Disaster Recovery Strategy Menggunakan *Software* Bacula dengan Metode *Full Backup-Restore*

Disaster Recovery Strategy Using Software Bacula With Full Backup-Restore Method

Eliza Adira Handrini[1], M. Teguh Kurniawan, S.T., M.T.[2], Adityas Widjajarto, S.T., M.T.[3]

[1,2,3]Prodi S1 Sistem Informasi, Fakultas Rekayasa Industri, Universitas Telkom
[1]**elizaadira@student.telkomuniversity.ac.id, teguhkurniawan@telkomuniveristy.co.id,**
[3]**adtwjrt@telkomuniversity.ac.id**

Abstrak

Data merupakan sekumpulan informasi mengenai suatu hal yang dapat dijadikan sebagai aset karena dapat menjadi sumber keuntungan bagi pelaku bisnis. Data harus dijaga dan disimpan pada sebuah tempat penyimpanan yaitu *data center*. *Data center* menjadi tempat penyimpanan data terpusat yang harus bekerja 24 jam sehingga *data center* harus memiliki cadangan bila terjadi hal yang tidak diinginkan seperti virus, pencurian data, ataupun bencana. *Disaster recovery center* (DRC) adalah *alternative data center*, bila data center mati maka DRC akan aktif dan terjadi alih fungsi. Terdapat strategi dalam menyelamatkan data yang dinamakan dengan *Disaster Recovery Strategy* (DRS), salah satu contoh DRS adalah dengan melakukan *remote backup-restore*. *Remote backup-restore* dapat dilakukan dengan bantuan *software*. Pada penelitian ini menggunakan *software* Bacula dengan metode *full backup-restore*. Metode *full backup-restore* adalah melakukan *backup-restore* pada seluruh *file*. Pengujian dilakukan untuk melihat integritas data dan kecepatan proses data setelah dilakukannya *backup* dan *restore*. Hasil pengujian menunjukan keaslian data terjaga pada pengujian integritas data dengan fungsi *hash* MD5 dan *digital signature* setelah dilakukannya proses *backup* dan *restore*. Kecepatan proses data ditinjau dari nilai *throughput* dan *delay*. *Restore* menghasilkan nilai lebih cepat dibandingkan dengan *backup*. Nilai *delay* pada proses *backup* dan *restore* memiliki rata-rata dibawah 150 ms, dalam kategori sangat bagus menurut versi TIPHON. Proses *remote backup-restore* dengan *software* Bacula menggunakan metode *full backup-restore* dapat mendukung *disaster recovery strategy* dan hasil pengujian integritas data dan nilai kecepatan proses data dapat dijadikan sebagai SLA dalam menjalankan DRS dengan *software* Bacula.

Kata Kunci: *Disaster Recovery Strategy*, Bacula, *Remote Backup-Restore*, *Full Backup-Restore*, Integritas Data, Kecepatan Proses Data.

Abstract

Data is a collection of information about a thing that can be used as an asset because it can be a source of profit for the business. Data must be maintained and stored in a storage area that is data center. Data center becomes centralized data storage that must work 24 hours so the data center must have a backup in case of unwanted things like viruses, data theft, or disaster. Disaster recovery center (DRC) is an alternative data center, when the data center is dead then the DRC will be active and the transfer function occurs. There is a strategy for saving data called Disaster Recovery Strategy (DRS), one example of DRS is to do a remote backup-restore. Remote backup-restore can be done with the help of software. In this research using Bacula software with full backup-restore method. Full backu-restore method used to backup-restore entire file. Goals of this research are to see data integrity and speed of data process after doing backup and restore. The test results show authenticity of data integrity with hash function MD5 and digital signature after the backup and restore process. The speed of the data process is reviewed from value of throughput and delay. Restore has value faster than backup. The delay value in the backup and restore process has an average of under 150 ms, in very good category according to TIPHON version. The remote backup-restore process with Bacula software using the full backup-restore method can support the disaster recovery strategy and the results of data integrity testing and the value of data processing speed can be used as SLA in running DRS with Bacula software.

Keywords*: *Disaster Recovery Startegy*, Bacula, *Remote Backup-Restore*, *Full Backup-Restore*, *Data Integrity*, *Speed of Data Process.

