# Web Development and Database Administration

# Level-IV

## Based on March 2022, Curriculum Version II




## Module Title: Database Backup and Recovery

## Module code: EIS WDDBA4 M07 1123

## Nominal duration: 24 Hour

Prepared by: Ministry of Labor and Skill

November, 2023

Addis Ababa, Ethiopia

# Tabel of content

**Tabel of content** ..... 0
Acknowledgment ..... 1
Acronym ..... 2
**Introduction to the Module** ..... 3
1.1. Architecture of database file system ..... 5
1.2. Risks and Failure Scenario ..... 8
1.3 OHS ..... 11
2.1. Introduction to Backup ..... 14
2.2. Methods for back-up and recovery ..... 14
2.3. Range of back-up and restoration ..... 19
2.4. Off-line back-ups ..... 22
2.5. On-line file back-ups ..... 22
2.6. Disk mirroring ..... 24
2.7. RAID ..... 24
2.8. Off-site back-up files ..... 28
2.9. Onsite Backup ..... 30
2.10. Hybrid storage ..... 31
Self-check 2 ..... 32
Operation sheet 2.1 Take backup ..... 33
Operation title: Take backup ..... 33
Operation sheet 2.2 Taking Database Offline ..... 35
Operation sheet 2.3 Take Full backup ..... 36
LAP Tests ..... 37
Unit Three: Database Recovery Points & Procedures ..... 38
3.1. Database recovery point ..... 39
3.2. Testing restore process ..... 43
3.3. Restore a database to a point in time ..... 44
Self-check 3 ..... 47
Operation sheet 3.1 ..... 48
LAP Test ..... 50

References ..... 51
Developer's Profile ..... 56

# Acknowledgment

**Ministry of Labor and Skills** wish to extend thanks and appreciation to the many representatives of TVET instructors and respective industry experts who donated their time and expertise to the development of this Teaching, Training and Learning Materials (TTLM).

# Acronym

API ----------Application Programming Interface

DBMS ---------- Database Management System

DVD ----------Digital Versatile Disc

ECC ----------Error-Correcting Code

ICT----------Information and Communication Technology

JDBC ----------Java Database Connectivity

LAN ----------Local Area Network

ODBC ----------Open Database Connectivity

RAID ----------Redundant Array of Independent Disks

SQL ----------Structured Query Language

SSMS ----------SQL Server Management Studio

WAN ----------Wide Area Network

# Introduction to the Module

The module "Complete Database Backup and Recovery" addresses the critical aspects of safeguarding and restoring databases, ensuring the continuity of valuable information systems.

**This module covers the units**:

- Database Architecture
- Database Backup Methods
- Database Recovery Points & Procedures

**Learning Objective of the Module**

At the end of the module the trainee will be able to:

- Identify and comprehend the file system architecture of a database.
- Recognize potential risks and failure scenarios associated with the database.
- Execute online file backups following organizational standards.
- Utilize advanced techniques such as disk mirroring and RAID configurations.
- Determine strategic recovery points based on backup arrangements and organizational guidelines.

**Module Instruction**

For effective use these modules trainees are expected to follow the following module instruction:

1. Read the specific objectives of this Learning Guide.
2. Follow the instructions described below.
3. Read this Learning Guide and understand it, and then do in practical.
4. Accomplish the “Self-check”.
5. If you earned a satisfactory evaluation from the “Self-check” proceed to “Operation Sheet”**.**
6. Do the “LAP test” if you are ready.

## **Unit one:** Database Architecture

This unit is developed to provide you the necessary information regarding the following content coverage and topics:

- Architecture of database file system
- Identify Risks and Failure Scenario
- OHS

This unit will also assist you to attain the learning outcomes stated in the cover page. Specifically, upon completion of this learning guide, you will be able to:

- Describe the file system architecture of a database.
- Identify potential risks that can impact the database architecture.
- recognize failure scenarios that may occur in a database environment
- Understand OHS

## 1.1. Architecture of database file system

Database architecture focuses on database design and construction for large enterprise database systems that manage massive amounts of information for organizations. Database architecture includes setting the standards for the security and programming aspects of these databases, as well as figuring out how these databases will operate and function within existing structures.

