

BAB 1 PENDAHULUAN

1.1 Latar Belakang

Pada perkembangan zaman yang kian pesat ini membuat teknologi menjadi salah satu alternatif bagi perusahaan maupun organisasi untuk terus maju dan bersaing menjadi yang terbaik. Segala kemajuan teknologi ini akan berdampak sangat besar terutama bagi organisasi non-profit [1]. Salah satu komponen yang menjamin tersedianya data untuk transaksi yang berbasis Teknologi Informasi beberapa diantaranya yaitu *server*, *database server*, dan *web server*. Mekanisme pemodelan data atau database yang baik, dengan *server* yang baik, dibutuhkan juga sistem yang bisa menjamin keberlangsungan bisnis dengan adanya *server* mempermudah kita mendapatkan informasi dengan cepat dan selalu terbaru.

Dalam teknologi tidak terlepas dari yang namanya bencana, terdapat 4 bencana menurut *Snedaker* pada tahun 2007 Terdapat juga klasifikasi bencana yang dibagi menjadi 4 ancaman, seperti: *Natural / Environmental Threats* (Kebakaran, banjir, dan gempa), *Human-caused Threats* (Pencurian, sabotase, *terrorist*), *Infrastructure Threats* (Permasalahan kelistrikan, *Overheating*, kesalahan penempatan bangunan), *IT-Specific Threats* (*Virus*, *malware*, kegagalan sistem) [2].

Maka dari itu, diperlukan *Disaster Recovery Planning* untuk membantu mencegah dan memulihkan data maupun kepentingan dokumen perusahaan pasca terjadinya bencana, *Disaster Recovery Planning* adalah perencanaan yang dibuat dalam bentuk dokumen fisik atau berbentuk *file* untuk perencanaan pemulihan pasca terjadinya bencana, dikutip dari IBM “*Disaster Recovery Planning* adalah petunjuk terperinci tentang cara menanggapi insiden yang tidak direncanakan. Hal itu misalnya bencana alam, pemadaman listrik, serangan dunia maya, dan insiden lainnya. Petunjuk tersebut berisi strategi untuk meminimalkan efek bencana, sehingga perusahaan dapat terus beroperasi atau segera melanjutkan operasi utama”. [19]. Terdapat pula jenis *Disaster Recovery Planning* (DRP) ada 4 jenis tipe *DRP* yang diketahui secara umum yaitu: *Virtualized disaster recovery plan*, *Network disaster recovery plan*, *Cloud disaster recovery plan*, *Data center disaster recovery plan* [19], Yang akan menjadi fokus dalam proses pemulihan pasca bencana.

Dalam pembuatan dokumen *Disaster Recovery Planning*, diperlukan standard khusus seperti *ISO/IEC 24762 ICT Disaster Recovery Services* untuk menjadi patokan apa saja yang perlu dilakukan pasca terjadinya bencana agar bisnis dapat berjalan dengan normal [13], *Disaster Recovery Planning* pada standardnya menurut *ISO/IEC 24762 ICT Disaster Recovery Services* memiliki 7 tahapan dokumentasi yang perlu dilakukan untuk menunjang keberhasilan *Disaster Recovery Planning* yaitu: Strategi Rencana Pemulihan Bencana, Fasilitas Rencana

Pemulihan Bencana, Rencana Pemulihan Bencana, Fungsional Tim dan Tanggung Jawab, Pengujian, *Training*, Maintenance dan Riwayat Revisi.

Pada tahap “Rencana Pemulihan Bencana” terdapat dokumen *backup* dan *recovery* dimana kedua hal tersebut tidak dapat terpisahkan dari sistem *backup*. Sistem *backup* merupakan proses melakukan *backup* sistem operasi, *file* dan data spesifik yang digunakan oleh sistem. *Backup* merupakan proses duplikasi *file* yang original ke *file* cadangan, *file* ini akan digunakan untuk menggantikan *file* utama yang telah korup, terhapus ataupun hilang, sehingga data aman terjaga [21], Dengan melakukan sistem *backup* semua data penting kita akan tersimpan dengan cara di duplikat agar terhindar dari hilangnya data. Selain itu, data *backup* biasanya disimpan menggunakan flash disk, hard drive, atau *hard disk* untuk mencegah hilangnya data berikut Terdapat juga jenis-jenis sistem *backup* yang umum diketahui yaitu: *Full Backup*, *Incremental Backup*, *Differential Backup* [19].