1. Pendahuluan

Data menjadi salah satu kunci pada perusahaan karena dianggap sebagai aset. Data harus disimpan secara terpusat, tempat penyimanan data adalah *data center*. *Data center* menjadi suatu hal yang penting bagi pelaku bisnis dan harus bekerja secara optimal selama 24 jam, sehingga diperlukan cara untuk mencegah bila terjadi

suatu bencana. *Data center* memiliki tempat yang diperuntukan sebagai *alternative*, yaitu *Disaster Recovery Center* (DRC). Menggunakan DRC sebagai *alternative recovery* merupakan hal penting untuk tetap melanjutkan kelangsungan kegiatan bisnis. Perancangan startegi dalam DRC dibahas dalam *Disaster Recovery Strategy* (DRS). Dalam DRS terdapat berbagai strategi untuk melakukan mitigasi (pencegahan) pada data agar tidak terjadi masalah, salah satunya dengan melakukan *backup-restore*. *Backup* dapat dilakukan sebagai suatu langkah untuk menyelamatkan data. *Backup* dapat dilakukan dengan berbagai cara, misalanya melakukan *backup* pada lokasi yang berbeda dari perusahaan dengan level keamanan yang sangat tinggi. Banyak *device* yang digunakan untuk *backup*, tetapi bila menggunakan *hardware backup* tidak dapat dilakukan secara fleksibel. Sehingga dilakukan *backup* secara *remote*. Terdapat 3 metode dalam *backup* salah satunya adalah *full backup-restore* yang dimana menyaliln seluruh *file* dan *directories*, sehingga mudah dalam pencarian file saat dibutuhkan. Dengan melakukan *backup-restore* secara *remote* dibutuhkan *software. Software* yang digunakan adalah Bacula. Bacula dapat berjalan pada beberapa sistem operasi.

Oleh karena itu, untuk menunjang penelitian pada kali ini penulis melakukan pengujian dengan melakukan simulasi *backup-restore* menggunakan metode *full backup-restore* dengan Bacula sebagai *software remote backup*. Berdasarkan hal tersebut maka hasil akhir dari penelitian ini berupa analisis dari integritas data dan kecepatan proses data *backup-restore* dengan metode *full backup-restore.*

2. Dasar Teori dan Sistematika Penelitian

2.1 Data Center

Menurut definisi dari *Telecommunication Industry Association* [1], *Data center* merupakan bagian dari bangunan yang memiliki fungsi utama sebagai ruang komputer dan area pendukungnya.

Menurut definisi dari Yulianti [2] *Data center* merupakan fasilitas yang digunakan untuk menempatkan beberapa kumpulan *server* atau sistem komputer dan sistem penyimpanan data (*storage*) yang dikondisikan dengan pengaturan catudaya, pengaturan udara, pencegahan kebakaran dan sistem pengamanan fisik.

Dapat disimpulkan *Data Center* merupakan suatu fasilitas atau bangunan sebagai tempat penyimpanan sistem komputer dan sistem penyimpanan data dengan memperhatikan standar pada pembangunan *Data Center*.

2.2 *Disaster Recovery Strategy*

Disaster Recovery Strategy adalah sebuah strategi yang dirancang untuk melanjutkan proses bisnis bila terjadi bencana [3]. Tujuannya memberikan solusi efektif untuk memulihkan semua proses bisnis yang dianggap penting, misalnya pemindahan layanan (*backup*) ke dalam DRC. Rencana tersebut adalah salah satu dari strategi penanganan dalam situasi darurat. Rencana yang telah dibuat harus saling terhubung antara satu dengan lainnya, tetapi rencana tersebut juga dapat dijalankan secara terpisah.

2.3 *Disaster Recovery Center*

Disaster Recovery Center (DRC) merupakan suatu hal yang sangat penting dan memiliki prioritas yang tinggi dalam suatu organisasi atau *department* sebagai tempat dimana data tersebut disimpan. DRC dapat dikatakan replika dari *data center* karena DRC langsung terhubung dengan *data center* dan akan mendapatkan data yang selalu ter-*update*. Bila terjadi suatu bencana yang mengenai data primer maka DRC langsung mengambil alih fungsi menjadi *primary site.* Infrastruktur dari *disaster recovery* mencakup *data center*, *Wide Area Network* (WAN), *Local Area Network* (LAN), *hardware*, dan aplikasi. Dari semua infrastruktur memiliki penanganan yang berbeda tergantung pada kebutuhan perusahaan [4].

Tujuan dari DRC adalah mengembalikan sistem operasi dalam waktu yang singkat dan dengan risiko kehilangan data yang kecil sehingga proses bisnis tidak terganggu. [5] sehingga tidak terjadi kerugian finansial dalam bisnis perusahaan.

2.4 *Backup* dan *Restore*

Backup adalah suatu proses untuk memindahkan atau menyalin sekumpulan informasi yang tersimpan di dalam *harddisk* pada komputer, dengan memindahkan dari suatu perangkat ke dalam perangkat lain atau lokasi lain. Sekumpulan informasi tersebut yang diubah menjadi data biasanya berupa *file* aplikasi, sistem, ataupun *database*. Pada umumnya *backup* tidak dilakukan hanya untuk melindungi dari kehilangan data, tetapi memungkinkan untuk mengembalikan salinan *file* yang lama dan yang telah dimodifikasi. [6]

Fungsi dari melakukan *backup* adalah sebagai cadangan data bila data yang tersimpan di dalam satu *device* tersebut hilang ataupun rusak akibat dari *virus*, bencana, kegagalan *hardware*, pencurian, *data corruption*, serangan berbahaya, dan kesalahan manusia. Tujuan dari melakukan *backup* adalah mengembalikan suatu data yang telah rusak ataupun hilang dan mengebalikan suatu data yang dibutuhkan pada masanya.

