IT2775 Operations Security
Backup Planning

Objectives

- **Conventional backups**   Backups
    1. Full
    2. Incremental
    3. Differential
- **Non conventional backups**
    1. Synthetic (Artificial)
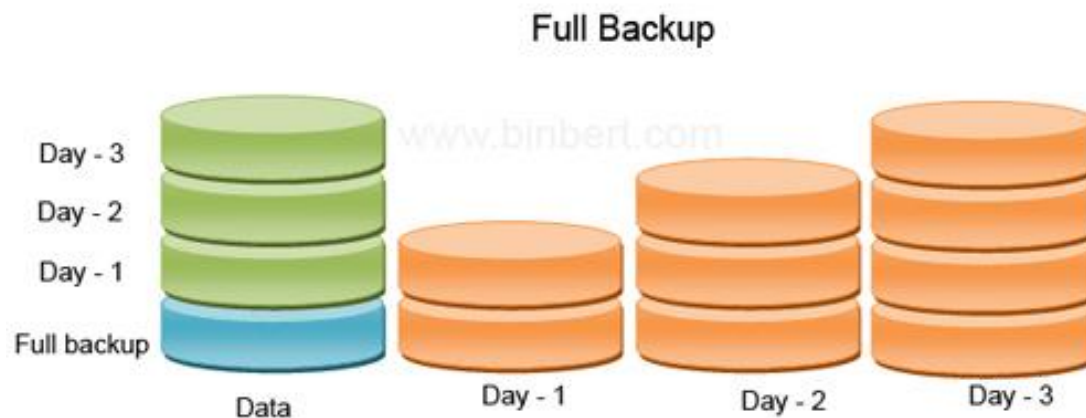   2. Copy
    3. Shadow Copies
- **Types of Data**
- **Backup Plan Design**

Conventional Backups

1. Full backup

   - Full backups are time consuming when dealing with sparsely modified data.

   - If stolen, data in the backup can be easily restored by unauthorized persons.

   - Inefficient use of storage for unmodified data.

   - Clears the archive bit.

Full Backup

Conventional Backups

2. **Incremental backup**
   - Backs up modified files after full/incremental backup.
     - Monitored by the backup software.
     - Requires archive bit, which is maintained by the OS.
       - bit is set when a file is modified.
       - bit is cleared after the file is backed up.
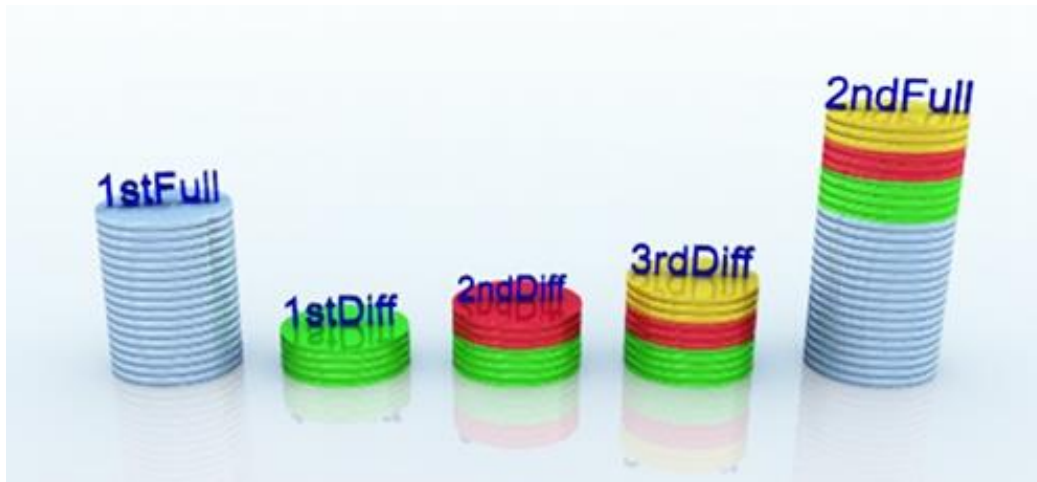
Conventional Backups

2. Incremental backup

   - Saves both time and storage.

   - Recovering requires the <u>last full backup</u> and <u>ALL incremental backups</u> up to the most recent backup.

     - Susceptible to errors as any issue in any of the backups may render the backup useless.

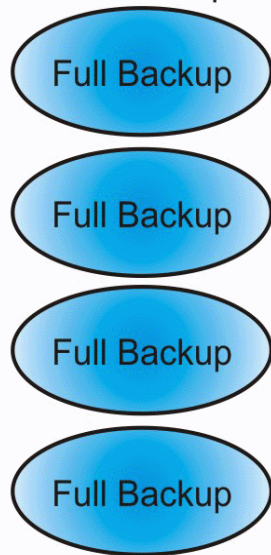   - Limit no. of incremental backups after a full backup.

