

LECTURE NOTES

Storage Management & Backup Recovery

Taslim Rochmadi, Ir., Dipl.Ing., Dr.

taslim@binus.ac.id



LEARNING OUTCOMES

1. Peserta diharapkan mampu mengidentifikasi deskripsi dari storage manajemen, backup dan recovery
2. Peserta diharapkan mengerti fungsi storage manajemen, manajemen backup serta recovery
3. Peserta dapat mengerti tentang bisnis continuity planning untuk itu bisa mengerti penggunaan storage, backup serta pelaksanaan recovery

OUTLINE MATERI :

1. Pengertian Manajemen storage
2. Pelaksanaan manajemen backup
3. Strategy backup
4. Disasters
5. Common enterprise risk
6. Pelaksanaan manajemen recovery
7. Urutan proses manajemen recovery
8. Pengertian Manajemen kontinuitas kerja perusahaan
9. BCP

ISI

Storage Management

- Enterprise Storage adalah suatu bidang pada teknologi informasi yang terfokus pada penyimpanan, perlindungan, dan pengambilan data dalam skala besar lingkungan.
- Disk Mirroring adalah penulisan data secara simultan ke dua disk atau banyak disk secara real time untuk memberikan redundansi 100% dari media penyimpanan.
- Replikasi adalah duplikasi data yang tersimpan melalui / pada jarak yang jauh.
- Backup adalah pekerjaan yang mengacu pada penyalinan file data untuk beberapa jenis media yang terpisah untuk perlindungan data dan untuk memfasilitasi pemulihan file, bila terjadi kerusakan.
- Pengarsipan adalah cara praktis/ sederhana untuk menyimpan dan menjaga data yang jarang digunakan dengan cara off-line, dan disusun dalam struktur terorganisasi untuk memudahkan pencarian lokasi dan pengambilan kembali/retrieval.
- Disaster Recovery/Pemulihan bencana adalah perencanaan yang komprehensif dan terstruktur dengan membentuk redundant komputer yang dapat digunakan untuk melindungi data dari bencana yang bersifat lokal.
- Problem Deskripsi

Process managing storage

- Capacity
- Performance
- Reliability
- Recoverability

Definition of Storage Management:

Manajemen penyimpanan adalah proses yang digunakan untuk mengoptimalkan penggunaan perangkat penyimpanan dan untuk melindungi integritas data bagi setiap media dimana ia berada.

Storage management capacity

- Providing sufficient data storage to authorized user at a resonable cost

Penyediaan data penyimpanan ini dalam rangka pemberian fasilitas, dimana data disimpan perusahaan dalam rangka penggunaan lebih lanjut.

- Alternative storage

Penyediaan penyimpanan data yang digunakan sebagai alternative, bila penyimpanan utama terdapat masalah.

- Utilization of large capacity storage device

Pemanfaatan dari storage dengan kapasitas yang telah tersedia, berapa bagian yang dipergunakan.

- Monitor disk space usage

Memonitor penggunaan space dari memori disk, untuk melihat karakteristiknya lebih detail

Storage Management Performance

- Performance considerations at processor side
 - Size and type of processor main memory
 - Number and size of buffers
 - Size of swap space
 - Number and type of channels
 - Device controller configuration
 - Logical volume groups

- Amount of disk array cache memory
- Storage area network(SAN)
- Network attached storage (NAS)

Storage management Reliability

- Disk configuration
 - Redundant array of inexpensive disk (RAID)
- Storage management recoverability
 - Backup
 - recovery

SAN

- Suatu network local dengan kanal fiber yang terlayani dengan switch
- Fabrics biasanya adalah dibagi oleh zonasi Fibre Channel, yang berguna untuk mencegah setiap server dari mengakses penyimpanan mereka serta tidak diperbolehkan untuk menggunakan.
- Setiap Fabric mempunyai name server sederhana yang mengelola login port dan berperan dalam proses zonasi
- Switch di dalam fabric dapat dihubungkan satu sama lain dengan menggunakan satu atau lebih ISLs (Inter Switch Link), ini untuk menyediakan ekspansi fabric tambahan dan port over-subscription
- zonasi fiber Channel segment, server, dan penyimpanan, menjadi kelompok-kelompok yang terisolasi yang tidak dapat mengakses penyimpanan yang tidak sah/bukan miliknya

There are two main methods of zoning, hard and soft, and two sets of attributes, name and port.