Restore adalah suatu proses pengembalian data setelah melakukan *backup* ke dalam tempat penyimpanan aslinya atau penyimpanan baru. *Restore* data dilakukan saat data yang dibutuhkan mengalami kerusakan, kecelakaan, atau bencana alam [7]. Pengembalian data yang telah di-*backup* dibutuhkan pembuktian dari integritas data.

Integritas data adalah keakuratan dan konsistensi data yang tersimpan dan tidak terjadi perubahan pada data setelah dilakukan pengembalian data. Integritas data dikelola melalui penggunaan pengecekan kesalahan dan rutinitas dalam melakukan validasi [8].

2.5 *Full Backup-Restore*

Full backup merupakan metode backup yang melakukan penyalinan (backup) seluruh file dan directories yang terdapat pada sistem. Dalam melakukan pengembalian (restore) membutuhkan waktu yang lebih singkat dibanding metode lain, namun dalam melakukan backup membutuhkan waktu yang lama.

Menggunakan metode *full backup-restore* dalam melakukan *backup* dan *restore* memiliki keunggulan dalam pencarian *file*. Karena metode ini melakukan *backup* dan *restore* pada seluruh *file* yang mengalami perubahan maupun yang tidak mengalami perubahan, sehingga data tidak ada pengurangan data. Karena metode ini melakukan *backup* dan *restore* pada keseluruhan *file* sehingga kekurangan dari metode ini adalah membutuhkan *storage* yang besar [4]

2.6 Bacula

Bacula adalah *software backup* peringkat ke 3 sekala *enterprise* yang paling populer menurut google *trends*. Merupakan *software backup* jaringan tingkat lanjut yang memungkinkan untuk melakukan pengelolaan *file* dalam penyalinan, *indexing, restore, verfication*, penjadwalan pekerjaan antar *server*, memungkikan untuk berjalan pada sistem operasi yang berbeda yang disebut dengan *cross platform*. Bacula dirancang untuk melindungi data sesuai dengan aturan yang telah ditetapkan oleh *user*. Bacula terbentuk atas 6 mayor komponen, yaitu [9]:

1. *Director Daemon (Director)*
   Merupakan program utama yang mengawasi semua aktivitas *backup, restore, verify,* dan *archive operation*. Administrator sistem menggunakan *director* untuk menjadwalkan *backup* dan memulihkan *file*.
2. *Storage Daemon* (SD)
   Merupakan layanan yang terdiri dari beberapa program perangkat lunak yang melakukan penyimpanan dan *recovery* atribut dan data *file* ke dalam media *backup* fisik atau *volume*. Dengan kata lain, *daemon storage* bertanggung jawab untuk membaca dan menulis pada *tape* (atau tempat penyimpanan lain).
3. *File Daemon* (FD)
   File daemon (juga dikenal sebagai program Klien) merupakan program perangkat lunak yang diinstal pada mesin yang akan di*backup*. Khusus untuk sistem operasi yang dijalankannya dan bertanggung jawab untuk menyediakan atribut dan data *file* saat diminta oleh *director*. *File daemon* juga bertanggung jawab atas bagian sistem *file* yang bergantung pada *restore* atribut dan data *file* selama *recovery operation*.
4. *Catalog* (*database*)
   Merupakan program perangkat lunak yang bertanggung jawab untuk memelihara *file indexing* dan *database volume* untuk semua *file* yang dicadangkan. *Catalog* mengizinkan administrator sistem atau *user* untuk menemukan dan mengembalikan *file* yang diinginkan dengan cepat. *Catalog* membedakan Bacula dari *backup programs* sederhana seperti tar dan bru, karena *catalog* menyimpan semua catatan *volume* yang digunakan, semua *job* yang sedang berjalan, dan semua *file* yang tersimpan. Bacula saat ini mendukung tiga *database* yang berbeda, MySQL, PostgreSQL, dan SQLite, salah satunya harus dipilih saat membangun Bacula.
5. Bacula *Console*
   Merupakan program yang memungkinkan administrator atau pengguna berkomunikasi dengan Bacula *director* yang sedang berjalan, Bacula *Console* tersedia dalam tiga versi yaitu *text-based console interface QT-based interface*, dan *xwWidgest Graphical interface*.

