BAB 2
LANDASAN TEORI

2.1 Profil perusahaan

PT.Helpy Malindo Makmur adalah perusahaan yang bergerak di bidang jasa dan *digital startup* yang berada di kota Bandung merupakan anak perusahaan dari perusahaan yang berkantor pusat di Malaysia. PT.Helpy Malindo Makmur merupakan perusahaan *digital startup* yang menyediakan layanan *mobile application* dimana pengguna bisa melakukan pemesanan layanan untuk *delivery*, *cleaning*, *massaging*, *auto-care*, *online shopping*, transportasi, dan layanan kesehatan.

PT.Helpy Malindo Makmur yang dipimpin oleh pengusaha asal Malaysia ini memiliki visi yaitu menjadi katalis untuk kehidupan yang lebih baik dengan pemanfaatan teknologi yang canggih. Hal ini sama dengan aplikasi yang dibangun oleh perusahaan tersebut yang bertujuan untuk membantu masyarakat untuk melaksanakan kegiatan sehari-hari dengan pemanfaatan teknologi yang canggih melalui aplikasi Helpy.

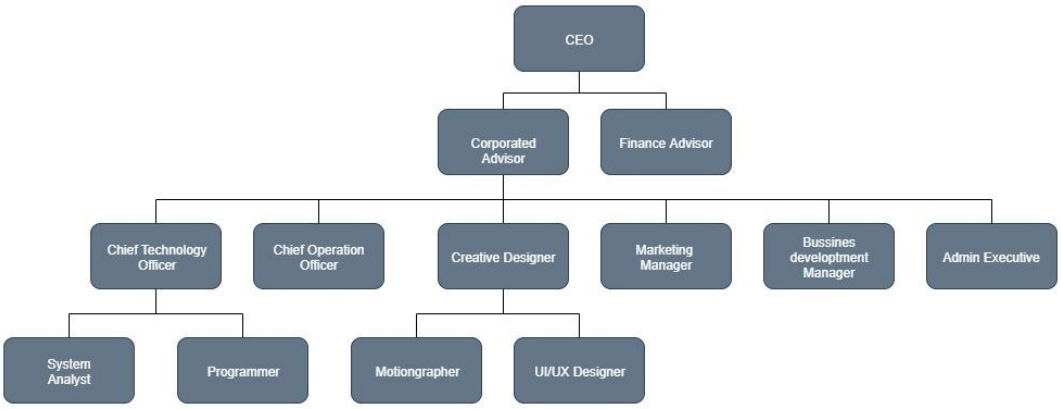
2.1.1 Logo Instansi

Perusahaan memiliki logo sebagai berikut :

Gambar 2.1 Logo Perusahaan

2.1.2 Struktur Organisasi

Sebuah perusahaan dalam menjalankan aktifitas serta tugasnya sebagai pelaku usaha melakukan kerja sama antar pegawai yang ada di dalam perusahaan tersebut untuk mencapai tujuan, maka dari itu dibuatlah sebuah struktur organisasi yang digunakan untuk menggambarkan hubungan kerjasama antar masing-masing bagian sesuai dengan posisinya. Dibawah ini merupakan struktur organisasi yang ada di lingkungan Perusahaan.



Gambar 2.2 Struktur Organisasi Perusahaan

Berdasarkan gambar diatas maka struktur organisasi dari Perusahaan dapat dijabarkan sebagai berikut.

1. CEO

   CEO (*Chief Executive Officer*) merupakan pejabat tertinggi yang mengatur, merencanakan, mengelola, dan menganalisis segala aktivitas fungsional bisnis seperti operasional, sumber daya manusia, keuangan, dan pemasaran perusahaan yang dipimpinnya, berikut adalah tugas dan fungsi yang dimiliki oleh seorang CEO.

   a. Merencanakan serta mengelola anggaran, mengamati dan menganalisis.
   b. Mengelola perusahaan sesuai dengan tujuan perusahaan.
   c. Merencanakan dan mengelola kinerja dari SDM yang berkompeten sehingga dapat ditempatkan pada posisi yang sesuai.

d. Merencanakan, mengelola, serta mengeksekusi perencanaan strategi bisnis atau korporat baik untuk jangka waktu menengah maupun panjang dengan mengacu pada visi dan misi perusahaan.
e. Meningkatkan performa operasional perusahaan.
f. Mengambil keputusan strategis yang berdampak baik bagi keberlangsungan perusahaan berdasarkan hasil analisis data dan fakta.
g. Menjaga kompetensi perusahaan dan meningkatkan performa utama perusahaan.
h. Menganalisis dan mengambil langkah paling prioritas bagi alokasi sumber daya dan penganggaran perusahaan.
i. Membuat kebijakan, prosedur, dan standar pada organisasi perusahaan.
j. Menganalisis permasalahan dalam perusahaan dan mengkoordinasikan manajemen dalam menyelesaikan masalah secara efektif dan efisien.

2. Corporate Advisor

   Corporate Advisor adalah seseorang yang betugas untuk memberikan nasihat terhadap kebijakan-kebijakan yang dibuat dan dilakukan oleh perusahaan, corporate advisor memiliki fungsi dan tanggung jawab yang mirip dengan Financial advisor.

3. Finance Advisor

   Finance Advisor merupakan gabungan dari dua kata dari *finance* yang artinya keuangan dan *advisor* dari kata *advice* yang berarti menasehati sehingga *advisor* adalah penasehat. Maka dari itu Finance Advisor bisa dikatakan sebbagai seseorang yang memberikan layanan dan informasi serta tata cara terkait urusan keuangan, yang meliputi pendapatan, keuntungan, klaim dan lain-lain. Berikut adalah tugas dari Finance Advisor.

   a. Melayani complain dari klien terkait produk asuransi yang diambil
   b. Melayani klaim dari peserta asuransi
   c. Memastikan klien yang melakukan complain atau klaim merasa puas dan tidak dirugikan.

4. Chief Operation Officer (COO)

   COO(*Chief Operation Officer*) merupakan pegawai yang mengawasi proses operasinal sebuah perusahaan, yang termasuk didalamnya adalah memastikan bahwa pelanggan mendapatkan pengalaman yang baik terhadap perusahaan.

5. Business Developtment Manager (BDM)

   BDM(*Business Developtment Manager*) merupakan seorang yang akan bertanggung jawab dalam menyusun target serta strategi jangka panjang yang akan digunakan oleh perusahaan.

6. Admin Executive

   Admin Executive merupakan pegawai yang akan melakukan pengelolaan terhadap arsip-arsip serta dokumen milik perusahaan.

7. Chief Technology Officer (CTO)

   CTO (*Chief Technology Officer*) merupakan orang yang bertanggung jawab pada kualitas akhir dari produk yang di bangun, dikarenakan CTO mengelola tim *engineer* selama proses pembangunan produk nya, seorang CTO juga memiliki posisi penting untuk bertindak sebagai ahli teknologi dan seorang leader.berikut adalah tugas dari seorang CTO.

   a. Menyatukan pengembangan produk.
   b. Memahami perkembangan teknologi saat ini dan pengadopsiannya.
   c. Mengelola pengembangan produk.

8. UI/UX Design

   UI/UX Designer adalah pegawai yang betugas sebagai orang yang melakukan desain terhadap *user interface* sistem yang dimiliki perusahaan sekaligus dengan seseorang yang akan membuat tingkat kepuasaan pelanggan terhadap sistem yang dibuat akan tinggi dengan melakukan riset terhadap perilaku pelanggan yang menggunakan sistem yang dibuat.

9. Marketing Manager

   Orang yang bertanggung jawab mengembangkan strategi pemasaran perusahaan. Marketing Manager meliputi kehumasan, riset pasar, dan pencitraan. Marketing Manager bertanggung jawab untuk membuat citra perusahaan untuk pihak luar. Tanggung jawab Marketing manager meliputi:

a. Mengembangkan strategi pemasaran
b. Melaksanakan riset pasar
c. Pencitraan

10. Creative Designer

Creative Designer merupakan seseorang yang bertanggung jawab untuk mewujudkan komunikasi verbal menjadi komunikasi visual agar semua pesan dari konsumen atau klien dapat diterima dengan baik. Berikut adalah tugas yang dimiliki oleh Creative Designer [3].

a. Bertemu klien untuk membahas tujuan bisnis dan kebutuhan pekerjaan.
b. Memperkirakan waktu yang dibutuhkan untuk menyelesaikan pekerjaan.
c. Mengembangkan prototype desain yang sesuai dengan tujuan klien.
d. Berpikir kreatif untuk menghasilkan ide-ide dan konsep-konsep baru dan mengembangkan desain interaktif.
e. Menggunakan inovasi untuk mendefinisikan kembali desain dalam keterbatasan biaya dan waktu.
f. Mempresentasikan ide dan konsep yang telah dibuat
g. Proofreadinguntuk menghasilkan karya yang akurat dan berkualitas tinggi.
h. Menunjukkan keterampilan ilustrasi dengan sketsa kasar.
i. Bekerja sebagai bagian dari tim dengan copywriter, fotografer, penata, ilustrator, desainer lain, account executive, pengembang web, dan spesialis pemasaran.

11. System Analyst

Sistem analis adalah seseorang yang bertanggung jawab untuk penelitian, perencanaan, kordinasi dan rekomendasi pemilihann kebutuhan untuk pembangunan sistem yang paling sesuai dengan kebutuhan bisnis perusahaan, seorang sistem analis memiliki peran yang besar dalam pengembangan sistem yang digunakan di perusahaan. Berikut adalah tugas dari sistem analis.

a. Menganalisa, mengkoreksi dan memperbaiki *error* yang terjadi.
b. Memperluas dan memodifikasi sistem untuk memenuhi kebutuhan baru, dapat juga digunakan untuk meningkatkan alur kerja.

c. Melakukan diskusi dengan manajemen untuk menentukan prinsip-prinsip kerja sistem yang digunakan.
d. Menentukan kebutuhan perangkat lunak dan perangkat keras yang dibutuhkan untuk mengatur atau membangun sitem.

12. Motiongrapher

Seorang motiongrapher adalah seseorang yang memiliki tugas untuk membuat, merancang dan menggabungkan ilustrasi, tipografi, fotografi dan videografi dengan menggunakan teknik animasi.

13. Programmer

Programmer adalah seseorang yang tugas nya adalah membangun program atau aplikasi yang digunakan untuk alat bantu manusia dalam mengerjakan rutinitasnya. Berikut adalah tugas dari seorang programmer.

a. Menulis program agar dapat menciptakan serangkaian *logic* dari instruksi komputer agar dapat mengikuti, menerapkan pengetahuan komputer.
b. Menganalisis, review dan menulis ulang program.
c. Menulis dokumentasi pengembangan program dan revisinya.
d. Membuat program beserta dengan alur kerja dan diagram nya.

2.1.3 Visi

Visi yang dimiliki oleh Perusahaan adalah sebagai perantara atau katalis yang berguna mewujudkan kehidupan yang lebih baik dengan pemanfaatan teknologi yang pintar.

2.1.4 Misi

Berikut adalah Misi yang diemban oleh Perusahaan.

a. Menciptakan serta menyediakan berbagai layanan memalui aplikasi yang berkelanjutan untuk membantu perekonomian masyarakat, komunitas dan juga linkungan sekitar.
b. Mengintegrasikan pengembangan sumber daya manusia, teknologi pintar, dan layanan berkualitas untuk membuat semua orang merasa bahagia dengan Helpy.

2.2 Simulasi

Simulasi adalah metode pelatihan yang memperagakan sesuatu dalam bentuk tiruan yang mirip dengan keadaan yang aslinya [4]. Sedangkan simulasi menurut Shannon (1975) simulasi adalah "proses merancang model sistem yang asli dan melakukan eksperimen dengan model ini untuk tujuan pemahaman perilaku sistem atau mengevaluasi berbagai strategi (dalam batas yang ditentukan oleh kriteria atau set kriteria) untuk pengoperasian sistem". Berdasarkan definisi mengenai simulasi oleh Kamus Besar Bahasa Indonesia (KBBI) dan Shannon (1975) maka dapat diambil kesimpulan bahwa simulasi adalah kegiatan untuk meniru atau memperagakan sesuatu semirip mungkin agar dapat lebih mudah untuk dipahami.

