



Curtin College

in association with



Curtin University



Disaster Recovery

Computer Systems 2000 (CS2000)

Trimester 2 2020

You are the IT Manager

- You get a call at 3:00AM
- This is what you see when you arrive at work



Disaster!

- The fire brigade leaves





Disaster Recovery

- Along with troubleshooting techniques, planning and implementing disaster recovery techniques are critical knowledge areas
- Server data may be threatened despite all fault tolerance measures taken.
 - *Identify both common and uncommon issues that might affect the network*
 - *list the measures to take, resources to use, and guidelines to follow before drawing up a robust recovery plan.*



Disaster Recovery Plan

- A DRP identifies steps to be performed in case:
 - *the company loses a key employee*
 - *the company is not able to access its servers*
 - *information on its network was lost*
 - *the office building was destroyed*
 - *information has been corrupted*



Disaster Recovery

- Servers are vulnerable to a multitude of threats
 - *Hackers*
 - *Natural disasters*
 - *Natural decay etc*
- A disaster is a catastrophic loss of all system functions due to an unavoidable cause.



Disaster Recovery

- The leading causes of data loss are:
 - *Hardware or System Malfunction 44%*
 - *Human Error 32%*
 - *Software Malfunction 14%*
 - *Viruses 7%*
 - *Natural Disasters 3%*



Increasing Vulnerability

- Businesses are becoming more reliant on IT
- Paper records are often not kept - all data is stored electronically
- Businesses rely on electronic communications
- IT systems are becoming increasingly complex and hard for the average person to maintain
- Viruses and hacking 'exploits' are becoming more common and more destructive
- Greater numbers of employees are being given access to corporate data, increasing the chance of damage or loss



Increasing Vulnerability

- Few corporations know the true value their data until they lose it
- Corporations are linking their computer systems to the Internet, thereby increasing the vulnerability of their data to external attack.
- The more a computer is used, the more it is relied upon. At the same time, increased use increases the likelihood of system failure.



Disaster Recovery Costing

- Consider how much mission-critical data is stored on the network, the cost (in dollars/hour) of downtime in the case of a failed server, and the data backup and restore needs of your company.
 - *Mirroring or duplexing hard drives.*
 - *Implementing a hot-swappable server.*
 - *Implementing server clustering or other high-availability solutions.*
 - *Keeping an inventory of spare server parts, such as hard drives and boards.*
 - *Replicating data to an offsite server.*
 - *Storing server backups at a remote site.*
- This justifies the infrastructure expense of the plan



Developing a DRP

- Predefine the conditions that may cause your recovery plan to go into effect:
 - *some threats are common to any system*
 - *others may be peculiar to a single organisation or location (e.g. in Australia, a bushfire plan would be critical. In Kansas, a tornado plan is important.)*
- Identify decision makers and their roles before, during and after an outage emergency
- Inventory the resources required to bring your IT systems back online
- Identify assumptions on backup technique, frequency and location for data vintage and retrieval



Developing a DRP

- Prioritise and sequence the restoration actions defined in your recovery plan into a detailed timeline and checklist
- Predefine an operation centre to coordinate status, issues and assignments
- Develop communication strategies for keeping your employees and customers informed
- Organise your recovery plan into a flexible, easily maintained tool
- Validate your recovery plan by conducting simulations based on real-life outage emergency declarations



What should a good DRP achieve?

- Provide for the safety and well-being of people on the premises at the time of a disaster
- Continue critical business operations
- Minimise the duration of a serious disruption to operations and resources (both information processing and other resources)
- Minimise immediate damage and losses
- Establish management succession and emergency powers
- Facilitate effective co-ordination of recovery tasks
- Reduce the complexity of the recovery effort
- Identify critical lines of business and supporting function



Cost of Data Loss

- IBM reports that
"Fifty percent of companies that lose critical business systems for 10 or more days never recover."
- For most companies, data is their business.
- If that data is lost or corrupted, or merely interrupted for a long enough period, the blow to the company can be fatal.
- When businesses in the following fields lost access to their data for the given time periods, 25% suffered immediate bankruptcy; 40% went bankrupt within two years and almost all were bankrupt after five years.