2.7 Kriptografi

Kriptografi (cryptography) berasal dari bahasa yunani yang memiliki arti sesuatu yang tertulis secara rahasia dan sembunyi. Menurut teminologinya, kriptografi adalah ilmu seni untuk menjaga keamanan data atau pesan saat dikirimkan, tanpa mengalami gangguan dari pihak ketiga yang berhubungan dengan keamanan informasi misalnya integritas data.

Kriptografi memiliki empat tujuan mendasar dalam aspek keamanan yaitu [10]:

1. *Confidelity* (kerahasiaan)
   Layanan yang memastikan bahwa pesan yang diterima oleh penerima dari pengirim tetap terjaga kerahasiaannya dan tidak diketahui oleh pihak lain. Untuk memastikan kerahasiaan data dengan cara membuat suatu algoritma matematis yang sulit dibaca dan dipahami.
2. *Authentication* (autentikasi)
   Layanan yang memastikan bahwa pesan diterima oleh orang yang berhak menerima dan dikirim oleh orang yang berhak mengirim. Berhubungan dengan otentikasi data pengirim dan penerima serta otentikasi keaslian data yang harus dapat diidentifikasi. Dan memastikan bahwa tidak ada penyusup.
3. *Data Integrity* (integritas data)
   Layanan yang dapat melakukan identifikasi dan memastikan bahwa pesan yang diterima oleh penerima adalah pesan yang asli tidak ada manipulasi (penghapusan, pengubahan, atau penambahan) data yang dilakukan oleh pihak lain.
4. *Non-Repudiation* (anti penyangkalan)
   Layanan yang dapat mencegah penagkalan dari pihak lain yang akan melakukan aksinya. Pengirim harus tidak bisa menyangkal pesan yang dia kirimkan.

Kriptografi memiliki beberapa algoritma yang terbagi menjadi dua kelompok dalam penggunaan kunci yaitu:

1. Algoritma Simetris
   Pada Algoritma kunci simetris memiliki kunci atau sandi yang sama antara proses enkripsi maupun dekripsi, sehingga algoritma ini dapat disebut juga sebagai *single-key algorithm.* Contoh algoritma yang menggunakan simetris : DES, *blowfish, twofish*, MARS, IDEA, 3DES, dan AES.
2. Algoritma Asimetris
   Pada algoritma kunci asimetris memiliki kunci yang berbeda pada proses enkripsi dan dekripsi. Pada proses enkripsi terdapat *public key* yang mana dapat diketahui oleh siapa saja, sedangkan pada proses dekripsi memiliki *private key* yang mana hanya dapat dilihat oleh yang berwenang yang memiliki kunci tersebut. Contoh alogitma yang menggunakan asimetris : RSA dan DSA.

2.8 *Quality of Service*

1. *Throughput*
   Throuhput adalah penghitungan mengenai kecepatan transfer data efektif yang terukur pada suatu ukuran waktu tertentu yang diukur dalam satuan bps (bit per *second*).

Tabel II 1 Rekomendasi *Throuhput* (Sumber : TIPHON)

Kategori *Throughput*	***Throughput* (bps)**
Sangat Bagus	100
Bagus	75
Sedang	50
Jelek	< 25

$$Throughput = \frac{\text{Paket data yang diterima}}{\text{Lama pengamatan}}$$

2. *Delay* (*Latency*)
   Delay adalah waktu tunda yang dibutuhkan data untuk menempuh jarak dari asal ke tujuan. *Delay* dapat dipengaruhi oleh jarak, media fisik, atau lamanya waktu proses.