2.3 *Virtual Machine*

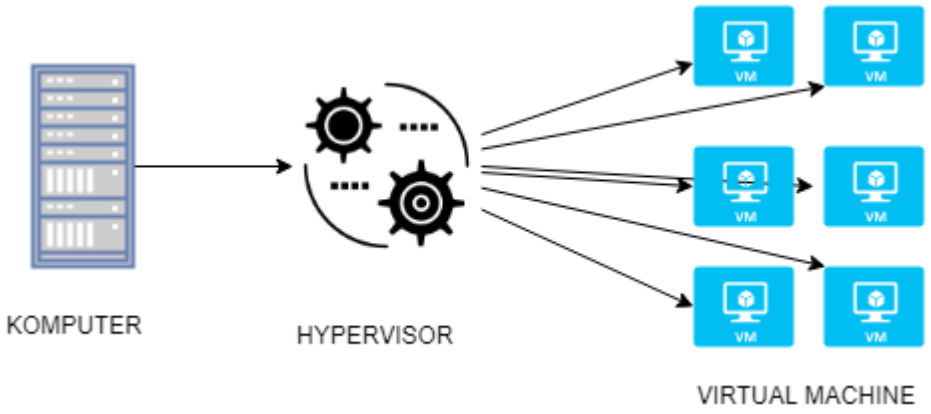
Virtual Machine adalah *software* komputer yang memiliki kemiripan seperti komputer fisik, yang dapat menjalankan sistem operasi dan aplikasi. *Virtual Machine* terdiri dari satu set spesifikasi dan file konfigurasi dan didukung oleh sumber daya fisik *host*. Setiap mesin virtual memiliki perangkat *virtual* yang menyediakan fungsionalitas yang sama seperti perangkat keras fisik dan memiliki manfaat tambahan dalam hal portabilitas, pengelolaan, dan keamanan [5]. Sedangkan *Virtual Machine* menurut Margaret Rouse adalah sistem operasi atau lingkungan aplikasi yang diinstal pada perangkat lunak, yang meniru perangkat keras [6]. Berdasarkan definisi mengenai *Virtual Machine* oleh VmWare dan Margaret Rouse dapat diambil kesimpulan bahwa *Virtual Machine* adalah suatu perangkat lunak yang dapat digunakan untuk mensimulasikan sistem operasi ataupun perangkat lunak ke dalam sebuah lingkungan *virtual.* Secara umum saat ini terdapat dua macam *Virtual Machine* yang memiliki fungsi yang berbeda yaitu *System Virtual Machines,* dan *Process Virtual Machine.*

1. *Process Virtual Machine* adalah platform virtual yang mengeksekusi proses individu. Jenis *Virtual Machine* ini digunakan hanya untuk mendukung proses, *Process Virtual Machine* akan dibuat ketika dibuat dan berakhir pada saat proses berakhir [7].

2. *System Virtual Machines* adalah sebuah *Virtual Machine* yang menyediakan lingkungan sistem yang lengkap dan persisten yang mendukung sistem operasi beserta banyak proses pengguna. *System Virtual Machines* menyediakan sistem operasi mode *guest* akses ke perangkat keras virtual, termasuk jaringan, I / O, prosesor dan memori [7].

2.3.1 Cara Kerja *Virtual Machine*

Cara kerja sebuah virtual machine yaitu dengan meniru komponen komputer fisik seperti CPU, memory, harddisk, dan jaringan dengan menggunakan sebuah *software* yang dibuat untuk virtualisasi, *software* tersebut akan membuat sebuah *virtual machine* yang isi nya dapat berfungsi seperti komponen fisik. Untuk membuat sebuah sistem dengan *virtual machine* diperlukan yang dinamakan dengan *hypervisor* yang berfungsi sebagai *layer* untuk mengatur seluruh *virtual* machine, dengan *hypervisor* maka didalam satu komputer fisik mampu terdapat beberapa *virtual machine* dalam satu komputer. Cara kerja dari *hypervisor* adalah dengan membagi-bagi *resources* yang ada ke beberapa *virtual machine* yang ada hal ini menyebabkan setiap *virual machine* seolah-olah memiliki *hardware* nya masing-masing.



Gambar 2.3 Visualisasi *Hypervisor*

Keuntungan dengan adanya *hypervisor* pada *virtual machine* adalah membuat setiap *virtual machine* secara *logic* terisolasi antara satu dan yang lainnya meskipun berjalan di komputer yang sama. Jika terdapat suatu *error* atau *malware* yang menyerang di salah satu *virtual machine* tidak akan berdampak pada *virtual machine* yang lainnya [8], [9].

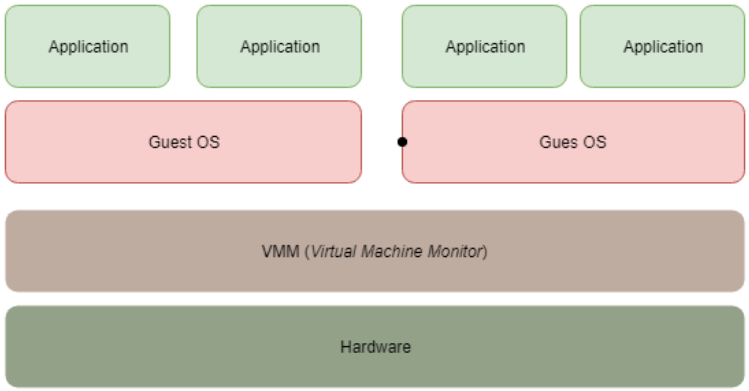
2.3.2 Virtualisasi

Virtualisasi menurut kamus Cambrigde adalah proses untuk merubah sesuatu yang ada di dunia nyata menjadi bentuk virtual / maya [10]. Berdasarkan definisi virtualisasi oleh kamus Cambridge, dapat disimpulkan bahwa virtualisasi adalah proses untuk membuat sesuatu yang bentuknya fisik menjadi sesuatu yang bersifat *logic*, seperti contohya adalah melakukan virtualisasi sistem operasi menggunakan *virtual machine* yang seolah olah sistem operasi tersebut benar-benar terinstall di sebuah komputer.

Untuk menunjang virtualisasi maka dibutuhkan *hypervisor*, *hypervisor* adalah sebuah proses yang membuat dan menjalankan *virtual machine, hypervisor* dapat membuat komputer yang bertindak sebagai *host* untuk menyuplai sumber daya seperti memori, prosessor, dan *storage* secara *virtual*. Saat ini terdapat dua tipe *hypervisor* yang ada diantaranya *hypervisor* tipe satu yang dapat disebut dengan *bare metal*, lalu ada *hypervisor* tipe kedua yaitu *hosted.*

1. *Hypervisor* Tipe 1 (*bare metal*)

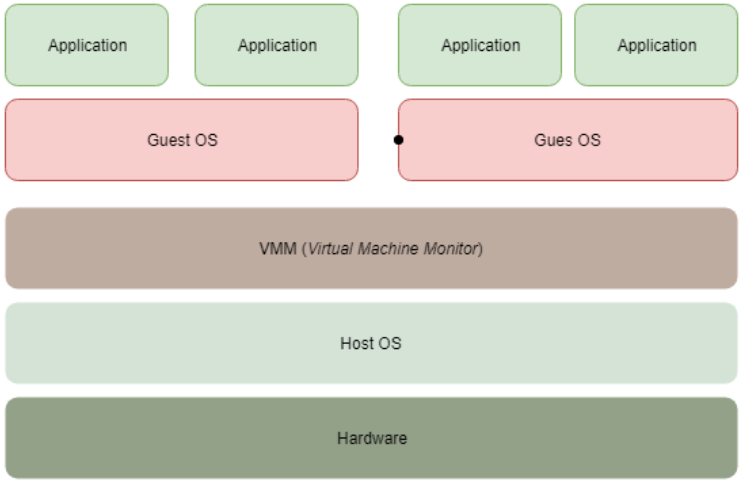
   Fitur dari *hypervisor bare metal* adalah manajemen sumber daya, dan juga *hypervisor* tipe satu ini memberikan performa, skalabilitas dan stabilitas yang lebih baik dikarenakan *hypervisor* akan mendapatkan akses kedalam *hardware* yang digunakan. Contoh dari *hypervisor* ini yaitu VMware ESXi, dan Microsoft Hyper-v.



Gambar 2.4 *Hypervisor* Tipe 1

2. *Hypervisor* Tipe 2 (*hosted*)

   Tipe *hypervisor* ini bekerja dengan cara mengkordinasikan permintaan untuk CPU, memori, disk, jaringan, dan sumber daya lain melalui sistem operasi *host* computer, hal ini akan mempermudah pengguna untuk menjalankan *virtual machine* pada perangkat komputer milik pengguna, contoh dari penggunaan *hypervisor* ini adalah Oracle Virtual Box, Solaris Zone, dan VMware Workstation.



Gambar 2.5 *Hypervisor* Tipe 2

Selain tipe dari *hypervisor* yang telah disebutkan diatas masih ada beberapa jenis *hypervisor* yang ada di pasaran saat ini, diantaranya adalah Hyper-V, KVM, XEN.

2.4 Data Center

Data center adalah salah satu infrastruktur yang digunakan untuk menempatkan sistem komputer dan komponen yang digunakannya misalkan *storage* serta jaringan yang berguna untuk komunikasi antar *server* dan *client*. Pada suatu *data center* didalam nya terdapat ratusan bahkan ribuan *server* yang tersusun pada rak *server***.** Bagi sebuah *data center* ketahanan merupakan hal yang sangat penting dikarenakan *data center* harus bekerja secara *non-stop,* maka dari itu dibutuhkannya duplikasi dari jaringan, *power-supply , bandwidth,* serta pendingin udara, untuk menjaga operasional dari sebuah *Data Center*.

Sebuah *data center* yang dibangun harus memenuhi beberapa kriteria yang harus dipenuhi agar *data center* yang dibangun tersebut memiliki performa yang maksimal dan dapat digunakan dalam jangka waktu yang lama. Kriteria yang dibutuhkan sebuah *data center* adalah sebagai berikut.

1. *Security*

   Security merupakan komponen dari suatu *data center* yang tidak boleh untuk dilewatkan apabila *data center* tersebut, keamanan bagi sebuah *data center* menjadi tantangan yang sangat besar mengingat suatu *data center* memiliki tingkat kerahasiaan yang tinggi, selain itu dengan selalu meningkatnya jumlah data serta perangkat yang digunakan. *Data center* harus menggunakan standar yang tinggi untuk memastikan integritas, kerahasiaan, serta *availability* dari sistem yang terdapat di dalamnya. Standar keamanan yang biasa digunakan untuk *data center* menggunakan standar internasional ISO 27001.

   ISO 27001 atau yang memiliki nama resmi ISO/IEC 27001:2005 adalah sebuah panduan yang berisi spesifikasi yang dapat digunakan untuk acuan mengenai keamanan sistem informasi atau *information security management system* (ISMS). ISO 27001 merupakan sebuah *framework* yang berisi aturan dan prosedur yang termasuk control terhadap manajemen resiko perusahaan. ISO 27001 dikembangkan untuk menyediakan model untuk membangun, menerapkan, mengoperasikan, memantau, meninjau, memelihara dan meningkatkan sistem manajemen keamanan informasi.

   Berdasarkan *guideline* ISO 27001 menggunakan pendekatan berdasarkan resiko terdapat enam bagian dalam proses perencanaan manajemen kemanan sistem informasi [11].

   a. *Define a security policy.*

      Define a security policy, membuat aturan mengenai manajemen kemamanan sistem informasi yang dimiliki perusahaan.

   b. *Define the scope of the ISMS.*

Define the scope of the ISMS, membuat cakupan dari ISMS yang akan digunakan berdasarkan analisis dari kebutuhan dan situasi dari perusahaan dan *stakeholder*.

c. *Conduct a risk assessment.*

Conduct a risk assessment, akan memberikan analisa tetang apa saja yang mungkin terjadi serta dampak yang mungkin akan ditimbulkan ke dalam sistem, serta tindakan yang harus dilakukan untuk mencegah resiko yang akan berpotensi mengancam sistem.

d. *Manage identified risks.*

Managed identified risks, merupakan cara suatu perusahaan mengidentifikasikan resiko yang mungkin terjadi dengan melakukan diskusi dengan seorang yang memiliki kedudukan di posisi *top management* dalam perusahaan tersebut.

