Riset dan E-Jurnal Manajemen Informatika Komputer
Volume 5, Number 2, April 2021
http://doi.org/10.33395/remik.v4i1.10916
e-ISSN : 2541-1330
p-ISSN : 2541-1332

Disaster Recovery Centre Menggunakan Hot Standby System Pada BPR Universal

[1]Andi Rosano, [2]Nur Ali Farabi
Universitas Bina Sarana Informatika
Jakarta, Indonesia
andi.aox@bsi.ac.id

Abstract— Kehidupan manusia pada saat ini tak bisa dilepaskan dari perkembangan teknologi informasi (TI), dimana manusia sudah sangat tergantung kepadanya. Bukan hanya individu manusia namun juga perusahaan, instansi pemerintah, institusi pendidikan pun juga sangat tergantung pada teknologi informasi. Pemanfaatan TI untuk kegiatan usaha keuangan, khususnya perbankan, sudah merupakan keharusan, baik operasional maupun layanan masyarakat dan promosi. Kegiatan bisnis BPR Universal yang mengandalkan TI sebagai sarana untuk meningkatan keuntungan dan kinerja tentulah menuntut tingkat ketersediaan sistem yang tinggi. Sistem dengan availabilitas tinggi sangat penting dimiliki. Oleh karena itu diperlukan sebuah perencanaan untuk mengatasi masalah jika terjadi gangguan pada infrastruktur TI, *server*, aplikasi dan data. Untuk mengatasi masalah yang timbul setiap saat dan akan menimbulkan *down time* yang lama pada sistem *data centre*, maka diperlukan sebuah *disaster recovery centre*. Banyak cara atau metode yang dapat digunakan, namun pada tulisan ini akan dibahas penggunaan metode *Hot standby* untuk menanggulangi kegagalan sistem akibat bencana. Sistem *hot standby* mengaktifkan semua infrastruktur TI *data centre* utama dan *data centre* cadangan, sehingga ketika terjadi masalah secara otomatis *data centre* cadangan akan langsung aktif untuk mengganti peran dari *data centre* utama dalam operasional.

Keywords—*backup, data enter, hot standby, down time,* availabilitas

I. PENDAHULUAN

Saat ini teknologi informasi (TI) berkembang sangat pesat, dan penggunaan TI telah masuk kedalam kehidupan setiap saat pada manusia modern. Banyak organisasi, instansi pemerintah, perusahaan, lembaga penelitian dan institusi pendidikan telah menjadikan TI sebagai komponen utama untuk meningkatkan pelayanan, kinerja, keuntungan, dan penghematan biaya operasional. Seperti halnya teknologi lain, suatu saat pasti akan mengalami kendala, seperti kemungkinan rusak, hilang atau tidak berfungsi sistem karena kesalahan manusia ataupun akibat bencana alam (Muhaemin, M., 2018).

Bencana pada TI bukan hanya disebabkan oleh kejadian alam (gunung meletus, banjir, gempa bumi, kebakaran hutan, dll). Tetapi bisa juga berupa serangan *hacker* pada *server* dan aplikasi, atau hilangnya data oleh virus juga merupakan bencana besar pada TI. Bencana tidak dapat dihindari namun kita bisa mengurangi kerugian akibat dari bencana tersebut. Karena bencana adalah suatu kejadian yang waktu terjadinya tidak dapat diprediksi, sifatnya merusak sekali, dan frekuensi terjadinya tidak menentu (Muhaemin, M., 2018).

Pada saat ini BPR Universal Tangerang belum memiliki sistem *Disaster Recovery Centre (DRC)*, yang ada hanya duplikat data hasil backup yang dilakukan setiap proses akhir hari bank. Sehingga apabila terjadi suatu bencana, baik karena faktor alam atau tindakan manusia, maka sistem TI BPR Universal akan mengalami gangguan operasional. Sistem dapat dilakukan pemulihan, namun memerlukan waktu lama dan pasti akan mengganggu operasional bank, yaitu pelayanan nasabah menjadi *offline* atau manual. Bank bisa terancam oleh resiko reputasi. Salah satu penyebab yang sering terjadi dan merusakkan data sistem TI pada

BPR Universal adalah putusnya sumber listrik dari PLN secara mendadak yang mengakibatkan sistem informasi bank dan layanan nasabah tidak bisa berfungsi. Selain hal itu sistem TI BPR Universal juga rawan dengan kebanjiran karena lokasi server berada di lantai bawah.