Conventional Backups

3. Differential backup
   - Backs up modified files after full backup.
   - Time and storage requirements are in between those of full and incremental backups.
   - Recovering requires the <u>last full backup</u> and <u>most recent differential backup</u>.
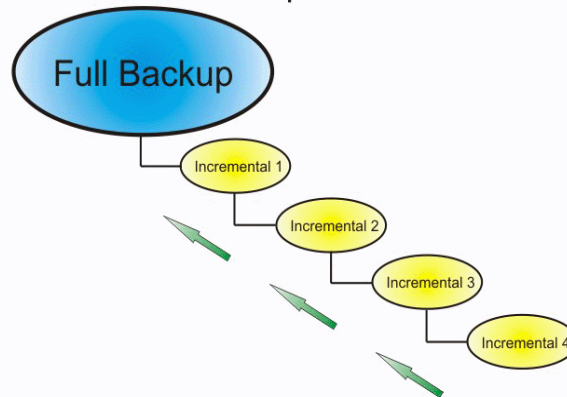   - Requires more time than recovering from full backup.

Full Backups

Full Backup

Full Backup

Full Backup

Full Backup

+ Each of these files is a standalone file which can be moved/copied/recovered independently.

− These files take much space on the drive.

Incremental Backups

Full Backup

Incremental 1

Incremental 2

Incremental 3

Incremental 4

+ These files take minimum space on the drive. Every incremental contains the data which was changed after the previous incremental backup operation was performed.
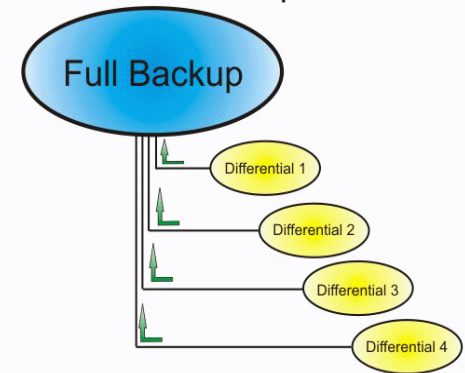
− These files work in "chain" and in order to recover you should have all the previous incremental backup files and the full backup.

− If the "chain" of incrementals is broken (one of the files is corrupted) you will not be able to recover next incrementals

Incremental Backups - example of failure

Full Backup

Incremental 1   Accessible

Incremental 2   Accessible

Incremental 3   Corrupted archive

Incremental 4   Inaccessible

Differential Backups

Full Backup

Differential 1

Differential 2

Differential 3

Differential 4

○ These files do not take too much space on the drive. Every differential contains the data which was changed after the full backup operation was performed.
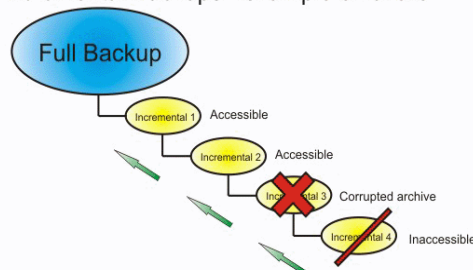
○ These files work in "pair" and in order to recover you should have full backup file.
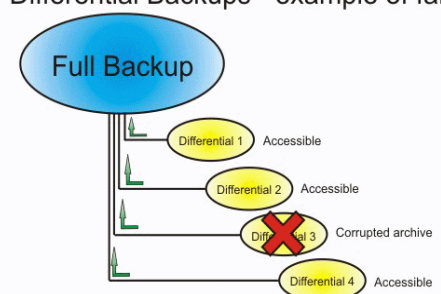
○ If one of the differentials is broken (the file is corrupted) it will not affect the previous or next differentials. Though if the full backup is corrupted you will not be able to recover.