Terdapat tiga proses yang digunakan untuk mengidentifikasi resiko sebagai berikut.

a. *Methods for identifying risks.*
b. *Criteria for assessing risks.*
c. *Criteria for risks acceptance.*

Untuk memastikan perkembangan dari ISMS yang digunakan ISO 27001 merekomendasikan pendekatan PDCA (*Plan*, *Do*, *Check*, *Act*).

1. *Plan*
   a. Menetapkan langkah keamanan untuk mencapai target dan menentukan individu yang bertanggung jawab.
   b. Menentukan indikator kinerja yang memunkinkan kinerja individu dapat diukur.
   c. Menentukan proses untuk mengukur kinerja, dan batas toleransi
2. *Do*
   a. Implementasi tindakan untuk koreksi apabila terjadi kecacatan atau ketidaksesuaian.
   b. Pengukuran yang berkelanjutan dari pencapaian tujuan.

3. *Check*
    a. Memantau indikator keamanan individu, serta membandingkan kinerja individu.
    b. Mengawasi penanggulangan yang diterapkan dan individu yang bertanggung jawab apabila sudah melampaui batas standar.
4. *Act*
    a. Membuat keputusan yang diperlukan untuk memulihkan efektifitas dari langkah-langkah keamanan.
    b. Pendokumentasian keputusan dengan cara yang baik beserta dengan penjelasan.

2. *Scalability*

    Scalability adalah kemampuan *data center* untuk tetap bekerja dengan baik ketika terjadi proses *upgrade* sistem sehingga proses bisnis tetap berjalan, dan *data center* akan menjadi lebih baik, dengan *Scalability* suatu *data center* akan meningkatkan efisiensi energi serta kemampuan untuk mengurangi biaya operasional *data center*.

3. *Manageability*

    Manageability adalah kemampuan *data center* harus dapat memberikan mode manajemen yang mudah dan terintegrasi terhadap seluruh *resource* yang dimilikinya sehingga akan mengurangi intervensi dari manusia melalui sistem yang terotomatisasi.

4. *Cost*

    Cost, suatu *data center* harus memiliki nilai ekonomi yang dapat memberikan bagi perusahaan yang menggunakannya berkat kemampuan yang dimiliki *data center* sehingga akan memberikan keuntungan bagi perusahaan.

5. *Availability*

    Availability sebuah *data center* harus memiliki kriteria *availability* yaitu kemampuan *data center* untuk memastikan ketersediaan layanan tetap berjalan tanpa ada masalah. Berdasarkan Anixter [12] ada empat jenis *data center* memiliki perbedaan dalam tingkat persentasi *availability* yaitu sebagai berikut.

Tabel 2.1 Spesifikasi Tier *data center*

	TIER			
	1	2	3	4
Availability	99,761%	99.841%	99.982%	99.995%
Maksimal *Downtime*	28.8 jam / tahun	22 jam / tahun	1.6 jam / tahun	0.04 jam / tahun

Data center dengan tingkat waktu *downtime* lebih kecil akan lebih baik dalam memberikan jaminan ketersediaan bagi sistem yang terdapat didalamnya.

2.4.1 Server

Server atau komputer *server* adalah komputer yang melayani semua komputer atau terminal yang terhubung kepadanya. Komputer ini merupakan sebuah perangkat yang memiliki fungsi sebagai pusat atau sebuah terminal. Bertugas dalam memberikan sumber daya serta ijin bagi komputer lain yang dibawahnya untuk terhubung secara bersama-sama namun masih dalam satu *server* [13]. Sedangkan *server* menurut Christensson, P *server* adalah komputer yang menyediakan data ke komputer lain. *Server* dapat melayani data ke sistem pada jaringan area lokal (LAN) atau jaringan area luas (WAN) melalui Internet [14]. Berdasarkan definisi diatas dapat disimpulkan bahwa *server* adalah komputer yang dapat memberikan layanan untuk menunjang kebutuhan komputer *client* yang terhubung ke dalam nya melalui suatu jaringan yang saling terhubung. Adapun jenis-jenis dari *server* ada berbagai macam yaitu.

1. *Web Server* adalah sekumpulan komputer yang digunakan untuk membagikan *website* atau konten ke banyak *user*, contoh dari *web server* adalah Apache Web Server, dan Nginx.
2. *Mail Server* adalah sebuah computer sentral yang digunakan untuk menyimpan pesan *email* milik *client* yang disimpan didalam sebuah jaringan yang dinamakan *Mail Server.*
3. *Cloud Server* atau bisa disebut *cloud computing* adalah istilah yang digunakan untuk menggambarkan layanan yang disediakan menggunakan *network* oleh server. *Cloud* menyediakan kemampuan penyimpanan dan pemrosesan yang

sangat besar dan terdistribusi, yang dapat diakses oleh perangkat apa pun yang tersambung ke *Internet*.

4. *Database server* adalah *server* yang memberikan layanan yang berkaitan dengan pengaksesan dan pengambilan data yang berada di *database*.
5. *Dedicated server* adalah *server* yang hanya boleh dan bisa digunakan oleh satu instansi saja, dengan menggunakan *dedicated server* pengguna dapat bebas untuk memilih sendiri sistem operasi yang akan digunakan.
6. *File server* adalah *server* yang bertugas untuk manajemen file data sehingga computer lain yang berada di dalam suatu jaringan yang sama dapat mengakses data tersebut, *file server* membuat pengguna dapat berkirim dan membagikan file tanpa menggunakan perangkat bantuan seperti *flashdisk*.
7. *Print server* adalah computer yang bertugas untuk mengerjakan proses yang berkaitan dengan mencetak dokumen, *print server* terkoneksi dengan jaringan computer yang bertujuan untuk melakukan proses cetak (*printing*) yang memerlukan lebih dari satu *printer*.
8. *Proxy server* dapat berupa komputer atau perangkat lunak yang dijalankan sebagai perantara antara klien.
9. *Blade server* adalah sasis dari *server* yang didalamnya menampung beberapa papan sirkuit elektronik yang berisi prosesor, memori, *network controller*, dan *port I/O.*
10. *Standalone server* adalah *server* yang berjalan secara independen tidak membutuhkan *server* yang lain.

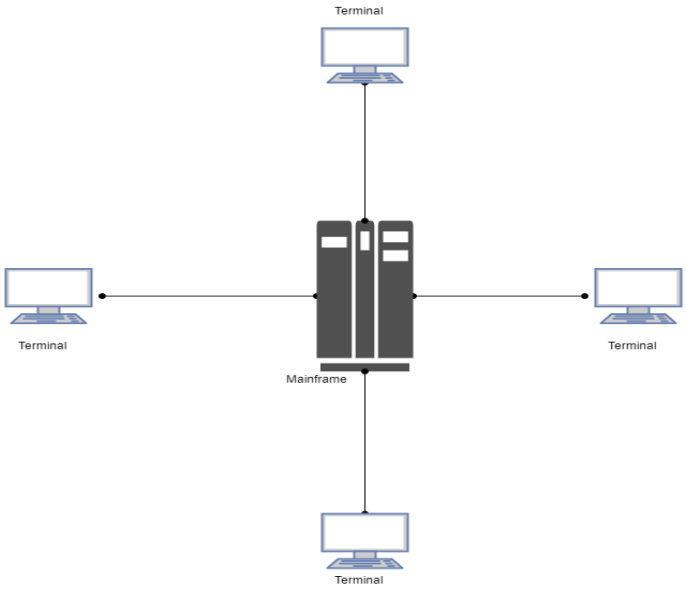
2.4.2 Arsitektur *Client/Server*

Client/Server adalah arsitektur dari jaringan computer yang dimana *client* meminta dan menerima *service* dari *server*. Komputer *client* menyediakan tampilan yang memungkinkan pengguna untuk meminta *service* dari komputer *server* yang hasilnya akan ditampilkan di komputer pengguna. Sedangkan menurut Premerlani (1998) *Client/Server* adalah suatu arsitektur dimana sumber daya *server* menyediakan komputasi untuk banyak komponen *client.* Sedangkan *client* adalah komputer yang terhubung ke sebuah *server* sehingga memungkinkan untuk menggunakan sumber daya serta *service* yang ada di *server* tersebut.

Arsitektur *client/server* ada tiga yaitu *one-tier architecture, two-tier architecture,* dan *three-tier architecture*.

1. *One-tier architecture* (Arsitektur *Mainframe*)

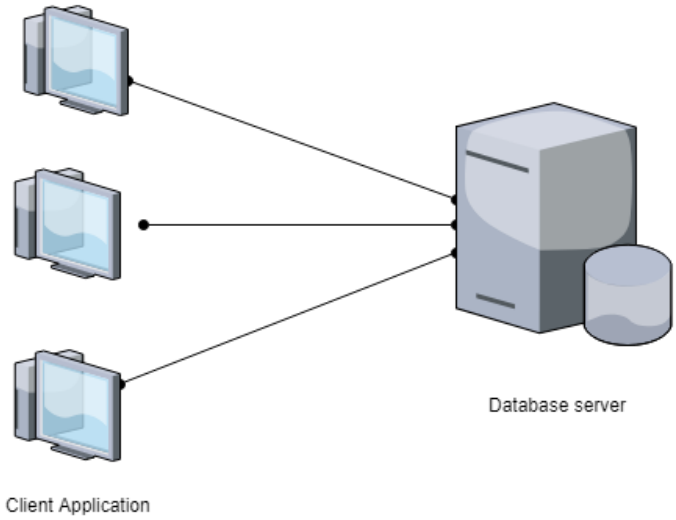
   Pada arsitektur ini hanya ada sebuah computer yang memilki sumber daya yang besar meliputi memori, prosessor serta media *storage* yang berukuran besar.



Gambar 2.6 One-tier Architecture

2. *Two-tier architecture*

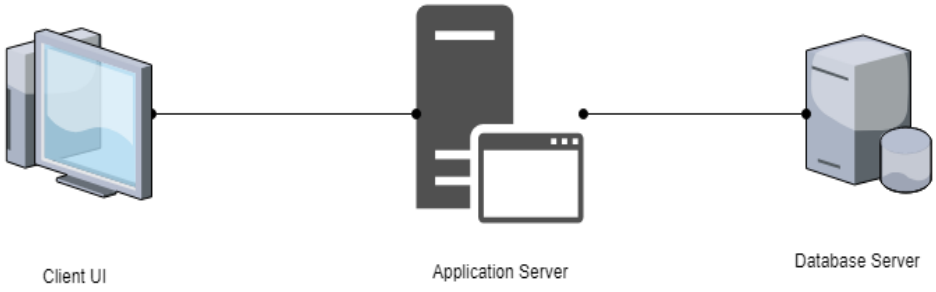
   Pada arsitektur *Two-tier* dibagi menjadi dua bagian yaitu *client application* dan *database server*, di dalam komputer klien terdapat aplikasi yang digunakan untuk mengakses ke *database server*. Karakteristik dari arsitektur *two-tier* adalah masing-masing domain akan mengelola sumber daya dengan pendekatan yang paling cocok sesuai dengan kebutuhan, ada yang memakai konfigurasi statis dan ada juga yang memakai protocol reservasi, lalu ketika ada dua domain yang bertetangga mengalokasikan sumber daya, akan ada suatu perjanjian anatara domain tersebut yang biasa disebut dengan *service level agreement* (SLA) [15].



Gambar 2.7 two-tier Architecture

3. *Three-tier architecture*

   Arsitektur klien / server *Three-tier architecture* adalah evolusi dari *Two-tier architecture*, arsitektur ini digunakan terutama untuk aplikasi bisnis dengan skala yang besar. Perbedaan utamanya adalah pada arsitektur *Three-tier architecture* adalah sebagian besar fungsi dipisahkan dalam lapisan tengah, disebut server aplikasi, dan juga setiap *client* dapat menggunakan beberapa aplikasi yang sekaligus dapat bekerja menggunakan beberapa *database* [16].