BPR Universal merupakan salah satu lembaga keuangan yang dituntut untuk bisa memberikan layanan keuangan prima, dan menjaga kepercayaan nasabahnya dengan dukungan layanan TI yang handal. Sehingga apabila terjadi gangguan operasional baik karena bencana alam, karena manusia, atau faktor teknis (listik mati, data komunikasi putus, atau jaringan *internet* tidak tersedia) maka layanan perbankan masih dapat diberikan dengan baik. Diharapkan pada saat sistem TI terganggu, maka sistem *DRC* akan menggantikan tugas *DCU (data centre* utama), untuk menyediakan semua layanan sisem keuangan bank dan memastikan bahwa pemulihan dapat dilakukan dengan secepatnya.

Disaster Recovery Centre (DRC) BPR Universal akan dibangun bekerjasama operasional dengan sebuah *Internet Service Provider (ISP)* penyedia jasa dan operasi *DRC*. *Data centre* utama terdapat di Kantor Pusat BPR Universal sedangkan *DRC* berada di lokasi yang berbeda namun masih dalam satu blok perkantoran. Pada artkel ini akan dibahas penerapan penggunaan *DRC* pemulihan ketika terjadi gangguan. Banyak metode yang bisa di implementasikan untuk *DRC*, namun metode yang akan digunakan BPR Universal adalah metode yang cukup sederhana dan sesuai dengan *budget* perusahaan yaitu model *Hot Standby DRC.*

II. TINJAUAN PUSTAKA

Untuk meminimalkan dampak dari suatu bencana pada sistem TI, diperlukan suatu manajemen dan tata kelola TI yang saling terkait, yaitu *Disaster Recovery Planning (DRP), Business Continuity Plan (BCP) dan Disaster Recovery Centre (DRC).*

2.1. Pengertian *DRP (Data Recovery Plan*

DRP (Disaster Recovery Plan) adalah kebijakan dan prosedur yang berupa persiapan pemulihan atau keberlangsungan operasional infrastruktur teknologi yang krusial bagi organisasi setelah terjadinya bencana, baik bencana yang disebabkan oleh tindakan manusia ataupun bencana alam (Rachmaningrum dan Falahah, 2011). Penerapan *DRP* pada sistem TI sangat diutamakan guna memperbaiki dan mempertahankan operabilitas dan availabilitas sistem, aplikasi dan semua fasilitas TI yang berada di lokasi berbeda (*data centre* cadangan). Di lain pihak *DRP* tidak boleh abai pada faktor rasional, *cost-effective, prevention* (pencegahan), *preparation* (persiapan) dan *recovery* (pemulihan).

2.2. Pengertian *BCP (Business Continuity Plan)*

BCP (Business Continuity Plan) adalah sekumpulan proses otomatis ataupun manual yang dirancang untuk mengurangi dampak terhadap fungsi-fungsi penting organisasi, sehingga menjamin keberlangsungan layanan operasional yang penting (Muhaemin, 2018). Namun demikian penerapan *BCP* di perusahaan haruslah memperhatikan isu terkini, situasi dan kondisi lingkungan perusahaan, juga tingkat kondisi pengetahuan dan pemahaman manajemen terhadap proses keberlanjutan bisnis (Amanda dan Supriadi, 2014). *BCP* dibuat untuk meminimalkan semua resiko yang bisa menimbulkan gangguan terhadap operasional sistem TI dan menekan kerugian keuangan serta meningkatkan kemampuan organisasi dalam pemulihan akibat bencana.

2.3. Pengertian *DRC (Disaster Recovery Center)*

Tidak seperti *DRP* dan *BCP* dimana hasil akhirnya adalah berupa dokumen-dokumen yang terkait dengan aturan dan langkah-langkah untuk meminimalkan dampak dari bencana pada sistem TI, *DRC* merupakan fasilitas cadangan ketika *DCU* (*data centre* utama) tidak dapat berfungsi akibat oleh suatu kejadian bencana, yang difungsikan untuk sementara waktu dalam rentang waktu saat proses pemulihan *DCU*, untuk menjaga keberlanjutan bisnis.

Pada implementasi suatu *DRC* haruslah terpenuhi kriteria : *availability, scalability, flexibility* dan *security*. *DRC* dimaksudkan sebagai tempat atau area penyimpanan serta pemrosesan data dan informasi pada saat kejadian bencana yang mengakibatkan *DCU* yang ada mengalami gangguan sementara, sebagian, atau rusak total sehingga memerlukan waktu dalam melakukan pemulihan (Budiman, K., et.al. 2019). Selain hal tersebut suatu *DRC* harus mampu menyesuaikan pertambahan data maupun perkembangan aplikasi tanpa harus melalukan perubahan yang signifikan. Disini faktor keamanan adalah faktor yang sangat penting, mengingat data merupakan adalah aset yang tak ternilai harganya bagi suatu organisasi.