Salah satu yang menjadi permasalahan dalam merancang suatu sistem *backup* adalah perancangan infrastruktur yang sesuai dengan karakter data atau karakter organisasi. Pada umumnya, untuk organisasi yang besar akan terdiri lebih dari satu *server* yang akan terintegrasi dan *server* itu akan berjalan di sistem operasi yang berbeda-beda sehingga dibutuhkan strategi bagaimana caranya mengintegrasikan data, mengupdate data dengan kondisi sistem operasi yang beragam yang dimana dengan beragam sistem operasi akan memunculkan cara pengolahan data yang berbeda-beda, sehingga harus mempelajarinya setiap kali memiliki *server* baru, yang akan mempersulit pihak pengelola *server*.

Dalam penelitian ini akan dilakukan penerapan sistem *backup* sebagai bagian dari *Disaster Recovery Planning* untuk membantu Organisasi Non-Profit dimana bisa membantu *backup server* secara otomatis dan terjadwal studi kasus yang digunakan adalah Wahana Visi Indonesia. Wahana Visi Indonesia merupakan organisasi kemanusiaan yang hadir untuk membantu pengembangan masyarakat, advokasi dan tanggap bencana yang sudah berdiri dari tahun 1998 [5]. Wahana memiliki banyak *website* dan aplikasi yang digunakan untuk membantu kelangsungan berjalannya organisasi, beberapa contohnya seperti wahanavisi.org yang digunakan untuk *website* utama untuk menampilkan informasi seperti Sponsor Anak, Donasi untuk bencana, menjadi relawan dan masih banyak lagi. Selanjutnya, ada chosen.wahanavisi.org *website* ini digunakan untuk anak yang membutuhkan bantuan dengan mengirimkan nama dan foto dan menunggu seseorang memilih anak tersebut agar anak tersebut mendapatkan donasi.

Saat ini Wahana Visi Indonesia melakukan *Disaster Recovery Planning* yang mengacu pada *Information Technology Infrastructure Library (ITIL)*[3], salah satu wujud menerapkan *Disaster Recovery Planning* adalah dengan memiliki dua kantor yang berbeda antara *Live Server / Production server* yang terdapat di kantor pusat di Bintaro dan *Backup server* yang berada di Wahid Hasyim 33, Jakarta Pusat untuk meminimalisir terjadinya kehilangan data akibat bencana alam maupun *human error*, dengan melakukan *backup* secara berkala dan sinkronisasi antar *server* dengan menggunakan sistem *backup* Veeam dan Veritas. Tetapi, sistem *backup* yang saat ini diterapkan mengalami hambatan terhadap versi *server* yang rendah, sehingga menyebabkan terganggunya keberlangsungan sistem *backup* sebagai salah satu bagian dari *Disaster Recovery Planning*. Selain itu, menggunakan segmen IP yang berbeda-beda untuk melihat transaksi antar jaringan yang terjadi diantara *backup server* dan *live server*, agar bilamana ada transaksi anomali dapat dengan mudah di deteksi.

Untuk menyimpan semua datanya saat ini Wahana Visi Indonesia menggunakan *server* fisik atau *bare metal server* yang jumlahnya terdapat sekitar enam belas *server* yang menggunakan sistem operasi yang beragam, mulai dari windows *server* 2008 hingga 2019 yang terbagi menjadi dua jenis *server* yaitu *production server / live server* dan *server backup* yang dua jenis *server* tersebut disimpan di dua lokasi. Lokasi yang pertama itu berada di Tangerang Selatan dan yang satu lagi berada di Jakarta Pusat, Penempatan *server* yang berjauhan ini digunakan untuk melakukan *Disaster Recovery Plan* mencegah hilangnya data dan meminimalisir kerugian ketika terjadi bencana, terutama pada kota ini sering terjadi banjir, sehingga pencegahan ini bisa menjadi solusi.

Wahana Visi Indonesia saat ini, menggunakan aplikasi untuk sistem *backup* menggunakan Veeam dan Veritas. Berikut sekilas pengenalan mengenai Veeam. “Veeam *Backup & Replication* adalah solusi perlindungan data dan pemulihan bencana yang komprehensif. Dengan Veeam *Backup & Replication*, Anda dapat membuat cadangan tingkat gambar dari mesin virtual, fisik, *cloud* dan memulihkannya. Teknologi yang digunakan dalam produk mengoptimalkan transfer data dan konsumsi sumber daya, yang membantu meminimalkan biaya penyimpanan dan waktu pemulihan jika terjadi bencana” [6].