Cost of Data Loss

Type of Business	Average Length of Data Loss
Banking	2 Days
Commerical	3.5 Days
Industrial	5 Days
Insurance	5.5 Days



Disaster Recovery

- Disasters that effect networks fall into 3 main categories
 - *Natural disasters*
 - Fire, Storm, floods
 - Data loss usually relates to destruction of hardware
 - Best defence is good documentation and physical security of backups
 - *Data destruction*
 - Easier to recover from than natural causes
 - Results from accidental deletion, malicious attack and viruses etc
 - Key is a good quality backup regime




Disaster Recovery

- *Equipment Failure*
 - Most common cause
 - Causes loss of productivity
 - Defences include
 - Contract with vendors for stocking replacement parts
 - Stock high risk spares on premises
 - Avoid “exotic” equipment in critical systems
 - Keep hardware current (obsolete parts may be hard to source)



Disaster Recovery Plan

- A disaster recovery plan is a policy and a set of procedures that documents how people and resources will be protected in case of a disaster, and how the organisation will recover from the disaster and restore normal functioning.
- 



Recovery Objectives

- Recovery time objectives (RTO)
 - *How long can my business continue to function without the critical IT services*
 - *Or how quickly must I recover the service from the 'decision to invoke'*

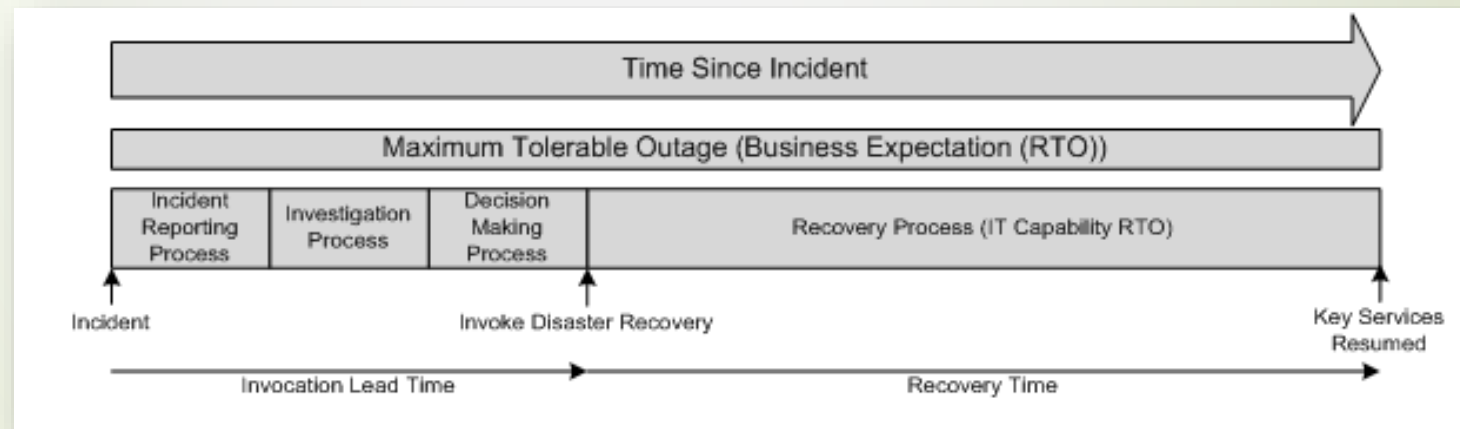


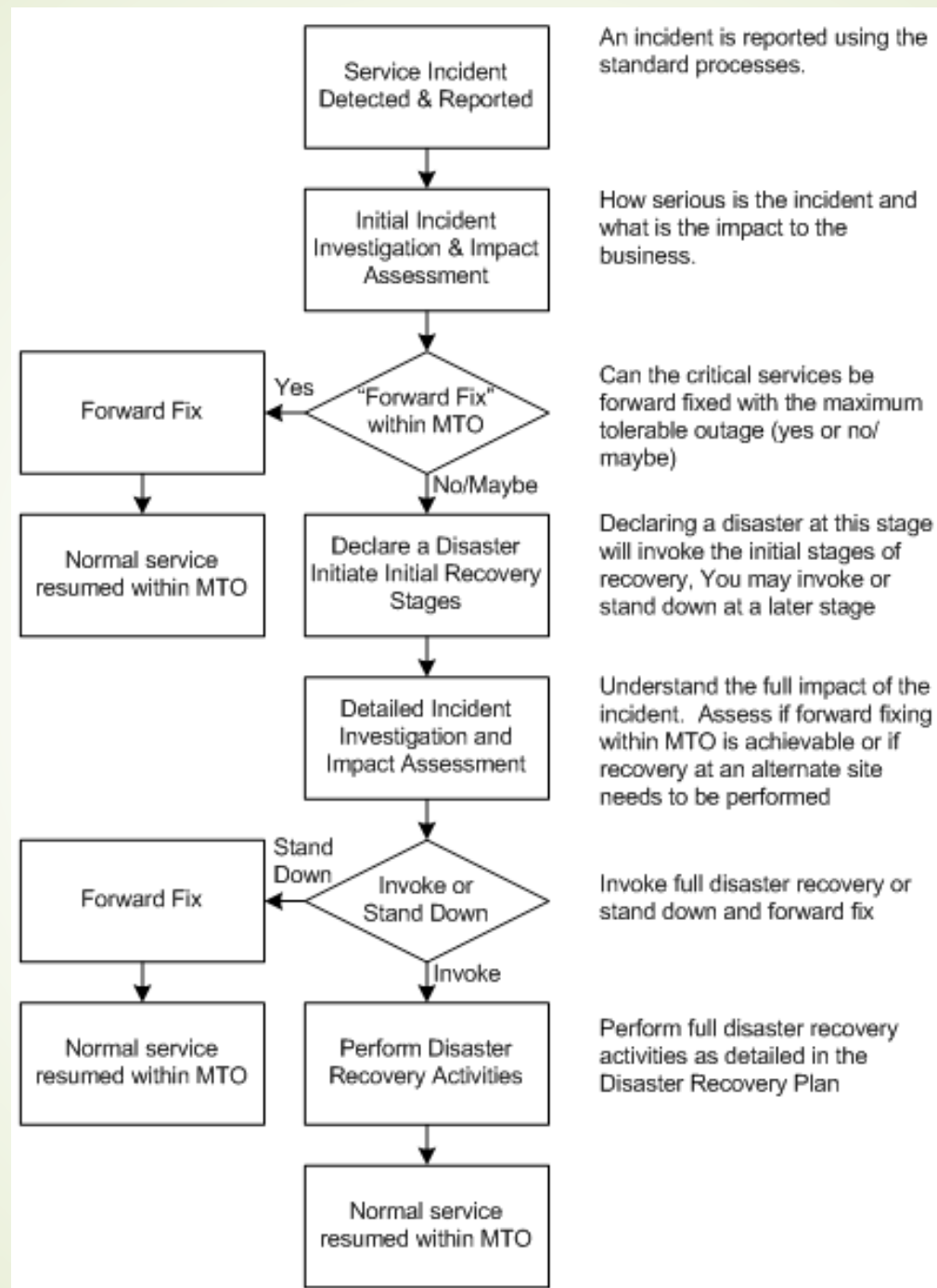
Recovery Objectives

- Recovery point objective (RPO)