2.4. Pengertian *Hot Standby System*

Hot Standby System adalah metode sistem *backup* siaga yang redundan di mana satu sistem berjalan secara bersamaan dengan sistem utama yang identik. Pada saat terjadi kegagalan sistem utama, sistem *backup* siaga ini segera mengambil alih peran menggantikan sistem utama. Adapun data dan perubahan data selalu dicerminkan secara *real time*. Dengan demikian, kedua sistem tersebut memiliki data yang identik (sama) dan terkini. Agar sistem ini bekerja dengan sempurna maka sarana komunikasi data harus selalu tersedia setiap saat, karena sinkronisasi data antara mesin *backup* dan mesin utama berlangsung terus menerus (Jia, Heping, 2018).

2.5. Regulasi Persyaratan *Data Center*

Perancangan dan lokasi suatu *data centre* utama harus memenuhi standar teknis. Peraturan Menteri

Komunikasi dan Informatika tahun 2013 tentang Pedoman Teknis Rancangan Pusat Data menyebutkan persyaratan teknis yaitu : Lokasi harus berada di tempat yang aman berdasarkan dari kajian Indeks Rawan Bencana Indonesia, Bangunan harus mempunyai akses jalan yang cukup dan fasilitas parkir, Lokasi sebaiknya berada di kawasan yang memiliki temperatur rendah dan kelembaban tinggi.

Sedangkan persyaratan arsitektur dan bangunan ruang komputer tidak berada di bawah area perpipaan, seperti kamar mandi, toilet, dapur, laboratorium dan ruang mekanik, jendela yang terkena secara langsung sinar matahari dan harus tertutup untuk mencegah paparan panas. Untuk akses kontrol dan keamanan *data centre* utama harus dilakukan pengamanan selama 24 jam penuh dan paling sedikit satu orang petugas keamanan per shift, yang dilengkapi sistem pemantau visual *(CCTV)*. Sedangkan akses ke dalam ruang komputer harus menggunakan mekanisme otentikasi. Ruang *data centre* utama harus dilengkapi dengan sensor peringatan kebakaran, deteksi asap dan pemadam kebakaran *(Fire Precautions, Smoke Detection and Fire Suppression)*. Ruang *data centre* harus di lengkapi dangan sumber listrik utama dan cadangan, antara lain *UPS (Uninterruptible Power Supply)* dan Genset, mesin pendinginan ruang *CPU* dan ventilasi. Memiliki sistem pengkabelan dan manajemen kabel yang baik. Sistem manajemen bangunan dan pemantauan keamanan yang lengkap.

Sedangkan Peraturan Menteri Komunikasi dan Informatika tahun 2013 tentang Pedoman Teknis Rancangan Pusat Data memberikan syarat untuk keberlangsungan operasional pada *DRC (Disaster Recovery Centre)* yaitu harus berjarak terhadap lokasi data centre utama yang meminimalkan resiko, biaya yang layak dan memenuhi *Service Level Agreement (SLA)* yang disyaratkan.

III. METODE BACKUP HOT STANDBY

Pada sebuah *DCU* terdapat perangkat keras antara lain meliputi *Server, Router, Switch* dan *Storage*. Gambar 1 menunjukkan topologi *DCU* BPR Universal saat ini. Sedangkan *DRC* direncanakan memiliki perangkat keras yang hampir sama dengan *DCU*, hanya berbeda pada kapasitas saja dimana ukuran lebih kecil namun memiliki unjuk kerja yang sama. Hal ini mengingat keterbatasan ruang pada ruangan *DRC* yang lebih kecil. Ruang *DRC* menggunakan suatu ruangan pada gedung berbeda namun satu blok dengan *DCU*. Gambar 2 menunjukkan topologi jaringan usulan *DRC* yang akan diimplementasikan untuk sistem bank.

Tabel 1 menjelaskan spesifikasi perangkat keras dan perangkat lunak yang digunakan *DRC* BPR Universal. Perangkat keras untuk *DRC* ini harus disesuaikan dengan kebutuhan aplikasi dan penyimpanan data operasional. Semakin tinggi spesifikasi perangkat keras akan semakin baik. Walaupun rencana *DRC* BPR Universal hanya terdiri dari 1 buah *server* dan 1 buah *server storage*, diperhitungkan cukup untuk memenuhi kebutuhan operasional bank.

