kontrol yang dilakukan untuk mencegah sebuah bencana yang akan terjadi.
2. Langkah deteksi, kontrol yang bertujuan untuk mendeteksi atau menemukan kejadian yang tidak diinginkan.
3. Langkah korektif, kontrol yang ditujukan untuk memperbaiki atau memulihkan sistem setelah bencana atau peristiwa.

Disaster recovery plan yang baik memastikan bahwa ketiga jenis kontrol didokumentasikan dan diuji secara teratur.

2.4. Disaster Recovery Plan

Disaster (bencana) diartikan sebagai suatu kejadian yang tidak bisa diprediksikan waktu terjadinya. Dalam Teknologi Informatika *disaster* ini bisa terjadi akibat kurangnya perencanaan atau juga dikarenakan hal-hal yang ada di luar kendali manusia. Beberapa contoh disaster yang sering ditemukan dalam penggunaan TI adalah adanya virus yang disebabkan kesalahan dalam penggunaan anti-virus yang dipilih. Juga bencana akibat kesalahan yang dilakukan SDM Operasional.

Disaster recovery plan mempunyai arti rencana pemulihan bencana. Timbulnya resiko bencana data mengakibatkan terganggunya operasioal bisnis, berdampak pada peningkatan biaya, munculnya permasalahan penyediaan layanan ke pengguna, turunya produktivitas lingkungan kerja, hingga memburuknya citra perusahaan di mata konsumer. Bisnis sebuah perusahaan sangat tergantung pada informasi dan aplikasi yang memprosesnya. Sehingga akan menjadi sangat mengkhawatirkan jika terjadi gangguan yang dapat melumpuhkan bisnis perusahaan. Oleh karenanya perusahaan harus mempunyai rencana dan strategi dalam menjamin kelangsungan bisnis pada saat terjadi suatu gangguan yang tidak direncakan. Rencana atau strategi ini dirumuskan dalam *Disaster Recovery Plan*.

Dalam konteks teknologi informasi, diantara upaya persiapan yang dimaksud adalah mengkondisikan sistem IT (*Information Technology*) untuk senantiasa tersedia ketika dibutuhkan oleh proses bisnis organisasi. Sistem IT perlu dipersiapkan untuk tetap dapat menungjang bisnis, bahkan ketika dampak yang ditimbulkan bencana mengancam operasional sistem dan layanan IT itu sendiri.

Disaster recovery plan (DRP) atau dikenal dengan istilah rencana pemulihan bencana menjadi solusi yang komprehensif untuk mebantu organisasi dalam melakukan antisipasi dan penanggulangan bencana yang berpotensi menggangu operasional sistem IT dinama akhirnya akan mengganggu juga sistem yang menunjang operasional bisnis penting dalam organisasi. Sebuah rencana pemulihan bencana (DRP) yang komprenesif meliputi:

- Analisis resiko dan dampak bencana
- Strategi penyediaan sistem IT dalam kesadaran darurat
- Rumusan prosedur antisipasi dan penanggulangan bencana terhada system IT.
- Serta perencanaan kebutuhan *disaster recovery center* (DRC)

Disaster Recovery Plan harus menangani tiga bidang, yaitu:(4)

1. *Prevention* (pra-bencana): Pra-perencanaan diperlukan (seperti menggunakan server mirror, memelihara situs hot sites, pelatihan tenaga pemulihan bencana) untuk meminimalkan dampak keseluruhan bencana pada sistem dan sumber daya. Pra-perencanaan ini juga memaksimalkan kemampuan sebuah organisasi untuk pulih dari bencana.
2. *Continuity* (saat bencana): Proses pemeliharaan inti, *mission-critical* sistem dan sumber daya “kerangka” (aset minimal yang dibutuhkan untuk menjaga sebuah organisasi dalam status operasional) dan/atau menginisiasi hot sites sekunder selama bencana.

Langkah-langkah continuity menjaga sistem dan sumber daya perusahaan.

3. *Recovery* (pasca bencana): Langkah-langkah yang diperlukan untuk pemulihan dari semua sistem dan sumber daya untuk menjadi status operasional normal. Organisasi dapat mengurangi waktu pemulihan dengan berlangganan ke *quick-ship* programs (penyedia layanan pihak ketiga yang dapat memberikan pra-konfigurasi penggantian sistem untuk setiap lokasi dalam jangka waktu yang tetap) atau dapat juga disebut dengan vendor.

Disaster Recovery Plan (DRP) sangat penting bagi perusahaan agar operasional perusahaan dapat tetap berjalan meskipun terjadi bencana. Apabila operasional perusahaan terhambat, maka perusahaan pun akan mengalami kerugian.