 - *from what time in my processing cycle am I going to be able to recover my data (how much data am I prepared to lose or have to re-enter from an alternate source).*
 - *There are several options:*
 - zero data loss, recovery to the point of failure
 - start of the current business day (SoD)
 - end of the previous business day (EoD)
 - intraday, a point between the last available backup either SoD or EoD and the failure
 - period end, the weekly or monthly backup.

Recovery Objectives

- There is an additional measure
 - The Maximum tolerable outage (MTO) is the maximum time that a business will survive from the initial service interruption.*







Disaster Recovery

- The plan should be developed and implemented cooperatively by different functional groups.
 - *Sysadmins*
 - *Vendors*
 - *Management*
- The disaster recovery plan incorporates many components, including:
 - *A complete list of responsible individuals.*
 - *A critical hardware and software inventory.*
 - *Prioritise inventory*
 - *Critical*
 - *Necessary*
 - *Deferrable*
 - *Detailed instructions on how to reconstruct the network.*



Level of Detail

- ▶ As a minimum include:
 - ▶ *the recovery process and flow of activities*
 - ▶ *high level activities, e.g.*
 - ▶ load operating systems
 - ▶ install application software
 - ▶ restore data
 - ▶ synchronise database
 - ▶ make configuration changes
 - ▶ post recovery checks
 - ▶ open service to users
 - ▶ *pre-requisites and dependencies for each activity*
 - ▶ *responsibilities, who will perform each activity.*
- ▶ Order is important!



