PEMBANGUNAN BACKUP, REPLIKASI DAN MONITORING SERVER SEBAGAI SOLUSI PENANGGULANGAN BENCANA PADA VIRTUALISASI SERVER DI DINAS KOMUNIKASI DAN INFORMATIKA PROVINSI JAWA BARAT

Ferly Adrianus[1], Angga Setiyadi, M.Kom[2]

[1,2]Teknik Informatika - Universitas Komputer Indonesia
Jl. Dipatiukur 112-114 Bandung
E-mail : ferly.pcrg10@gmail.com[1] , angga.setiyadi@email.unikom.ac.id[2]

ABSTRAK

Dinas komunikasi dan informatika (DISKOMINFO) adalah Instansi pemerintahan yang besar dan memiliki pegawai cukup banyak serta cakupan kerja yang besar, sehingga memiliki data yang besar untuk dikelola dan tentunya harus terorganisir dengan baik. Untuk memenuhi kebutuhan pengelolaan data tersebut, DISKOMINFO membutuhkan komputasi yang besar, dimana ruangan *server* yang sudah penuh dan belum memiliki *backup server* serta belum optimal dalam penggunaan *server* ditambah dengan besarnya biaya yang dikeluarkan untuk perawatan seluruh *server* (*maintenance* dan listrik).

DRC virtualisasi *server* menggunakan *type HOT* dengan *tools* yang digunakan Vmware ESXi 5.5 , Veeam *backup & replication* versi 9 dan *Network Attached Storage (NAS)* dengan sistem operasi FreeNAS 9.10, dimana *backup* dan replikasi menjadi skenario dalam penanggulangan bencanya. Kemudian untuk melihat status *server* dibangun program monitoring *server* dan memberikan notifikasi ketika terdapat *server down*. Beberapa *server* dilakukan konsolidasi kedalam satu fisik *server* serta membangun *backup server* dengan cara melakukan replikasi *server*.

Berdasarkan hasil pengujian yang telah dilakukan, penerapan DRC virtualisasi *server* sangat efektif. Dimana waktu *downtime* hanya 1-3 detik sehingga sistem informasi berjalan dengan stabil pada kondisi *main server* mengalami *down*. Dan juga dapat mengoptimalkan penggunaan *server* dan menekan biaya pembelian atau perawatan *server*. Dengan replikasi dan *restore* dapat melakukan penambahan, perbaikan dan *maintenance server* dengan cepat.

Kata kunci : Virtualisasi, ESXi, Veeam, *Backup* dan Replikasi *server*, *Failover*, *Restore*, FreeNAS, *Network Attached Storage* (NAS), Penanggulangan bencana.

1. PENDAHULUAN

Dinas komunikasi dan informatika (DISKOMINFO) adalah sebuah instansi yang bertanggung jawab atas pengolahan informasi dalam lingkungan pemerintahan Provinsi Jawa Barat. Instansi pemerintahan yang besar dan memiliki pegawai cukup banyak serta cakupan kerja yang besar, sehingga memiliki data yang besar untuk dikelola dan tentunya harus terorganisir dengan baik. Saat ini DISKOMINFO memiliki web *server*, mail *server*, database server,dan aplikasi *server* yang jumlah keseluruhan telah mencapai dua puluh enam server. Dalam jangka waktu satu sampai dua tahun DISKOMINFO dapat melakukan pengadaan *server* baru sebanyak tiga unit untuk memenuhi kebutuhan komputasi. Dengan penambahan *server* tersebut tentunya DISKOMINFO harus mengeluarkan biaya cukup besar dan ruangan *server* semakin tahun semakin penuh serta biaya listrik yang terus meningkat.

Penambahan *server* juga akan mempengaruhi naiknya suhu ruangan *server*. Pendingin ruangan bisa masuk dalam perangkat pengadaan baru untuk menjaga suhu ruangan server tetap dingin. Tentunya menjadi masalah jika setiap melakukan pengadaan *server* baru DISKOMINFO harus mengeluarkan biaya yang sangat besar dan biaya listrik yang terus meningkat. Ruangan untuk menempatkan *server* semakin penuh dan suhu ruangan akan meningkat jika pendingin ruangan tidak dilakukan penambahan. Permasalah lain yang dihadapi DISKOMINFO adalah belum optimalnya penggunaan dari *server*, sehingga penambahan *server* baru merupakan langkah yang tidak efisien dan belum memiliki *disaster recovery center* sebagai upaya untuk memulihkan layanan teknologi informasi jika terjadi bencana. Pada tahun 2016, *server* DISKOMINFO yang pernah *down* diantaranya adalah *server* yang memiliki *hostname* eoffice.jabarprov.go.id, nms.jabarprov.go.id, intranet.jabarprov.go.id dan diperta.jabarprov.go.id dengan rata-rata lama downtime kurang dari tiga jam. *Down server* tersebut melumpuhkan pelayanan yang ada di DISKOMINFO dan menunggu hingga *server* tersebut up kembali untuk melakukan pelayanan.

