

Manajemen *Backup* Data untuk Penyelamatan Data Nasabah pada Sistem Informasi Perbankan (Studi Kasus: PT BankXYZ)

¹Andi Rosano, ²Djadjat Sudaradjat
Universitas Bina Sarana Informatika
Jakarta, Indonesia
andi.aox@bsi.ac.id

Abstract

Data sistem informasi *online* pada PT Bank XYZ merupakan *database* yang tersimpan pada web/email *server* bank yang dapat diakses secara *online* oleh pemakai. Beberapa faktor internal telah menjadi penyebab kerusakan *server* dan berakibat tidak beroperasinya sistem. Salah satu cara untuk menyelamatkan data dari kehilangan atau kerusakan adalah melalui manajemen *backup* data yang pelaksanaannya dijalankan secara teratur. Solusi untuk masalah ini adalah penggabungan metode *full backup* dan *incremental backup* dalam manajemen *backup* data, dimana metode ini sangat mudah digunakan serta ekonomis. Langkah berikutnya setelah *backup data* adalah proses *restore* yang merupakan proses pengembalian atau *recovery* data yang sangat penting apabila terjadi kerusakan data. Pada tulisan ini akan dibahas metode *backup* data dalam upaya penyelamatan data *online*. Dalam pemilihan metode *backup* ini sangat tergantung pada keandalan sistem dan kinerja, sehingga proses penyelamatan data dilakukan dengan tepat dan aman.

Keywords: *backup, database, incremental, online, recovery, restore, server*

I. PENDAHULUAN

Seiring dengan perkembangan komputer dan membesarnya volume data, saat ini kebutuhan adanya *backup* data menjadi hal yang tak bisa dihindari untuk dilakukan. *Backup* adalah aktivitas menyalin atau membuat turunan objek (file atau *database*), sehingga objek salinan tersebut dapat dipakai untuk memulihkan data asli yang rusak karena berbagai sebab. Pertambahan data yang disimpan pada media *hard disk web* sebagai data *online* berbanding lurus dengan pertambahan informasi yang disajikan. Oleh karena itu dibutuhkan persiapan bilamana terjadi kerusakan data. Dapat dilihat pada gambar 1, volume kehilangan data dari tahun ke tahun semakin meningkat. Sekitar 70% kegiatan bisnis pasti dirugikan akibat kehilangan data ini yang diakibatkan oleh berbagai kasus kecelakaan, a.l. terhapusnya data tanpa sengaja, kegagalan proses pada sistem, terpapar virus, kebakaran, atau bencana lain, hal ini akan mempercepat pertumbuhan layanan *backup* data (Yanuardi, 2004).

Sebagai lembaga keuangan yang telah mempunyai banyak nasabah tentunya tidak bisa terlepas dari data, baik data informasi nasabah maupun data transaksi *online*, yang semua terkait dengan informasi publik dan kerahasiaan. Data transaksi *online* adalah data yang tersimpan pada beberapa *server* yang merupakan aktivitas transaksional nasabah. Sedangkan data informasi nasabah adalah data tetap yang berupa informasi segala identitas dan jatidiri nasabah bank. Semua informasi dan transaksi dapat diakses oleh pengguna secara *online* melalui media/jaringan internet. Secara garis besar, sumber ancaman/gangguan terhadap *server* terbagi menjadi dua sumber, yaitu sumber internal dan sumber eksternal. Sumber bahaya



internal meliputi faktor keteledoran manusia dan kerusakan sistem, misalnya sistem *crash*. Bisa juga akibat gangguan listrik yang menyebabkan lenyapnya data-data penting tanpa disengaja. Sedangkan bahaya eksternal umumnya berbentuk *malware* dan *virus* yang berasal dari jaringan internet. Hal ini mengakibatkan *hardware* dan *software* tidak berfungsi secara normal serta *database* mengalamikerusakan (Aldasouqi, 2015).