- Soft Zoning atau zonasi Lunak membatasi akses ke penyimpanan melalui hak akses, yang disimpan dalam switch Simple Name, zonasi tidak dilakukan dengan perangkat keras, dan jika sumber (resource) sudah tahu lokasi perangkat, maka ia dapat mengaksesnya.

- Hard zoning atau zonasi keras membatasi komunikasi aktual di seluruh fabric melalui hardware routing yang ada dalam saklar switch (hardware). Unauthorized akses tidak diijinkan ke penyimpanan.
- Port Zoning atau Port zonasi membatasi port dari berbicara dengan port yang tidak sah dengan menetapkan mana dari nomor port yang diperbolehkan dalam zona.
- Zonasi Nama ini membatasi akses berdasarkan Nama secara World Wide, yang dikelola oleh Name Server Sederhana.
- sistem NAS adalah perangkat penyimpanan yang dapat diakses melalui jaringan Ethernet standar.
- Perangkat NAS menjadi system logis (logical system) untuk penyimpanan file bagi jaringan area lokal.
- NAS dikembangkan untuk menjawab permasalahan yang mempunyai kompleksitas dan biaya lebih tinggi yang terkait dengan sistem SAN, misal untuk jarak yang agak jauh atau hal lainnya/ ini berarti NAS ingin mengurangi kompleksitas dan biaya.
- Harga alat NAS biasanya jauh lebih rendah dibandingkan penyimpanan SAN yang setara, karena harga komoditas yang berbasis jaringan.

RAID

- RAID, berarti redundant array disk yang murah, (kemudian dikenal sebagai redundant array of independent disk,) adalah sistem penyimpanan yang menggunakan beberapa hard drive untuk muncul sebagai sebuah disk logis/ tunggal ke server.
- RAID menggabungkan beberapa hard drive dengan system paritas, atau mekanisme koreksi kesalahan, untuk melindungi data dari kegagalan setiap disk yang ada/ individual disk.
- RAID memiliki beberapa tingkat, sesuai kebutuhan; dipakai untuk memenuhi spesifikasi dengan karakteristik kinerja dalam Raid itu sendiri (kebutuhan itu yaitu - 100% perlindungan, kinerja maksimum, transfer kecepatan tinggi gambar, baik secara keseluruhan membaca / menulis kinerja, dll)
- Enam tingkat atau RAID awalnya ditentukan. Saat ini ada lebih dari selusin kombinasi yang berbeda dari enam tingkat asli, ini dapat diperoleh dari modifikasi tingkat asli, dan definisi dari vendor RAID.
- Satu atau lebih user-definable-RAID adalah inti dari subsistem penyimpanan yang paling modern.

Tingkat RAID paling sering dilaksanakan meliputi:

The most commonly implemented RAID levels include:

- RAID 0: Striped without data protection (JBOD – Just a Bunch of Disks)
- RAID 1: Mirrored (100% redundancy)
- RAID 3: Striped data (dedicated parity disk)
- RAID 5: Striped (parity evenly distributed across disks)

Common nested RAID levels:

- RAID 6: Striped data with parity blocks distributed across two disks
- RAID 01: A mirrored set of striped disks
- RAID 10: A striped set of mirrored disks
- RAID 30: A stripe across dedicated parity RAID systems
- RAID 100: A stripe of a stripe of mirrors

RAID configuration metrics include:

- Failure rate
- Mean time to data loss (MTTDL)
- Mean time to recovery (MTTR)
- Unrecoverable bit error rate (UBE)
- Atomic Write Failure

DAS & SAN

- Direct Attached Storage (DAS) refers to digital storage directly attached to a server or workstation.
- Storage area network (SAN) is a network designed to connect computer storage such as independent disk subsystems and tape libraries to servers.
- SANs are normally built on a specialized network infrastructure specifically designed to handle storage communications.