The design of a DBMS depends on its architecture. Selecting the correct Database Architecture helps in quick and secure access to data. It can be centralized or decentralized or hierarchical. The architecture of a DBMS can be seen as either single tier or multi-tier. The tiers are classified as follows:

### 1.1.1. Single tier architecture

The simplest of Database Architecture are 1 tier where the Client, Server, and Database all reside on the same machine. In other word, it keeps all of the elements of an application, including the interface, Middleware and back-end data, in one place. Developers see these types of systems as the simplest and most direct way.

- The database is directly available to the user. It means the user can directly sit on the DBMS and uses it.
- Any changes done here will directly be done on the database itself. It doesn't provide a handy tool for end users.
- The 1-Tier architecture is used for development of the local application, where programmers can directly communicate with the database for the quick response.

For example; when you install a DB in your system and access it to practise SQL queries it is tier-one architecture. But such architecture is rarely used in production



Figure 1.1: Single tier architecture

### 1.1.2. Two-tier Architecture

The two-tier is based on Client Server architecture.

It is like client server application.

The direct communication takes place between client and server. There is no intermediate between client and server.

Applications on the client end can directly communicate with the database at the server side. For this interaction, API's like: ODBC, JDBC are used.

The user interfaces and application programs are run on the client-side.

The server side is responsible to provide the functionalities like: query processing and transaction management.

To communicate with the DBMS, client-side application establishes a connection with the server side

2 tier architecture provides added security to the DBMS as it is not exposed to the end user directly.

A two-tier architecture is a database architecture where

1. Presentation layer runs on a client (PC, Mobile, Tablet, etc)
2. Data is stored on a Server.

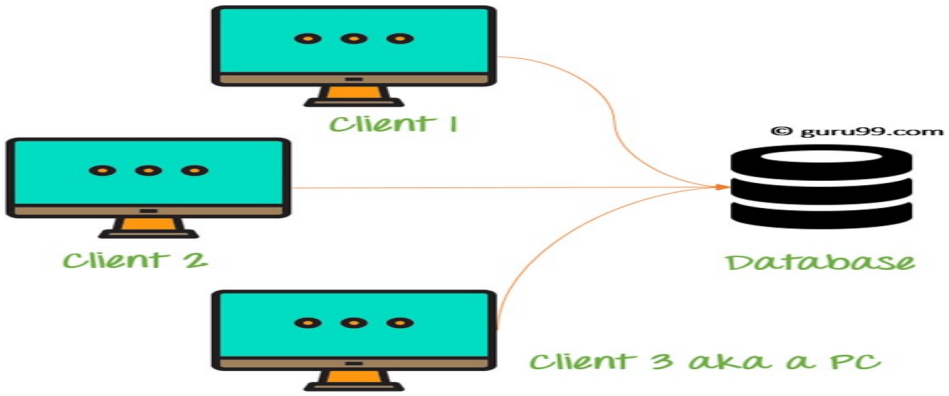



Figure 1.2. Two Tier architecture

### 1.1.3. Three-tier Architecture

It is an extension of the 2-tier architecture. A 3-tier architecture separates its tiers from each other based on the complexity of the users and how they use the data present in the database. The three tier architecture is the most popular DBMS architecture.

This architecture has different usages with different applications. It can be used in web applications and distributed applications. 3-tier architecture has following layers;

- Database server (Data) Tier − at this tier, the database resides along with its query processing languages. We also have the relations that define the data and their constraints at this level.
- Application (Middle) Tier – also called business logic layer and it processes functional logic, constraint, and rules before passing data to the user or down to the DBMS. This DBMS architecture contains an Application layer between the user and the DBMS, which is responsible for communicating the user's request to the DBMS system and send the response from the DBMS to the user.