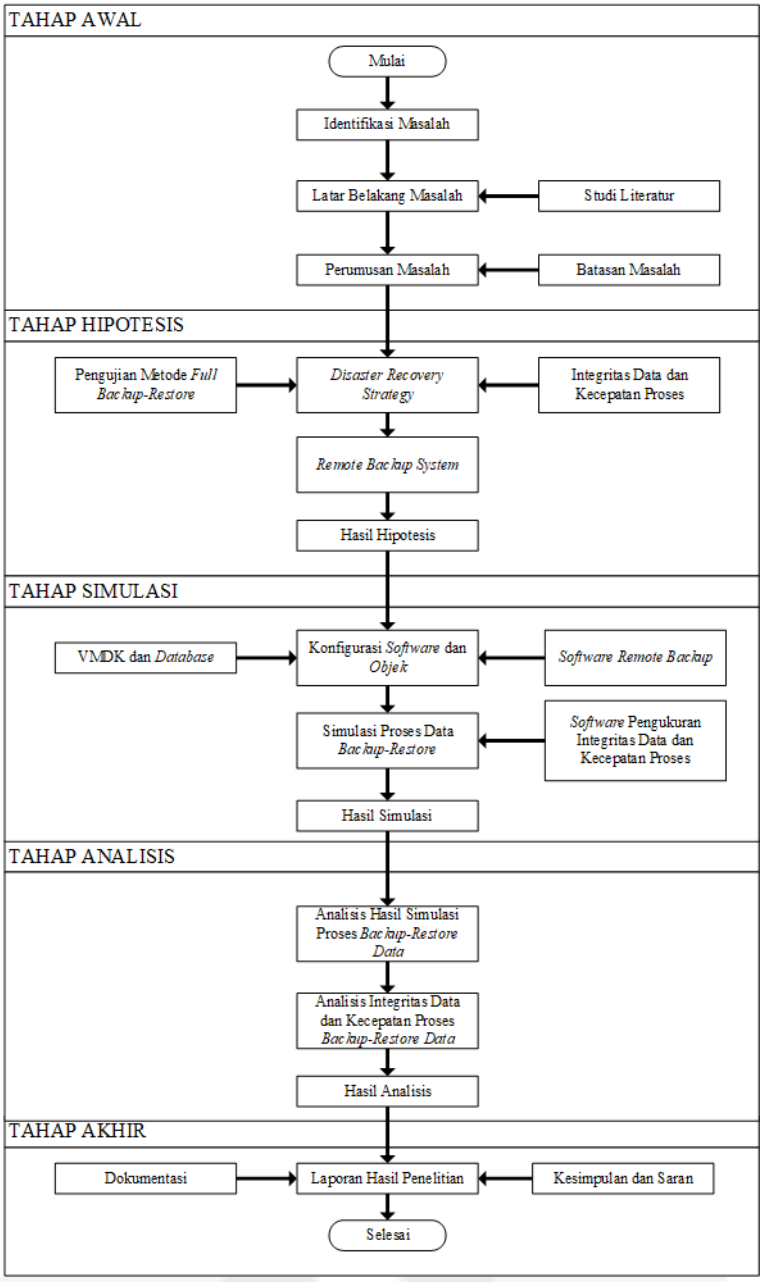
Tabel II 2 Rekomendasi Waktu *Delay* (sumber: TIPHON)

Kategori Latensi	**Besar *Delay* (ms)**
Sangat Bagus	< 150
Bagus	150 – 300
Sedang	300 – 450
Jelek	>450

$$Delay = \frac{\text{Total } delay}{\text{Total paket yang diterima}}$$

2.9 Sistematika Penelitian

Sistematika pemecahan masalah adalah bagian yang menjelaskan tentang tahapan-tahapan yang akan dilakukan dalam melakukan penelitian. Tahapan dimulai dari identifikasi masalah hingga tahapan akhir yaitu laporan hasil penelitian. Sistematika tahapan-tahapan adalah sebagai berikut:



Gambar 2-1 Sistematikan Penelitian

3. Pengujian Sistem dan Analisis

3.1. Pengujian Sistem

Pengujian integritas data dilakukan dengan parameter dan objek yang berbeda, dirangkum pada Tabel 3-1.

Tabel 3- 1 Rangkuman Pengujian

Parameter Uji	Objek	Uraian Pengujian	Hasil dari Pengamatan
Algoritma MD5	*Virtual Machine*	1. *Hash* MD5 sebelum *backup* 2. *Hash* MD5 setelah *restore*	*hash backup = hash restore* (ok)
Digital Signature RSA	MySQL *Database*	*Database Employee* (SHA 256, *department*.frm)	*Verified* Ok
		Penambahan *Database Finance* (SHA 384, *income*.frm)	*Verified* Ok
		Penambahan *Database Marketing* (SHA 512, *payment*.frm)	*Verified* Ok

Pengujian integritas data dilihat dari objek:

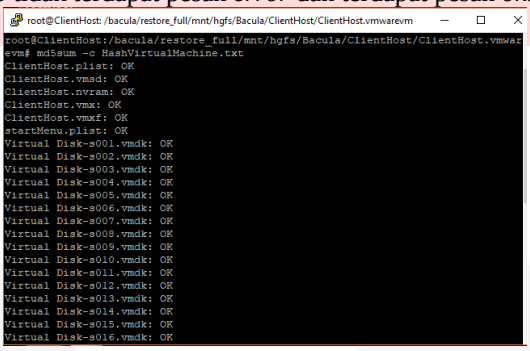
1. VMDK, diuji dengan menggunakan algoritma MD5 untuk melihat ada tidaknya perubahan *message digest* antara *file* sebelum di-*backup* dengan *file* setelah di-*restore yang* terdapat pada setiap *file* VMDK. Pengujian dilakukan sebelum *backup* dan setelah *restore*. Melakukan *hash* dengan MD5 pada VMDK sebelum *backup* dan melakukan autentikasi dengan membandingkan hasil *hash* sebelum *backup* dengan *hash* setelah *restore*. Didapatkan hasil *hash backup* sama dengan *hash restore* dengan pesan *ok.*
2. *Database*, diuji dengan menggunakan konsep *digital signature* untuk melihat ada tidaknya perubahan pada *file* dengan melakukan autentikasi *file* menggunakan *public key* yang telah dibuat. Pengujian *database* dilakukan tiga kali *backup-restore* dengan melakukan penambahan tabel *database* pada pengujian kedua dan ketiga. Hasil dari pengamatan setelah dilakukan penambahan pada *database* saat melakukan verifikasi pengujian pertama, kedua, dan ketiga didapatkan hasil dengan pesan *verified ok.*