Untuk mengatasi *down server* dan agar pelayanan bisa tetap berjalan dengan stabil maka dibutuhkan sistem *disaster recovery center*, dimana backup dan replikasi *server* sebagai skenario dari *disaster recovery center*. Tentunya data dan sistem layanan informasi yang terus berjalan merupakan hal yang sangat penting. DISKOMINFO membutuhkan *backup* jika layanan informasi yang berjalan mengalami gangguan atau sebuah bencana yang tidak diduga. Replikasi dibutuhkan ketika sistem yang ada akan di buatkan replika yang akan di gunakan pada lokasi lain ataupun di terapkan pada perangkat baru yang akan menggantikan perangkat lama. Replikasi juga digunakan untuk membuat sebuah sistem replika dari sistem utama sebagai backup jika terjadi bencana pada sistem utama. Replikasi dilakukan agar tidak terjadi perbedaan sistem yang berjalan dengan sistem *backup* dan sistem yang diterapkan pada perangkat yang baru dengan fungsi sama dengan sistem utama.

Untuk mengatasi permasalahan ini, maka pada DISKOMINFO dibutuhkan konsolidasi *server*-server tersebut kedalam sebuah *server* fisik menggunakan virtualisasi. Dengan demikian dapat mengurangi jumlah penggunaan server secara fisik. Dan membangun *Disaster recovery* virtualisasi server sebagai upaya untuk menanggulangi bencana.

Berdasarkan permasalah yang diteliti, maka maksud dari penulisan laporan proposal skripsi ini adalah membangun sistem *disaster recovery* virtualisasi *server* di DISKOMINFO Jawa Barat.

Tujuan dalam penelitian ini adalah :

1. Menjaga kestabilan layanan teknologi informasi yang berjalan pada DISKOMINFO.
2. Meminimalisir waktu *down time* sistem selama bencana berlangsung.
3. Mengoptimalkan penggunaan *server* secara fisik di DISKOMINFO.
4. Meminimalisir biaya pengadaan *server* ,listrik yang digunakan dan tempat ruangan *server*.

2. ISI PENELITIAN

2.1 Backup

Dalam teknologi informasi, cara kerja dari *backup* adalah membuat data cadangan dengan cara menyalin atau membuat arsip data komputer sehingga data tersebut dapat digunakan kembali apabila terjadi kerusakan atau kehilangan. Jadi tujuan *backup* untuk mengembalikan data apabila data hilang, baik karena terhapus atau rusak (*corrup*) dan mengembalikan data ketitik tertentu pada masa lalu.[4]

Backup mengharuskan pengguna menggandakan data, yang akhirnya menghabiskan kapasitas media penyimpanan. Ini mendorong ditemukannya teknologi-teknologi untuk mengefesienkan penyimpanan data *backup*, misalnya deduplikasi dan kompresi. Faktor melakukan *backup* adalah virus, kerusakan hardisk, bencana alam, hilang dan kerusakan lainnya dikarenakan banyak penyebab.[4] Sehingga keuntungan dari backup dapat menggunakan data terakhir yang di backup ketika data utama mengalami kerusakan atau hilang. Hal ini dapat mengurangi kerugian ketihal hal yang tidak dinginkan terjadi pada data penting.

Metode *Backup* yang di kenal dalam dunia it ada 4, yaitu sebagai berikut:

1. *Full backup* :
   Salinan lengkap komputer termasuk data *user* dan sistem operasi itu sendiri
2. *Incremental backup* (*backup* peningkatan)
   Menyalin semua data yang berubah sejak terakhir kali melakukan *full backup* atau *differential backup.* Kelebihannya pada waktu yang lebih singkat, *Backup* lebih cepat dari pada *full backup*, membutuhkan tempat sementara yang lebih kecil daripada yang dibutuhkan oleh *full backup*. Dan kekuranganny awaktu untuk *restore* sangat lama.
3. *Differential backup*
   Sama dengan tipe incremental tapi *archive bit* tidak dihapus setelah *backup*. Ini dilakukan setelah *full backup*, setelah terjadi perubahan data dan waktu *backup* tidak terlalu lama.
4. *Mirroring* (*backup* cermin)
   Sama dengan *full backup*, tetapi data tidak di padatkan atau dimampatkan (dengan *format* .tar, .zip, atau yang lain). Kelebihannya pada metode *backup* yang paling cepat bila dibandingkan dengan metode yang lain karena menyalin data dan *folder* ke media tujuan tanpa melakukan pemadatan. Kekurangannya menyebabkan media penyimpanannya harus cukup besar. [5]

2.2 Replikasi

Replikasi adalah suatu teknik untuk melakukan *copy* dan pendistribusian data dan objek-objek *database* dari satu *database* ke *database* lain dan melaksanakan sinkronisasi antara *database* sehingga konsistensi data dapat terjamin. Dengan menggunakan teknik replikasi ini, data dapat didistribusikan ke lokasi yang berbeda melalui koneksi jaringan lokal maupun internet. Replikasi juga memungkinkan untuk mendukung kinerja aplikasi, penyebaran data fisik sesuai dengan penggunaannya, seperti pemrosesan transaksi *online* dan DSS (*Desiscion Support System*) atau pemrosessan *database* terdistribusi melalui beberapa *server*.[6]

Keuntungan replikasi tergantung dari jenis replikasi tetapi pada umumnya replikasi mendukung ketersediaan data setiap waktu dan dimanapun diperlukan.