2.5. Disaster recovery center

Disaster Recovery Center merupakan suatu fasilitas dalam perusahaan yang berfungsi untuk mengambil alih fungsi suatu unit ketika terjadi gangguan serius yang menimpa satu atau beberapa unit kerja penting di perusahaan, seperti pusat penyimpanan dan pengolahan data dan informasi. *Disaster Recovery Plan* (DRP) dan *Disaster Recovery Center* (DRC) sudah bukan hal yang baru di dunia IT Indonesia, bahkan Bank Indonesia telah mensyaratkan seluruh bank agar memiliki DRP/DRC contohnya adalah ketika terjadi malapetaka yang menimpa sejumlah perusahaan besar dunia yang bermarkas di *world trade center* tetap dapat beroperasi (segera pulih kegiatan operasionalnya dalam waktu cepat), karena mereka telah mempersiapkan sejumlah DRC untuk mengantisipasi bencana yang tidak dikehendaki tersebut.

2.6. Database

Primary database mengacu pada pengertian production database yang memiliki tingkat availibilitas tinggi. *Primary database* adalah *database* utama yang digunakan, database ini diharapkan mampu diakses setiap saat, maka dari itu jika terjadi failure dan primary database mati, maka otomatis pengaksesan terhadap primary database tersebut juga tidak dapat dilakukan.

Standby database merupakan duplikat dari database utama (jumlah mungkin lebih dari satu) yang harus identik dengan database utama yang sewaktu-waktu bisa digunakan jika database utama mengalami crash atau maintenance yang memiliki kemungkinan kea rah down time. Peralihan dari database utama ke standby database akan memiliki dua istilah berbeda berdasarkan penyebabnya. Istilah pertama yaitu failover : jika peralihan disebabkan crash atau power failure. Istilah kedua switchover, jika peralihan memang dikehendaki atau dipersiapkan sebelumnya seperti adanya pemadaman listrik terjadwal. Pemeliharaan server.

3. METODE PENELITIAN,

Dalam penelitian ini metode yang digunakan dalam menganalisis adalah *Recovery Time Objektive* (RTO) dan *Recovery Point Objective* (RPO), karena *disaster recovery system* dengan *standby database* merupakan salah satu solusi yang memenuhi persyaratan dari RTO dan RPO perusahaan. Dengan demikian *high availability* terhadap *database server* dan *storege server* PT. Sigma Solusi Integrasi pun tercapai dengan *standby database.*

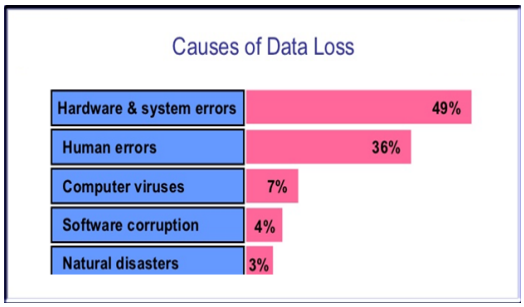
4. RANCANGAN DISASTER RECOVERY DIUSULKAN

4.1. Sistem diusulkan

Perancangan system diusulkan merupakan *high availability system* dengan *standby database* dilakukan dalam beberapa tahap. Berikut adalah tahapan-tahapan tersebut adalah:

- Mempelajari latar belakang dan tujuan perusahaan
- Analisis proses bisnis
- Analisis teknologi informasi perusahaan
- Analisis RTO dan RPO
- Merancang arsitektur *logical disaster recovery center* (DRC)
- Melakukan konfigurasi *standby database* pada *primary database* dan *standby database.*

4.2. Konsep Standby Database



Source: Disaster Recovery Journal

Gambar 1: *Caused of Data Loss*

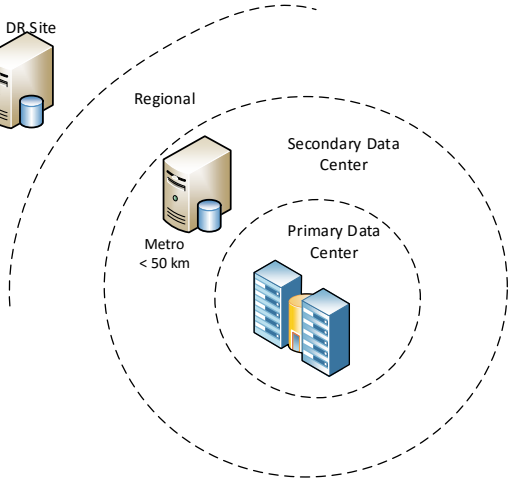
Berdasarkan gambar di atas, menurut survey yang dilakukan oleh *Disaster Recovery Journal*, penyebab *data loss* terbesar adalah karena *hardware* dan *system error*. Akan tetapi terdapat tiga persen (3%) penyebab data *loss* yang disebabkan oleh *natural disaster*, oleh karena itu berdasarkan konsep *backup* dan *recovery* yang sudah dijelaskan di atas, salah satu metode *backup* dan *recovery* yang dapat menangani *failure* dan *error* yang berhubungan dengan *disaster* adalah *standby database*, standby database adalah suatu solusi *backup* dan *recovery* yang mempunyai tujuan utama sebagai berikut:

- *Disaster protection*.
- Proteksi terhadap *data corruption*.
- *Supplemental reporting*.