Selanjutnya, Wahana Visi Indonesia juga menggunakan Veritas. Berikut sekilas penjelasan mengenai Veritas. “Veritas *NetBackup* -- dikenal sebagai Symantec *NetBackup* dari tahun 2005 hingga 2016 -- adalah rangkaian perangkat lunak *backup* dan pemulihan yang dirancang untuk pengguna perusahaan” [7]. Veritas ini kompatibel dengan semua windows *server*, memiliki ukuran aplikasi yang lebih kecil dari veeam, namun Veritas ini memiliki tampilan yang tidak user friendly atau sulit dioperasikan oleh pengelola *server* Wahana Visi

Indonesia. Sampai saat ini, Wahana Visi Indonesia melakukan *backup* dengan cara remote desktop menggunakan aplikasi yaitu Veeam atau Veritas ke masing-masing *server*.

Maka dari itu, Menurut wawancara yang dilakukan bersama Bapak Alexander Suseno selaku *Infrastructure and Cloud Analyst* yang bertanggung jawab untuk mengelola, monitoring dan penanggung jawab *Disaster Recovery Planning* di Wahana Visi Indonesia, “Wahana Visi Indonesia membutuhkan sistem *backup* dengan kriteria: sistem *backup* dapat digunakan oleh sistem operasi 2008 hingga 2019, sistem *backup* otomatis yang dapat dijadwalkan baik perhari, per minggu maupun per bulan, sistem *backup* yang mudah dioperasikan / *user friendly*, *server* dapat di-*image*, dan sistem *backup* menggunakan media jaringan untuk berkomunikasi, tidak menggunakan *hard disk*, *tape*.”. Sistem *backup* pun harus mampu memperbaiki alur proses *backup* mempermudahnya dengan membuat terpusat dan terjadwal, sehingga tidak perlu lagi menggunakan dua aplikasi berbeda dan hanya monitoring *backup* melalui satu *server control* saja.

1.2 Rumusan Masalah

Dari latar belakang yang dijabarkan penulis merumuskan masalah yang terjadi pada Wahana Visi Indonesia yaitu terdapatnya limitasi terhadap versi sistem operasi tertentu pada sistem *backup* yang saat ini digunakan oleh Wahana Visi Indonesia, untuk dapat mendukung multi sistem operasi windows dan multi *server* yang berdampak pada kesulitannya organisasi dalam melakukan *backup* bilamana terjadi bencana.

1.3 Batasan Masalah

Dalam tahap pengembangan sistem informasi ini terdapat pula batasan masalah yang perlu diketahui untuk memfokuskan peneliti pada permasalahan yang dihadapi:

- a. Penelitian dilakukan menggunakan sistem operasi *virtual* atau *VMware* pribadi (atas kesepakatan izin penelitian dengan perusahaan) dikarenakan keterbatasan dalam mengakses informasi.
- b. Penelitian yang dilakukan hanya berfokus kepada divisi atau departemen *IT Enterprise* sebagai pihak pengoprasian *server* dan *IT Ministry* sebagai pihak pengoprasian aplikasi.
- c. Penelitian yang dilakukan berfokus pada proses *backup server* dengan sistem operasi *Windows Server* 2008 hingga 2019.
- d. Penelitian ini hanya berfokus pada implementasi sistem *backup* sebagai salah satu tahapan pada *Disaster Recovery Planning*.
- e. Penelitian ini hanya berfokus pada *Full Backup* dari 3 jenis backup yang dijelaskan yaitu: *Full Backup*, *Incremental Backup* dan *Differential Backup*.

1.4 Tujuan Penelitian

Dari rumusan masalah yang telah dibuat ada pula tujuan untuk melakukan penelitian ini adalah membantu menutupi kekurangan sistem *backup* divisi *IT Enterprise* dengan:

- a. Melakukan implementasi menggunakan aplikasi yang sudah ada di luar dua aplikasi yang sebelumnya digunakan, dengan *backup* yang lebih cepat dan dapat membackup yang mencakup semua versi *server*.
- b. Menetapkan satu sistem *backup* terpusat yang dapat melakukan kontrol ke semua jenis sistem operasi windows *server*.