II. TINJAUAN PUSTAKA

2.1. Pengertian Backup Data

Backup dapat diartikan sebagai proses membuat salinan data sebagai cadangan bila terjadi kehilangan atau kerusakan data asli. Salinan data yang dibuat disebut dengan “*data backup*”. Manfaat dari proses *backup* diantaranya : untuk mengembalikan kondisi suatu sistem komputer yang mengalami kerusakan atau kehilangan data, mengembalikan suatu file yang tanpa sengaja terhapus atau juga rusak. Dan juga salah satu kegiatan yang harus dilakukan oleh pengelola *database* untuk melakukan penyalinan sistem, data, dan aplikasi.

Backup data harus dilakukan untuk mengatasiterjadinya kerusakan sistem dari luar maupun dalam sistem yang disengaja atau tidak. Proses *backup* dalam teknologi informasi mengacu pada penyalin data, sehingga salinan tambahan tersebut bisa digunakan untuk mengembalikan (*restore*) setelah peristiwa kehilangan data (Afif, 2013).

Backup sangat berguna terutama untuk dua tujuan yaitu untuk memulihkan keadaan setelah bencana (*disaster recovery*) dan untuk mengembalikan beberapa file yang sengaja dihapus atau rusak. Konsistensi data dalam proses *backup* harus dijaga sebelum melakukan *backup* data. Mengecek konsistensi data dengan membandingkan data pada struktur direktori dengan data pada blok. Lalu, apabila ditemukan kesalahan maka program *backup* akan mencoba memperbaiki. Pengecek konsistensi data inilah yang disebut dengan *Recovery*.

Backup dapat dibagi berdasarkan lingkup datanya menjadi (Handrini, 2018) :

- Full Backup
- Incremental Backup
- Mirroring Backup

2.2. Media Penyimpanan Data (Storage)

Berbicara masalah proses *backup* tidak akan terpisahkan dengan masalah media penyimpanan data (*storage*). Setiap *backup* dilakukan dengan pertimbangan dimana tempat data *backup* akan disimpan. Data *backup* harus disimpan sedemikian rupa sehingga teratur dengan baik. Keteraturan tersebut dapat berupa catatan kertas dengan daftar media *backup* dengan informasi isi datanya yang disimpan, atau dapat pula berupa pengaturan yang canggih dengan index komputer, katalog atau *database* relasional. Perbedaan dalam penggunaan model penyimpanan data akan memberi manfaat yang berbeda. Pengambilan manfaat ini berkaitan erat dengan skema/jadwal rotasi *backup* yang digunakan (Ngo, 2016).

Pemilihan media penyimpanan data *backup* menjadi pertimbangan yang sangat penting dalam proses *backup*. Ada banyak tipe media penyimpanan yang dapat dipilih dengan kelebihan dan kekurangannya masing-masing.

2.3. Pengertian Restore data

Restore dan *recovery* adalah proses penting setelah *backup*. *Backup* akan menjadi sia-sia bila proses pengembalian dan perbaikan data sistem sulit atau tidak dapat dilakukan. Untuk mencapai tujuan ini ada beberapa pendekatan yang harus diperhatikan, yaitu proses *backup* harus dilakukan dengan aturan yang jelas. Dihindari melakukan *backup* dengan tidak terstruktur. Selain itu, banyak *software* yang ada di pasaran (baik gratis maupun berbayar) yang memberikan kemudahan *backup* data. Dengan *software* yang sama biasanya proses *restore* dan *recovery* data akan lebih mudah dilakukan. Beberapa *software* untuk *backup* memiliki fasilitas penjadwalan otomatis pada prosesnya. Fitur ini sangat bermanfaat untuk digunakan karena menjamin proses *backup* selalu dilakukan dengan teratur (Douglas, 1995).

2.4. Server Remote Data Back-up

Server Remote Data Backup adalah *server* yang menyimpan seluruh data utama secara keseluruhan dan terletak di tempat yang jauh. Apabila repositori pusat kehilangan datanya, maka sistem menggunakan data dari *backup* repositori yang berada di lokasi jarak jauh. Seperti yang ditunjukkan pada Gambar 1, jika klien menemukan bahwa data tidak tersedia di repositori pusat, maka klien diizinkan untuk mengakses file dari repositori jarak jauh (Sharma, 2012).