- While SAN technology is usually considered to be a Fibre Channel fabric network using the SCSI command set, it can just as easily be structured as a network using TCP/IP over Ethernet.
- One protocol designed to create a SAN over Ethernet is iSCSI which uses the same SCSI command set over TCP/IP.
- FCP, FC-IP, iFCP, and SAS are common protocols used in a SAN.
- SAN connections include one or more servers (hosts) and one or more disk arrays, tape libraries, or other storage devices.

Tape-disk

- Tape perpustakaan/library (kadang-kadang disebut tape silo atau jukebox tape) adalah perangkat penyimpanan yang besar yang berisi tape drive satu atau lebih, sejumlah slot untuk menahan kaset tape, pembaca barcode untuk mengidentifikasi cartridge tape dan metode otomatis / robot untuk memuat kaset.
- Autoloader adalah sebuah data yang lebih kecil perangkat penyimpanan yang terdiri dari setidaknya satu tape drive (drive), sebuah metode loading kaset ke dalam drive (robot), dan tempat penyimpanan kaset (the magazine).
- Jenis lain dari autoloaders dapat beroperasi dengan Disk Optical dan CD-ROM.
- Sebuah tape drive adalah perangkat perifer yang membaca dan menulis data yang disimpan pada gulungan pita magnetik atau cartridge. Ini dapat dioperasikan di streaming atau memulai / menghentikan mode, dengan atau tanpa menjalankan kompresi data.
- Pita magnetik adalah non-volatile, penyimpanan media yang terdiri dari lapisan oksida magnetik pada strip plastik tipis.
- Magneto-optical disk dan tape storage optik menggunakan banyak konsep yang sama seperti penyimpanan magnetik, tapi tidak yang biasa adalah pita magnetik.
- Media perekaman optik digunakan terutama untuk Tulis-Sekali-Baca-banyak-kali (WORM), Write-Once-Read-Many.

Tapes and drives come in various formats. These formats include:

Digital Data Storage (DDS)

- Digital Linear Tape (DLT)
- Linear Tape-Open (LTO)
- Advanced Intelligent Tape (AIT)
- Quarter Inch Cartridge (QIC)

Primary-Secondary-Nearline-Offline

- Penyimpanan primer adalah memori internal yang dapat diakses oleh central processing unit tanpa menggunakan input komputer / saluran output.
- penyimpanan sekunder adalah memori yang tidak secara langsung melekat pada unit pengolahan sentral komputer, yang membutuhkan penggunaan masukan komputer / saluran output. Penyimpanan sekunder digunakan untuk menyimpan data yang tidak digunakan secara aktif.
- Near-line penyimpanan adalah media penyimpanan yang dapat dipanggil tanpa intervensi manual, tetapi biasanya pada cost of incurring (biaya menimbulkan penundaan) yang signifikan. (yaitu - langsung pengambilan data dari sebuah perpustakaan tape atau jukebox optik.
- Off-line penyimpanan adalah penyimpanan komputer menengah yang harus dimasukkan ke dalam drive penyimpanan oleh operator manusia sebelum komputer dapat mengakses informasi yang tersimpan di medium.

Possible Infrastructure Service Interconnections with Storage Management:

- Configuration Management
- Event Management
- Availability Management
- Performance and Capacity Management
- Operations Management
- Network Management
- Security Management
- Inventory
- Business Process Management

Service Interconnections with Storage Management

- Reporting Management
- SLA Management
- Knowledge Management
- Asset Management
- Notification and Escalation Management
- Problem Management
- Change Management

Backup Recovery

- Backup/Cadangan pada teknik komputer mengacu pada menyalin data ke media yang terpisah untuk memfasilitasi pemulihan file yang hilang atau rusak, dan untuk melindungi organisasi dari bencana besar.
- Pemulihan data adalah proses menyelamatkan data daripada keadaan rusak, gagal, media penyimpanan rusak atau tidak dapat diakses, atau ketika tidak dapat diakses secara normal.
- Backup data dilakukan pada jadwal yang didefinisikan yang menjamin proses pemulihan memenuhi persyaratan bisnis.