Pemasangan instalasi *DRC* bertujuan untuk meminimalkan dampak yang timbul oleh bencana yang mungkin terjadi, dan ini merupakan salah satu unsur penting dalam sebuah sistem TI. Ada banyak metode *backup data* yang dapat diterapkan pada implementasi *DRC* antar *server* utama dengan *server* cadangan. Pada tulisan ini akan dibahas penggunaan metode *backup data* dengan *snapshots*. Semua data yang tersimpan pada sistem *DCU* akan disalin sama persis ke sistem *DRC*. *Backup data snapshots* digunakan pada *server storage* sedangkan *backup data differensial* digunakan pada *server cloud*. Cara kerja *backup data snapshot* yaitu data digandakan ketika sistem sedang beroperasi dengan cara melakukan penguncian seluruh data sementara waktu, dan kemudian dilakukan *snapshot* pada seluruh data kemudian dilanjutkan dengan melepas kembali penguncian setelahnya, agar sistem dapat beroperasi kembali (Afif dan Suryono, 2013). *Differential backup* bekerja dengan cara data yang digandakan hanya data baru atau data yang mengalami perubahan. Pada proses *backup* ini, data tidak pernah dilakukan *marking* (Afif dan Suryono, 2013).

Differential backup adalah metode yang sangat cocok bila diterapkan pada komputasi awan *(cloud computing*), terutama sistem yang terdapat banyak aplikasi dan data yang setiap saat mengalami perubahan dan penambahan, misalnya sebuah bank. Metode ini biasa disebut sebagai replikasi *master to slave synchronous*. Replikasi *master to slave synchronous* adalah sebuah cara penggandaan data yang pada proses replikasi akan terjadi saat suatu transaksi/proses penulisan data pada master selesai dilakukan (Suryana, 2014).

Pada implementasi *DRC (Disaster Recovery Centre)* ada tiga metode yang dapat digunakan, yaitu *Warm Standby, Hot Standby, dan cold standby*. *Hot standby* adalah suatu metode dimana sistem *DRC* dihasilkan dari penggandaan data sistem *DCU*, sehingga semua perangkat lunak dan data pada *DRC* sama persis dengan yang ada di *DCU*. Ketika terjadi masalah pada *DCU* maka secara otomatis *DRC* akan mengambil alih tugas dari *DCU* (Mulyani, Dewi M., et al. 2017). Perbedaan antara satu metode dengan yang lainnya terdapat pada cara pengoperasian manual dan otomatis dalam menggantikan tugas *DCU*. Pada BPR Universal akan digunakan metode *hot standby*.

Aplikasi *Heartbeat* difungsikan sebagai sensor pendeteksi apakah status *DCU* normal atau sedang mengalami gangguan. Aplikasi *heartbeat* dipasang pada kedua sistem *data centre (DCU* dan *DRC)* dan saling berkomunikasi dan bertukar informasi melalui saluran *Transport Control Protocol/Internet Protocol (TCP/IP)*. Informasi yang dipertukarkan antar kedua sistem adalah semua sumber daya komputer, *server*, dan jaringan, yang meliputi kondisi jaringan, aplikasi dan status *server* itu sendiri. Bila salah satu informasi tersebut tidak tersedia maka sistem *DRC* akan mengambil keputusan bahwa sistem *DCU* mengalami kegagalan dan sekaligus mengambil alih tugas dari *DCU*. Gambar 3 menjelaskan bagaimana kerja aplikasi *heartbeat* ketika mengalihkan

tugas dari *DCU* ke *DRC*. Pada kondisi ini *DCU* akan menonaktifkan jaringan sementara waktu.

IP Address pada sistem *DCU* akan dipergunakan oleh sistem *DRC*. Pada saat *DRC* dalam kondisi demikian akan memiliki dua buah *IP Address. IP Address* pertama adalah *IP Address* asli atau miliknya sendiri, sedangkan *IP Address* kedua adalah *IP Address virtual* dan bersifat sementara. Sehingga ketika nasabah mengakses sistem informasi bank secara otomatis permintaan tersebut diarahkan menuju *DRC*. Pada saat *DCU* sudah kembali normal, maka *IP Address virtual* pada sistem *DRC* dihapus, kemudian jaringan pada sistem *DCU* akan diaktifkan kembali dan semua layanan dikembalikan ke sistem *DCU*.