Dalam suatu Sistem *Standby Database*, terdapat satu Production Database yang disebut dengan *primary database* dan satu sampai sembilan standby database, jika primary database mengalami kerusakan akibat disaster atau datanya menjadi *corrupt*, maka user bisa melakukan proses *failover* ke *standby database*, hal ini berarti *standby database* akan menjadi primary database yang baru, *user* juga bisa melaksanakan proses *query* pada *standby database* dengan mengubah *mode*-nya menjadi *read-only*, hal ini membuat fungsi *standby database* bisa juga untuk *reporting*, kemudian cara agar standby database selalu identik dengan *primary database* adalah dengan *primary database* selalu mengarsipkan *online redo log* menjadi *archived redo log*, sedangkan *data redo log* yang lama disediakan untuk operasi seperti media *recovery*, lalu *archived redo log* yang telah dikirimkan sebelumnya secara berkesinambungan di-*apply* di data *redo log* *standby database* untuk menerapkan segala perubahan yang terjadi di *primary database*.

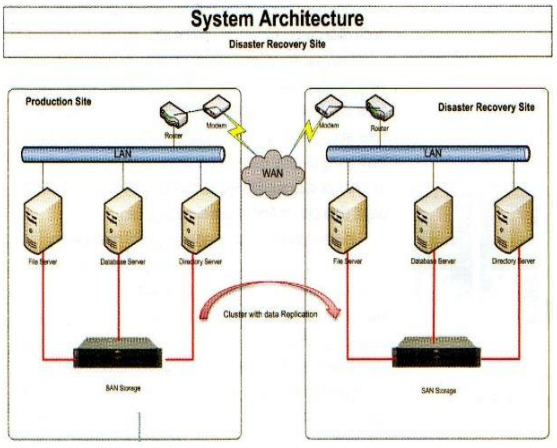
4.3. Arsitektur Disaster Recovery Center

Kemungkinan distribusi bencana,
Yang disebut bencana atau radius ancaman, mempengaruhi solusi kelangsungan bisnis. Probabilitas dan tingkat kerusakan dari gempa bumi banjir, kebakaran,angina topan, siklon atau ancaman teroris bervariasi sesuai dengan daerah dimana pusat data fisik berada. Agar tetap efektif, situs cadangan tidak harus berada dalam radius bencana.



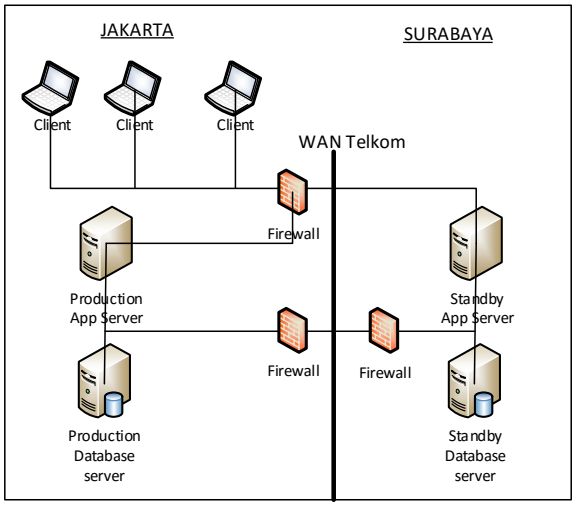
Gambar 2: Data Center

Perancangan arsitektur DRC dimulai dengan melihat arsitektur *data center* utama perusahaan, di mana arsitektur DRC akan menggunakan arsitektur yang sama dengan *data center* utama. Antara *data center* utama dan DRC sendiri terhubung secara logikal seperti gambar berikut.