BACKUP MANAGEMENT

Backup strategies include:

- Snapshot Backups
- Full Backup
- Differential Backup
- Incremental Backups
- Continuous Backups (CDP)
- Disk Mirroring

Backup issue considerations:

- Backup time to completion
- Multiple media backup
- Backup software
- Hardware considerations
- Application/Database Status
- Backup Window
- Backup Resources
- Data Validation

There are six primary metrics relating to data backup:

- Recovery Point Objective (RPO)
- Backup Window
- Restore Time
- Retention Time
- Backup Validation
- Open File backup

Backup and Recovery Management

- Different roles of data backups
- Backup procedures
- Recovery strategy
- Validation and Verification

Types of backups

There are primarily six different types of backups for online and offline methodologies:

- Full backup
- Incremental backup
- Differential backup
- Mirroring
- Snapshots
- CDP

Backup Window

Space Requirements

Types of Damage

There are two types of Damage:

- Physical Damage
- Logical Damage

Techniques are used by these repair programs

- Consistency checking
- File System Structure Analysis
- Troubleshooting
- Component repair or replacement

Data compression

- Kompresi data juga disebut coding sumber, adalah proses pengkodean informasi saat menggunakan bit yang lebih sedikit (atau informasi-bearing unit lainnya) dari sebuah metode unencoded akan menggunakan melalui skema pengkodean tertentu.

Storage Devices include:

- Hard disk drive
 - SCSI Disk
 - ATA Disk
- Magnetic tape
- Magneto-optical and optical tape storage
- Optical disc
- WORM

RECOVERY MANAGEMENT

Recovery manajemen adalah suatu pengelolaan terhadap system, baik itu system bisnis maupun system untuk melakukan service tertentu, dimana bila terjadi kerusakan atas system tersebut diperlukan suatu usaha untuk mengembalikan pada posisi sebelumnya. Atau dalam hal ini adalah suatu usaha dalam mengelola setiap kerusakan menjadi baik atau sehat kembali.

Disasters

Akibat sesuatu bencana alam yang tidak dapat kita prediksi sebelumnya adalah Disaster.

Disasters are the result of an unforeseen natural event (a physical event e.g. a fire, tornado, hurricane, flood, earthquake, etc.) or the consequences of human error.

The current data protection market is characterized by several factors:

- The loss incurred by having data unavailable
- Recovery time frame

- Business continuity strategy (partial or full restoration)
- Level of data protection required by the business.

Common enterprise risks include:

- Fire
- Natural Causes (wind, earthquake, ice storm, etc.)
- Power or Communications Outages
- War and Regional Conflicts
- Terrorist Attacks
- Civil Disruptions
- System and/or Equipment Outages
- Human Error
- Computer Viruses
- Governmental or Legal Intervention
- Loss of key personnel

Preventions Against Disasters include

- Offsite Backups
- Surge Protectors
- Uninterruptible Power Supply (UPS)
- Emergency generators
- Fire prevention systems
- Anti-virus software
- Redundant computing facilities

Disaster recovery plan

A good disaster recovery plan acknowledges the following important factors:

- Customers
- Facilities
- Knowledge Workers
- Business Information
- Security of data
- Classification of data for staged recovery

Disaster Recovery Process:

- Buy new equipment (hardware) or repair or remove viruses, etc.
- Call software provider and reinstall software
- Retrieve offsite storage discs
- Reinstall all data from back-up source
- Re-enter data from the previous week or latest copy

Disaster Recovery Technology:

- Virtual Tape library
- Synchronous replication software and technology
- Virtual PBX/hosted phone service

Key Backup and Recovery Terms:

- Recovery Point Objective (RPO)
- Recovery Time Objective (RTO)

BCP

- Business Continuity Planning (BCP) is a methodology used to create a plan describing how an organization will resume critical functions either partially or completely which were interrupted within a predetermined time following a disaster or disruption.

BCP manual consists of:

1. Impact analysis

Recovery requirements consist of the following information:

- Resolution time frame
- Business requirements
- Technical requirements

2. Threat analysis - Common threats include the following:

- Disease
- Earthquake
- Fire
- Flood
- Cyber attack
- Hurricane
- Utility outage
- Terrorism

3. Definition of impact scenarios

(Note: One paper from Deloitte and Touche lists as:

- a) Emergency response (protection of life and safety)
- b) Disaster assessment (identify scope and criticality of the disaster)
- c) Short term recovery (restore critical services)
- d) Long term recovery (restore all services and capabilities)

e) Return to pre-disaster operations (fall-back process to return services to the primary data center) (RC)