Level of Detail

- Should you include the detailed activities for installing an operating system or restoring a database?
- The detailed recovery activities should be held locally by the team responsible for performing these activities.
 - *The SOE instructions will be used for business-as-usual activities, minor incidents, AND disaster recovery.*
- The DR plan only needs to reference these documents
 - *Don't allow the key purpose of the DR plan to be lost in unnecessary or duplicated detail.*



Disaster Recovery Testing

- The key objectives of a DR test are;
 - *Exercise the recovery processes and procedures*
 - *Familiarise staff with the recovery process and documentation*
 - *Verify the effectiveness of the recovery documentation*
 - *Verify the effectiveness of the recovery site;*
 - *Establish if the recovery objectives are achievable*
 - *Identify improvements require to the DR strategy, infrastructure, and recovery processes*



Common Mistakes in Testing

- Operating within your comfort zone
 - *Recovering the servers you know you can recover whilst avoiding the more difficult components*
 - *Not testing the recovery of a service but focusing on the hardware, systems, and applications.*
 - Remember, a particular service may require several servers to be recovered, it may also require data held on local drives and network attached devices, and network connectivity from the data centre to the user
- *Trying to achieve too much too soon and overstating your DR capability and readiness*
- *Not planning appropriately, testing and live invocation are very different.*
 - In a live invocation you do not have a live environment to protect. Consider the impact that testing may have on your live services



Disaster Recovery

- Disaster recovery plans requires maintenance
 - *Perform scheduled maintenance at regular intervals to review the plan and modify it, if necessary.*
 - *Perform unscheduled maintenance when a security-related event occurs*
- A good set of examples are available on Moodle



Backups



- Making a backup of data is a mandatory requirement.
 - *In personal computers making a backup is a necessary but neglected task*
- Backup plan should include
 - *What should be backed up?*
 - *How large will the backups be?*
 - *Which backup medium (or media) should be used?*
 - *When should backups occur?*
 - *Who is responsible for initiating and maintaining backups?*
 - *Where should the backup media be stored?*
 - *How often should backups be tested?*
 - *What should be done when data is lost?*
 - *How fast can the system be restored?*



A Note on Backups

- **Note:** The archive bit is a file attribute that is set whenever a file is modified. This bit is turned off after the backup completes, indicating to the system that the file has been backed up.
- If the file is changed again before the next backup, the bit will be turned on
- Using the archive bit in determining changed files can cause confusion if the user is not careful, if the data selection for more than one backup job overlap.



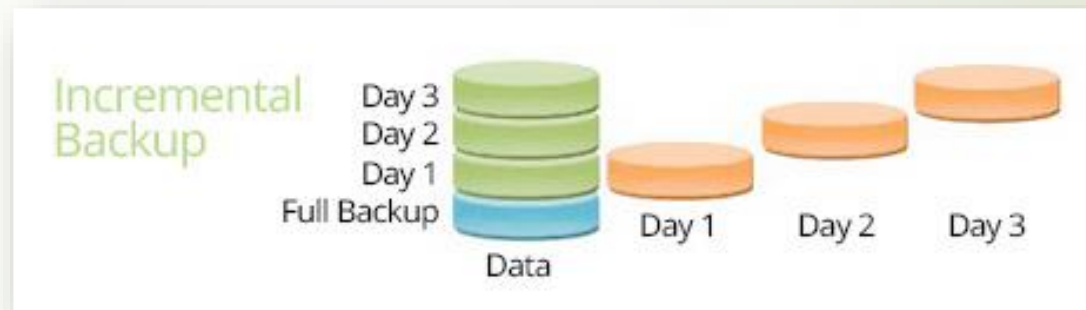
Backup Types

- **Full**
 - *Backs up all data*
- **Copy**
 - *Backs up selected files regardless of the archive bit*
- **Daily**
 - *Only backs up files that were changed during the current day.*
 - *Does not alter archive bit*
- **Appended**
 - *An option that backs up onto media until space runs out*
 - *Overwrites oldest*