IV. HASIL DAN PEMBAHASAN

Topologi Infrastruktur *DCU (data centre* utama) dan *DRC (data recovery centre)* memiliki model yang mirip, hal ini untuk memudahkan proses duplikasi data, pengembangan sistem kedepan dan pertimbangan untuk pemeliharaan sistem.

Gedung dimana *DCU* berada terhubung melalui jaringan intranet bank dengan gedung *DRC*. Keberhasilan proses duplikasi data, sangat ditentukan oleh unjuk kerja jaringan intranet ini. Gambar 2 menggambarkan topologi jaringan yang digunakan untuk *DRC*.

Pada *DCU* terdapat *server* data secara fisik, namun pada *DRC* tidak terdapat server data secara fisik, karena fungsinya digantikan oleh sistem komputasi awan *(cloud computing)* berupa *Virtual Machine (VM)*. Sistem komputasi awan atau *VM* merupakan suatu model komputasi yang dijalankan dalam sebuah jaringan komputer dimana sumber daya antara lain *processor*, *memory*, *hard disk* dan jaringan seolah berperan sebagai sebuah layanan (Suryana, 2016). Teknologi ini dipakai karena dapat menjadi solusi untuk *DRC* tanpa perlu menginstal ulang maupun menggunakan komputer yang berbeda untuk suatu aplikasi (Atirah et al., 2012).

Proses pelaksanaan *backup data* dilakukan pada saat *DCU* dan *DRC* dalam keadaan operasional (kondisi *live*), setiap periode waktu yang ditentukan. *Backup* data server komputasi awan *(cloud computing)* dilakukan secara *realtime* atau seketika, hal ini disengaja karena server komputasi awan harus melakukan sinkronisasi data dengan cepat, agar datanya selalu terbaharui. Sehingga pada saat terjadi gangguan serius pada *server data centre* utama, misalnya maka server *DRC* dapat beroperasi dengan data dan informasi terbaru.

Proses *backup data* menggunakan sistem *Distributed Replicated Block Device* dengan metode *differential backup*. *Backup data* ini dilakukan dalam mekanisme *block devices*, bukan dalam bentuk data mentah (Budiman, K., et.al., 2019). *Backup data* menggunakan metode *differential backup* dapat dianalogikan sebagai *Redundant Array of Idependent Disk (RAID)*. Perbedaannya adalah pada *RAID* yang dilakukan adalah duplikasi isi dan data atau paritisi suatu *hard disk* ke *hard disk* atau partisi lain dalam satu komputer, sedangkan pada metode *differential backup*, dilakukan duplikasi isi dan data atau partisi suatu *hard disk* ke *hard disk* lain pada komputer yang berbeda melalui media jaringan. Sehingga setiap aplikasi yang dijalankan pada *DCU* dengan sendirinya akan terjadi sinkronisasi dengan *DRC* (Jia, Heping, 2018). Untuk proses *backup data storage server* dilakukan secara periodik (mingguan atau bulanan) dengan menggunakan metode *snapshot backup*. Data yang terdapat pada *storage server* merupakan data akumulasi hasil entri dan transaksi selama sistem beroperasi. *Snapshot backup* melakukan duplikasi pada volume data atau sistem dan biasanya pada *hard disk array*, *hard disk* lokal dan jaringan.

Posisi dan lokasi *DRC* berada adalah hal yang sangat penting untuk dipertimbangkan. Beberapa kriteria dan persyaratan wajib dipenuhi dalam penentuan lokasi *DRC*. Kesalahan dalam menentukan lokasi *DRC* bisa berakibat fatal. Contoh kasus adalah *DRC* yang seharusnya saat terjadi bencana sistem TI bisa tetap berjalan tetapi karena *DRC* terkena dampak dari bencana tersebut akhirnya malah tidak bisa berfungsi. Aspek-aspek lain yang harus diperhatikan pada saat penentuan lokasi *DRC* adalah lokasi yang memenuhi keamanan serta syarat bangunan sipil, tersedia cadangan sistem catu daya, sirkulasi udara yang baik, terdapat sistem pengamanan akses, ada sistem monitoring kondisi lingkungan, mempunyai sistem komunikasi data yang baik dan diterapkannya tata kelola standar *data centre* (Dewannata, 2015). Oleh sebab itu *DRC* BPR Universal ditempatkan pada gedung lain yang ada di lokasi sama namun terpisah areal parkir. Hal ini disebabkan karena BPR Universal sudah memiliki gedung lain dalam satu areal yang memenuhi standar untuk dijadikan lokasi *DRC*, yaitu telah memiliki ruangan/bangunan khusus yang dapat digunakan sebagai *data centre*, tersedianya *backup* sumber tegangan (*UPS*, Genset), dan infrastruktur TI yang ada cukup untuk memenuhi kebutuhan jaringan lokal dan terdapat sumber daya manusia yang memiliki keahlian dan sertifikasi TI.