Recovery requirement documentation

Recovery requirement documentation may include information on:

- Desks Manual workaround solutions (interim floor plans and user equipment needs)
- Recovery personnel (short term, long term, specialists, etc.)
- Application and data (All, or categorized by value to the business)
- Maximum outage allowed for the applications
- Peripheral requirements
- Unique business environment requirements

Disaster Recover Plan and BCP are sometimes synonymous

Disaster Recovery Plan Purpose and Objectives

hardware redundancy

The following is a list of hardware redundancy that is recommend:

- Failover or Clustered processors
- Redundant array of inexpensive disk (RAID) devices
- Dual access paths
- Dual I/O controllers
- Dual power supplies
- Uninterruptible power source (UPS)

Nature of failures include:

- Human factor
- Hardware failure
- Transaction failure

– Disaster

Outages

Outages are classified into two categories:

- Planned outages
- Unplanned outages

Availability

Availability adalah ukuran waktu yang dibutuhkan server atau proses berfungsi normal kembali, serta ukuran waktu proses pemulihan yang dibutuhkan setelah kegagalan komponen. High Availability adalah perkiraan yang setara dengan sistem dan data yang dapat tersedia hampir sepanjang waktu, 24 jam sehari, 7 hari seminggu, dan 365 hari setahun.

- Availability is a measure of the time that a server or process is functioning normally, as well as a measure of the time the recovery process requires after a component failure.
- High availability roughly equates to a system and its data available almost all the time, 24 hours a day, 7 days a week, and 365 days a year.