Pada saat ini penggunaan model *remote data backup server* diimplementasikan untuk pelaksanaan sistem *mirroring backup*, dimana setiap terjadi perubahan data pada *server* utama maka di *remote server* juga secara otomatis ter-update juga datanya.



III. METODE PROSES BACKUP DATA

Pada PT Bank XYZ yang menjadi lokasi penelitian, manajemen bank telah memutuskan menggunakan model *mirroring system*. Dimana lokasi *Disaster Recovery Center (DRC)* terletak di kota lain diluar kantor pusat. Hal tersebut dipilih untuk menghindari terjadinya *local accident* pada kantor pusat, misalnya kebakaran, dan sebagainya. Yang menjadi jembatan penghubung antara sistem utama dan sistem *backup (DRC Center)* adalah jaringan *internet* dengan memilih salah satu *provider* internet terkemuka di Indonesia. Jembatan penghubung ini juga digandakan dengan menggunakan teknologi *Radiolink* dari provider terpilih.

Dengan demikian hubungan antara kantor pusat dan sistem *backup (DRC Center)* dijamin mendekati 100 persen *uptime*-nya. *Software* aplikasi yang digunakan beroperasi 24 jam penuh, sehingga seluruh data, baik yang disimpan di sistem utama maupun *backup* tidak ada perbedaan. Sedangkan test *switch-over* secara rutin dilakukan setiap 3 (tiga) bulan sekali dengan melibatkan seluruh staff operasional dan seluruh transaksi perbankan yang ada (Bank Mega, 2017). Adapun sistem-sistem yang beroperasi pada PT Bank XYZ dapat dilihat pada tabel 3 dibawah.

IV. HASIL DAN PEMBAHASAN

Pengetesan hasil *backup mirroring system* ini adalah dengan melakukan *test switch-over*, yakni memindahkan operasional sistem dari mesin utama ke mesin *backup* dalam kurun waktu tertentu, dan dengan kegiatan yang normal. Sedangkan mesin operasional diperlakukan sebagai mesin *backup*. Untuk pelaksanaan ini perlu dibuatkan *scenario* pengetesan dan standar prosedur yang baku. Hasil dari proses *switch-over* ini dianggap sukses apabila operasional bank tidak terganggu dan berjalan normal dengan mesin *backup*. Setelah pengecekan data dan transaksi dipastikan normal, berarti test sistem *backup* dinyatakan berhasil.

Dalam pelaksanaan test *backup mirroring system* ini digunakan sampel pengetesan beberapa cabang utama bank yang dianggap mewakili jumlah nasabah dan jumlah transaksinya. Setiap cabang utama dipakai sebagai sampel pengetesan dengan pertimbangan bahwa jumlah nasabah dan jenis transaksi perbankan yang dilakukan mewakili seluruh jenis transaksi perbankan yang ada.

Proses *switch-over* dimulai dengan proses awal hari (*start of Day*), hal ini di dengan pertimbangan bahwa test mewakili siklus operasional bank yang normal. Apabila dalam 30 menit pertama setelah dilakukan *switch-over* tidak timbul permasalahan yang serius dan hasil pengecekan menyatakan normal, barulah sistem dilanjutkan selama 24 jam penuh.

Namun apabila dalam 30 mnit pertama setelah *switch-over* dilakukan terjadi masalah yang bersifat fatal, misalkan semua transaksi gagal, atau staf bank tidak bisa login ke sistem, dan sebagainya, maka proses *switch-over* dianggap gagal. Sistem harus dikembalikan ke posisi semula.

Siklus operasi bank harus dipenuhi, antara lain adalah proses awal hari (*start of day*) dan proses akhir hari (*end of day*) yang dilakukan secara penuh, hingga dihasilkan laporan hasil proses akhir hari yang lengkap. Apabila test dilaksanakan di akhir bulan, maka siklus proses akhir bulan (*end of month*) juga bisa ditest sekaligus (PT Bank Mega, 2017).