Adapun keuntungan lainnya adalah :

1. Memungkinkan beberapa lokasi menyimpan data yang sama. Hal ini sangat berguna pada

saat lokasi-lokasi tersebut membutuhkan data yang sama atau memerlukan *server* yang terpisah dalam pembuatan aplikasi laporan.

2. Aplikasi transaksi *online* terpisah dari aplikasi pembacaan seperti proses analisis *database* secara *online*, data *smarts* atau *data warehouse*.
3. Memungkinkan otonomi yang besar. Pengguna dapat bekerja dengan meng-*copy* data pada saat tidak terkoneksi kemudian melakukan perubahan untuk dibuat database baru pada saat terkoneksi
4. Data dapat ditampilkan seperti layaknya melihat data tersebut dengan menggunakan aplikasi berbasis Web.
5. Meningkatkan kinerja pembacaan.
6. Membawa data mendekati lokasi individu atau kelompok pengguna. Hal ini akan membantu mengurangi masalah karena modifikasi data dan pemrosesan *query* yang dilakukan oleh banyak pengguna karena data dapat didistribusikan melalui jaringan dan data dapat dibagi berdasarkan kebutuhan masing-masing unit atau pengguna.
7. Penggunaan replikasi sebagai bagian dari strategi *standby server*.

Replikasi dapat digunakan apabila sebuah organisasi atau perusahaan didukung oleh *hardware* dan aplikasi *software* dalam sebuah sistem yang terdistribusi. Aplikasi yang berbeda mempunyai kebutuhan yang berbeda untuk otonomi dan konsistensi data. Replikasi diperlukan dalam sistem terdistibusi apabila kondisinya sebagai berikut ini:

1. Mengcopy dan mendistribusikan data dari satu atau lebih lokasi.
2. Mendistribusikan hasil *copy* data berdasarkan jadwal.
3. Mendistribusikan perubahan data ke *server* lain.
4. Memungkinkan beberapa pengguna di beberapa lokasi untuk melakukan perubahan dan kemudian menggabungkan data yang telah dimodifikasi.
5. Membangun aplikasi data yang menggunakan perlengkapan *online* maupun *offline*.
6. Membangun aplikasi Web sehingga pengguna dapat melihat *volume data* yang besar.

Metode Replikasi

1. *Snapshot replication*

Mendistribusikan data yang dapat dilihat pada saat tertentu tanpa melakukan *update*. Biasanya digunakan pada saat memerlukan tampilan data seperti : daftar harga, katalog, data yang digunakan untuk pengambilan keputusan. Data-data ini sifatnya hanya '*read only'*.

Replikasi ini membantu pada saat :

a. data sebagian besar statis dan tidak sering berubah
b. dapat menerima *copy* data yang telah melewati batas waktu yang ditentukan.
c. Datanya sedikit.

2. *Transactional replication*

Memelihara kekonsistenan transaksi yang terjadi.

3. *Merge replication*

Merge replication memungkinkan pengguna bekerja dan merubah data sesuai dengan wewenangnya. Pada saat *server* tidak dikoneksikan ke seluruh lokasi dalam topologi, replikasi merubah ke nilai data yang sama. [6]

2.3 Perbedaan *Backup* dengan Replikasi

Perbedaan *backup* dengan replikasi, secara definisi garis besar *backup* melibatkan pembuatan salinan atau salinan data. Sedangkan replikasi adalah tindakan penyalinan dan kemudian memindahkan data antar situs perusahaan. Hal ini biasanya diukur dalam *Recovery Time Objective* (RTO) atau lamanya waktu pemulihan yang dibutuhkan dan *Recovery Point Objective* (RPO) atau toleransi kehilangan data yang dapat diterima. Secara kebutuhan *backup* membutuhkan perpustakaan *tape* (biasanya VTL melakukan *backup disk-to-disk*) dan beberapa tempat untuk menyimpan kaset arsip ataupun media penyimpanan lainnya. Sedangkan kebutuhan pada replikasi adalah infrastruktur yang identik, segingga membutuhkan biaya tambahan untuk menyediakan infrastruktur yang identik.[7]

Backup berfokus pada kepatuhan dan pemulihan terperinci, seperti memulihkan email pengguna tunggal dari 5 tahun yang lalu. *Backup* biasanya digunakan untuk segala hal di perusahaan, mulai dari *server* produksi kritis hingga *desktop*. *Backup* biasanya bergantung pada *snapshots* yang merupakan salinan kumpulan data yang diambil pada titik yang telah ditentukan sebelumnya. Cara yang relatif murah untuk menghindari kehilangan data. Hanya saja tidak menjamin kelangsungan operasi.