1.5 Manfaat Penelitian

Dari rumusan masalah yang telah dibuat dapat pula manfaat pada penelitian yang dilakukan yaitu mempermudah Wahana Visi Indonesia untuk melakukan *backup* terpusat sehingga setiap data yang masuk dapat dicadangkan baik di multi *server* maupun multi sistem operasi untuk mencegah hilangnya data akibat bencana maupun perbuatan manusia.

1.6 Metode Pengembangan Sistem

Adapun metode yang digunakan untuk menjadi acuan penelitian ini berhubungan penelitian ini merupakan penelitian deskriptif kualitatif. Jaringan menjadi bagian yang paling penting karena sistem *backup* ini berkomunikasi dengan media jaringan. Berikut merupakan langkah-langkah metode pengembangan *Network Development Life Cycle* (NDLC) [10]:

1. Analisis

Merupakan tahap pertama bertujuan untuk melakukan analisa kebutuhan yang diperlukan serta analisa permasalahan yang muncul, analisa kebutuhan pengguna serta analisa topologi atau analisa jaringan yang sebelumnya diterapkan, terdapat beberapa cara yang digunakan pada tahap ini seperti wawancara, studi literatur, ataupun membaca dokumentasi.

2. Desain

Tahap selanjutnya merupakan tahapan perancangan infrastruktur jaringan komputer untuk menghubungkan semua komputer di lokasi organisasi dan ruang *server* tempat semua peralatan jaringan komputer pada *server* disimpan. Pada tahap ini pembuatan topologi, estimasi kebutuhan yang ada dilakukan.

3. Simulasi

Pada langkah ini, simulator yang akan digunakan dipilih. Ini adalah model NE besar, dan konfigurasinya memiliki kemampuan jaringan yang luas yang ditentukan. Ada beberapa simulasi yang juga menggunakan metode uji langsung. Contoh perangkat lunak pengujian jaringan yaitu *Cisco Packet Tracer*.

4. Implementation

Implementasi merupakan langkah penting dalam menentukan sukses tidaknya suatu proyek yang sedang dibangun, dimana kerjasama tim diuji di lapangan untuk memecahkan masalah teknis dan non teknis.

5. Monitoring

Tahap monitoring dilakukan pasca implementasi merupakan langkah penting untuk memastikan komputer dan jaringan komunikasi berfungsi sesuai keinginan dan tujuan awal proyek.

6. Management

Isu-isu kebijakan sangat penting di tingkat manajemen atau peraturan. Kebijakan harus dikembangkan oleh pihak-pihak yang terlibat untuk membuat atau mengatur sistem yang dibangun dan berjalan dengan baik dalam suatu perusahaan.

1.6 Sistematika Penulisan

Sistematika dalam pembuatan laporan tugas akhir ini terdiri dari 6 bab yang akan dijabarkan sebagai berikut:

1.1 Bab 1 Pendahuluan

Bab ini berisi latar belakang, rumusan masalah, batasan masalah, tujuan dilakukannya penelitian, metodologi yang dilakukan selama penelitian dan sistematika penulisan laporan tugas akhir.

1.2 Bab 2 Analisis Masalah

Bab ini memuat informasi terkait organisasi tempat penulis melakukan penelitian tugas akhir serta analisis masalah yang terdiri dari jangkauan masalah serta kesimpulan yang didapat dari analisis masalah dan dihasilkan solusi yang berisi kebutuhan implementasi aplikasi yang akan diterapkan.

1.3 Bab 3 Spesifikasi Kebutuhan Perangkat Lunak

Bab ini berisi spesifikasi apa saja yang dibutuhkan terkait requirement-requirement dari perusahaan dalam membuat suatu perangkat lunak.

1.4 Bab 4 Perancangan Sistem

Pada bab ini akan menjelaskan perancangan sistem *backup* otomatis yang akan dibangun yang meliputi perancangan *server*, perancangan jenis *backup* dan perancangan *backup*.

1.5 Bab 5 Implementasi Sistem

Bab ini berisi tentang implementasi sistem yang telah dirancang dilihat dari sisi fungsionalitas sistem dan kesesuaian dengan requirement yang telah ditempatkan.

1.6 Bab 6 Pengujian Sistem

Bab ini berisi tentang Pengujian yang telah diimplementasikan pada bab sebelumnya, menguji kesesuaian sistem dengan kebutuhan organisasi.

1.7 Bab 7 Kesimpulan Dan Saran

Bab ini berisi kesimpulan dari hasil perancangan dan pengembangan sistem yang dibuat serta saran untuk pengembangan lebih lanjut.