Setelah test *switch-over* dilakukan dengan baik, maka dilakukan *switch-back* ke mesin operasional. Segala hal penting yang terjadi dalam pengetesan dicatat dan kemudian dilaporkan secara resmi kepada manajemen. Semua kekurangan dan kelemahan prosedur harus segera dilakukan perbaikan, untuk kesempatan pengetesan selanjutnya yang akan dilakukan secara rutin.

Semua catatan dan permasalahan kecil yang timbul kemudian dijadikan bahan materi perbaikan prosedur, sehingga dari waktu ke waktu proses *switch-over* semakin membaik.

V. KESIMPULAN

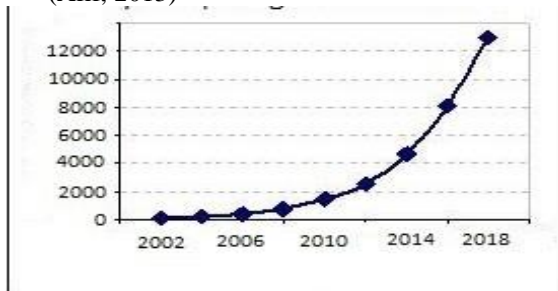
Beberapa faktor yang harus diperhatikan dalam proses *backup* data adalah harus ada (dibuat) standar prosedur untuk proses pelaksanaannya, dan harus mudah untuk dilaksanakan dan berjalan sedapat mungkin tanpa perlu campur tangan pengguna. Dalam hal ini, pengguna hanya yang menentukan lokasi dimana letak data tersebut akan di-*backup*, dan seberapa sering frekuensinya. Apabila mungkin dilakukan secara otomatis menggunakan *software*. Harganya dicari yang semurah mungkin tanpa mengorbankan kualitas serta lokasi *backup* yang harus berada di lokasi yang berbeda. Data hasil proses *backup* harus mudah dikembalikan (*restore*) sehingga semua usaha *backup* yang dilakukan tidak sia-sia.

Faktor penting lain yang harus diperhatikan dalam membuat sistem *backup* data adalah dengan memperhatikan seberapa sering pemakai melakukan perubahan pada datanya, sehingga penjadwalan *backup* data dapat dilakukan mingguan, bulanan, atau tahunan bergantung banyaknya perubahan data yang terjadi dalam rentang waktu tersebut.

VI. GAMBAR DAN TABEL

Dibawah ini adalah beberapa gambar dan tabel yang dapat lebih menjelaskan uraian tulisan ini :

Tabel 1 Perkembangan Ukuran Data
 (Afif, 2013)

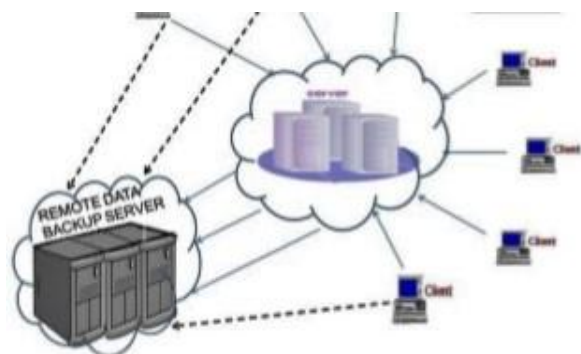


Tabel 2
 Kelebihan dan Kekurangan Metoda Backup
 (Afif, 2013)

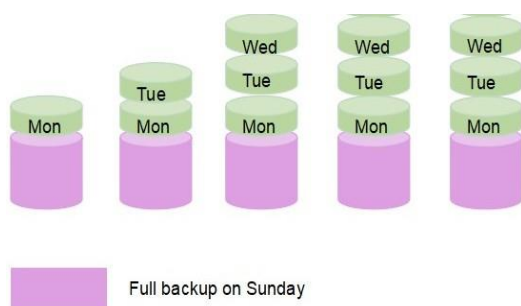
Incremental backup	<ul style="list-style-type: none"> - Membutuhkan waktu yang lebih singkat. - Jika banyak melakukan incremental backup, maka data yang di backup semakin kecil ukurannya. - Backup lebih cepat daripada full backup dan membunhkan tempat sementara yang lebih kecil daripada yang dibutuhkan oleh full backup. 	<ul style="list-style-type: none"> - Waktu untuk restore sangat lama.
Mirror backup	<ul style="list-style-type: none"> - metode backup yang paling cepat 	<ul style="list-style-type: none"> - data tidak di padatkan atau dimampatkan (dengan format .tar, .zip, atau yang lain) dan tidak bisa di lindungi dengan password.