Gambar 4 menginformasikan keadaan operasional *DCU* (*data centre* utama) pada kondisi normal, dimana seluruh operasional sistem TI disediakan layanannya *DCU*. Sistem *hot standby* merupakan jenis *DRC* yang tercepat (kesiapan 90%) yang diatur secepat mungkin dalam melayani operasional bisnis, dan aplikasi, dimana link data komunikasi yang sama sudah terpasang dan sudah siap di lokasi *DRC* (Ardiyanto, 2014). *DRC* secara menerus melakukan penggandaan data serta sinkronisasi (penyamaan) data dengan sistem *DCU*, dan selalu siap ketika *DCU* mengalami gangguan atau kerusakan.

Namun dilain pihak apabila sistem *DCU* mengalami gangguan atau kerusakan hingga tidak beroperasi atau

sistem gagal diakses, secara otomatis sistem *DRC* akan beroperasi menggantikan peran sistem *DCU*. Proses perpindahan koneksi *(switch over)* layanan operasional sistem TI menggunakan Aplikasi *Heartbeat. Heartbeat* adalah aplikasi dasar untuk *Linux High Availability (Linux-HA)* yang menjalankan *script* inisialisasi *HA* dan saat *node* atau *server* mati dan hidup (Afif dan Suryono, 2013). Aplikasi ini akan mengecek status koneksi pada *DCU* dan *DRC*. Konsepnya adalah apabila modul kontroler mengetahui bahwa sistem *DCU* tidak bisa dihubungi, maka kemudian permintaan secara otomatis akan dialihkan ke sistem *DRC*. Gambar 5 menunjukkan kondisi pengambil alihan tugas sistem *DCU* oleh sistem *DRC*.

Pada saat sistem *DCU* kembali normal, maka otomatis semua layanan operasional akan ditangani kembali oleh sistem *DCU*, dan proses sinkronisasi atau penyamaan data dari sistem *DRC* ke sistem *DCU* akan terjadi. Proses ini bertujuan untuk memperbaharui data *(updating data)* pada sistem *DCU*. Proses ini bisa disebut dengan pemulihan sistem. Dengan demikian terjaga konsistensi data pada kedua sistem tersebut.

Gambar 6 menunjukkan tampilan sistem *DCU*. Terdiri dari dua server komputasi awan *(cloud computing), server data, storage server* dan *storage* lain. Dua *server* komputasi awan bertujuan untuk membentuk sistem *cluster* agar mendapatkan kinerja lebih baik dan dapat menampung *VM (Virtual Machine)* lebih banyak. Sistem *cluster* diperlukan untuk meningkatkan kinerja beberapa komputer agar menjadi suatu sistem tunggal sumber daya komputasi yang melakukan pekerjaan besar (Brian et al., 2014). Sedangkan *server* data merupakan *server* difungsikan untuk menyimpan data informasi nasabah dan data transaksi. *Storage Server* merupakan gabungan *server* dan *storage* yang membentuk sebuah *Network Attach Storage (NAS)* yang fungsinya adalah sebagai media penyimpan data bagi *server* komputasi awan dan *server* data.

V. KESIMPULAN

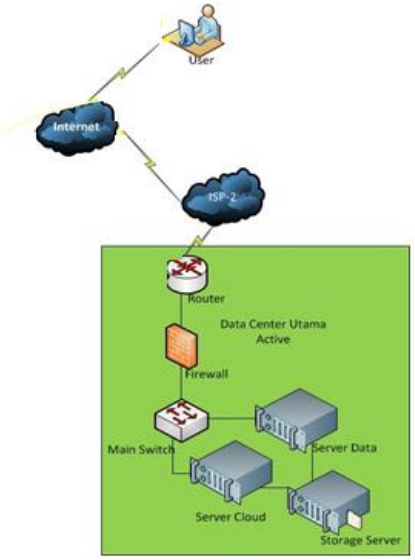
1. Ketersedian *DRC (Data Recovery Centre)* adalah suatu keharusan dalam usaha pemulihan sistem setelah terjadinya bencana, dan dapat mengatasi kekhawatiran akan kehilangan data saat terjadi suatu bencana, serta menjaga integritas data.
2. Metode *Hot Standby* memberikan solusi dengan tingkat ketersediaan *(High Availability)* yang tinggi pada ketersediaan aplikasi, informasi dan data.
3. Lokasi penempatan *DRC* harus memenuhi syarat sangat penting untuk menghindari dampak bencana berfungsi sebagai sistem *data centre* cadangan.
4. Metode *hot standby* yang diterapkan pada *DRC* bank lebih efektif ketika dukungan infrastruktur sistem TI bekerja optimal.
5. Kesalahan dalam penerapan metode *backup data* dapat mengakibatkan terjadinya inkonsistensi data dan menyebabkan potensi kerugian finansial yang besar.

