

Implementasi Sistem *Backup* Data Perusahaan Sebagai Bagian dari *Disaster Recovery Plan*

Implementation of Corporate Data Backup Systems As Part of a Disaster Recovery Plan

Eko Haryadi¹, Abdussomad² dan Robi³

¹Universitas Bina Sarana Informatika

E-mail : Eko.ehy@bsi.ac.id

^{2,3}STMIK Nusa Mandiri Jakarta

E-mail : ²shomadresas@gmail.com, ³robi.rbs@nusamandiri.ac.id

Abstrak--- *Backup data merupakan sebuah aktivitas yang harus dilakukan secara baik dan teratur. Pemahaman setiap user terhadap pentingnya penyelamatan data dan proses Backup terhadap data mutlak diperlukan. Perusahaan harus mempunyai sebuah standard operating procedure untuk bisa menjaga data yang dimiliki sebagai sebuah asset yang tidak ternilai harganya. Backup data merupakan salah satu bagian dari disaster recovery plan perusahaan. Pemanfaatan teknologi dan infrastruktur jaringan mutlak diperlukan dalam melakukan proses Backup data. Proses Backup dan recovery harus dituangkan dalam disaster recovery plan atau juga bisa dituangkan dalam standard operating procedure perusahaan dan harus diterapkan secara nyata dalam aktivitas sehari-hari. Salah satu teknologi yang bisa diterapkan adalah dengan memanfaatkan virtual mesin dan Veeam untuk melakukan proses Backup data perusahaan.*

Kata Kunci--- *VMware, Veeam, Backup, Recovery*

Abstract--- *Data Backup is an activity that must be done well and regularly. Understanding of each user towards the importance of saving data and the process of Backup of data is absolutely necessary. The company must have a standard operating procedure to be able to maintain the data owned as an invaluable asset. Data Backup is one part of the company's disaster recovery plan. The use of technology and network infrastructure is absolutely needed in the process of data Backup. The Backup and recovery process must be outlined in the disaster recovery plan or it can also be stated in the company's standard operating procedures and must be applied in a real way throughout the day. One of the technologies that can be applied is to use virtual machines and Veeam to process company data Backups.*

Keywords--- *VMware, Veeam, Backup, Recovery*

1. PENDAHULUAN

Data merupakan *asset* perusahaan yang sangat penting sehingga perlu di jaga dan mutlak untuk dibuatkan suatu sistem untuk bisa merawatnya. Terdapat berbagai bentuk data perusahaan yang perlu disiapkan sistem pemeliharannya, diantara adalah data-data pekerjaan karyawan, database serta data hasil pengolahan dari sebuah transaksi. Semua bentuk data diatas diperlukan suatu manajemen atau sistem dalam mengolah dan memeliharanya. Salah satu sistem yang harus di buat adalah dengan melakukan manajemen *Backup* data yang baik dan benar. Sistem *Backup* data yang baik dan benar akan membantu baik manajemen perusahaan atau juga para pelaku dibidang teknologi informasi untuk bisa menyimpan data perusahaan sebaik mungkin dan mengembalikan data tersebut apabila diperlukan oleh pihak yang membutuhkannya. Sistem *Backup* data yang baik dan benar merupakan salah satu dari penerapan *Disaster Recovery Plan*. Sistem *Backup* data akan membantu perusahaan dalam menghindari dari

resiko kerugian akibat dari kehilangan data ataupun kerusakan data. Terdapat banyak faktor yang menyebabkan data perusahaan hilang atau rusak, bisa terjadi karena virus, kelalaian user, sabotase, kegagalan sistem ataupun terjadi karena bencana alam atau bencana kebakaran gedung.

2. LANDASAN TEORI

2.1 *Backup dan recovery*

File *Backup* merupakan penyalinan sebuah file yang disimpan ditempat yang berbeda dengan file aslinya. Proses pencadangan (*backing up*) merupakan proses penyalinan yang bisa digunakan untuk menggantikan file yang rusak atau digunakan dalam proses mengembalikan data (*restore data*). Definisi lain menyebutkan bahwa *Backup* adalah kegiatan menyalin file atau database sehingga salinan tersebut dapat digunakan untuk memulihkan data asli yang rusak karena berbagai sebab[1]. Melakukan *Backup* pada database agak sedikit berbeda dengan melakukan *Backup* pada *server* dan *client* Ada beberapa pertimbangan dalam