Differential Backups - example of failure

Full Backup

Differential 1   Accessible

Differential 2   Accessible

Differential 3   Corrupted archive

Differential 4   Accessible

Acronis
Compute with confidence

www.acronis.com

Full vs. Differential vs. Incremental

	Mon.	Tues.	Wed.	Thurs.	Fri.
Changed File	A	B	C	D	E

Full Backup	A B C D E	A B C D E	A B C D E	A B C D E	A B C D E

Differential Backup	A	A B	A B C	A B C D	A B C D E

Incremental Backup	A	B	C	D	E

BACKUP TYPE	DATA BEING BACKED UP	CLEARS THE ARCHIVE BIT?	BACKUPS NEEDED TO RESTORE AFTER A SYSTEM CRASH
Full	Everything	YES	Full only
Differential	Data changed since last Full backup	NO	Full + last Diffrential
Incremental	Data changed since last Full backup or Incremental backup	YES	Full + all Incremental backups done since last Full backup
Copy	*Everything*	*NO*	*Copy only*

	No. of Records created	No. of Records backup by different Backup Type at day end			
		Incremental	Differential	Full	Restore
Sun	*Full backup of 1000 records*				
Mon	100				
Tue	100				
Wed	200				
Thu	300				
Fri	100				
Sat	50				

Full, Incremental, Differential Backups

Type	Data Selection	Backup / Restore Time	Archive Attribute
Full	All selected data	High / Low (one tape set)	Cleared
Incremental	New files and files modified since the last backup	Low / High (Multiple tape sets)	Cleared
Differential	All data modified since the last full backup	Moderate / Moderate (No more than 2 sets)	Not Cleared

Non conventional Backups

1. Synthetic (Artificial) Full backup
   - Uses a previous full backup and subsequent incremental or differential backups to create a new "full backup".
   - Allows a full backup to be created w/o running backup job.
     - When operations don't allow full backups to complete.

2. Copy backup
   - Makes a copy of the files but does not clear the 'archive bit' after making a copy.
     - Full backup: clears the 'archive bit'.

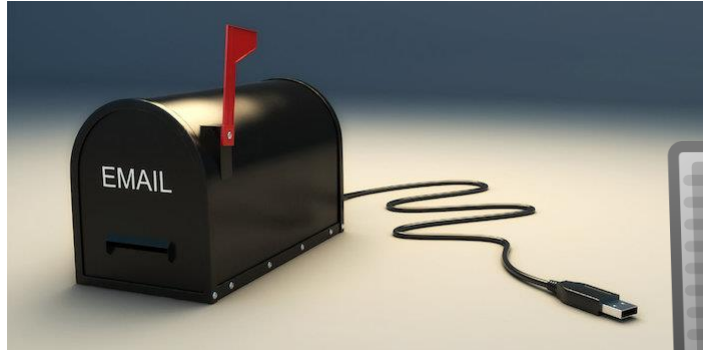# Non conventional Backups

3. Shadow Copies

    - Past versions of files as modified by users over time.

    - Possible to inspect and restore past versions of files.

    - Available in Windows 2008 for shared folders

    - Supported by various backup software.

    - Shadow copies usually stored on a separate hard disk from the actual shared folder.
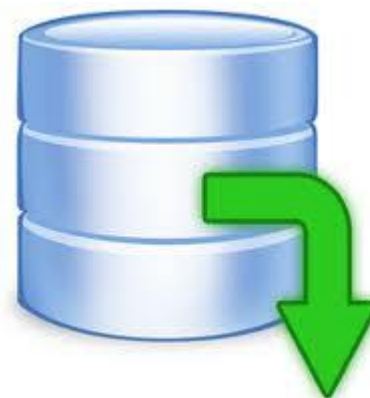
Types of Backup Data

1. User Data
   - Mailboxes
   - Users' profile
   - Home directory
   - …

2. System Data
   - Web site data
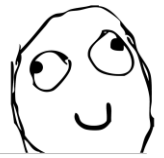   - Application data and logs
   - Databases dump
   - …

Types of Backup Data

3. System Software and Configuration

- Operating system, application software and licenses.

- System, application and security configuration.

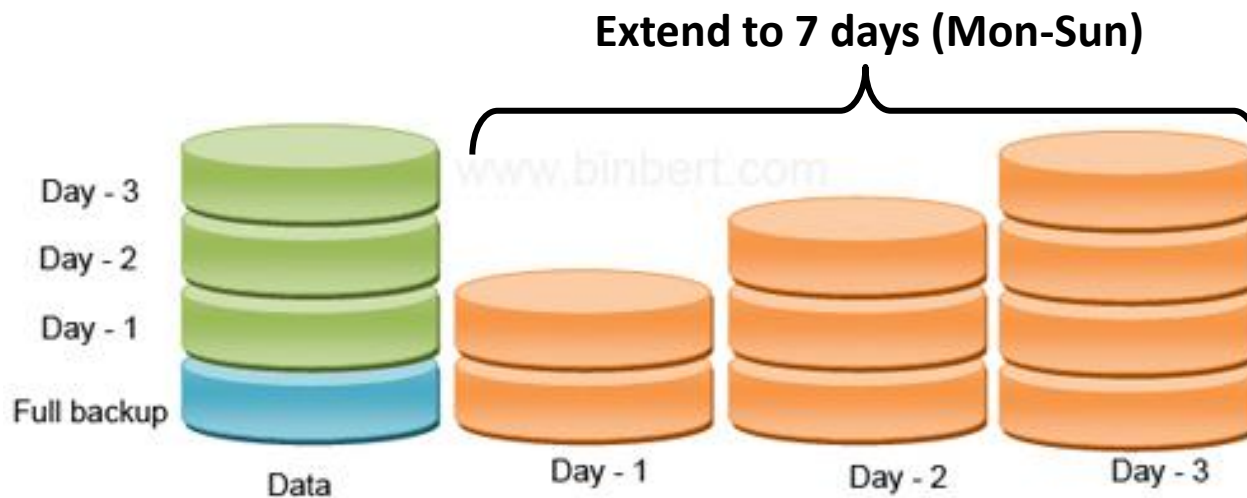- Technical and user documentation.