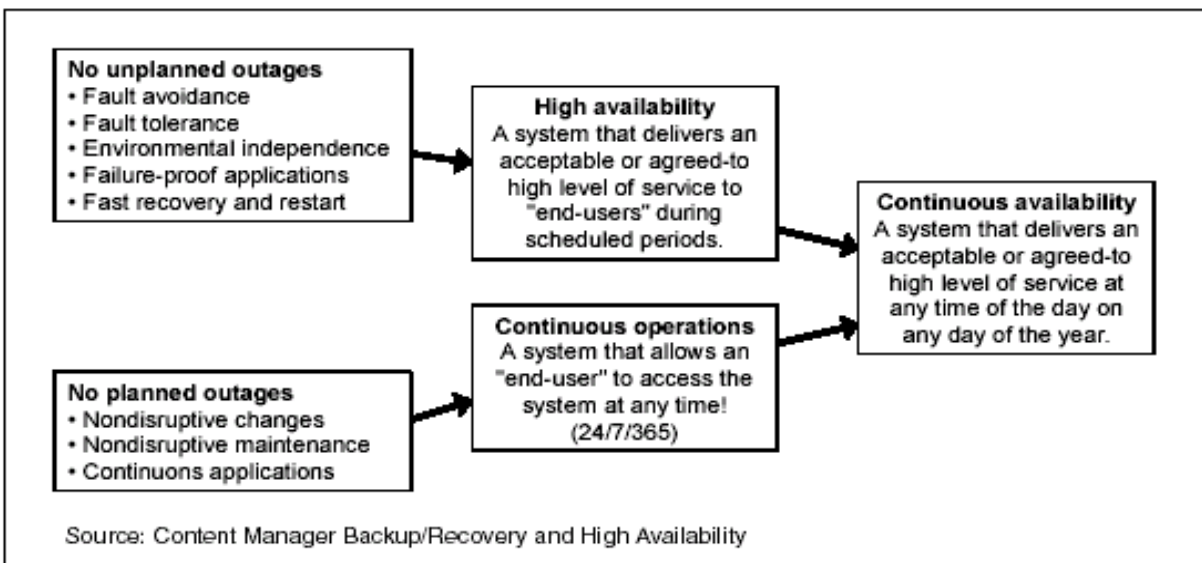


Figure 1-1 High availability and continuous availability

High Availability

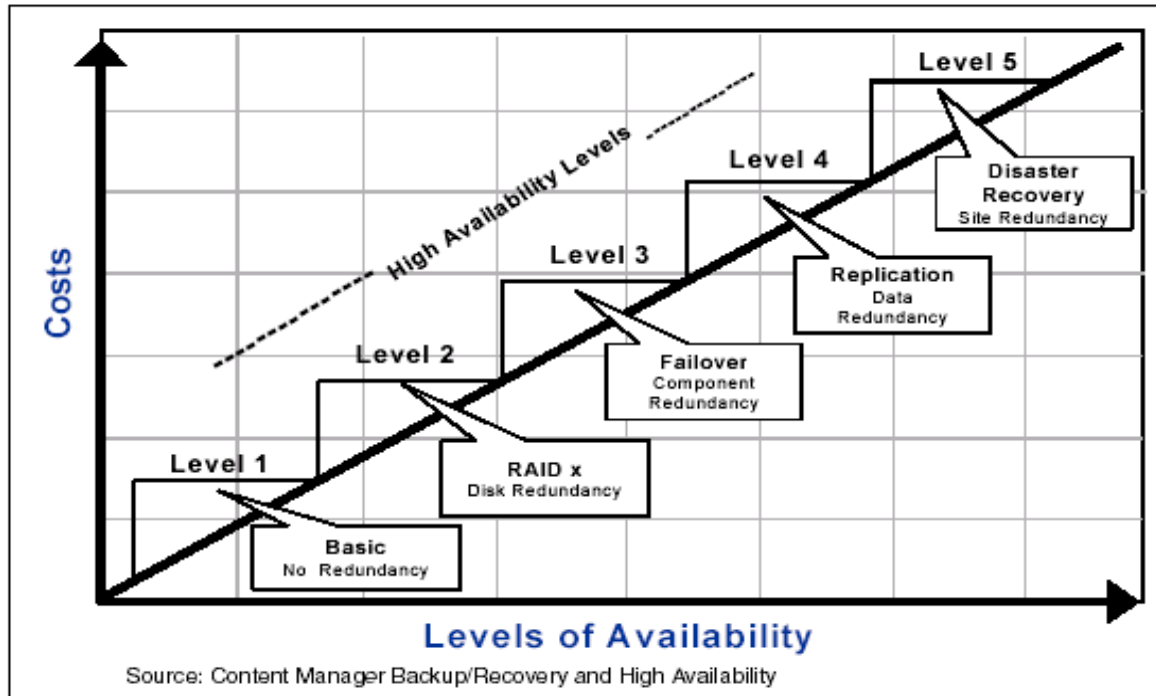


Figure 1-2 High availability tiers

Level of availability

Five level of availability are:

- Level 1: Basic systems, no redundancy
- Level 2: RAID x, disk redundancy
- Level 3: Failover, component redundancy
- Level 4: Replication, data redundancy
- Level 5: Disaster recovery

tiers of disaster recovery

The seven tiers of disaster recovery are:

- Tier 0 - No off-site data

- Tier 1 - Data backup with no hot site
- Tier 2 - Data backup with a hot site
- Tier 3 - Electronic vaulting
- Tier 4 - Point-in-time copies
- Tier 5 - Transaction integrity
- Tier 6 - Zero or little data loss
- Tier 7 - Highly automated, business-integrated solution

BCP

Business Continuity Planning (BCP) adalah metodologi yang digunakan untuk membuat rencana yang dapat menjelaskan bagaimana organisasi akan melanjutkan fungsi kritis, baik sebagian atau seluruhnya, bilamana ada yang terganggu. Dan interupsi gangguan ini dapat diperkirakan sebelumnya, serta pengembaliannya dapat diperkirakan dalam waktu yang telah ditentukan setelah bencana atau gangguan itu.

Facts about business continuity include:

Fakta yang terdapat untuk kelangsungan bisnis meliputi:

- Periode pemulihan Tradisional, yaitu 72-jam, untuk bisnis yang penting, proses pemulihan selama waktu 72 jam tidak lagi cukup baik.
- Periode pemulihan selama 4 sampai 24 jam, ini waktu pemulihan baru, dan bertujuan untuk point recovery ini telah biasa digunakan.
- Pemulihan untuk Tujuan besar, Kebutuhan ini untuk memastikan resumption and recovery dapat dilakukan, suatu pemulihan proses bisnis end-to-end di perusahaan.
- Konfigurasi Aktif / pasif antara dua lokasi untuk dapat dilakukannya pemulihan 30-60 menit.
- Untuk aplikasi paling kritis dibutuhkan Availability berkelanjutan, yaitu 24x7,