  For a user, this application tier presents an abstracted view of the database. End-users are unaware of any existence of the database beyond the application. At the other end, the database tier is not aware of any other user beyond the application tier. Hence, the application layer sits in the middle and acts as a mediator between the end-user and the database.
- User (Presentation) Tier − End-users operate on this tier and they know nothing about any existence of the database beyond this layer. At this layer, multiple views of the database can be provided by the application. All views are generated by applications that reside in the application tier. Example your PC, Tablet, Mobile, etc.)
    - The goal of Three-tier architecture is:
        - To separate the user applications and physical database
        - Proposed to support DBMS characteristics
        - Program-data independence
        - Support of multiple views of the data

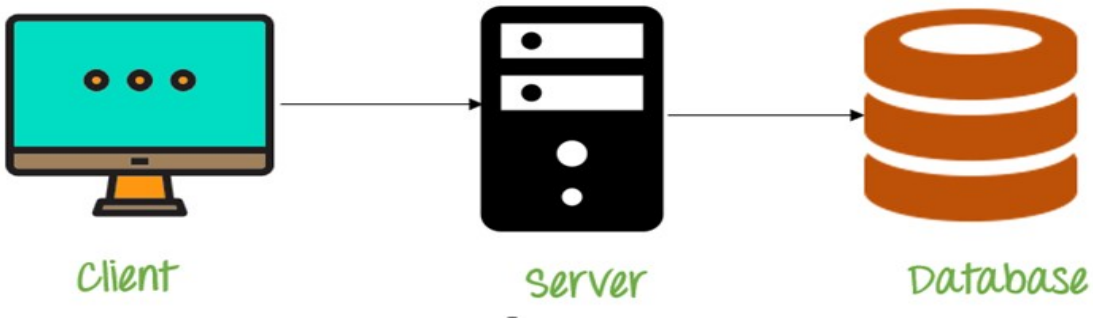



Figure 1.3. Three-tier Architecture Diagram

- **N-tier architecture:** N-tier architecture would involve dividing an application into three different tiers. These would be the Logic tier, presentation tier, and data tier.

## 1.2. Risks and Failure Scenario

A database is the means of organizing information so it can be easily managed, updated and retrieved. Losing a database would also mean losing the associated data. This means that if a business loses its databases for any number of reasons, with no backups stored, it is fair to assume that they will most likely lose the data too. There are many types of failures that can affect database processing. Some failures affect the main memory only, while others involve secondary storage. There are different scenarios or causes that could lead to a database loss. Some of them include;

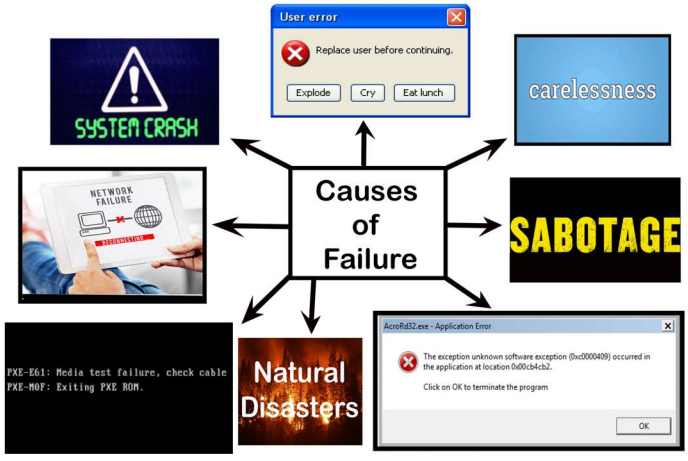



Figure 1.4. Cause of database failure

- **Power Failure**

Power failures can lead to hardware failure. The affected hardware components could be cables, power supplies or storage devices. It can render the data either inaccessible or simply result in data loss. One would need to isolate the affected area before investigating if the database was affected by the power failure.