3.2. Analisis Integritas Data

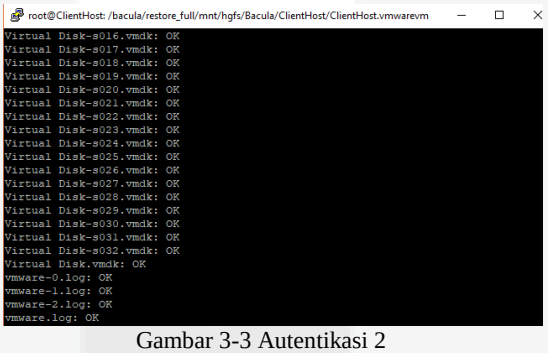
1. MD5 *Checksum*

MD5 merupakan salah satu fungsi *hash* yang banyak digunakan. Fungsi *hash* adalah sebuah fungsi yang yang mentranslasikan sebuah *message digest* pada setiap pesan. Fungsi *hash* biasanya digunakan untuk mewujudkan layanan kamanan seperti keutuhan data.

Setelah melakukan pengujian integritas data menggunakan fungsi *hash* MD5 dapat dibuktikan dengan Gambar 3-2, dan Gambar 3-3 tidak terdapat pesan *error* dan terdapat pesan *ok.*



Gambar 3-2 Autentikasi 1



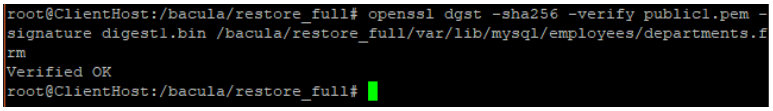
Gambar 3-3 Autentikasi 2

Dari data hasil pengujian skenario ditinjau dari segi keamanan informasi terdapat 3 ciri yang mengacu pada "CIA Triad" yaitu, *confidentiality* (hanya administrator yang mengetahui keberadaan data), *integrity* (terbukti tidak adanya perubahan data terbukti dari Gambar 3-1 dan Gambar 3-2 yang bertuliskan ok), *dan availability* (data tersedia bagi pengguna data setelah dilakukannya *restore*). Pengujian ini telah memenuhi ketiga aspek tersebut menerangkan bahwa penggunaan fungsi *hash* MD5 untuk melakukan *backup* dan *restore* dengan cara *remote backup* menggunakan *software* Bacula dapat dipastikan keamanannya. Sehingga dapat dijadikan sebagai acuan *service level aggrement* dalam melakukan DRS.

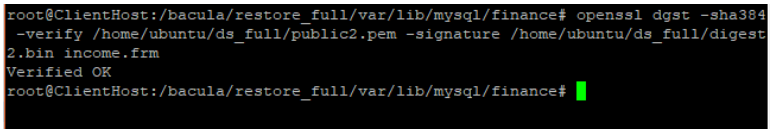
Remote backup merupakan salah satu dari DRS yang harus dimiliki oleh setiap pelaku bisnis yang sudah menjadikan data sebagi aset pada perusahaan. Dari hasil pengujian skenario *remote backup* dapat dipastikan keamannnya dari sisi keamanan informasi, sehingga hasil dari analisis pengujian integritas data menggunakan fungsi *hash* MD5 dapat dijadikan pertimbangan dalam melakukan *backup* dan *restore virtual machine* yang berisikan sistem operasi dan aplikasi menggunakan *software* Bacula dalam perusahaan.