Replikasi berfokus pada pemulihan kelangsungan bisnis kembalinya operasi yang cepat dan mudah setelah terjadi bencana atau kerusakan sistem. Meminimalkan tujuan waktu pemulihan (RTO) adalah poin utama dari replikasi. Replikasi sering digunakan untuk aplikasi *mission-critical* yang harus selalu aktif dan berjalan. Berfokus pada memastikan bahwa aplikasi bisnis dan proses selalu tersedia, bahkan setelah bencana. Tentunya biaya untuk *set up* replikasi mahal, dibutuhkannya kesiapan infrastruktur dan biaya perawatannya.[7]

2.4 *Disaster Recovery Center* (DRC)

Disaster Recovery Center adalah kemampuan infrastruktur untuk melakukan kembali operasi secepatnya pada saat terjadi gangguan yang signifikan seperti bencana besar yang tidak dapat diduga sebelumnya. Contohnya adalah ketika terjadi malapetaka yang menimpa sejumlah perusahaan besar dunia yang bermarkas di *Word 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.

Secara umum DRC berfungsi untuk:

1. Meminimalisasi kerugian finansial dan non finansial dalam menghadapi bencana alam berupa fisik dan informasi data penting bagi perusahaan.
2. Meningkatkan rasa aman dalam hubungan bisnis diantara personel, supplier, investor, dan pelanggan.

Infrastruktur *disaster recovery* mencakup fasilitas *data center*, *wide area network* (WAN) atau telekomunikasi, *local area network* (LAN), *hardware*, dan aplikasi. Dari tiap bagian ini harus menentukan strategi *disaster recovery* yang paling tepat agar dapat memberikan solusi yang efektif dan sesuai dengan kebutuhan perusahaan.[9]

Sesuai dengan peraturan di Indonesia bahwa lokasi DRC memiliki jarak minimum >40 km dari pusat *Data Center* dan berada di luar radius mitigasi bencana (Gunung Berapi, Tsunami, Banjir, dan lain-lain). Lokasi DRC kami juga tidak berada pada jalur patahan geologi, Indek Rawan Becana Rendah di Indonesia, akses jaringan memadai dan mudah diakses.

Type DRC

1. *Cold* DRC

   Cold DRC ini menyediakan sistem yang sama seperti dilokasi *data center* dimana aplikasi dan data akan di *upload* sebelum fasilitas DRC bisa digunakan, namun proses pemindahan dari *data center* ke lokasi DRC akan dilakukan secara manual.
2. *Warm* DRC

   Warm DRC akan menyediakan komputer dengan segala komponennya, aplikasi, *link* komunikasi, serta *backup* data yang paling *update*, dimana *system* tidak otomatis berpindah tetapi masih terdapat proses manual meskipun dilakukan seminimal mungkin.
3. *Hot* DRC

   Hot DRC ini mengatur secepat mungkin operasional bisnis, sistem dengan aplikasi, *link* komunikasi yang sama telah dipasang dan telah tersedia di lokasi DRC. Data secara *continue* di *backup* menggunakan koneksi langsung antara *data center* dan lokasi DRC, dan operasional bisnis akan berjalan pada saat itu juga tanpa harus mematikan sistem di *data center* lama.[9]

2.5 Vmware vSphere / ESXi

VMWare vSphere adalah sebuah *platform* virtualisasi yang digunakan sebagai *platform* virtualisasi berbagai macam piranti khususnya yang terkait dengan piranti *server*. Virtualisasi di sini artinya bahwa sebuah piranti fisik, yang bisa dilihat sebagai bentuk sebuah PC atau yang terkait dengannya, dapat dipecah menjadi beberapa piranti virtual yang masing-masing berdiri sendiri dan mempunyai fungsionalitasnya masing-masing. Tentu saja tidak semua perangkat PC dapat diberikan perlakuan semacam ini. Hanya perangkat-perangkat khusus seperti *server* yang dapat dilakukan perlakukan semacam ini, dengan hasil yang baik. Logo dari VmWare vSphere dapat dilihat pada gambar 2.2 sebagai berikut.



Gambar 2. 2 Logo Vmware vSphere.

Vmware ESXi digunakan untuk membentul *virtual machine* di mana terdapat konfigurasi disk, *file* dan lain-lain yang membentuk menjadi seakan sebuah konfigurasi fisik sebuah *hardware* yang utuh. ESXi dapat diibaratkan sebagai sebuah sistem operasi yang melandasi terbentuknya sebuah *virtual machine* .[11]

2.6 *Veeam Backup and Recovery*

Veeam Backup & Replication dibangun secara spesifik untuk lingkungan virtual perusahaan. *Software* ini diciptakan khusus untuk melakukan proses *backup* dan *recovery virtual machines* (VM), tanpa memperdulikan *platform* virtual apa yang gunakan, sistem operasinya, ataupun jenis penyimpanan (*storage*)nya. Logo *veeam* dapat dilihat pada gambar 2.3 sebagai berikut.



Gambar 2.3 Logo *Aplication* Veeam *Backup* and *Replication*.

Dengan lisensi tunggal dan konsol terpadu, aplikasi ini dapat memproteksi seluruh infrastruktur virtual dengan fungsi-fungsi yang menjadi standar industri. Misalnya *Instant* VM *Recovery*, *granular file* dan *application recovery*, *nearcontinous data protection* (*near* CDP), dan masih banyak lagi.