Gambar 2.8 Three-tier Architecture

Didalam arsitektur *three-tier* ada yang disebut dengan *Application Server* yang berguna sebagai *Middleware* antara klien dan *database server*, *Middleware* sendiri adalah sebuah perangkat lunak terpisah yang berjalan di mesin yang berbeda yang mengerjakan *logic* dari aplikasi [17].

2.5 Disaster Recovery

Disaster Recovery adalah serangkaian protokol yang berfungsi untuk menghindari kehilangan data akibat adanya bencana, penanganan yang dapat dilakukan dengan *Disaster Recovery* mancakup *human-error*, *cyber attack*, dan gangguan yang mungkin saja terjadi dikarenakan kerusakan *hardware*. *Disaster Recovery Plan* adalah metode yang biasa digunakan oleh perusahaan yang basisnya di bidang IT, *Disaster Recovery Plan* mencakup prosedur untuk merespon keadaan darurat dengan menyediakan *backup* serta mengelola proses yang sedang berjalan pada saat gangguan terjadi, tujuan utama dari *Disaster Recovery* adalah untuk menjamin keberlangsungan sistem yang tentunya ini sangat penting di dunia bisnis.

Ada dua parameter yang sangat penting untuk *Disaster Recovery* yang pertama adalah RPO(*Recovery Point Objective*) dan RTO (*Recovery Time Objective*), RPO mendeskripsikan tentang interval waktu yang berlalu selama gangguan terjadi sebelum jumlah data yang hilang pada saat gannguan terjadi. Sedangkan RTO adalah waktu yang dibutuhkan untuk mengembalikan data yang hilang setelah gangguan terjadi.

Disaat proses bisnis yang dijalankan perusahaan sangat mengantungkan pada keberlangsungan sistem atau bisa disebut dengan *high availability*, maka toleransi terhadap *downtime* sistem semakin berkurang. Banyak studi yang telah menunjukan bahwa banyak perusahaan yang menderita kebangkrutan akibat dari adanya kehilangan data yang signifikan, namun dengan adanya *disaster recovery*(DR) akan sangat membantu dalam mencegah resiko yang telah disebutkan terjadi.

Tahap persiapan untuk menghadapi bencana dengan perencanaan *disaster recovery* membutuhkan pendekatan yang komprehensif yang mencakup *hardware* dan *software,* perlekapan sistem jaringan, sumber daya, konektivitas dan pengujian yang aka memastikan bahwa sistem *disaster recovery* yang dibangun telah mencapai salah satu syarat penting yaitu mencapai target RTO dan juga RPO.

Menurut Paul Kirvan [18] prinsip objektif dari program *disaster recovery* adalah untuk membangun, menguji dan mendokumentasikan rencana yang telah terstruktur sehingga mudah untuk dipahami oleh seluruh tim yang terlibat, dan

secara tidak langsung akan membantu perusahaan melakukan *recovery* secepat mungkin dan efektif. Prinsip objektif lainnya yaitu sebagai berikut.

a. Memastikan bahwa setiap karyawan benar-benar mengerti akan tugas mereka dalam implementasi DRP.
b. Kebutuhan untuk memastikan bahwa kebijakan operasional akan dipatuhi dalam semu kegiatan yang telah direncanakan..
c. Memastikan bahwa seluruh rencana hemat biaya.
d. Kebutuhan untuk mempertimbangkan implikasi terhadap pada situs DR yang lain milik perusahaan.
e. Kemampuan untuk *disaster recovery* berlaku untuk pelanggan, vendor dan pihak lain yang terlibat.

2.5.1 *Disaster*

Disaster menurut kamus Cambridge adalah situasi yang sangat buruk yang dapat menghancurkan rencana, kesuksesan, atau kemampuan perusahaan untuk beroperasi [19]. Sedangkan menurut Undang-Undang Nomor 24 tahun 2007 tentang penanggulangan bencana menyebutkan bahwa definisi dari bencana adalah rangkaian peristiwa yang dapat mengancam serta menggangu kehidupan masyarakat yang dapat disebabkan oleh faktor alam atau faktor non-alam maupun faktor manusia sehingga mengakibatkan timbulnya korban jiwa manusia, kerusakan lingkungan, kerugian harta benda, dan dampak psikologis.

Sedangkan di dalam dunia teknologi informasi bencana dapat juga membuat sistem yang sedang berjalan dapat terganggu bahkan mengalami sistem *down* dikarenakan adanya gangguan tersebut, gangguan yang dapat menimpa dunia teknologi informasi diantaranya sebagai berikut.

1. *Hardware failure*

   Hardware failure yang menimpa suatu sistem akan membuat sistem tersebut tidak dapat digunakan secara maksimal atau bahkan tidak dapat dijalankan dengan normal, dikarenakan adanya komponen *hardware* yang rusak atau tidak dapat berfungsi normal.

Penyebab terjadinya *hardware failure* dapat dipengaruhi oleh lingkungan sekitar tempat sistem tersebut berada, beberapa penyebab yang dapat mengakibatkan *hardware failure* diantaranya sebagai berikut ini.

a. Debu pada komponen komputer.
b. Komponen komputer yang sudah lawas / melebihi batas pakai.
c. Komponen komputer mengalami panas berlebih sehingga komponen menjadi rusak.
d. Arus listrik yang tidak stabil yang merusak komponen komputer.
e. Komponen komputer yang digunakan tidak terpasang dengan baik.

Untuk menghindari terjadinya *hardware failure* pada sistem yang digunakan maka perlu perawatan serta melakukan *upgrade* komponen agar mampu mengimbangi permintaan untuk komputasi.

2. *Software failure*

Software failure merupakan gangguan yang terjadi pada perangkat lunak yang digunakan oleh sistem seperti *database*, dan aplikasi. Akibat dari *software failure* dapat mengakibatkan sistem tidak dapat diakses dan juga aliran data akan terganggu yang diakibatkan oleh *software failure*. Beberapa penyebab yang dapat menyebabkan terjadinya *software failure* diantaranya sebagai berikut.

a. *Software* yang digunakan merupakan *software* versi lawas sehingga tidak dapat mengatasi beban kerja yang berat.
b. Proses *update* dan *patching* sistem perangkat lunak yang gagal, akan mengakibatkan sistem *crash* sehingga tidak dapat digunakan.
c. Adanya *bugs* didalam perangkat lunak yang digunakan, dengan adanya *bugs* tersebut akan mempermudah akses *malware* untuk masuk ke dalam sistem dan merusak perangkat lunak yang terkena *malware* tersebut.
d. Adanya serangan *cuber attack* yang bertujuan untuk merusak sistem sehingga sistem tidak dapat digunakan, dan juga dapat terjadinya kebocoran data.

Untuk mengurangi potensi terjadi *software failure* maka perlu memperhatikan *software* yang digunakan dengan cara melakukan *update*,

patching, serta meningkatkan keamanan sistem dengan menggunakan *firewall* atau *anti-virus*.

3. *Human Error*

Human error merupakan gangguan pada sistem yang diakibatkan oleh pengaruh pengguna sistem, *human error* dipengaruhi oleh SDM yang mengoperasikan sistem tersebut, berikut adalah beberapa penyebab yang mengakibatkan terjadinya gangguan terhadap sistem akibat dari *human error*.

a. Kesalahan pada saat suatu program dieksekusi yang dapat mengakibatkan *software corrupt* atau rusak, selain itu juga dapat menyebabkan kehilangan data.
b. Kurangnya pemahaman terhadap sistem yang digunakan, hal ini menyebabkan sistem *crash* dikarenakan pengoperasian sistem yang tidak sesuai dengan kebutuhan.
c. Adanya unsur ketidaksengajaan dalam penggunaan sistem sehingga menyebabkan kerusakan pada sistem, seperti kesalahan melakukan *format* data sehingga data hilang, selain itu dapat juga merusak komponen *hardware* yang digunakan sistem.

Maka dari itu untuk mengurangi potensi terjadinnya *human error* perlu dilakukan pelatihan terhadap SDM yang akan menggunakan sistem tersebut sehingga akan mengurangi potensi adanya gangguan yang berasal dari *human error*.

Berdasarkan definisi menurut kamus Cambridge dan Undang-Undang Nomor 24 tahun 2007 maka dapat disimpulkan bahwa *disaster* atau bencana adalah keadaan yang dimana keadaan tersebut dapat menyebabkan kerugian yang sangat besar baik itu kerugian material maupun non-material, jika di dalam dunia bisnis dan perkantoran maka bencana dapat menyebabkan kerugian yang dapat mengancam keberlangsungan suatu instansi apabila tidak mempunyai *planning* untuk menghadapi keadaan darurat.

2.5.2 *Recovery*

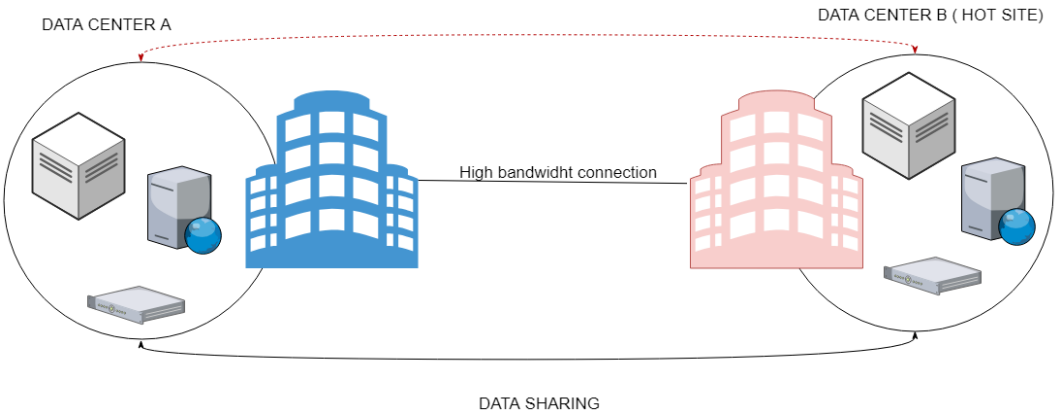
Recovery menurut kamus Cambridge adalah proses mendapatkan kembali sesuatu yang hilang atau rusak [20], Sedangkan menurut kamus KBBI *recovery*

atau restorasi dalam Bahasa Indonesia adalah mengembalikan atau memulihkan kepada keadaan semula [21]. Berdasarkan kamus Cambridge dan kamus besar Bahasa Indonesia maka dapat disimpulkan bahwa *recovery* adalah kegiatan atau proses untuk mengembalikan suatu sistem atau keadaan ke keadaan sebelum terjadinya suatu bencana atau kerusakan. Contoh dari *recovery* adalah *data recovery*. Cara kerja dari *data recovery* adalah dengan melakukan *backup* data dengan menggunakan *data recovery services* yang digunakan untuk mengambil data yang tidak sempat di *backup* namun masih tersimpan di *fragment harddisk*.

Dalam proses nya *recovery* membutuhkan suatu fasilitas yang dapat digunakan sebagai fasilitas *recovery* yang digunakan sebagai tempat untuk merelokasi sistem yang terkena dampak dari bencana seperi banjir, kebakaran, dsb. Maka dari itu terdapat strategi *backup site* yang digunakan diantaranya sebagai berikut [22].