- ...

Backup Plan Design

- Frequency of change for backup data.
    - User Data: High
    - System Data: Depends
    - System S/w and Configuration: Low
- Considerations for effective backup plan.
    - Avoid duplicates: less frequent for static data.
    - Minimise resources: time and storage for backups.
    - Easier to manage security of backups.
- Effective backups need to be constantly managed and maintained.

Backup Plans

- Plan 1: Daily full
  - Backup Time: Back up files that don't even change.
  - Storage Space: A lot of file duplication.
  - Recovery Time: Only 1 full backup needed.
- May be suited for small servers/company.

Extend to 7 days (Mon-Sun)

Day - 3
Day - 2
Day - 1
Full backup

Data

Day - 1

Day - 2

Day - 3

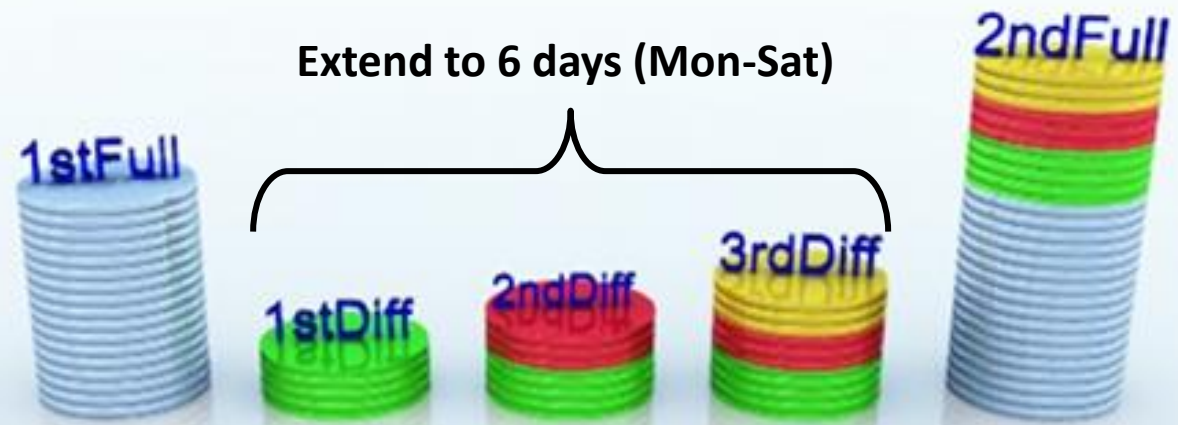**Backups needed
to recover to Tues:** ✓

Backup Plans

- Plan 2: Weekly full, daily incremental
  - Backup Time: Only back up files that change.
  - Storage Space: Least amount of file duplication.
  - Recovery Time: Needs max of 1 full + 6 incremental.
- Minimises duplication but risk of data loss higher.

Backup Plans

- Plan 3: Weekly full, daily differential
  - Backup Time: Back up files that change since last full.
  - Storage Space: Later differentials are larger in size due to duplicates towards the end of the week.
  - Recovery Time: Needs 1 full + 1 differential backups

Extend to 6 days (Mon-Sat)

1stFull

1stDiff 2ndDiff 3rdDiff

2ndFull

Backups needed to recover to Tues:

✓ ✓

Tape Rotation

Type	Frequency	Number of Sets
Son	Daily	7 Sets
Father	Weekly	4 Sets (plus one to be held off site)
Grandfather	Monthly	12 sets

Summary

- **Conventional backups**
  1. Full
  2. Incremental
  3. Differential

- **Non conventional backups**
  1. Synthetic (Artificial)
  2. Copy
  3. Shadow Copies

- **Types of Data**

- **Backup Plan Design**