VI. GAMBAR DAN TABEL

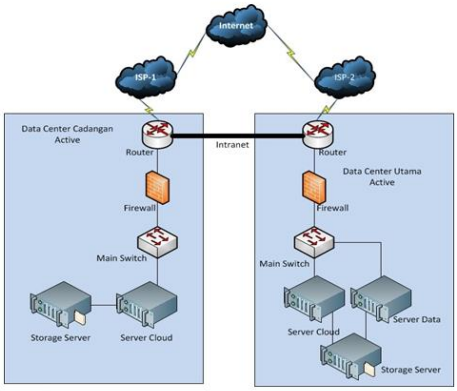
Dibawah ini adalah beberapa gambar dan tabel yang dapat lebih menjelaskan uraian tulisan ini :

Tabel 1
Daftar Perangkat DRC

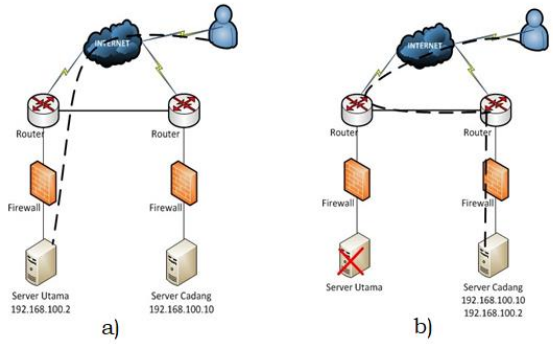
	Perangkat Keras	Spesifikasi	Perangkat Lunak
1	*Server cloud*	CPU : 2 x Intel Xeon 3 GHz Memory : 12 GB NIC : 2 unit 1 GB Hardisk : 2 x 1 TB	Proxmox VE Versi 3.4
2	*Server Storage*	Kapasistas : 25 TB	FreeNAS versi 9.3
3	*Router*	Mikrotik RB10000AH	RouterOS
4	*Switch*	TP-LINK	



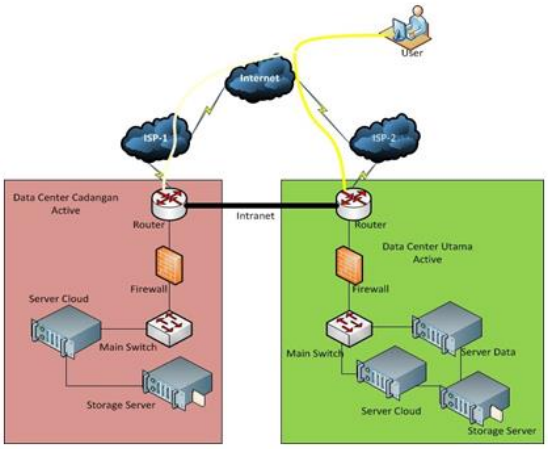
Gambar 1
Topologi jaringan asli *DCU*



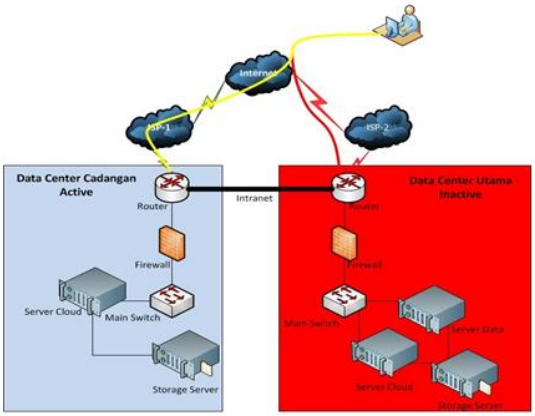
Gambar 2
Topologi jaringan Usulan untuk DRC