Tabel 3
 Aplikasi (Sistem) yang beroperasi pada Bank(Rosano, 2011)

5	Call Center & Helpdesk System	AT&T
6	Consumer Loan System	Server
7	Corporate Loan System	Server
8	Human Resources System	Server
9	e-Procurements System	Server
10	General Affairs System	Server
11	KYC (Know Your Customer System)	Server
12	Tax Centralized System	Server
13	Dokumen Tracking System	Server
14	Hotline Service System	AT&T
15	Loan Origination System	Server
16	e-Recruitment System	Server
17	Appraisal Management System	Server
18	Credit Risk Rating System	Server
19	Prepaid Card System	Server
20	MERCA System	Server
21	Sel Assesment Online System	Server
22	Internet Banking System	Server
23	UKM System	Server
24	Payroll System	Server
25	Mobile Banking System	Server
26	ATM System	IBM AS400



Gambar 1 Remote Backup Data(Sharma, 2012)

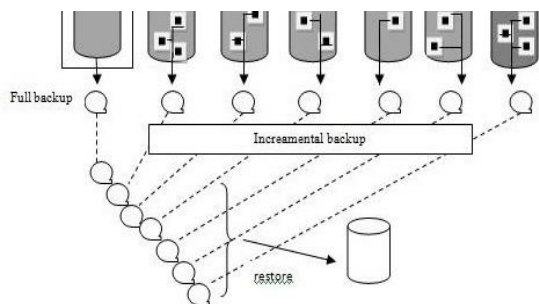




Gambar 2 Proses Kerusakan Data (Afif, 2013)

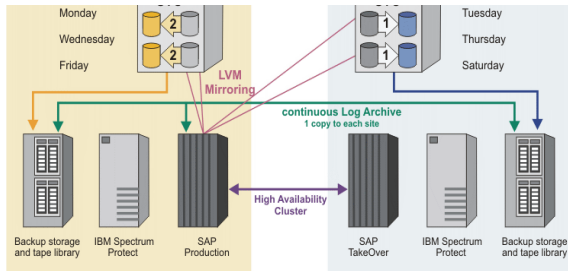


Gambar 3 Full Backup (Normal Backup) (Afif, 2013)

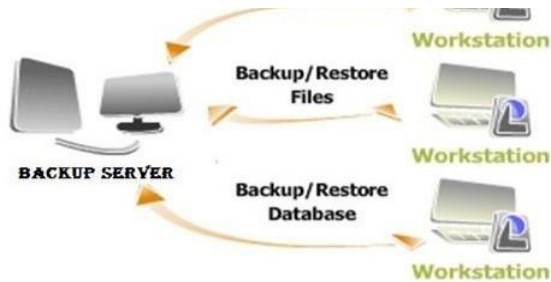


Gambar 3.a Incremental Backup(Afif, 2013)

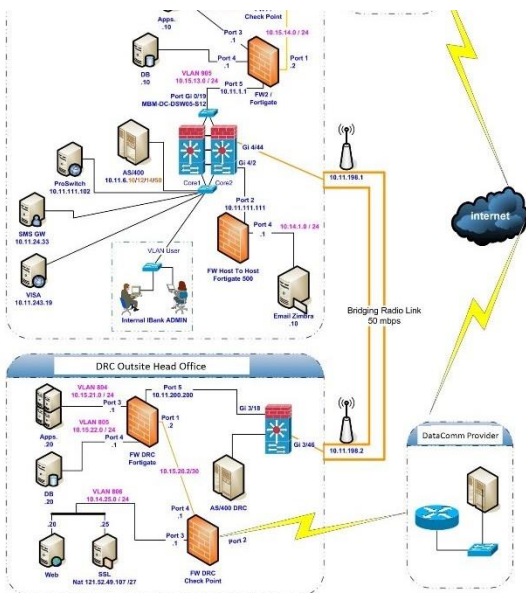
Gambar 3.b Incremental Backup Content (Afif, 2013)