- Fakta adanya Keragaman geografis, ini sangat penting

Secara Grafis dapat diperlihatkan hubungan antara biaya dan kehilangan data dalam suatu system, atau availability yang akan diperoleh akibat ketersediaan biaya atau kemungkinan kehilangan data

Cost versus Loss

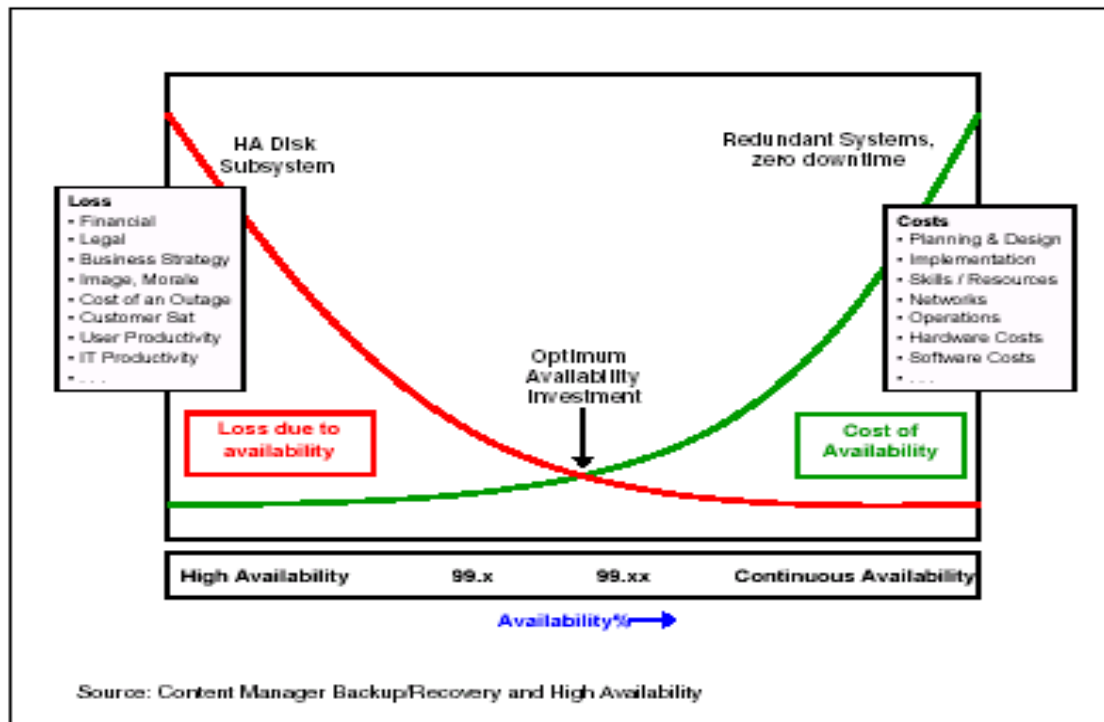


Figure 1-4 Cost versus lost

Business Continuity solution design

Suatu rancangan yang mengarah pada penyelesaian bisnis yang kontinyu, adalah bagaimana merancang sejak dari awal, kemudian layanan IT yang diterapkan dapat memberikan layanannya sebaik mungkin. Untuk itu pada saat pertama kita perlu melakukan pertanyaan berikut, sebagai dasar perencanaan yang baik.

- Berapa besar kehilangan data yg organisasi mampu untuk tetap berjalan?
- Apa tujuan titik pemulihan bagi organisasi / recovery point objective (RPO)?
- Berapa lama organisasi mampu dalam keadaan system offline ?

- Apakah tujuan waktu pemulihan bagi organisasi /recovery time objective (RTO)?

Kemudian ada faktor-faktor diantaranya adalah : yang berkontribusi biaya tinggi, factor solusi desain yang menjadikan bisnis dapat continue, infrastruktur, hubungan service dan backup; secara lengkap dapat dilihat dibawah ini.