perencanaan *Backup* dan *recovery* [2]. Hal pertama yang harus dipertimbangkan adalah jenis *database* apa yang akan di *Backup*. *Database* sistem dan *database* pengguna sering memiliki kebutuhan dan *recovery* yang berbeda. Sebagai contoh *database master* adalah *database* yang sangat penting dalam untuk seluruh operasi dari Microsoft SQL server, apabila *database master* gagal maka keseluruhan server akan mengalami masalah yang sama. Proses *Backup* pada *database master* tidak perlu dilakukan setiap jam tetapi bisa dilakukan setelah *database* dibuat, mengubah nilai-nilai konfigurasi, konfigurasi login SQL atau aktivitas lain yang mengakibatkan perubahan-perubahan pada *database* di dalam sebuah server. Hal yang kedua adalah seberapa penting data dalam *database* tersebut. Penting atau tidaknya sebuah data dalam *database* tergantung dari perusahaan tersebut menilai data tersebut. Derajat kepentingan sangat menentukan jenis *Backup* yang harus dilakukan. Hal yang ketiga adalah seberapa sering perubahan-perubahan dilakukan pada *database*. Frekuensi perubahan bisa menentukan seberapa sering *database* harus di *Backup*. Untuk sebuah *database* yang sifatnya *read only* maka *database* tersebut tidak perlu di *Backup* secara teratur. Hal keempat adalah seberapa cepat *recovery data* bisa dilakukan. Ini menjadi sangat penting untuk mempertimbangkan lamanya waktu yang diperlukan untuk melakukan *recovery* terhadap data yang hilang. Hal yang kelima adalah perlengkapan yang dimiliki untuk melakukan *Backup*. Untuk hal ini maka diperlukan perangkat keras untuk melakukan *Backup*. Apabila perangkat keras tidak tersedia maka *Backup* tidak bisa dilakukan. Ada beberapa media yang bisa digunakan yaitu mencakup *tape drive*, *drive* optik, *drive harddisk* yang bisa dilepas atau juga ke *harddisk* biasa.

Tipe-tipe dasar *Backup* data meliputi beberapa hal[2] ;

Back up database full, jenis *Backup* ini digunakan untuk melakukan *Backup* sepenuhnya dari *database* yang meliputi semua objek, tabel sistem, dan data. sewaktu *Backup* ini dimulai, SQL server akan mengkopi semua yang ada di dalam *database* dan juga menyertakan semua log-log dalam transaksi yang diperlukan pada saat *Backup* berlangsung. *Full Backup*, data diduplikasi secara keseluruhan baik data yang sudah pernah diduplikasi maupun belum pernah kedalam media yang terpisah. *Backup* dilakukan secara berkala[4]. *Snapshot Backup*, data diduplikasi secara *live* dengan melakukan penguncian terhadap seluruh data untuk sementara waktu dan kemudian dilakukan *snapshot* terhadap data tersebut yang dilanjutkan dengan dilepas agar dapat beroperasi kembali. *Incremental Backup*, data yang diduplikasi hanya data yang belum pernah dilakukan *Backup*. Bila terjadi perbedaan *byte* pada data, maka hanya perbedaan dari *byte* data tersebut yang akan diduplikasi.

Backup dilakukan secara berkala[4]. *Backup differential* adalah *Backup* yang dirancang untuk melakukan *Backup* pada data yang telah berubah sejak *Backup full* berakhir. *Backup log* transaksi merupakan *Backup* terhadap log-log transaksi yaitu *record-record* berangkaian dari semua modifikasi *database* dan digunakan selama operasi *recovery* untuk *commit* yaitu operasi menulis ke dalam *database*, yang terakhir adalah *Backup file* dan grup file. Jenis *Backup* ini dalam *database* cenderung untuk *Backup file database* dan file ketimbang seluruh *database*. Untuk *recovery* ada beberapa jenis yang bisa dilakukan dalam *database*, yaitu *Simple Recovery*, model *recovery* ini biasanya hanya akan dilakukan pada semua data yang dipulihkan hingga ke titik *Backup* yang terakhir. Strategi *Backup* ini akan terdiri dari strategi *Backup full* dan *differential*. *Full recovery* merupakan model *recovery* yang di rancang untuk *database-database* yang perlu dipulihkan hingga ke titik kegagalan atau ke titik tertentu dari waktu[2].