- **Disk Failure**

While power failures can lead to disk failure, they can also fail due to physical damage or a logical failure. Such failures are due to head crashes or unreadable media, resulting in the loss of parts of secondary storage. They are the most dangerous failures and one of the most common causes of data loss.

- **Human Error (Carelessness)**

This is the failure due to unintentional destruction of data or facilities by operators or users. An employee may unintentionally delete some data or may modify the data unknowingly in a way that would cease the DBMS from interacting with the database effectively. When DBMS software is unable to interact with the database, it causes a ripple effect since the remaining third party applications relying on the DBMS to interact with the database also lose access to it. Human error is the number one cause of data loss.

- **Software Corruption**

Companies using traditional in-house IT infrastructures are more at risk of software corruption than those relying on cloud-based services. While cloud vendors provide flexibility and scalability of resources, traditional IT environments have fixed sets of hardware resources which they manually upgrade.

When the number of end users in a company increase, the applications using the same resources are divided even further among the new users, causing problems such as freezing and crashing of the operating systems and applications in the middle of using the software. Crashing causes the end user to lose the unsaved data.

Repeated crashing can especially cause serious damage if the user is working on a database. These are logical errors in the program that is accessing the database, which cause one or more transactions to fail. Software failure may include a failure a failures related to software such as, operating systems, DBMS software, application Programs and so on.

- **Virus Infection**

An enterprise cannot operate safely without the use of a good security solution. Cyber-attacks are the biggest threat a company faces today and it is imperative that the security solution performs real-time scanning. Depending on the type of virus, it could have the ability to steal, corrupt, modify and even delete the complete database.

- **Natural Disasters**

Natural disasters such as fire, floods, earthquake, tsunami, etc have the ability to destroy the entire infrastructure. In such an event, there is absolutely no way to even find, let alone recover, the data.

- **Disgruntled Employees**

A disgruntled employee could provide essential and confidential information to outsiders, causing untold damage to an organization. And if the employee has access or gains unauthorized access to systems or applications, he/she can inject a virus or delete data to halt the company's day to day operations.

- **Hardware Failure**

Hardware failure may include memory errors, disk crashes, bad disk sectors, disk full error and so on. Hardware failure can also be attributed to design errors, poor quality control during fabrication, overloading and wear out of mechanical parts.

- **System Crash**

System crashes are due to hardware or software errors, resulting in the loss of main memory. This could be the situation that the system has entered an undesirable state, such as Dead Lock, which prevents the program form continuing with normal processing.

- **Network Failure**

Network failure can occur while using a Client-server configuration or distributed database system where multiple database servers are connected y common network. • Network failure such as communication software failure or aborted asynchronous connections will interrupt the normal operation of the database system.

- **Sabotages**

These are failures due to international corruption or destruction of data, hardware or users.

## 1.3 OHS

Occupational Health and Safety (OHS) requirements for database backup and recovery are crucial to ensure the well-being and safety of individuals involved in managing and maintaining databases. While OHS standards may vary by region and organization, here are some general guidelines to consider when it comes to the occupational health and safety aspects of database backup and recovery:

- **Training and Competency**

Ensure that personnel responsible for database backup and recovery are adequately trained and competent in their roles. Provide ongoing training to keep them updated on the latest backup and recovery procedures and technologies.

- **Ergonomics**

Design workstations and environments with ergonomic principles in mind to prevent musculoskeletal issues among personnel. Ensure that seating, lighting, and computer equipment are conducive to a healthy working environment.

- **Workload Management**

Monitor and manage the workload of personnel involved in database backup and recovery to prevent stress and burnout. Encourage breaks and time away from the computer to reduce the risk of repetitive strain injuries.

- **Emergency Procedures**

Establish clear emergency procedures for unexpected situations during database backup and recovery processes. Ensure that personnel are aware of evacuation plans and procedures in case of emergencies.