1. *Hot Site*

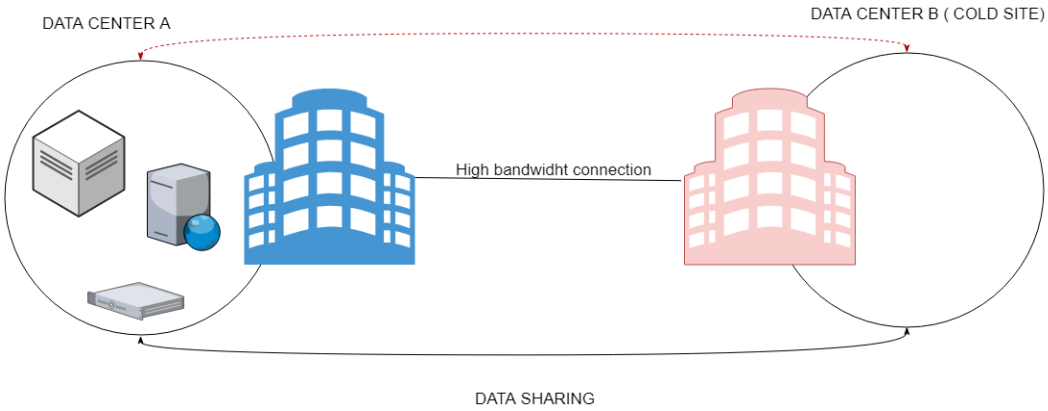
   Hot Site merupakan salah satu strategi *recovery* dengan cara memiliki *data center* yang serupa dengan yang digunakan, fitur yang paling penting dari *hot site* adalah lingkungan *data center* ini akan berjalan secara bersamaan dengan *data center* yang utama, jika tiba-tiba terjadi kejadian bencana maka *hot site* dapat langsung mengambil alih, namun dengan model ini memiliki kekurangan yaitu harus memilki bujet yang besar untuk menerapkannya.



Gambar 2.9 *Hot Site*

2. *Cold Site*

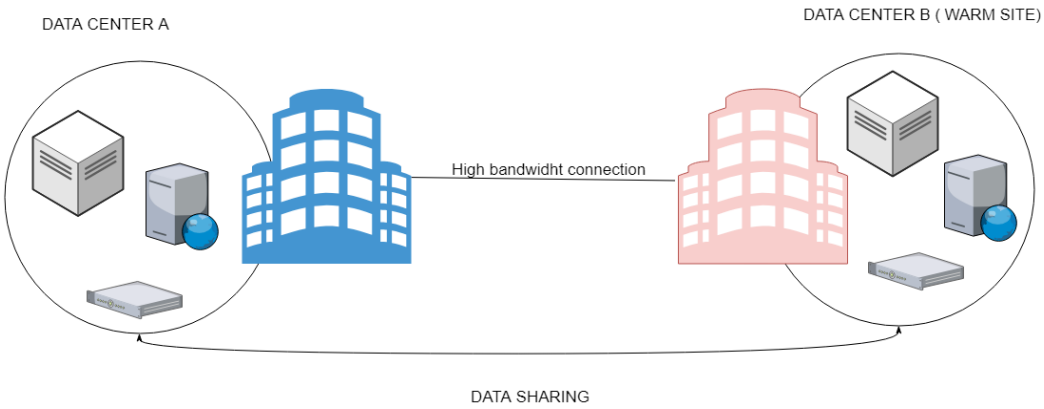
   Cold Site merupakan salah satu strategi yang dapat digunakan untuk *recovery* namun *cold site* berbeda dengan *hot site*, *cold site* tidak dipakai apabila tidak terjadi bencana, jika ingin menggunkan *cold site* maka harus melakukan *set up* koneksi serta software. Dengan begitu biaya dari *cold site* lebih rendah daripada *hot site*.



Gambar 2.10 *Cold Site*

3. *Warm Site,*

   *Warm Site h*ampir menyerupai *Hot Site* yang mempunyai *data center* yang menyerupai *data center* yang utama tetapi yang membedakannya dengan *hot site* adalah *data center warm site* tidak aktif sebelum adanya proses *fail over* .



Gambar 2.11 *Warm Site*

2.5.3 RPO (*Recovery Point Objective*)

RPO(*Recovery Point Objective*) adalah ukuran jumlah data maksimum yang hilang yang dapat diterima serta direkam oleh waktu, atau usia maksimum data yang diizinkan saat memulihkan sistem klien. RPO diukur dari saat transaksi pertama hilang atau dari saat layanan tidak tersedia. Dengan kata lain RPO adalah jumlah data yang hilang namun masih dapat ditoleransi apabila terjadi suatu gangguan. Sebagai contoh RPO dapat diasumsikan sebagai batas waktu yang digunakan sebagai titik poin untuk melakukan *recovery*. Dalam membuat suatu RPO biasa diterapkan yang dinamakan dengan SLA (*Service Level Agreement*) yang digunakan sebagai perjanjian antara penyedia layanan dan klien.

2.5.4 RTO (*Recovery Time Objective*)

RTO(*Recovery Time Objective*) adalah waktu yang dibutuhkan untuk mengembalikan data yang hilang setelah gangguan terjadi, hal ini bertujuan agar menjamin kontinuitas dari sistem tersebut, atau RTO akan menentukan jumlah waktu *downtime* yang dapat di toleransi untuk setiap *services* yang digunakan sebelum operasional kembali [23]. Dengan kata lain RTO adalah waktu yang dapat ditoleransi ketika suatu *services* sedang dalam keadaan *down* hingga *services* tersebut berjalan seperti semula kembali.

2.5.5 *Disaster Recovery Plan*

Disaster Recovery Plan (DRP) merupakan sebuah rencana yang berfokus kepada persiapan dan juga respon yang harus dilakukan ketika suatu bencana terjadi. Untuk membangun sebuah *Disaster recovery Plan* membutuhkan waktu yang cukup lama dalam pembuatannya dikarenakan butuh banyak sekali yang harus di analisis, namun sebagai permulaan dapat dibangun sebuah rencana *disaster recovery* sementara. Ada beberapa prosedur yang harus dilakukan untuk membuat sebuah rencana *disaster recovery*, sebagai berikut.

1. *Build the emergency response team*, yang pertama adalah dengan membuat sebuah *team* yang dapat membuat lingkungan *disaster recovery* sesuai dengan kebutuhan bisnis.
2. *Procedure for declaring a disaster*, yang kedua adalah membuat sebuah aturan yang dapat digunakan oleh tim yang bertugas sebagai *emergency response*

team untuk menentukan apakah sebuah situasi yang terjadi termasuk ke dalam bencana atau tidak.

3. *Invoke the DR plan*, yang ketiga adalah usaha untuk menjalankan program atau rencana yang sudah ditetapkan sebagai *disaster recovery plan* (DRP).
4. *Communicate during a disaster*, yang keempat adalah prosedur yang digunakan untuk menentukan siapa saja anggota dari *emergency response team* yang harus dihubungi ketika terjadi suatu bencana dan apa yang harus di katakana kepada media apabila diperlukan.
5. *Identify basic recovery plans*, yang kelima adalah mengidentifikasi setiap dasar dari rencana yang ditujukan untuk membuat sistem yang terkena dampak bencana kembali berjalan seperti normal.
6. *Develop processing alternatives*, yang keenam adalah membuat suatu rencana alternatif untuk menjalankan sistem yang *down* ke tempat lain yang layak untuk kembali menjalankan sistem tersebut.
7. *Enact preventive measures*, yang ketujuh adalah lankah yang harus dilakukan oleh suatu organisasi agar dapat dengan cepat dan mudah untuk membuat proses *recovery* menjadi mudah, dengan mengukur segala kemungkinan yang akan terjadi ketika adanya bencana.
8. *Document the interim DR plan*, yang kedelapan adalah seluruh rencana, prosedur, list kontak, serta informasi vital yang telah dibuat harus di bukukan atau didokumentasikan pada saat proses perencanaan.
9. *Train the emergency response team members*, yang terakhir adalah dengan melatih seluruh anggota *emergency response team* untuk menghadapi segala kemungkinan yang akan terjadi agar dapat dengan tepat mengatasi masalah yang terjadi.

Meskipun *Disaster Recovery Plan* (DRP) ini merupakan hal yang sangat penting tetapi penerapan DRP ini akan mungkin saja mengalami pertentangan dikarenakan tidak adanya ROI (*Return Of Investment*) yang diterima oleh organisasi selain dari *data security*, baik *disaster recovery* maupun *data security* hanya bertindak sebagai persiapan yang digunakan untuke menghadapi suatu bencana yang belum pasti terjadi. Ada beberapa alasan mengapa DRP harus

diterapkan dan merupakan suatu investasi yang menguntungkan pada suatu sistem, sebagai berikut.

1. *Disaster preparation and survival*, yang pertama adalah suatu *Disaster Recovery Plan* (DRP) yang mumpuni akan membuat suatu organisasi selamat dan mampu bertahan dari sebuah ancaman, hal ini didapatkan karena hasil perencanaan dan persiapan yang matang.
2. *Disaster Avoidance*, yang kedua adalah *Disaster Recovery Planning* (DRP) sering kali merujuk kepada peningkatan sebuah proses dan sistem IT yang mengakibatkan sistem tersebut menjadi lebih tangguh terhadap ancaman. Berikut adalah contoh sebuah kejadian yang terjadi dengan menggunkan DRP dan yang tidak.

Tabel 2.2 Contoh kejadian dengan DRP dan non-DRP

Kejadian dengan DRP dan tanpa DRP		
Kejadian	**Tanpa DRP**	**Dengan DRP**
Server Crash dan *data Corruption*	Membutuhkan waktu yang lama untuk membangun ulang data dari media *backup.*	Dapat langsung melakukan *recovery data* yang bersumber dari media *backup.*
Angin topan, gunung Meletus, dan Tsunami	Mengalami padam listrik dengan waktu yang cukup lama.	Mengalihkan seluruh pemrosessan kedalam *server* alternatif
Gempa Bumi	Kerusakan dari *server* dan ditambah dengan padam nya listrik untuk waktu yang lama	Kerusakan pada *server* dapat diminimalisir dengan pembuatan struktur bangunan yang sesuai standar, memiliki *power supply* cadangan yang dapat digunakan untuk *backup* aliran listrik.
Kebakaran	Kerusakan dari *server* yang diakibatkan oleh asap yang membutuhkan waktu yang lama untuk *restore* data dari media *backup.*	Adanya sistem pencegahan dan pendeteksi api serta asap yang terpasang sehingga dapat meminimalisir dampak yang terjadi.
Sabotasi	Membutuhkan waktu yang lama untuk	Dapat langsung melakukan *recovery*

	memperbaiki data yang *corrupt*	dikarenakan sudah memiliki *backup.*
Banjir	Server harus dipindahkan dan secara tidak langsung harus dimatikan.	Mengalihkan seluruh pemrosessan kedalam *server* alternatif
Cuaca Buruk, yang menyebabkan peningkatan daya listrik	Tidak adanya cadangan dari *power supply* yang mengakibatkan *downtime* yang lama	Terdapat *backup* dari *power supply* alternatif sehingga *downtime* dapat dimimalkan

3. *Due diligence and due care*, yang ketiga adalah organisasi yang belum pernah sama sekali mengalami kehilangan data atau mengalami *data corrupt* biasanya akan mengabaikan DRP, dengan mengabaikan kebutuhan akan DRP akan menjadi masalah yag serius jika suatu saat terjadi sebuah ancaman atau bencana [24].

2.5.6 Business Continuity Plan

Business Continuity Plan (BCP) adalah proses yang terlibat dalam menciptakan sistem pencegahan dan pemulihan dari potensi ancaman terhadap perusahaan. Rencana tersebut memastikan bahwa personel dan aset dilindungi, dan dapat berfungsi dengan cepat jika terjadi bencana, BCP akan mendefinisikan setiap resiko yang dapat mempengaruhi kinerja dari perusahaan, sehingga BCP sangatlah penting bagi suatu perusahaan sebagai bagian dari strategi manajemen resiko, resiko disini termasuk bencana alam seperti banjir dan kebakaran, serta serangan *cyber* [25]. BCP umumnya disusun sebelumnya dan melibatkan masukan dari para *stakeholder* dan pegawai. Poin-poin yang perlu diperhatikan untuk membuat *Business Continuity Plan* yang baik adalah sebagai berikut.

1. *Contact point*

   Berisi mengenai kontak pegawai yang dapat dihubungi ketika jam kerja, diluar jam kerja, dan ketika dalam keadaan darurat.

2. *Roles* dan *responsibilities*

   Berisi tentang struktur organisasi perusahaan yang jelas yang isinya terdapat tanggung jawab serta posisi setiap pegawai yang terlibat di dalam BCP.