2.2. Disaster recovery Planning (DRP) dan Business Continuity Planning (BCP)

Disaster recovery Planning dan *Business Continuity Planning*[3], *DRP* adalah merupakan bagian perencanaan dari sebuah institusi untuk melakukan tahapan tertentu yang nantinya akan menjamin kelangsungan pelayanan (khususnya dari segi sistem informasi) yang diberikan tanpa mengurangi kapabilitas serta kinerja dari sebuah sistem jika terjadi sebuah bencana didalamnya. Sedangkan *BCP* adalah merupakan perencanaan kelanjutan proses bisnis dan layanan dari sistem informasi pasca terjadinya bencana yang menimpa sistem informasi tersebut. Meskipun keduanya terkait dengan pemulihan, *DRP* dan *BCP* adalah kegiatan yang berbeda dengan yang berbeda fokus, sasaran, dan hasil. *DRP* berfokus pada pemulihan sistem dan aplikasi TI. Ini terutama didorong dari perspektif teknis. *BCP*, di sisi lain, prihatin dengan pemulihan dan dimulainya kembali kegiatan bisnis di seluruh organisasi. Dengan demikian, *DRP* adalah bagian dari *BCP*. Karena ruang lingkup *BCP* adalah organisasi, itu harus (di bagian paling bawah) paling tidak didukung oleh manajemen senior organisasi[6].

2.3 Veeam Backup dan Replicatioin

Merupakan aplikasi yang dikembangkan oleh Veeam untuk lingkungan *virtual* yang dibangun di atas *VMware vSphere* dan *Microsoft Hyper-V hypervisors*. Perangkat lunak ini menyediakan fungsi pencadangan, pemulihan, dan replikasi untuk mesin *virtual*, server fisik dan *workstation* serta beban kerja berbasis *cloud*[5].

3. METODA

Mengadopsi metode NDLC yang digunakan dalam penelitian ini merupakan kategori penelitian

kuualitatif yang bersifat deskriptif, dimana *framework* yang digunakan adalah *Network Development Life Cycle (NDLC)* yang menjadi model penting dalam proses perancangan jaringan komputer.

NDLC sendiri merupakan siklus proses yang berupa tahapan dari mekanisme yang dibutuhkan dalam suatu rancangan proses pembangunan atau pengembangan suatu sistem jaringan komputer.

Berikut adalah tahapan dalam Metode *Network Development Life Cycle*[7].

a. Analisis

Merupakan tahap awal yang melakukan analisa kebutuhan yang diperlukan serta analisa permasalahan yang muncul, analisa keinginan pengguna dan analisa topologi atau analisa jaringan yang telah ada, ada beberapa cara yang dilakukan pada tahapan ini, seperti wawancara, *study literature*, atau dengan membaca *blue print* dokumentasi.

b. Desain

Pada tahap ini, dilakukan perancangan infrastruktur jaringan komputer untuk menghubungkan semua lokasi di area produksi, gudang dan ruang *server* dimana semua peralatan utama perangkat jaringan komputer tersimpan. Pada tahap ini dibuat gambar topologi, estimasi kebutuhan yang ada.

c. Simulasi

Pada tahap ini akan dilakukan pemilihan simulator yang akan digunakan. besar model elemen jaringan, dan memiliki berbagai kemampuan jaringan yang nyata dalam konfigurasi. Ada beberapa simulasi yang memang juga menggunakan cara pengujian langsung.

d. Implementation

Pada tahapan ini akan memakan waktu lebih lama dari tahapan sebelumnya. Dalam implementasi ini akan menerapkan semua yang telah direncanakan dan *designed* sebelumnya. Implementasi merupakan tahapan yang sangat menentukan dari berhasil atau gagalnya *project* yang akan dibangun dan ditahap inilah *Team Work* akan diuji di lapangan untuk menyelesaikan masalah teknis dan non teknis.

e. Monitoring

Setelah implementasi maka tahapan monitoring merupakan tahapan yang penting, agar jaringan komputer dan komunikasi dapat berjalan sesuai dengan keinginan dan tujuan awal dari perancangan.

f. Management

Pada tahap manajemen atau pengaturan, salah satu yang menjadi perhatian khusus adalah masalah *Policy*, kebijakan perlu dibuat oleh pihak terkait untuk membuat atau mengatur agar sistem yang telah dibangun dan berjalan dengan baik perusahaan.