2. *Digital Signature*

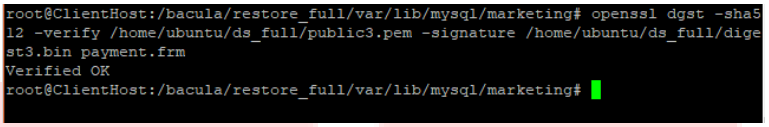
Dari hasil pengujian skenario setelah melakukan *backup* dan *restore* kemudian dilakukan autentikasi antara hasil data yang telah dilakukan *restore* dengan *public key*. Gambar 3-4, Gambar 3-5, dan Gambar 3-6 menunjukan hasil dari autentikasi tidak ada pesan *error* dan terdapat pesan *verified ok.*



Gambar 3-4 Hasil *Digital Signature* Objek Pengujian 1



Gambar 3- 5 Hasil *Digital Signature* Objek Pengujian 2



Gambar 3-6 Hasil *Digital Signature* Objek Pengujian 3

Dari hasil pengujian skenario dapat diartikan pesan hasil data *restore* sesuai dengan *public key* yang dibuat. Pengujian integritas data menggunakan konsep *digital signature* dengan menggunakan *hash* SHA terjamin keamanan dan keutuhan datanya pada proses *backup* menggunakan *software* Bacula. Penggunakan SHA dengan membedakan bit dalam melakukan *hash* tidak ada pengaruh pada pengujian skenario ini. Data yang telah dilakukan *backup* sama dengan data hasil *restore* yang dibuktikan dengan pesan *verified ok* yang menandakan tidak terjadi perubahan pada data.

Pengujian integritas data dengan *digital signature* merupakan salah satu konsep yang dapat digunakan dalam melihat orisinalitas suatu data jika digunakan dalam DRS pada *remote backup restore* menggunakan *software* Bacula. Konsep ini dapat dijadikan sebagai acuan SLA dalam melakukan *remote backup restore* dalam penyedia layanan DRS.

3.3. Analisis Kecepatan Proses

1. *Throughput*

Tabel 3-2 adalah hasil yang didapatkan dari pengujian kecepatan proses data dengan parameter *throughput* saat pengujian *backup* dan *restore*. *Throughput* sebagai gambaran waktu kecepatan yang dibutuhkan dalam proses *backup*. *Throughput* juga kemampuan suatu jaringan dalam melakukan pengiriman data. Biasanya *throughput* selalu dikaitkan dengan *bandwith*, tetapi *bandwith* bersifat tetap dan *throughput* bersifat dinamis sesuai dengan lalu lintas data yang sedang terjadi.

Tabel 3-2 Hasil Pengujian *Throughput*

Hasil Pengujian *Throughput* (KBps)		
Pengujian Objek	*Backup*	*Restore*
Pertama	2386.0951	5866.9152
Kedua	3349.4853	10878.3045
Ketiga	3271.8751	4713.6071

Pada proses pengujian *backup* didapatkan nilai lebih rendah dibandingkan dengan pengujian *restore*, dikarenakan saat proses melakukan *backup* data dikompresi dalam bentuk GZIP dan saat *restore* data yang sampai sudah dalam bentuk UNGZIP sehingga besar jumlah ukuran paket yang diterima lebih besar dibandingkan dengan jumlah ukuran paket *backup*.

Pada Tabel 3-2 terlihat kenaikan dan penurunan yang terjadi pada setiap proses *backup* dan *restore* dari ketiga pengujian, hasil tersebut disebabkan oleh beberapa faktor. Berdasarkan topologi pengujian simulasi maka faktor yang mempengaruhi yaitu, media transmisi yaitu kabel UTP, spesifikasi dari instrument fisik dan besar *bandwith* yang didapat.

2. *Delay*

Tabel 3-3 adalah hasil yang didapat dari pengujian kecepatan proses dengan parameter uji *delay*. Penghitungan *delay* dimaksudkan untuk melihat waktu yang dibutuhkan untuk pengiriman data dibandingkan dengan banyaknya paket yang dikirim.

Tabel 3-3 Hasil Pengujian *Delay*

Hasil Pengujian *Delay* (ms)		
Pengujian Objek	*Backup*	*Restore*
Pertama	0.6041	0.2482
Kedua	0.4321	0.1356
Ketiga	0.3739	0.2186

Hasil yang didapat dari pengujian *delay backup* dan *restore* menunjukan keseluruhan nilai *delay* dibawah 1 ms, hasil ini dikarenakan pada melakukan pengujian skenario topologi yang dirancang saling terhubung dengan kabel UTP sehingga tidak menghasilkan nilai *delay* yang besar. *Delay* dapat dipengaruhi karena hambatan dari luar seperti jaringan internet.

Pada hasil pengujian *backup* pada objek 1-3 terlihat penurunan terhadap nilai *delay*. Pada hasil pengujian *restore* terlihat adanya kenaikan dan penurunan nilai *delay*. Nilai ini dipengaruhi oleh beberapa faktor diantaranya, media transmisi, media fisik, dan waktu proses yang lama dalam jaringan LAN.

Dalam pengaplikasian konsep *remote backup* antara DC dan DRC menggunakan jaringan internet untuk menghubungkan jarak keduanya, sehingga nilai yang didapat dari hasil pengujian ditambahkan dengan nilai *delay* internet yaitu 50 ms. Sehingga nilai yang di dapat terlihat pada Tabel 3-4

.