Backup Types

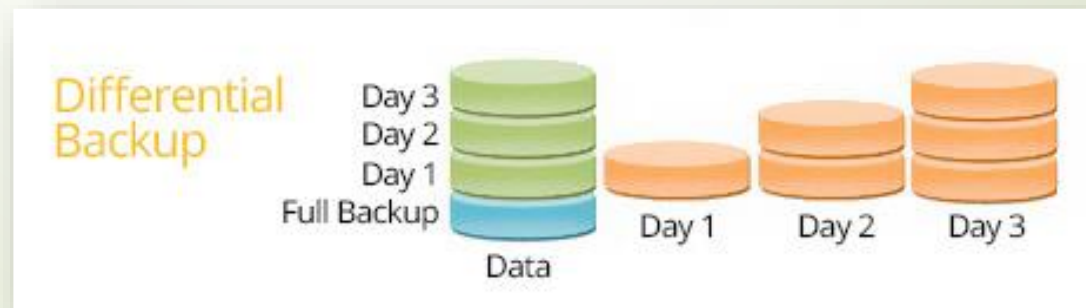
➤ Incremental

- *Backs up files that are new or altered since the last full or incremental backup*



➤ Differential

- *Backs up files new or modified since last full backup*



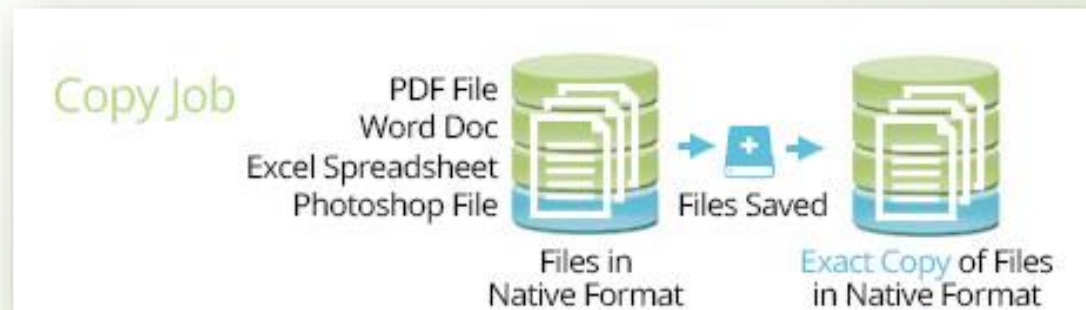
Backup Types

- An image-based backup, also known as disaster recovery or disk imaging, allows you to create a full disk backup of the entire system (or one or more partitions), including your operating system, your applications and all of your data rather than just your files and folders. This type of backup is saved as a single file that is often referred to as an image.



Backup Types

- Copy jobs differ from backup jobs in that they result in the exact same set of files selected, saved in their native and uncompressed file format.
- These files are simply being “copied” or transferred to your desired storage destination device on a manual or scheduled basis, but should never be considered a backup or take the place of regular backups.





Specialised Backup Types

■ Open Files

- *Locked files may change during backup*
- *Takes a “snapshot” disabling changes to the file*

■ Databases

- *Data may not be current due to write behind caching*

■ Email

- *Commonly only restore single mailbox*
- *Brick level backups enable mailbox by mailbox backup/restore*

■ Mobile

- *Not often available when backups are run*
- *Sync is often used*

■ Snapshots

- *Often used prior to system changes*

■ Bare Metal

- *Based on disk imaging*

What backup storage device to choose?

- A few options:
 - External Hard Drive(s)
 - NAS or SAN Devices
 - Tape Drives
 - Network Storage
 - FTP
 - RDX Removable Disk Drive
 - Online Backup (Amazon S3 or other)
 - File Sharing Services (Dropbox, OneDrive, etc.)
 - USB Media (Flash, Thumb Drive)





Tape Rotation

- Structured backup scheme include
 - *Schedule*
 - *Details about which files are backed up*
 - *Where the backup is stored*
 - *How it can be retrieved*
- The backup scheme will specify the backup rotation method
 - *Determines how many backup tapes or other media sets are needed*
 - *The sequence in which they are used and reused.*
 - *Designated administrators will have the responsibility for designing and managing the backup scheme and for restoring data when needed.*



Tape Rotation

- ▶ Grandfather-Father-Son method
 - ▶ *Daily tape sets are used Monday through Thursday*
 - ▶ *Weekly tape sets every Friday*
 - ▶ *Monthly tape sets on the last day of each month*
 - ▶ *It is a usual practice to rotate daily tape sets weekly, weekly tape sets monthly, and monthly tape sets annually.*
 - ▶ Daily Tapes sets = 4
 - ▶ Weekly Tapes sets = 4
 - ▶ Monthly Tapes sets = 12