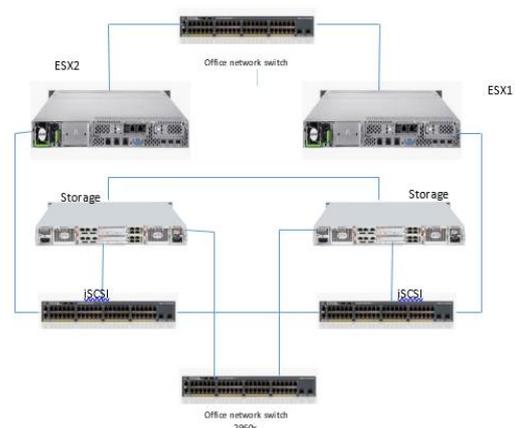
4. HASIL DAN PEMBAHASAN

Dalam tulisan akan banyak membahas menge-

nai perangkat jaringan, perangkat komunikasi teknologi informasi serta penggunaan *virtual* mesin yang mana semuanya akan digunakan dalam *Backup* data.

4.1. Topologi VMware dan Storage

Perencanaan untuk proses *Backup* dan restore dilakukan sebaik mungkin. Perencanaan yang baik meliputi aturan proses *Backup* yang terdiri dari spesifikasi versi, tempat penyimpanan *Backup* serta *procedure* yang dilakukan untuk proses *restore*. Perbedaan prosedur akan terjadi dengan memper timbangkan lokasi penyimpanan, banyaknya data yang di *Backup* serta banyaknya sistem yang terlibat. Secara umum *Backup* bisa dilakukan dengan beberapa cara, baik dengan menggunakan *tape backup*, *harddisk external* atau juga dengan menggunakan *storage* khusus yang dikombinasikan dengan mesin *virtual*. Sebagai tahap awal maka perlu disebutkan konfigurasi dari *storage* yang akan dipakai yaitu type Huawei Hyper Metro cluster dengan spesifikasi Dual-Controller, 128 GB cache, 20x 1.2TB 10k SAS HDDs in RAID6 configuration, 8 TB net capacity serta 2x Cisco C2960X-24TS-L Switches untuk iSCSI network. Sedangkan operasi yang bisa dilakukan meliputi Synchronous mirror antara Storage 1 and 2 (“HyperMetro”), iSCSI Mapping ke ESXi hosts (Multipathing) sehingga terjadi Transparent Failover, dan melakukan sinkronisasi secara transparan. Secara topologi maka bisa digambarkan sebagai berikut :



Gambar 1. Topologi VMware dan Storage

Topologi di atas menggambarkan hubungan antar mesin-mesin virtual esx1 dan esx2 yang tersimpan di ruang *server* berbeda, masing-masing mesin esx akan terhubung ke *storage* melalui *switch* iScsi yang telah di konfigurasi. Setiap *storage* yang ada akan terhubung ke *switch* yang lainnya sebagai *switch management* dengan menggunakan *Vlan2000*.

4.2. Veeam Backup proses

Proses instalasi dimulai dengan memilih *directory* dan file *setup.exe* untuk versi 64bit. Proses instalasi akan membutuhkan *.net.Framework*, pada saat instalasi berlangsung maka secara otomatis *.net* akan diinstal dan harus dipastikan *server* terkoneksi ke internet. Proses instalasi akan dimulai dan dipastikan lisensi untuk veeam sudah tersedia dan bisa digunakan. Setelah instalasi selesai, selanjutnya adalah konfigurasi veeam Backup dan Replikasi. Sistem akan meminta untuk konfigurasi *VMware virtual centre*. Langkah selanjutnya adalah penentuan *Backup Repository*. Setelah selesai maka selanjutnya adalah konfigurasi untuk *simple mail transfer protocol (SMTP)* dan *error message* dengan mengaktifkan “*enable E-mail Notification*” selanjutnya adalah menetapkan *Backup job* dengan menentukan jenis *Backup* yang akan dibuat misalnya dengan menggunakan *Backup incremental* atau *reversed incremental*. Pada proses ini harus ditentukan, waktu terbaik untuk melakukan *Backup* dan penentuan hari serta jam untuk proses *Backup*.