Gambar 4 System Mirroring Backup Data (Handrini, 2018)



Gambar 5 Proses Restore Data (Rosano, 2011)



REFERENS

Gambar 6

Topologi Banking System Mirroring (PT Bank Mega, 2017)

- [1] Idasouqi, Awajan, A., 2015. Perancangan Sistem Otomatisasi Backup Data Menggunakan *File Transfer Protocol* Berbasis Jaringan LAN (Studi Kasus STMIK TIME Medan). Jurnal TIMES, Vol.IV, No.1, 26-30, ISSN:2337-3601.
 - [2] Afif, M.F., Suryono, 2013. Implementasi *Disaster Recovery Plan* dengan sistem *Fail Over* menggunakan *DRBD* dan *Heartbeat* pada *Data Center* FKIP UNS. Indonesian Journal on Networking and Security (IJNS).
 - [3] Douglas, J. Fletcher, 1995, *Data Backup and Restore System for a Computer Network Having Generic Remote File System Agents for Providing Backup and Restore Operations*, Longwood, Seagate Technology inc.
 - [4] Handrini, E.A., Kurniawan, M.T., Widjajarto, A. 2018. *Disaster Recovery Strategy* Menggunakan *Software Bacula* dengan Metode *Backup-Restore*. *E-Proceeding of Engineering*, 5(2).
 - [5] Li Xiao-lei, 2009. *Research On Data Backup And Recovery Technology In SCADA System*, Department of Computer Science, North China Electric Power University, Changping District, Beijing, 102206, China
 - [6] Ngo, H.B., Huynh, T.V., 2016. *Enterprise Application Backup and Restore in Cloud Computing*. International Journal of Computer and Electrical Engineering, 8(2).
 - [7] PT. Bank Mega, 2017. *Data Center System Reference Manual*, Operational Division, Jakarta.
 - [8] Rosano, A., 2011. Efisiensi Biaya dan Optimasi *Data Rate* pada Jaringan *System Banking Online* (Studi Kasus PT Bank Mega), *Tbk.*. Tesis, Magister Teknik, Universitas Mercu Buana.
- Dari studi ini, metode gabungan *full backup* dan *incremental backup* merupakan metode yang secara moderat baik karena lebih mudah dalam pengerjaannya, serta lebih ekonomis dalam hal media penyimpanan sehingga metode gabungan ini diharapkan dapat saling mengatasi segala kekurangan dari setiap metode yang ada baik dari metode *full backup* maupun *incremental backup*.
- Metode *mirroring backup* sangat bagus dan paling sempurna dengan data yang *real-time*. Namun memerlukan infrastruktur, *hardware*, dan *software* yang cukup mahal. Juga memerlukan *effort* yang cukup rumit dalam proses pengertesannya. Apabilamanajemen memandang penting soal pelayanan kepada nasabah, maka *metode mirroring backup* ini menjadi pilihan yang sesuai.
- Sharma, Kruti, Singh, Kavita R., 2012, *Online Data Backup and Disaster Recovery Techniques in Cloud Computing : A Review*, Journal Computer Science Engineering, YCCE, Nagpur (MS), 441 110, India.
- [9] Stiawan, Deris, 2005. *Sistem Keamanan Komputer*, Elex Media Komputindo.
 - [10] Wijayani, Sila. 2008. Pembangunan *Disaster Recovery Plan* Untuk Sistem Informasi Manajemen Terintegrasi ITB, Tugas Akhir.
 - [11] Yanuardi. A., 2004. *Strategi Backup dan Recovery Data pada Disaster Recovery Center*, Engineer pada Lab. Solusi TI-TELKOM R & D Center.