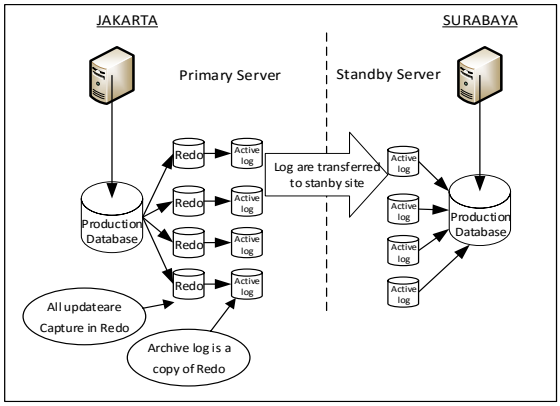


Gambar 3: Arsitektur Sistem DRC

4.4. Arsitektur Network diusulkan



Gambar 4: Topologi Jaringan



Gambar 5: *Logical Standby database*

Pada gambar di atas database primary akan merekam transaksi yang akan disimpan ke redo log lalu redo log mengkompres menjadi *archive* dan melakukan transfer ke *standby database*, *archive* yang sudah di *stanby database* selanjutnya akan direcovery secara otomatis dan melakukan sinkronisasi dengan data yang sama pada *primary database*.

5. SIMPULAN dan SARAN

5.1. Kesimpulan

Dari hasil percobaan yang dapat disimpulkan dalam menanganni beberapa kondisi:

1. *Standby database* dapat meminimalisir *downtime* yang terjadi pada proses bisnis suatu perusahaan.
2. *Standby database system* dapat membuat proses bisnis tetap berjalan walau *primary database* tidak bisa diakses.
3. *Disaster recovery* menunjukkan tingkat availibilitas yang tinggi bila terjadi failure pada *primary database*.
4. Kesesuaian data terjamin dengan adanya sinkronisasi primary database dengan *standby database* mengunakan *real-time*.

5.2. Saran

Beberapa saran yang dapat disampaikan yaitu

1. Diperlukan karyawan khusus untuk dapat melakuan evaluasi dan pemeliharaan terhadap sistem DRC.
2. Log files selama proses archiving dapat dikompresi dan dapat dibacup pada eksternal disk.
3. Evaluasi terhadap *bandwith* jaringan untuk mengoptimalkan proses sinkronisasi data antara *primary database* dan *standby database*.

REFFERENSI

Abbey, M. Corey, M.J, dan Abramson, I. (1999). ***Orecle8i A Beginner's Guide***. California, Mc. Graw-Hill Companies, Inc.

Albert, C.J. dan Dorofee, A.J. (2002). ***Managing Information Security Risk: The OCTAVE Approach***. Addison-Wesley.

Anttalainen, T. (2003). ***Introduction to Telecomunication Network Engineering***. 2nd ed. London, Artech House.

Chan, I (2006). ***Oracle Database High Availability Overview***, 11g Release 2 (10.2). USA, Oracle Corporation.

Connolly, T. dan Begg, C. (2005). ***Database system***, edisi ke-4. California, Addison Wesley Publishing Company. Inc.

Cyran M. (2005). ***Oracle Database Concepts***, 10g Release 2 (10.2). Oracle Corporation.

Dawes. C., Bryla, B., Johnson, J. C., dan Weishan, M. (2005). ***OCA: Oracle 11g Administration I Study Guide***. Sybex.

Hoffer, J.A., George, J.F., dan Valacich, J.S. (1999). ***Modern System Analysis and Design***, USA, Addison Wesley Longman, Inc.

Maiwald, E. dan Sieglein, W. (2002). ***Security Planning & Disaster Recovery California***, Mc. Graw-Hill/Osborne.

Mansuri, Eko. S,. (2015). ***Analisis Pemanfaatan Hotspot Terhadap Mutu Pembelajaran Mahasiswa di Universitas Borobudur***. JUPITER, 1(2).

O'Brien, J.A.. (2003). ***Pengantar sistem informasi: Perspektif Bisnis dan Managerial***, Edisi ke-12. New York, Mc. Graw-Hill Companies, Inc.

Peltier, T.r. (2005). ***Information Security Risk Analysis***, Second Edition. Florida, Auerbach Publications.

Ray, A. (2006). ***Oracle Data Guard in Oracle Database 11g Release 2 – Business Continuity for the Enterprise***. Oracle Corporation.

Schumpmann, V. (2006). ***Oracle Data Guard Broker, 11g Release 2 (11.2)***. Oracle Corporation.

_____. (2008). ***Oracle Data Guard Concepts and Administration, 10g Release 2 (10.2)*** Oracle Corporation.

Siti, Mardhiyah, Pebruari 2012. "Implementasi Physical Standby Database Menggunakan Oracle 9i Data Guard", http://library.gunadarma..ac.id/repository/view/12882/implementasi-physical-standby-database-menggunakan-oracle9i-datad-guard.html, Pebruari 2012.

Virginia, Beecher., July 2013, "High Availability Overview", http://docs.oracle.com/cd//E11882_01/server.112/e17157.pdf, July 2013.