Factors contributing to higher costs include:

- Faktor yang menjadikan biaya tinggi adalah lebih kompleknya operasional TI sebagai akibat dari pertumbuhan kapasitas penyimpanan yang eksponensial dan diversifikasi sistem operasi, missal karena pertumbuhan dari Windows ® dalam dua dekade terakhir dan munculnya Linux ® pada akhir 1990-an.
- Akibat dari Era baru e-bisnis, yang membutuhkan solusi dapat beroperasi selamanya atau 24 jam sehari, 7 hari seminggu, 365 hari setahun (7x24x365), serta terjadinya dispersi secara lebih global dalam pertukaran informasi antara situs.
- System data digital terus berkembang secara dramatis, dan lebih banyak data yang sangat penting yang digunakan untuk bisnis.
- meningkatnya kompleksitas akibat keperluan untuk perlindungan data dengan cara baru dan dengan persyaratan peraturan yang baru pula.

For a Business Continuity solution design, the following factors need to be considered:

Untuk solusi perencanaan Business Continuity, faktor-faktor berikut perlu dipertimbangkan:

- Mengkategorikan persyaratan berdasarkan nilai, terhadap bisnis yang dilakukan.
- Mengidentifikasi critical aplikasi dan critical data.
- Tentukan biaya downtime.
- Mengembangkan solusi dengan memikirkan kebutuhan dan biaya.
- Waktu Pelaksanaan.
- Provision for periodic testing/Penyisihan untuk pengujian secara berkala.

- Untuk disaster recovery /pemulihan, disesuaikan dengan strategi disaster recovery pusat data/data center , dalam hal memenuhi keseluruhan tujuan dari kelangsungan bisnis perusahaan.
- Dari 7 tiers pada disaster recovery, tier yang mana yang ingin kamu ikuti?
- Dalam High availability, mana dari 5 tingkat ketersediaan yang ingin kamu capai?

When planning for business continuity, you should consider the following:

Ketika merencanakan untuk kelangsungan bisnis, Anda harus mempertimbangkan hal berikut:

- Information-based business model.
- Transaction-based (versus batch-based) processing.
- Distributed work environment.
- People-based business.

Possible Infrastructure Service Interconnections with Backup and Recovery Management

Kemungkinan adanya hubungan atau interkoneksi antara Service Infrastruktur dengan Backup& recovery adalah:

- Configuration Management
- Event Management
- Operations Management
- Availability Management
- Performance and Capacity Management
- Network Management & Security Management
- Inventory
- Business Process Management
- Resource Management (w/ Utility Computing)

Possible Relationship Service Interconnections with Backup and Recovery

Management yang berhubungan dengan pelaksanaan antara layanan dan backup & recovery adalah :

- Reporting Management
- SLA Management
- Knowledge Management
- Asset Management
- Notification and Escalation Management
- Problem Management

SIMPULAN

Manajemen storage berubungan erat inti kepentingan perusahaan dan dengan persoalan kontinuitas kerja perusahaan. Hal ini disebabkan hampir semua system IT service didalamnya menggunakan alat penyimpan atau storage yang apabila ada gangguan padanya akan mempengaruhi system kerjanya. Operasioal IT,yang melayani system bisnis atau perusahaan dengan demikian membutuhkan manajemen pengelolaan yang baik untuk Backup dan Recovery. Karena selain fungsi menyimpan harus ada fungsi memproteksi serta me-retrieve atau memudahkan pencarian data. Dan Recovery ini adalah fungsi yang penting untuk menjadikan aktivitas tetap dapat dilakukan, karena setiap kerusakan harus dapat diselesaikan dan diperbaiki hingga kembali sehat bekerja dengan baik.

Salah satu pengelolaan yang baik bila dalam penyimpanan ini disediakan backup yang berarti memberikan redundansi atau cadangan data yang telah ada disimpan pada tempat yang berlainan. Penggunaan backup akan memberi keamanan yang baik terhadap kerusakan atau kehilangan data, serta kerusakan sistem.

Manajemen recovery pada tujuan awalnya adalah sebagai bagian dalam system untuk menjadikan system dapat bekerja normal kembali setelah terjadi kerusakan atau kesalahan. Namun dengan kemampuan manajerial backup dan recoveri ini maka fungsi bisnis dapat bekerja dengan continue.

DAFTAR PUSTAKA

1. Rich Schiesser, IT Systems Management (second edition) (2010), chapter 12 &17