Tidak peduli menggunakan VMware, HyperV, atau kombinasi keduanya, *Veeam* sudah mendukung rilis *hypervisor* terbaru: VMware vSphere 5.1 dan Windows *Server* 2012 *HyperV*.[13]

2.7 Analisis Masalah

Dalam menganalisis masalah sistem *server* yang berjalan di DISKOMINFO Jawa Barat, dilakukan wawancara dan observasi lansung ke pegawai terkait dan ruangan server. Berdasarkan hasil analisis masalah yang dilakukan, maka dapat disimpulkan beberapa permasalahan pada sistem server di DISKOMINFO Jawa Barat, yaitu :

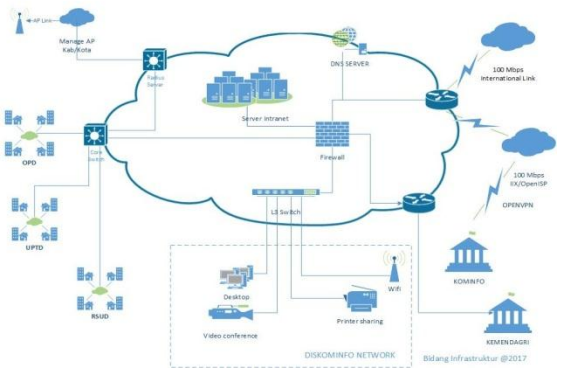
1. DISKOMINFO tidak memiliki *disaster recovery* dalam infrastruktur teknologi informasi dalam

menanggulagi bencana di DISKOMINFO. Sehingga ketika infrastruktur teknlogi informasi mendapatkan bencana maka, pelayanan yang ada tidak dapat berjalan.

2. Bagaimana menerapkan *disaster recovery* pada teknologi virtualisasi dengan *backup*, replikasi di DISKOMINFO. Langkah ini diambil untuk melakukan konsolidasis *server*, dengan menerapkan virtualisasi *server* dapat menghemat jumlah *server* yang digunakan secara fisik. Dengan melakukan *backup* dan replikasi memberikan kemudahan dalam menanggulangi bencana dan dalam penambahan sistem yang sama.
3. Belum maksimalnya penggunan dari server yang dimiliki oleh DISKOMINFO. Dari seluruh server yang ada, penggunaan *server* belum optimal, dilihat dari persentase penggunaan memory dan prosessor masih dibawah 40%. Hanya beberapa *server* saja yang mencapai diatas persentase 40% seperti *server* aplikasi pada waktu tertentu.
4. Besarnya biaya yang di keluarkan DISKOMINFO untuk pengadaan *server* dan infrastruktur pendukung pada setiap tahunnya. Dalam satu tahun DISKOMINFO dapat melakukan penambahan *server* sebanyak tiga unit *server*. Tentunya untuk pengadaan tiga unit *server* mengeluarkan biaya yang besar dan juga penambahan biaya listrik.

2.8 Analisis Topologi Jaringan DISKOMINFO

Adapun topologi jaringan yang tersedia pada DISKOMINFO saat ini adalah seperti pada gambar 3.3. *Server* yang terdapat di DISKOMINFO diakses oleh instansi pemerintahan yang berada di Jawa Barat seperti: RSUD, KEMENDAGRI, OPD, UPTD dan juga dari *link* internasional. *Client* yang akan terhubung ke *server* DISKOMINFO melalui *core switch*, DNS *server* DISKOMINFO dan *firewall*. Tentunya *server* tersebut juga memiliki layanan publik yang akan di akses oleh masyarakat umum.

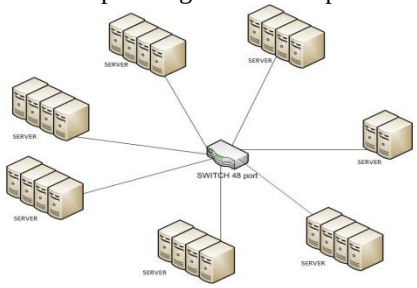


Gambar 2.4Topologi *logic network* DISKOMINFO.

Server yang terdapat pada DISKOMINFO dapat di akses dari berbagai tempat. Pada gambar 3.3 terdapat dua puluh enam *server* yang terdapat di DISKOMINFO di akses oleh banyak instansi pemerintahan seperti KEMENDAGRI, cabang DISKOMINFO, RSUD, UPTD,OPD dan Manage AP Kab/Kota serta *link* internasional. *Desktop, wifi* dan *video conference* yang terdapat pada DISKOMINFO dapat mengakses *server* dengan melewati *core switch* dan *firewall*.

2.9 Analisis Topologi Jaringan *Server* DISKOMINFO

Pada gambar 2.5 adalah topologi jaringan *server* yang tersedia saat ini di DISKOMINFO. Terdapat dua puluh enam *server* detail *server* .Pada topologi jaringan *server* ini tidak terdapat *server backup*. Sehingga ketika bencana terjadi dapat mengakibatkan pelayanan DISKOMINFO terganggu dan terhenti sampai dengan *server* di perbaiki.