Tabel 3-4 Nilai Delay Digabungkan dengan Delay Internet

***Delay* Internet (ms)**				
Pengujian Objek	*Backup*	*Backup'*	*Restore*	*Restore'*
Pertama	0.6041	50.60	0.2482	50.24
Kedua	0.4321	50.43	0.1356	50.13
Ketiga	0.3739	50.37	0.2186	50.21

Menurut standar *delay* versi TIPHON, *delay* memiliki standar sangat baik pada angka kurang dari 150ms. Dari Tabel 3-4 hasil yang di dapatkan berdasarkan dengan landasan teori masuk dalam kategori sangat bagus.

Berdasarkan hasil analisis dari parameter uji *throughput* dan *delay* disandingkan dengan penerapan DRS dengan *software* Bacula dapat dikatakan menunjang proses bisnis pada perusahaan. Dimana dalam pengujian menggunakan metode *full backup restore* yang dimana melakukan *backup* dan *restore* pada keseluruhan data, tetapi *delay* yang dihasilkan bernilai sangat baik versi TIPHON

4. Kesimpulan

4.1. Proses *remote backup-restore* dengan *software* Bacula menggunakan metode *full backup-restore* dapat mendukung *disaster recovery strategy.* Penggunaan metode *full backup-restore* memudahkan bagi para pelaku bisnis dalam pencarian seluruh data, karena metode ini melakukan *backup* dan *restore* pada keseluruhan *file.*

4.2. Hasil pengujian integritas data, melakukan *backup* dan *restore* dengan *software* Bacula dengan menggunakan *hash* MD5 dan *digital signature* masih terjaga keamanan dan keaslian datanya.

4.3. Hasil pengujian kecepatan proses data, didapatkan nilai sangat baik versi TIPHON dari hasil pengujian *delay* dan memiiki nilai *throughput* yang tinggi untuk proses *restore*.

Daftar Pustaka:

[1] Telecommunication Industry Association, 2012.

[2] D. E. Yulianti and H. B. Nanda, "Best Practice Perancangan Fasilitas Data Center," p. 11, 2008.

[3] S. Adedayo, "Disaster Recovery Strategy and Maintenance Plan," 2014.

[4] F. Ridho, N. P. Yudho and R. H. P, "Disaster Recovery Center (DRC)," 14 November 2012. [Online]. Available: https://www.slideshare.net/fariderdotcom/disaster-recovery-center-and-disaster-recovery-plan. [Accessed 20 November 2017].

[5] R. K. Rolen, "Global Journal of Computer Science and Technology Interdiciplinary," *Disaster Recovery Center Establishment for T4 Data Center to Run the IT System in Power Utilities* , p. 13, 2013.

[6] D. Sampaio and J. Bernadino, "Open Source Backup System for SMEs," pp. 824-825, 2015.

[7] M. Rouse, "Data Restore," July 2017. [Online]. Available: http://searchdatabackup.techtarget.com/definition/restore.

[8] M. D.Sinaga, "Integritas Basis Data," 18 October 2017. [Online]. Available: dinus.ac.id/repository/docs/ajar/Integritas_Basis_Data.ppt. [Accessed 5 Desember 2017].

[9] H. M. d. Faria, Bacula The Open Source Backup Software, Brazil: Brazilian Bacula Users Community, 2016.

[10] A. Ginting, R. R. Isnanto and I. Pertiwi, "Implementasi Algoritma Kriptografi RSA untuk Enkripsi dan Deskripsi Email," *Jurnal Teknologi dan Sistem Informasi* , pp. 253-258, 2015.

[11] R. Wulandari, "ANALISIS QoS (QUALITY OF SERVICE) PADA JARINGAN INTERNET (STUDI KASUS : UPT LOKA UJI TEKNIK PENAMBANGAN JAMPANG KULON – LIPI)," *Jurnal Teknik Informatika dan Sistem Informasi* , pp. 163-164, 2016.

[12] gtslearning, CompTIA Security+ SY0-401 Official Study Guide, London: gtslearning, 2014.

[13] A. F. Latif, Analisis dan Perancangan Power Management Green Data Center di Direktorat Sistem Infomrasi Telkom Menggunakan Standar TIA-942 dengan Metode PPDIOO Life-Cycle Approach, Bandung, 2016.

[14] W. Jaya, 23 January 2016. [Online]. Available: https://www.kompasiana.com. [Accessed 7 Oktober 2017].

[15] H. Apriyanto, 20 Februari 2015. [Online]. Available: http://www.lipi.go.id. [Accessed 19 Maret 2018].

[16] R. Sadikin, Kriptografi Untuk Keamanan Jaringan, Yogyakarta: Andi Offset, 2012.