3. *Risk level*

   Pengkategorian dari resiko yang mungkin akan terjadi pada perusahaan.

4. *Continuity* dan *Recovery Service Levels*

   Waktu yang diperlukan untuk merespon terhadap gangguan, lalu melakukan implementasi BCP dan melakukan *recovery*.

5. *Business Continuity Reviews*

   Bagaimana dan kapan suatu instansi akan melakukan review terhadap prosedur BCP yang dibuat.

6. *Business Continuity Processes*

   Sekumpulan prosedur yang dibuat bertujuan untuk memberikan petunjuk kepada pegawai ketika gangguan terjadi, dan solusi yang harus digunakan untuk menghandel masalah tersebut.

7. *Incident Reporting* dan *Documentation*

   Metode yang digunakan untuk mendokumentasikan serta merekam insiden yang terjadi dan apa dilakukan ketika bencana terjadi.

8. *Testing*

   kriteria dan persyaratan pengujian untuk rencana pada saat terjadi bencana.

9. *Training*

   Training diperlukan oleh staf atau pegawai yang terlibat didalam BCP dan proses *Disaster recovery* berlangsung [26].

10. *Strategy*

    Strategy berkaitan dengan seluruh komponen serta objek-objek yang terkait dengna strategi yang digunakan oleh perusahaan untuk keperluan bisnis yang harus dipernuhi setiap hari dengan tetap memastikan keberlangsungan bisnis.

11. *Application and Data*

    Application and Data berkaitan dengan *software* yang digunakan untuk melaksanakan bisnis, dan juga metode yang digunakan untuk memastikan adanya *software* yang menyediakan kemampuan *high availabitliy*.

12. *Technology*

    Technology merupakan objek yang berkaitan dengan sistem yang digunakan oleh perusahaan untuk mengaktifkan fungsi *backup* untuk aplikasi dan data.

13. *Facilities*

    Facilities berkaitan dengan fasilitas infrastruktur yang dimiliki untuk menunjang kemampuan *disaster recovery* ketika sistem utama *down*.

Selain komponen yang telah disebutkan diatas *Business Continuity Plan* dapat disederhanakan menjadi tiga komponen kunci utama untuk keberlangsungan aplikasi dan proses bisnis di perusahaan [27].

1. *High Availability*

   High Availability menyediakan kemampuan untuk memastikan proses dari aplikasi akan tetap berjalan normal ketika sistem sedang *down.*

2. *Continuos operations*

   Continuous operations merupakan kemampuan pengaman yang memastikan bahwa setiap sistem akan tetap berjalan ketika adanya gangguan dengan menyediakan *backup services* yang siap untuk digunakan.

3. *Disaster Recovery* (DR)

   Disaster recovery merupakan metode untuk memulihkan *data center* ke dalam suatu sistem DR yang dipersiapkan untuk menghadapi bencana.

2.6 Command Prompt (CMD)

Command Prompt (CMD) adalah aplikasi bawaan sistem operasi Windows yang berfungsi sebagai *command line interpreter* untuk mengeksekusi perintah masukan yang biasanya berupa *script* untuk *troubleshoot*, fungsi administrasi dari Windows, nama resmi dari *Command Prompt* adalah *Windows Command Processor* [28]. Contoh *command line* yang dapat digunakan di CMD adalah ipconfig yang berguna untuk melihat ip address dari semua koneksi yang ada di Windows mulai dari *ip address* Wifi, *Ethernet*/LAN, VmNet (*ip address virtual*).

2.7 Google Chrome

Google Chrome merupakan *browser* yang dikembangkan oleh Google dan diperkenalkan pada tanggal 3 September 2008 yang merupakan versi beta dari Google Chrome di sistem operasi Windows XP keatas. Yang membuat Google Chrome saat ini menjadi aplikasi *browser* yang populer adalah kemudahan untuk digunakan ketika melakukan *surfing* di dunia maya yang menjadikan Google Chrome semakin populer, saat ini Google Chrome sudah kompatibel di berbagai

sistem opearasi baik itu di Linux, Mac OS, Android, IOS dan ChromeOS, fitur yang teradpat di Google Chrome sangat bervariasi diantaranya adalah.

1. *Incognito Mode*

   Incognito mode adalah fitur yang diberikan oleh Google Chrome yang fungsinya untuk mencegah *browser* untuk merekam segala aktivitas yang dilakukan oleh pengguna diantaranya adalah mencegah untuk menyimpan *history, cookies*, inputan, atau data situs yang dikunjungi. Tetapi aktivitas pengguna tetap terekam oleh penyedia jasa internet atau ISP.

2. *Chrome Developer Tools*

   Fitur ini berguna bagi pengguna yang sedang atau ingin mengembangkan suatu *website*, dengan menggunakan *Chrome Developer Tools* ini membuat pengguna dapat melihat serta menganalisis tampilan, komponen teknis serta melakukan inspeksi komponen dan atribut dari *website* tersebut.

3. *Bookmarks*

   Bookmarks merupakan fitur yang penting di Google Chrome yang fungsi nya adalah untuk menyimpan data situs atau *website* yang ingin dibuka kembali suatu saat tanpa perlu mencarinya terlebih dahulu di *search engine*.

4. *Support plugins/Extensions*

   Dengan adanya fitur yang mendukung penggunaan *plugin* yang dapat diinstal sert di konfigurasi dengan mudah di Google Chrome membuat pengguna semakin dimudahkan untuk menggunakan *browser* ini, contoh *plugin* yang populer digunakan adalah *Adblock, IDM, SpeedTest, dan Unsplash Instant*.

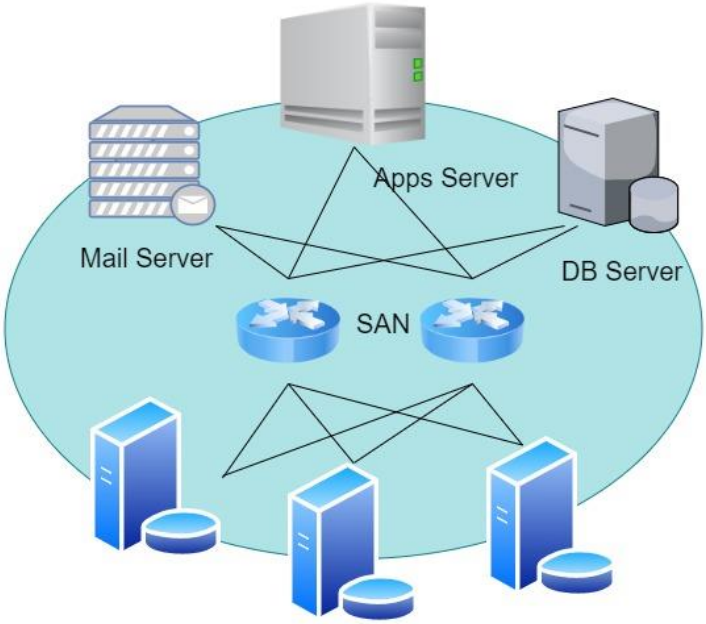
2.8 Shared Storage

Shared Storage adalah media penyimpanan data yang dapat diakses oleh banyak komputer atau *server*. Penggunaan *shared storage* dalam *data center* sangatlah penting mengingat *data center* merupakan infrastruktur strategis yang operasionalnya harus tetap dijaga agar tetap beroperasi tanpa masalah, dengan *shared storage* data yang disimpan tetap akan bisa digunakan ketika salah satu *host* atau sistem *down* dengan cara menggunakan sistem yang lain untuk menggunakan sumber daya yang disimpan di dalam *shared storage* tanpa perlu khawatir adanya

potensi data kehilangan atau kerusakan data akibat adanya sistem *down*. Ada beberapa bentuk dari *shared storage* saat ini diantaranya adalah sebagai berikut.

2.8.1 Storage Area Network (SAN)

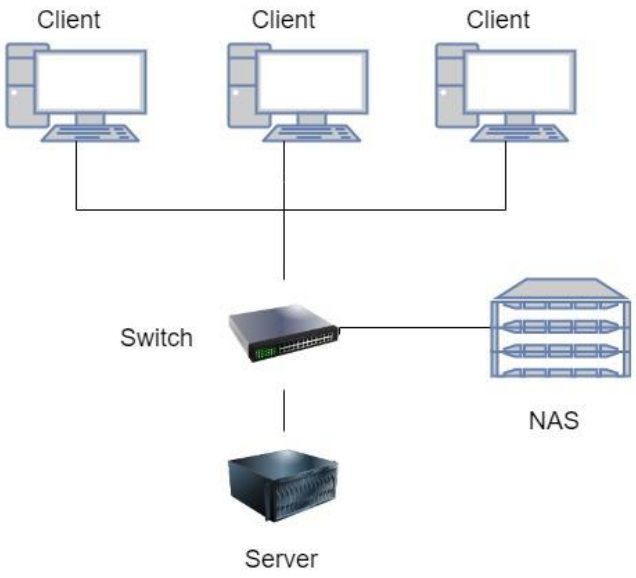
SAN merupakan media penyimpanan data yang khusus digunakan untuk meningkatkan kemampuan *high availability* dengan menggunakan koneksi internet berkecepatan tinggi, keunggulan yang diberikan SAN adalah sistem *backup* yang tersentralisasi yang tersimpan di satu disk local, selain itu SAN juga memberikan perlindungan berupa sistem *failover* yang menyediakan layanan jaringan yang berkelanjutan meskipun *server* sedang *down* [29].



Gambar 2.12 *Storage Area Network* (SAN)

2.8.2 *Network Attached Storage* (NAS)

NAS merupakan media penyimpanan yang terkoneksi dengan jaringan, pengguna yang terkoneksi dengan NAS akan dapat mengakses data dari sistem penyimpanan data yang tersentralisasi. Yang menjadi ciri khas dari NAS adalah kemudahan untuk digunakan, memiliki kapasitas yang besar dan memiliki harga relative murah.



Gambar 2.13 ***Network Attached Storage*** **(NAS)**

NAS dapat diakses melalui beberpa cara diantara nya adalah melalui jaringan local melalui FTP, selain itu mengakses NAS juga dapat dilakukan dengan menggunakan aplikasi manajemen *storage* melalui koneksi internet.

2.8.3 *Storage Server*

Storage Server merupakaan salah satu tipe dari *server storage*, namun *storage server* penggunaanya difokuskan untuk media penyimpanan yang dapat di-*share* melalui koneksi internet, *storage server* dapat juga disebut dengan *file server*.

2.8.4 *Cloud Storage*

Cloud Storage merupakan salah satu jenis *cloud computing* yang berfungsi untuk menyimpan data di suatu *server, cloud storage* mampu diakses menggunakan jaringan internet.

2.9 Fault Tolerance

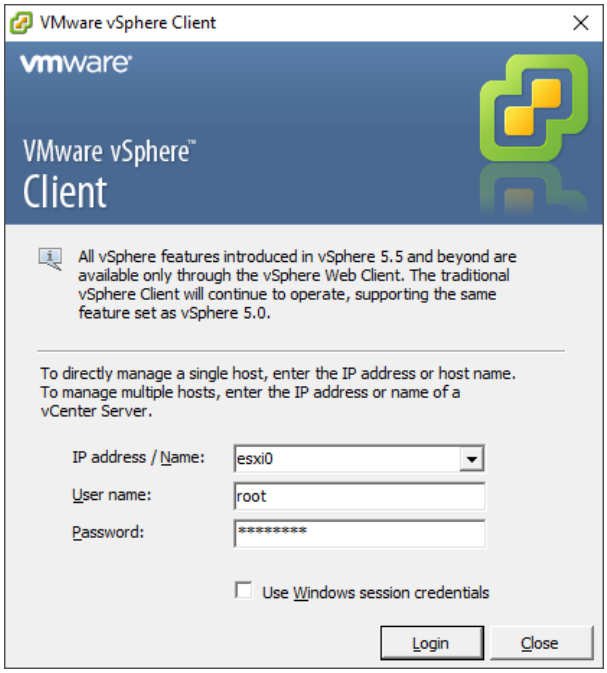
Fault tolerance adalah kemampuan perangkat atau sistem untuk memberikan pelayanan dengan dengan mentoleransi terjadinya gangguan atau kesalahan pada sistem yang dapat merusak atau membuat sistem tidak berfungsi secara normal, *Fault tolerance* akan membuat tiruan atau melakukan proses *mirroring* serta replikasi secara terus menerus terhadap sistem utama (*primary*) dan sistem cadangan (*secondary*). Sehingga apabila terjadi bencana seperti *host* yang

menampung *virtual machine primary* tiba-tiba mengalami gangguan yang mengakibatkan *host* tersebut *down*, maka *fault tolerance* akan mengambil alih atau melakukan proses *failover* untuk memindahkan operasional dari *virtual machine primary* ke dalam lokasi *virtual machine secondary* yang berbeda *host*.