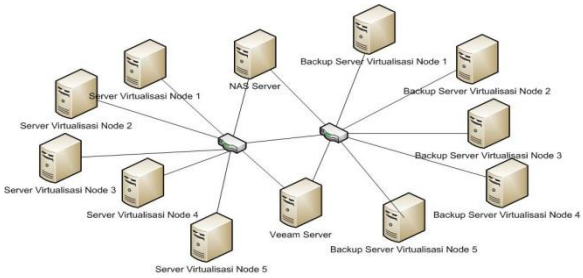


Gambar 2.5 Topologi jaringan *server* DISKOMINFO.

Topologi yang digunakan dalam jaringan *server* DISKOMINFO adalah topologi *star*. Untuk bisa saling komunikasi *server* hanya menggunakan satu jalur.

2.10 Topologi Jaringan Yang Akan Dibangun

Berikut ini adalah perancangan topologi jaringan virtualisasi *server* yang akan di bangun, dapat dilihat pada gambar 2.6. Dengan mempertahankan infrastruktur jaringan yang ada, namun perangkat *server* yang digunakan hanya menggunakan lima *server*, dimana *server* lainnya di konsolidasikan ke dalam satu fisik *server* menggunakan teknologi virtualisasi. Dalam satu fisik *server* terdapat lima hingga enam *server* yang dikonsolidasikan. Banyaknya *server* yang dapat dikonsolidasikan dalam satu fisik *server* bergantung pada spesifikasi fisik *server* dan beban tugas yang diemban dari *server*.



Gambar 2.6 Topologi Jaringan *Server* Yang Diusulkan.

Topologi yang di gunakan tetap menggunakan topologi *star*. Lima *server* digunakan

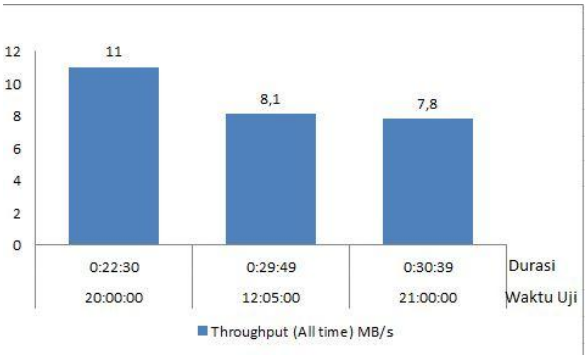
sebagai main *server* virtualisasi dan lima *server* lainnya sebagai *backup server* virtualisasi. Satu *server* sebagai *server* NAS untuk media penyimpanan data *backup* virtualisasi *server* dan satu *server* sebagai *server* yang bertugas mengatur proses *backup*, *replikasi*, *failover* dan monitoring *server*. Sehingga jumlah *server* yang digunakan adalah dua belas unit *server*. Jumlah *server* yang digunakan berkurang dari dua puluh enam *server* dan menghemat jumlah *server* sebanyak empat belas *server*. Dimana empat belas *server* yang lainnya dapat digunakan untuk kebutuhan lainnya.

2.11 Pengujian Backup Virtualisasi *Server*

Pada pengujian *backup* dilakukan dengan dua metoda yaitu *full backup* dan incremental *backup*. Pengamatan pengujian ini dilakukan sebanyak tiga kali pada waktu dan hari yang berbeda, dimana ukuran VM 100 GB . Hasil pengujian *backup* dengan metoda *full backup* dapat dilihat pada tabel 2.1 berikut.

Tabel 2.1 Pengujian *Full Backup*.

Pengujian ke-	Waktu Uji	Durasi	Throughput (All time) MB/s	Status
1	20:00 WIB	0:22:30	11.0	Sukses
2	12:05 WIB	0:29:49	8.1	Sukses
3	21:00 WIB	0:30:39	7.8	Sukses



Gambar 2.7 Statistik Pengujian *Full Backup*.

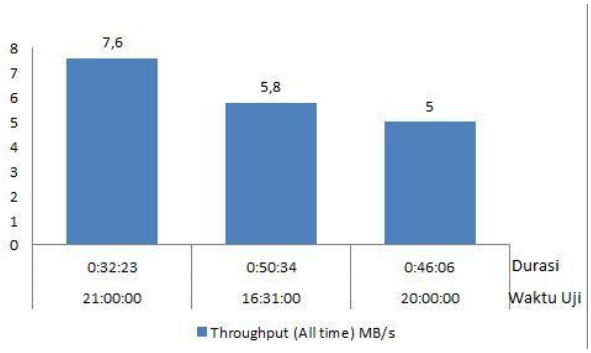
Berdasarkan hasil pengujian yang telah dilakukan, terlihat bahwa semakin besar *throughput* maka durasi dalam melakukan *backup* semakin cepat. *Full backup* dapat diselesaikan dengan rata-rata durasi 27 menit.

2.12 Pengujian Replikasi Virtualisasi *Server*

Pada pengujian replikasi dilakukan dengan dua metoda yaitu *full* replikasi dan *incremental* replikasi. Pengamatan pengujian ini dilakukan sebanyak tiga kali pada waktu dan hari yang berbeda, dimana ukuran VM 100 GB . Hasil pengujian replikasi dengan metoda *full* replikasi dapat dilihat pada tabel 2.2 berikut.

Tabel 2.2 Pengujian *Full* Replikasi.