Gambar 3
Cara kerja aplikasi *heartbeat*,
(a) kondisi normal, (b) kondisi pada saat *DCU* mengalami gangguan



Gambar 4
Kondisi *DCU* utama beroperasi normal



Gambar 5
Kondisi *DCU* mengalami gangguan
(*DRC* menggantikan operasi *DCU*)

Gambar 6
Server dan *storage server* di *DCU*

VII SARAN

Dari studi ini, metode *hot standby system* merupakan metode yang secara moderat baik karena mudah implementasinya, lebih ekonomis apabila lokasi *DCU* dan *DRC* relatif berdekatan. Metode ini sesuai untuk perusahaan yang sangat mementingkan ketersediaan data *online* secara menerus, namun memiliki ukuran data yang sedang. Untuk lebih bagusnya disarankan menggunakan sarana data komunikasi dengan kecepatan transfer data yang tinggi sehingga sinkronisasi berlangsung dengan sangat cepat.

REFERENSI

[1] Afif, M.F., Suryono, 2013. Implementasi *Disaster Recovery Plan* dengan sistem *Fail Over* menggunakan *DRBD* dan *Heartbeat* pada *Data Center* FKIP UNS. Journal on Networking and Security (IJNS).

[2] Amanda. A. A., dan Supriadi, A. P., 2014. Konsep Penyusunan Kerangka Kerja *Business Continuity Plan* Teknologi dan Sistem Informasi, Seminar Nasional Sistem Informasi Indonesia.

[3] Ardiyanto, Putri; K. S., Gustini L.; Gustini. L.; Kusuma. S., Wendy, 2014. *Managing Disaster Pada Data Centre*, https:// id.scribd.com/doc/211589649/Managing-Disaster-Pada-Data-Centre-Paper di download tanggal 1 - Juli – 2015.

[4] Atirah, Niswar M.; Ilham. A. A., 2012, Implementasi *Virtual Document* pada *Cloud Computing*, Universitas Hasanudin Makasar.

[5] Brian, W.K., et al. 2013. Perancangan PC Cluster untuk Render Animasi 3D, E-Journal Teknik Elektro dan Komputer.

[6] Budiman, K., et.al., 2019, *Disaster recovery planning with distributed replicated block device in synchronized API systems*, 6th International

Conference on Mathematics, Science, and Education (ICMSE 2019), IOP Publishing.
[7] Dewannanta. D., 2015, Perancangan Jaringan Komputer - *Data Centre*, www. ilmukomputer.org di download tanggal 1- Juli - 2015.
[8] Jia, Heping; at.al., 2018. *Reliability of demand-based warm standby system with common bus performance sharing*, https://journals.sagepub.com/doi/abs/10.1177/1748006X18807301,SAGE Journals, 29 Oktober 2018.
[9] Muhaemin, M. 2018. Mengembangkan Business Continue Planning (BCP) Dengan Pendekatan Kuantitatif Studi Kasus : SIAK-DITJEN ADMINDUK KEMENDAGRI, Jurnal Sistem Informasi, Teknologi Informasi, dan Komputer (JUST IT), FT-UMJ, Volume 9 No 1 Tahun 2018.
[10] Mulyani, Dewi M., et al., 2017. Analisa Infrastruktur Data Center Virtualisasi Dan *Disaster Recovery* Berbasis Site Recovery Manager Dalam Pemenuhan Service Level Agreement Pada PT XYZ, Jurnal Teknik Elektro UMT, Volume 1 No 1 2017.
[11] Rachmaningrum. N., dan Falahah., 2011. Studi kelayakan *Disaster Recovery Plan* Pada Infrastruktur Jaringan Komputer (Studi Kasus Jaringan Komputer Universitas Widyatama), Seminar Nasional Informatika, C-30 – C-36.
[12] Rancangan Peraturan Menteri Komunikasi dan Informasi, 2013. Tentang Pedoman Teknis Pusat Data, https://web. kominfo.go.id/sites/default/files/RPM% 20PEDOMAN%20PUSAT%20DATA.pdf
[13] Suryana, R., 2016. Pengembangan Server Jaringan LAPAN Bandung Menggunakan Komputasi Awan Berbasis *Insfrastructure As a Service* (IaaS), Berita Dirgantara, Vol. 17. No. 2, Halaman 53 – 62.
[14] Suryana. R., 2014. *Backup Data* Geomagnet Menggunakan Metode Replikasi Pada Repositori Sains Antariksa, Bunga Rampai Makalah Workshop Riset Medan Magnet Bumi dan Aplikasinya, Halaman 83 - 90.