- **Security Measures**

Implement security measures to protect personnel from potential cybersecurity threats during backup and recovery operations. Provide guidelines on handling sensitive data securely to prevent data breaches and unauthorized access.

- **Equipment Safety**

Regularly inspect and maintain all equipment used in database backup and recovery to ensure it meets safety standards. Provide guidelines for the safe use of backup and recovery tools and equipment.

- **Health Monitoring**

Implement health monitoring programs to identify and address any health issues among personnel promptly. Encourage regular health check-ups and screenings to monitor the overall well-being of employees.

- **Documentation and Procedures**

Document clear and detailed procedures for database backup and recovery tasks. Include safety guidelines and precautions within the documentation to ensure safe work practices.

- **Communication Protocols**

Establish effective communication protocols to ensure that team members can communicate efficiently during backup and recovery operations. Encourage open communication about any concerns related to health and safety.

- **Regulatory Compliance**

Stay informed about relevant OHS regulations and ensure compliance with local, regional, and national standards.

# Unit Two: Database Backup Methods

This unit is developed to provide you the necessary information regarding the following content coverage and topics:

- Introduction to Backup
- Types of backup
- Backup and Restoration Methods
- Full Offline Backups
- Online File Backups
- Disk Mirroring and RAID Configurations
- Off-site Backup Copies
- Onsite Backup

This unit will also assist you to attain the learning outcomes stated in the cover page. Specifically, upon completion of this learning guide, you will be able to:

- Define Backup
- Define Types of backup
- evaluate different backup and restoration methods
- Perform a full offline backup of a database
- Adhere to organizational and security standards during the backup process
- Execute online file backups following organizational standards
- set up and utilize disk mirroring
- Establish procedures for creating off-site and On-site backup copies

## 2.1. Introduction to Backup

Backup is the process of creating a copy of data to protect against accidental or malicious deletion, corruption, hardware failure, ransom ware attacks, and other types of data loss. Data backups can be created locally, offsite, or both.

Restore is the process of retrieving data from a backup. This might mean copying data from backup media to an existing device or to a new device. It also could mean copying data from the cloud to a local device or from one cloud to another.

Recovery refers to the process of restoring data and operations (e.g., returning a server to normal working order following hardware failure).

Restore and recovery times can vary widely depending on the backup format and data recovery methods you choose. Additionally, restore needs also vary (e.g., restoring a single file vs. an entire server). Finally, critical data may live on workstations, local servers, and in the cloud. These are important considerations when selecting a backup and recovery solution. The most common type of database backups are:

- Logical backup - backup of data is stored in a human-readable format like SQL
- Physical backup - backup contains binary data

## 2.2.Methods for back-up and recovery

### 2.2.1. Types of Backup

There are different types of backup, and each backup process works differently.

Table 2.1. Comparison of backup type

| A comparison of different types of backup | | | | |
|---|---|---|---|---|
| Backup | Full | Mirror | Incremental | Differential |
| Backup 1 | All data | All data Selected | - | - |
| Backup 2 | All data | All data Selected | Changes from backup 1 | Changes from backup 1 |
| Backup 3 | All data | All data Selected | Changes from backup 2 | Changes from backup 1 |
| Backup 4 | All data | All data Selected | Changes from backup 3 | Changes from backup 1 |

### 1. Full backups

The most basic and complete type of backup operation is a full backup. As the name implies, this type of backup makes a copy of all data to a storage device, such as a disk or tape. The primary advantage to performing a full backup during every operation is that a complete copy of all data is available with a single set of media. This results in a minimal time to restore data, a metric known as a recovery time objective. However, the disadvantages are that it takes longer to perform a full backup than other types (sometimes by a factor of 10 or more), and it requires more storage space.

Thus, full backups are typically run only periodically. Data centers that have a small amount of data (or critical applications) may choose to run a full backup daily, or even more often in some cases. Typically, backup operations employ a full backup in combination with either incremental or differential backups.