Pengujian ke-	Waktu Uji	Durasi	Throughput (All time) MB/s	Status
1	21:00 WIB	0:32:23	7.6	Sukses
2	16:31 WIB	0:50:34	5.8	Sukses
3	20:00 WIB	0:46:06	5	Sukses



Gambar 2.8 Statistik *Full* Replikasi.

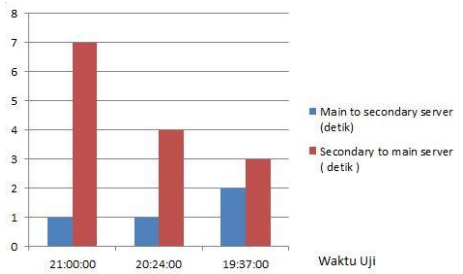
Dapat disimpulkan durasi rat-rata dalam melakukan *full* replikasi 43 menit. Durasi waktu yang lebih lama dibandingkan dengan *full backup* dimana memiliki selisih durasi rata-rata 16 menit.

2.13 Pengujian *Failover* Virtualisasi *Server*

Pengujian *failover* dilakukan sebanyak tiga kali, dimana untuk pengujian ini dilakukan pengamatan waktu *down* ketika *main server down* hingga di *take over* oleh *secondary server* dan waktu *down* ketika perpindahan dari *secondary server* ke *main server* ketika sudah *up* kembali. Hasil pengamatan yang telah dilakukan dapat dilihat pada tabel 2.3 berikut.

Tabel 2.3 Pengujian *Failover*.

Pengujian ke-	Waktu (WIB)	*Down Time*		Status Pengujian
		Main to secondary server (detik)	*Secondary to main server* (detik)	
1	21:00	1	7	Sukses
2	20:24	1	4	Sukses
3	19:37	2	3	Sukses



Gambar 2.9 Statistik Pengujian *Failover*.

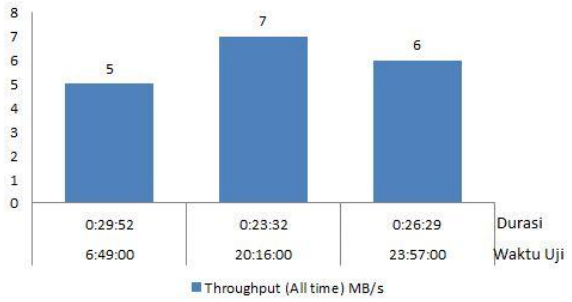
Pada pengujian *failover*, *down time* rata-rata ketika *main server* mengalami *down* dan di *take over secondary server* diperoleh 1,3 detik. Dan ketika peralihan kembali dari *secondary* ke *main server* diperoleh 4.6 detik.

2.14 Pengujian *Restore* Virtualisasi *Server*

Pengujian *restore* VM dilakukan sebanyak tiga kali, dimana pengujian dilakukan pada waktu dan hari yang berbeda dengan VM yang sama. Hasil pengujian *restore* dapat dilihat pada tabel 2.4 berikut.

Tabel 2.4 Pengujian *Restore*.

Pengujian ke-	**Waktu Uji (WIB)**	**Durasi**	***Throughput* (*All time*) MB/s**	**Status**
1	6:49	0:29:52	5	Sukses
2	20:16	0:23:32	7	Sukses
3	23:57	0:26:29	6	Sukses



Gambar 2.10 Statistik Pengujian *Restore*.

Pada pengujian *restore*, dari waktu yang berbeda diperoleh durasi *restor* 26 menit dengan rata-rata throughput 6 MB/s dimana besarnya data *restor full* VM 100 GB

2.15 Pengujian Monitoring Virtualisasi *Server*

Perangkat lunak yang dibangun untuk melakukan monitoring *server* berbasis web. Sehingga diperlukan pengujian terhadap perangkat lunak. Pengujian perangkat lunak merupakan tahapan untuk menemukan kesalahan dan kekurangan pada perangkat lunak yang dibangun sehingga bisa diketahui apakah perangkat lunak tersebut telah memenuhi kriteria sesuai dengan tujuan atau tidak. Adapun metode pengujian yang digunakan pada perangkat lunak ini adalah metode pengujian *Black box*. Pengujian *Black box* berfokus pada persyaratan fungsional perangkat lunak. Metode pengujian *black box* ini terdiri dari dua tahapan pengujian, yaitu tahapan pengujian alpha dan tahapan pengujian beta.

Berdasarkan hasil pengujian dilakukan maka dapat disimpulkan bahwa monitoring *server* yang dibangun sudah berjalan sesuai dengan yang diharapkan baik itu dari segi validasi maupun proses penanganan kesalahan. Adapun kesimpulan yang didapatkan dari hasil wawancara pada tahap pengujian beta, bahwa penelitian yang dilakukan saat ini sangat dibutuhkan DISKOMINFO, dengan menerapkan virtualisasi satu fisik *server* dapat menangani beberapa *server* aplikasi yang berjalan di DISKOMINFO nantinya. Pengoptimalan penggunaan *server* dapat dicapai, mudah dalam melakukan *maintenance* dan *replacement server* serta efisiensi dari sumber daya baik dari segi penggunaan listrik dan server secara fisik dapat ditekan atau diminimalisir. Monitoring *server* yang dibangun memberikan kemudahan dalam melakukan monitoring status *server* dan mudah dalam penggunaannya.