Hal yang menjadi perhatian pada saat pembangunan sistem dengan kemampuan *zero downtime* atau dapat disebut juga sistem yang memiliki ketangguhan terhadap gangguan, ide utama dari pembuatan kemampuan *fault tolerance* adalah didasarkan pada kebutuhan terhadap sistem yang dapat bertahan tanpa harus adanya *maintenance* dalam waktu yang lama[30].

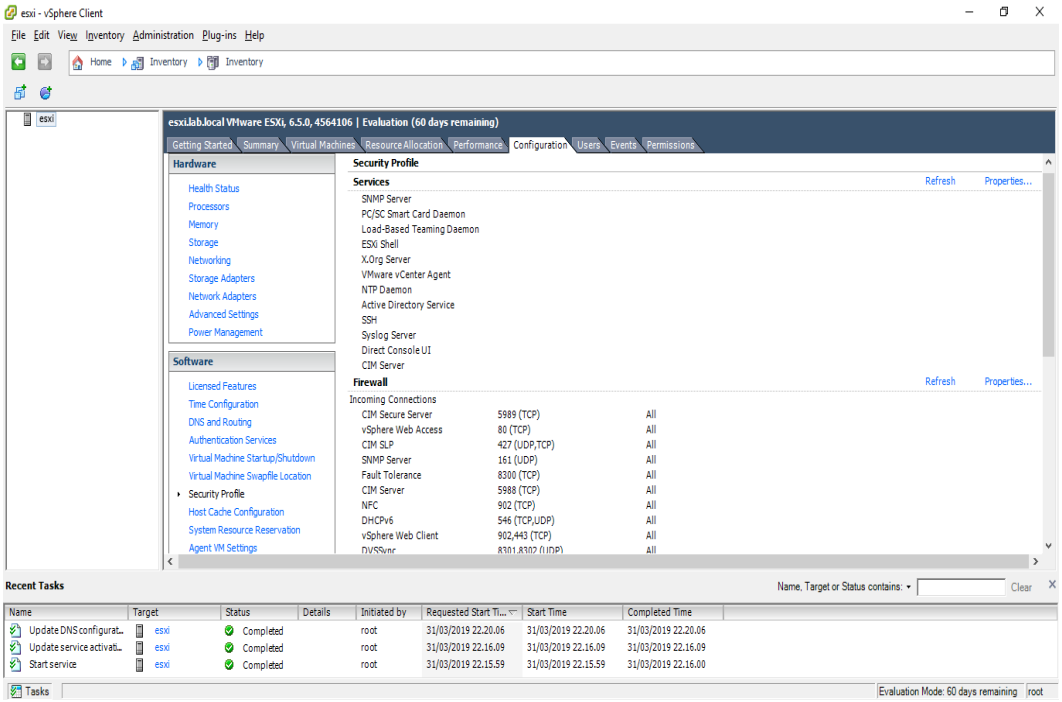
2.10 VmWare vSphere Client

VmWare vSphere Client merpauakan aplikasi yang digunakan untuk mengelola vCenter Server dan ESXi, dengan menggunakan vSphere Client dapat memberikan akses *administrator* untuk mengelola fungsi yang teradapat di vSphere tanpa harus masuk secara langsung ke *server* vSphere.



Gambar 2.14 Login ke vSphere Client

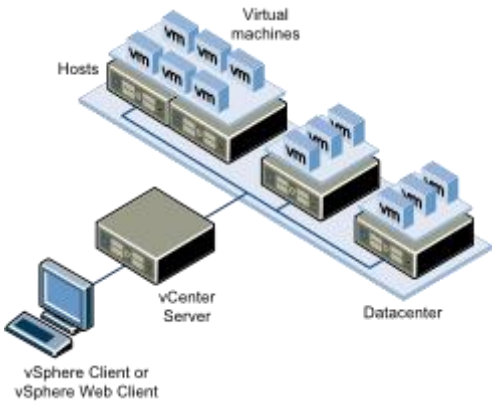
Setelah berhasil *login* maka akan masuk ke dalam vSphere yang dituju dengan tampilan seperti gambar dibawah ini.



Gambar 2.15 Tampilan awal vSphere Client

2.11 vCenter Server

VmWare vCenter Server adalah aplikasi manajemen serta monitoring *data center* yang dikembangkan oleh VmWare, vCenter Server memberikan sistem yang tersentralisasi untuk manajemen serta operasi dari kumpulan *virtual machine* yang tergabung dalam lingkup vSphere, dengan menggunakan vCenter Server seorang administrator sistem akan dengan mudah untuk mengatur sumber daya serta dengan mudah melakukan evaluasi performa *virtual machine* yang berada di dalam *virtual data center*, dengan sistem informasi yang berisikan tentang seluruh detail mengenai *server* dan *resource* yang digunakan untuk simulasi *data center*[31].



Gambar 2.16 vCenter Server dalam vSphere

Sebuah *virtual data center* membutuhkan vCenter Server sebagai aplikasi untuk manajemen sumber daya yang digunakan di *data center* tersebut, fitur yang dimiliki oleh vCenter Server sangat membantu dalam manajemen *data center* fitur tersebut sebagai berikut [5][32].

1. *Simple Deployment*

   Proses *deployment* akan menjadi sangat sederhana.
2. *Extensible and Sclability Across Hybrid Cloud*

   Dengan vCenter Server akan mempermudah dalam proses *upgrade* ke dalam sistem *cloud* vSphere.
3. *Centralized Control and Visiblity*

   vCenter Server akan memberikan kemampuan untuk melakukan administrasi seluruh infrastruktur vSphere ke dalam satu lokasi, dengan didukung vSphere Client berbasiskan HTML5 sehingga dapat digunakan di segala jenis *browser*.
4. *Improved Management*

   Penggunaan vCenter Server akan meningkatkan manajemen *virtual machine* dengan berbagai macam fitur yang ditujukan untuk mempermudah manajemen sistem.
5. *Proactive Optimization*

   Dengan menggunakan vCenter Server seorang administrator sistem dapat melakukan manajemen hingga 70.000 *virtual machine* dan 5000 *host*. Penggunaan vCenter Server dapat menggunakan fitur *vSphere HA* dan DRS *cluster.*

6. *Plug-in Extensibility*

   VmWare vCenter Server memungkinkan administrator sistem untuk melakukan konfigurasi aplikasi pihak ketiga dengan menggunakan vCenter Server, berikut adalah plug-in yang telah didukung oleh vCenter Server.

   a. Dell EMC OpenManagement Integration for VMware vCenter
   b. Huawei Technologies Storage NGC (Flex and HTML 5)
   c. IBM Storage Enhancements for vSphere
   d. IBM Spectrum Protect vSphere Web Client
   e. Infinidat Powertools (HTML 5)
   f. Lenovo XClarity Integrator for VMware vCenter
   g. NimbleStorage vSphere Web Client
   h. StorMagic [33].

2.12 vCenter Server Appliance (VCSA)

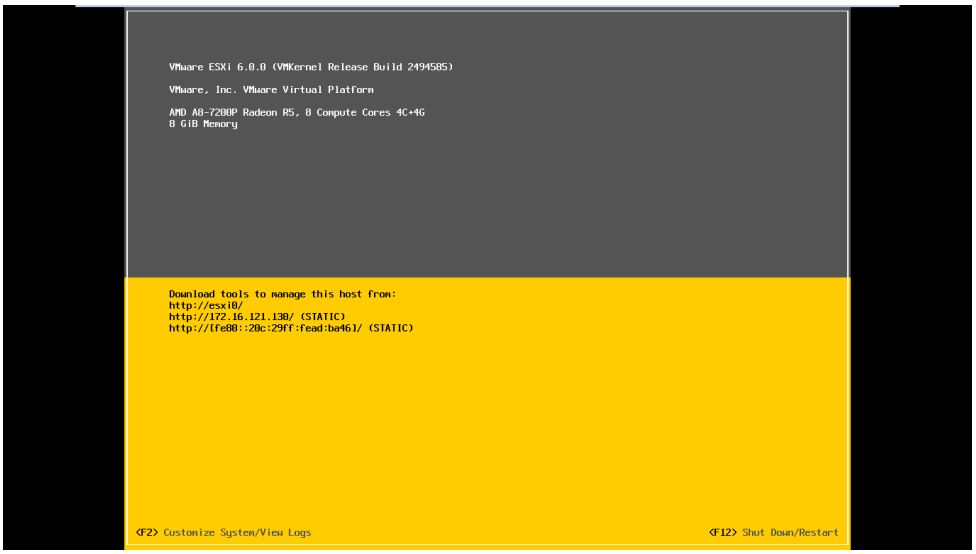
vCenter Server Appliance merupakan sistem manajemen buatan VMware yang berfungsi sebagai aplikasi untuk melakukan manajemen *virtual machine* atau *data center*, vCenter Server Appliance berupa *virtual machine* yang berbasiskan Linux yang telah dikonfigurasi ulang untuk memaksimalkan untuk melakukan manajemen vCenter Server, vCenter Server Appliance menggunakan *database* PostGreSQLyang tertanam didalam sistem vCenter Server Appliance.

Jika pada proses pembangunan *data center* menggunakan fitur vCenter HA maka vCenter Server Appliance akan membuat *virtual machine* yang baru yang berfungsi sebagai tempat untuk melakukan *failover* dan monitor vCenter Server Appliance. *Virtual machine* tersebut dapat juga disebut sebagai vCenter Server Appliance-peer (VCSA-peer) yang berfungsi sebagai *passive node* pada vCenter HA, sedangkan vCenter Server Appliance-Witness (VCSA-Witness) yang berfungsi sebagai pengawas antara VCSA dan VCSA-peer ketika terjadi proses *failover*.

2.13 VmWare ESXi

VmWare ESXi merupakan sistem operasi yang berbasiskan *hypervisor* tipe 1 yaitu *bare-metal* yang artinya dapat berdiri sendiri tanpa sistem operasi lain, ESXi sendiri merupakan singkatan dari *Elastic Sky X Integrated* yang dikembangkan oleh

VmWare, penamaan ESXi pada awalnya merupakan hasil dari pengembangan dari VmWare ESX hingga versi 4.1 yang pada akhir nya berhenti pada versi 5, VmWare kemudian melanjutkan pengembangan ke ESXi hingga versi terbarunya saat ini sudah mencapai versi 6.7.



Gambar 2.17 VmWare ESXi versi 6.0

Fitur yang diberikan oleh VMware ESXi adalah ketika ESXi diterapkan pada suatu *data center* akan sangat mudah dan cepat dikarenakan ukuran dari ESXi ini ringan, peningkatan keamanan dengan kemampuan enkripsi yang kuat serta akses berdasarkan *role* yang diterima tiap *user*, performa yang dapat mengakomodasi setiap aplikasi hingga 128 CPU *virtual*, 6 TB RAM, serta 120 *devices* yang diperlukan [34], dan ESXi menggunakan GUI yang mudah dimengerti sehingga mengelola nya jadi lebih mudah, dengan dibantu menggunakan VmWare vSphere Client.