Proses untuk akses ke veeam Backup bisa menggunakan *remote desktop protocol* yaitu dengan mengakses desktop dari jarak jauh dan tanpa masuk langsung ke *server* tersebut. Secara umum untuk proses *Backup* harus ditentukan, misalnya menggunakan *Backup incremental forever*. *Incremental forever Backup* sering digunakan oleh sistem *Backup* dengan disk-ke-disk-ke-tape. Gagasan dasarnya adalah bahwa, seperti cadangan tambahan, cadangan tambahan selamanya dimulai dengan mengambil cadangan penuh dari kumpulan data. Setelah itu, hanya pencadangan inkremental yang dilakukan.



Gambar 2. Login masuk ke Veeam Backup

Proses login ke Veeam Backup bisa dilakukan dengan menggunakan *default user* admin untuk masuk ke *Windows Server*. Untuk proses *Backup* dilakukan dengan cara semua data di VM (*full Backup*) atau juga dengan menggunakan *incremental forever*.

Untuk setiap proses *Backup* yang telah dilakukan akan mendapatkan notifikasi proses

Backup telah selesai dan sukses dan bisa dilakukan lewat email untuk mengirimkan informasi tersebut.

Configuration Backup			
To: Backup Repository 1			
Monday, June 10, 2019 10:00:18 AM			
Start time	10:00:01 AM	Data size	23.9 MB
End time	10:00:18 AM	Backup size	1.8 MB
Duration	0:00:17	Compression	13.45x
Details			
Catalog	Items	Size	Packed
Configuration catalog	160	137.0 KB	16.6 KB
Backups catalog	413	1.6 MB	96.8 KB
Sessions catalog	4754	22.2 MB	1.7 MB
Tape catalog	1	156.0 B	136.0 B

Veeam Backup & Replication 9.5.0.1536

Gambar 3. Backup Configuration jobs

Untuk proses *restore* data maka disarankan dengan menggunakan pilihan *Guest file* hal ini dilakukan untuk menghindari proses *restore* data dengan metode *full Backup*. Apabila *restore full Backup* dilakukan maka akan menghentikan proses mesin *virtual* lainnya dan mengakibatkan mesin *server* tepat penyimpanan data akan terhenti selama proses *restore* berlangsung. Berikutnya adalah menentukan *restore point* dan lokasi penyimpanan data untuk proses *restore*.

4. SIMPULAN

Penentuan infrastruktur jaringan komputer dengan *VMware* dan instalasi *Veeam backup* dan *replication* sangat menentukan keberhasilan proses implementasi manajemen data atau *backup* data perusahaan. Instalasi dan konfigurasi mempunyai peranan sangat penting sehingga target implementasi manajemen *backup* data bisa dicapai sesuai target yang telah ditentukan yaitu mempunyai sistem manajemen *backup* yang akurat, terkendali dan memberikan kepastian jangka panjang untuk perusahaan dalam hal ketersediaan data untuk menunjang kinerja perusahaan dan karyawan.

DAFTAR PUSTAKA

- [1] Elyyani (2012). “*Metode Manajemen Backup Data Sebagai Upaya Penyelamatan Data Online Web Lapan Bandung*”, Berita Dirgantara 13 (1), 22–27.
- [2] William, R S (2009). “*Microsoft SQL server 2005 Administrator’s Pocket consultant*”, Microsoft Press.
- [3] Rizky, S. (2018). “*Disaster Recovery Planning*”, (July). Retrieved from <https://www.researchgate.net/publication/326314137>
- [4] Andry, J., (2018). “*Pengembangan Aplikasi backup dan Restore Secara Otomatisasi menggunakan SDLC untuk mencegah bencana, Sains, Teknologi, dan Ilmu Kesehatan*” Vol. 1 No. 1 (March). 30-38.

- [5] Software, V. (2016). “*Veeam Backup & Replication, user Guide for Vmware Vsphere*”.
- [6] Cervone, H. F. (2017). “*Disaster recovery planning and business continuity for informaticians*”. <https://doi.org/10.1108/DLP-02-2017-0007>
- [7] Setiawan, D. (2009). “*Fundamental Internetworking Development & Design Life Cycle*”. Fasilkom Unsri, (April), 1–13