3. PENUTUP

Dari hasil analisis dan implementasi yang dilakukan, dapat diambil beberapa kesimpulan yaitu :

1. Rancangan sistem penanggulangan bencana dengan solusi *backup*, replikasi dan *failover* pada virtualisasi *server* ini berhasil dilakukan. File *backup* sistem dapat di *restore* dan menggantikan file sistem yang rusak, serta hasil replikasi *server* yang dilakukan persis sama dengan dengan main *server*. Pada pengujian sistem ini mampu memperoleh waktu *downtime* dengan nilai 1-3 detik pada saat terjadi proses *failover* dari *main* ke *secondary server*.
2. Rancangan sistem penanggulangan bencana pada teknologi virtualisasi *server* mampu menjaga kestabilan layanan teknologi informasi yang berjalan di DISKOMINFO pada saat main *server down*.
3. Dengan di implementasikannya teknologi virtualisasi server, penggunaan *server* secara fisik dapat dioptimalkan.
4. Biaya yang dikeluarkan untuk kebutuhan teknologi informasi dapat diminimalisir.

Menyadari bahwa penyelesaian tugas akhir ini masih jauh dari sempurna, untuk itu diharapkan dapat menjadi bahan atau salah satu referensi bagi pembaca lainnya agar dapat terciptanya sistem

penanggulangan bencana pada virtualisasi server yang lebih baik. Beberapa saran yang dapat dilakukan untuk pengembangan tugas akhir ini, antara lain :

1. Menambah node server ESXi dan untuk *manage node* - *node* ESXi tersebuat dapat gunakan Vmware Vcenter.
2. Menambahkan *mirror server* NAS untuk *recovery* data jika terjadi bencana pada NAS.
3. Dapat menerapkan VMFS *volume* atau Fibre *channel* dan NFS dalam menambahkan *datastore* ESXi *server*.
4. Dapat menggunakan tool lainnya pada saat skenario *backup* dan replikasi pada virtualisasi *server* seperti NAKIVO *backup* dan replikasi.

DAFTAR PUSTAKA

[1] Novi. (2015, Mei) prezi.com. [Online]. https://prezi.com/4ewtum1s9xjp/logo-adalah-suatu-identitas-yang-dipergunakan-untuk-menggamb/

[2] Sartika Wulandari. id.scribd.com. [Online]. https://id.scribd.com/doc/220441465/Visi

[3] Handoko Reksohadiprodjo, "Struktur Organisasi," p. 74, 1992.

[4] Tiwo Satriatama, "Pengertian, Tujuan, Fungsi, Kriteria dan Pentingnya Backup Data ," November 2015.

[5] Dony Donker. scribd. [Online]. https://id.scribd.com/document/28184829/Kinerja-Windows

[6] TSI Perbankan. elearning.gunadarma.ac.id. [Online].learning.gunadarma.ac.id/docmodul/AS400/./04Replikasirev.pdf

[7] Chris Mellor. (2012, february) Zerto. [Online]. http://www.zerto.com/blog/replication/backup-and-replication-what-is-the-difference/

[8] Muhammad Dzulkarnaen, "Implementasi Layanan Jaringan," Telkom University, Bandung, April 2016.

[9] Nugroho P Yudho, Robby Hasan P Farid Ridho, "Disaster Recovery Center and Disaster Recovery Plan ," November 2012.

[10] Adian Fatchur Rochim, Kodrat Iman Satoto Krisnawan Hartanto, "Implementasi Virtual Private Server Menggunakan Xen Hypervisor," Universitas Diponegoro, Semarang, 2011.

[11] Ibnu Febry Kurniawan Rachmad Aziz, "Implementasi Teknologi Awan untuk Layanan Infrastruktur," Universitas Negeri Surabaya, Surabaya, 2016.

[12] Gilby Benaya Lesar, "PERANCANGAN DAN PEMBANGUNAN NETWORK ATTACHED STORAGE UNTUK DATA CENTER AKADEMIK SEKOLAH DASAR," Universitas Komputer Indonesia, Maret 2015.

[13] PT.mandawanimandiri. mandawani.com. [Online]. http://www.mandawani.com/id/solusi/backup-recovery.html

[14] Ahmad Paudji Hendra Suputra, "Perancangan dan Implementasi Jaringan Small Office Home Office Berbasis Network Attached Storage," Universitas Komputer Indonesia, Bandung, 2015.

[15] Melwin Syafrizal, Pengantar Jaringan Komputer, Dwi Prabantini, Ed. Yogyakarta: Penerbit Andi, 2005.

[16] Mulia Rizqina, "Bandwitd Monitor," Universitas Islam Negeri Sunan Kalijaga, Yogyakarta, 2012.

[17] Afwan Bahtiar, "Monitoring Jaringan dengan PRTG Traffic Grapher," Universitas Diponegoro, Semarang, 2009.

[18] Ceppy Efraim, Sandy Hermawan Sidik Nurcahyo, "Pembangunan Website di CV.Surya Mitra Buana," Universitas Komputer Indonesia, Bandung, 2016