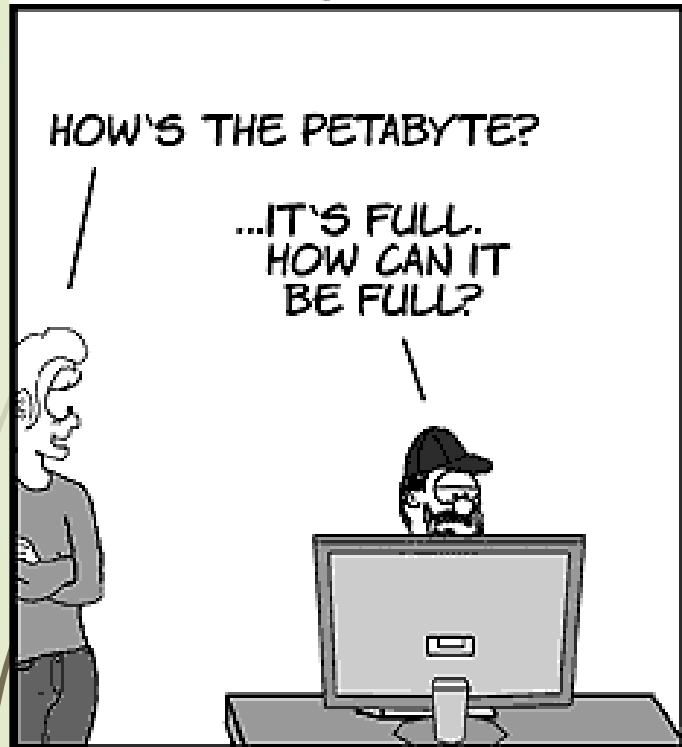
Tape Rotation

- Leaning tower or Tower of Hanoi method
- *Tape sets are staggered with one tape set for every two days, and different sets every four, eight, sixteen, and thirty-two days, respectively.*

Day	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Media Set	A		A		A		A		A		A		A		A	
		B				B				B				B		
				C								C				
								D								
																E

Media Set	Used Every
A	2 Days
B	4 Days
C	8 Days
D and E	16 Days alternating between set D and E

USER FRIENDLY by J.D. "Illiad" Frazer



YOU RAN A BACKUP LAST
NIGHT, RIGHT?

YES. THE JOB WAS
HALTED BECAUSE
THERE'S NO MORE
DISK SPACE.

The woman is now standing next to the man, looking at him. The man is still looking at the monitor.

MIKE...YOU HAVE YOUR
BACKUP BACKING UP
YOUR BACKUPS.

RECURSIVES!
SPOILED AGAIN!

The woman is now standing next to the man, looking at him. The man is still looking at the monitor.



Data Retention

- Every organisation should have a well-defined legal policy concerning the retention and destruction of data.
 - *Corporate policy and legal and regulatory requirements dictate how to retain and destroy data records.*
 - *Because it is difficult to attain legal and regulatory compliance, corporate legal departments must assume advisory roles and act as internal consultants to ensure adherence to these standards.*
 - *Failing to properly retain information may result in legal issues and fines.*



Replication



- Replication is the process of sharing and synchronising data across multiple devices or servers.
- The replication process can be performed by one of three methods:
 - *disk-to-disk replication*
 - Data across multiple storage disks to ensure consistency among redundant resources.
 - Recover individual files without the need to scan the entire backup volume.
 - This replication method can enhance the availability of data in a distributed system
 - Usually performed using disk mirroring
 - The advantage of this type of replication is its high-speed access to the replicated data



Replication



- *server-to-server replication*
 - Replicates data across multiple servers
 - *The changes made on one server are replicated simultaneously on different servers.*
 - Allows the read activity to be scaled across multiple servers.
 - Implemented in scenarios that demand high throughput
 - Achieved by implementing an appropriate clustering technique



Replication

- *site-to-site replication*

- The disaster recovery plan should include provisions for offsite locations that can be used as temporary offices
- Backup site locations and replacement equipment can be classified as;
- hot
 - *Fully equipped and of adequate capability*
- warm
 - *Partial, minimal capability*
- cold
 - *Facilities only, equipment must be purchased and configured*