2.14 VMware Workstation

VMware Workstation adalah aplikasi *open source* yang dikembangkan oleh VMware yang pada tahun 1999, yang dikembangkan agar pengguna dapat membuat *virtual machine* di dalam satu mesin atau komputer dan menggunakanya pada saat yang bersamaan dimana *virtual machine* tersebut dapat menggunakan sistem operasi nya masing-masing. VMware Workstation merupakan *hypervisor* yang dapat digunakan pada sistem operasi dengan arsitektur x64 Windows atau Linux.

Varian yang terdapat di pasaran saat ini adalah varian VMware Workstation Player yaitu varian yang tidak berbayar atau bukan untuk penggunaan komersial, sedangkan VMware Workstation Pro adalah varian yang dapat digunakan dengan masa uji coba gratis selama tiga puluh hari sebelum dikenakan biaya penggunaan.

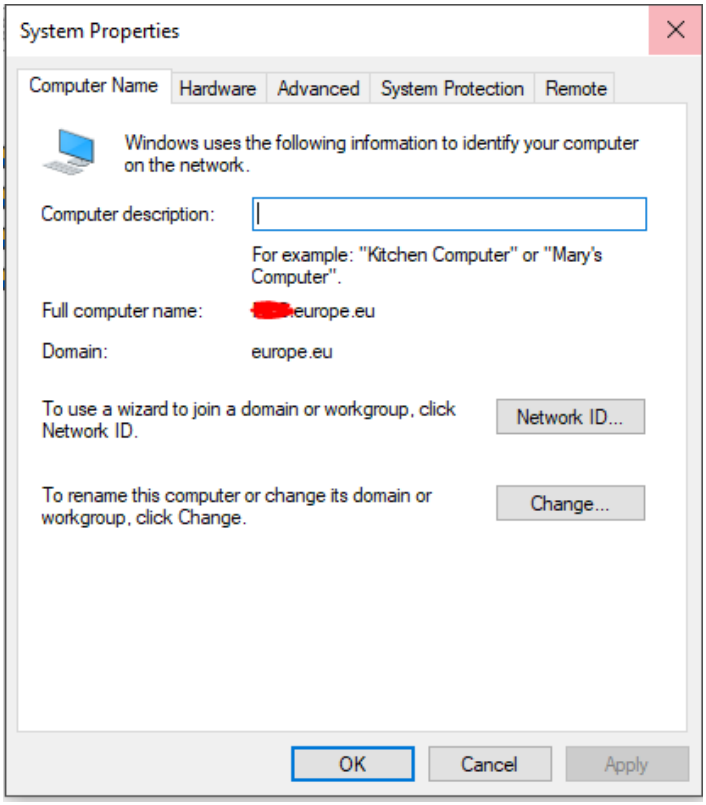
2.15 Windows Server 2012 R2

Windows Server 2012 R2 merupakan sistem operasi buatan Microsoft yang merupakan pengembangan dari Windows 8 yang ditujukan untuk sistem operasi *server*. Pada versi 2012 R2 telah menerima banyak pembaruan sistem diantaranya adalah Windows Server 2012 R2 sudah mendukung Hyper-V3.0 yang meemberikan keuntungan dalam proses skalabilitas, lalu adanya pembaruan dalam sistem *active directory* dimana pada versi 2012 R2 memungkinkan untuk seorang *administrator* sistem mempromosikan *server* berbasis *cloud* ke dalam *domain controller* tanpa harus melakukan konfigurasi pada *server* tersebut.

2.16 FQDN (*Fully Qualified Domain Name*)

Fully Qualified Domain Name (FQDN) merupakan struktur lengkap dari sebuah *domain name* yang digunakan untuk sebuah komputer atau *host.* FQDN akan merepresentasikan tiga level hirarki DNS(*Domain Name System*), sebuah alamat FQDN komputer atau *host* akan memiliki alamat unik sehingga perangkat tersebut dapat diakses melalui internet. Contoh penggunaan dari sebuah FQDN adalah ketika membutuhkan sebuah akses protokol dengan menggunakan FTP maka harus menggunakan sebuah FQDN atau IP Address sebagai alamat tujuan nya. Sebuah FQDN memiliki komposisi yang terdiri dari [*hostname*].[*domain*].[*tld*], contoh dari alamat FQDN adalah seperti ***esxi.europe.eu*** yang dimana esxi merupakan *hostname,* lalu *europe* adalah *domain*, dan *eu* merupkan tld.

Untuk melakukan pengaturan FQDN pada sistem operasi Windows dapat melalui *control panel* → *All Control Panel Items* → *System* → *Advanced System Settings* seperti pada gambar dibawah ini.



Gambar 2.18 *Setting* FQDN pada sistem operasi Windows

2.17 vSphere Replication 8.0.0

VMware vSphere Replication merupakan sistem replikasi buatan VMware yang merupakan ekstensi untuk WMware vCenter Server, vSphere Replication menyediakan *virtual machine* berbasiskan *hypervisor* yang berguna untuk melakukan replikasi dan *recovery* sistem. vSphere Replication melindungi setiap *virtual machine* yang telah di *register* didalam sistem replikasi agar dapat terlindungi ketika terjadi sistem *down* dengan cara mereplikasi *virtual machine* dari lokasi primer ke lokasi sekunder.

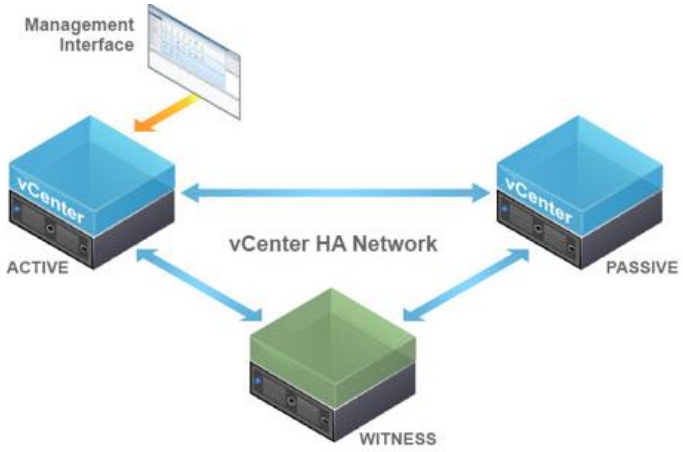
vSphere Replication menyediakan beberapa keuntungan yang diberikan ketika sudah di implementasikan ke dalam sistem diataranya adalah sebagai berikut.

a. Perlindungan data dengan biaya yang lebih rendah per *virtual machine*.
b. Solusi replikasi yang flexibel terhadap media penyimpanan pada lokasi primer dan lokasi sekunder.
c. Biaya keseluruhan yang rendah pada setiap replikasi.
d. Replikasi yang cepat dan efisien [35].

2.18 vCenter HA

vCenter HA merupakan salah satu bagian dari vCenter Server yang memiliki peran sangat penting untuk menjaga ketersediaan dari vCenter Server. vCenter HA pertama kali diperkenalkan pada sistem vSphere 6.5 yang hanya terdapat pada versi vcenter VCSA. vCenter HA berfungsi ketika *node* utama dari vCenter Server mengalami sistem *crash* pada saat beroperasi, maka vCenter HA akan otomatis mengambil alih seluruh proses dan memindahkannya ke dalam *node* pasif sehingga vCenter akan kembali berjalan normal.

Komponen yang membangun sebuah vCenter HA terdiri dari *Active node*, *Passive node* ,dan *Witness node* , vCenter HA membutuhkan jaringan yang berbeda dari jaringan *management* vCenter agar proses *failover* tidak membebankan jaringan *management*



Gambar 2.19 Topologi vCenter HA / VCHA

Active node dalam VCHA berfungsi sebagai tempat utama vCenter Server yang sedang berjalan, dengan terus melaukan replikasi data ke *passive node* dengan menggunakan jaringan khusus vCenter HA untuk berkomunikasi dengan *Passive node* dan *Witness node*. *Passive node* merupakan tiruan dari *Active node* yang tercipta pada saat vCenter HA dikonfigurasi, *Passive node* akan terus menerima *update* dan sinkronisasi dari *Active node* melalui jaringan vCenter HA, agar pada saat vCenter pada *Active node* mengalami *crash* maka *passive node* akan dapat mengambil alih fungsi vCenter Server. Sedangkan *Witness node* berfungsi sebagai

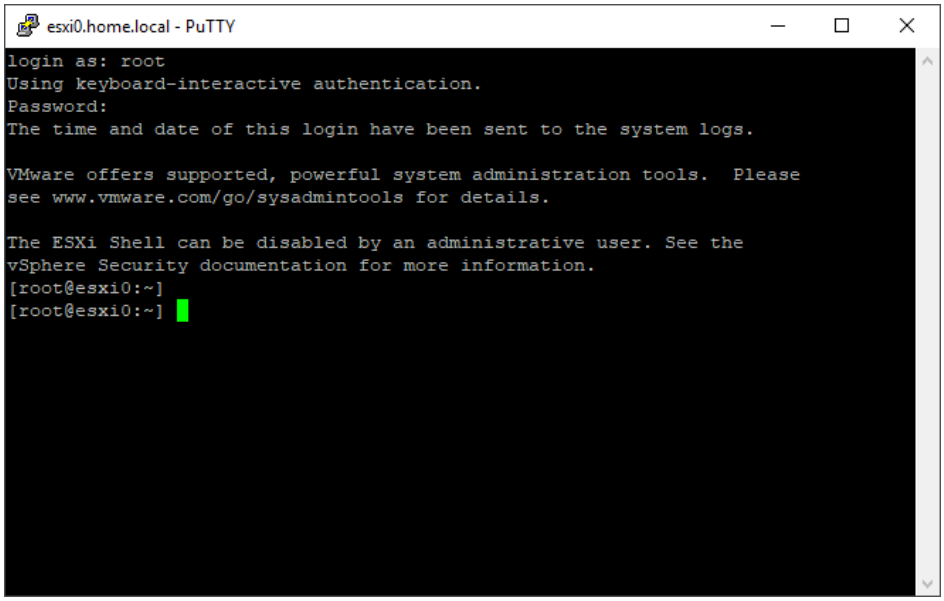
pengawas antara *active* dan *passive node* ketika keduanya tidak dapat berkomunikasi.

2.19 Lenovo xClarity

Lenovo xClarity merupakan *plug-in* buatan Lenovo untuk VMware vCenter Server, dengan menggunakan Lenovo xclarity yang diinstall di dalam sistem vCenter Server maka akan menyediakan *services* yang berguna untuk salah satu fitur yang dimiliki oleh vCenter Server yaitu *Proactive HA* yang dimana xclarity akan bertindak sebagai *provider* untuk parameter kesehatan *virtual machine, host*, dan *cluster* didalam vCenter Server. Agar dapat menggunakan *plug-in* ini diharuskan untuk menginstall Lenovo xclarity integrator untuk melakukan konfigurasi jaringan koneksi dengan vCener Server dan Lenovo xclarity administrator untuk sistem *management resource* yang telah tersentralisasi yang ditujukan untuk mengurangi kompleksitas, dan meningkatkan ketersediaan terhadap *server* .

2.20 PuTTY

PuTTY merupakan aplikasi *open source* yang dikembangkan Simon Tatham dan pertama kali diluncurkan pada tanggal 8 Januari 1999, PuTTY sendiri adalah aplikasi yang dapat membuat penggunanya untuk melakukan komunikasi serta terknoneksi secara *remote* kedalam sistem yang berbeda-beda melalui berbagai macam protokol komunikasi [36], penggunaan PuTTY biasanya digunakan untuk melakukan koneksi antara sistem UNIX dan Windows, dengan menggunakan PuTTY penggunannya dapat mengkontrol serta terkoneksi kedalam sistem UNIX tersebut melalui *console* PuTTY di sistem operasi Windows. Berikut adalah contoh apliakasi PuTTY yang telah terkoneksi dengan *host* ESXi yang dijalankan di sistem operasi Windows.



Gambar 2.20 Koneksi PuTTY dan ESXi

Dapat dilihat pada gambar 13 terdapat label **esxi0.home.local** yang merupakan *domain* dari *host* ESXi yang telah terkoneksi via PuTTY sehingga pengguna dapat melakukan konfigurasi *host* ESXi melalui aplikasi PuTTY ini.