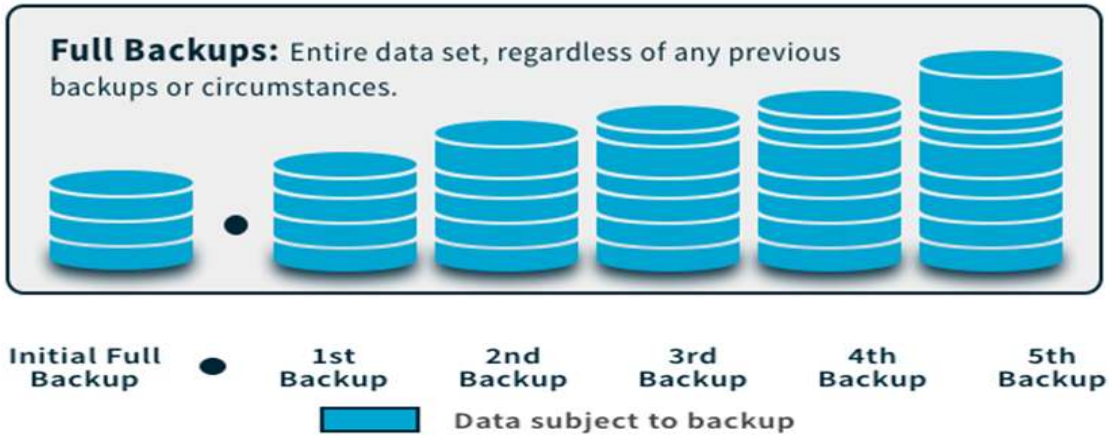



Figure 2.1. The way full backup perform

### 2. Incremental backups

An incremental backup operation will result in copying only the data that has changed since the last backup operation of any type. An organization typically uses the modified time stamp on files and compares it to the time stamp of the last backup. Backup applications track and record the date and time that backup operations occur in order to track files modified since these operations.

Because an incremental backup will only copy data since the last backup of any type, an organization may run it as often as desired, with only the most recent changes stored. The benefit of an incremental backup is that it copies a smaller amount of data than a full. Thus, these operations will have a faster backup speed, and require fewer medium to store the backup.

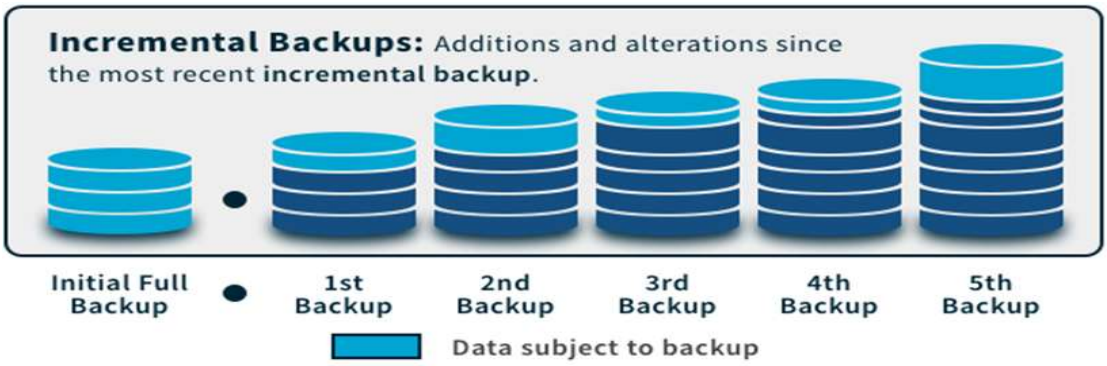



Figure 2.2. The way incremental backup perform

### 3. Differential backups

A differential backup operation is similar to an incremental the first time it is performed, in that it will copy all data changed from the previous backup. However, each time it is run afterwards, it will continue to copy all data changed since the previous full backup. Thus, it will store more backed up data than an incremental on subsequent operations, although typically far less than a full backup. Moreover, differential backups require more space and time to complete than incremental backups, although less than full backups.

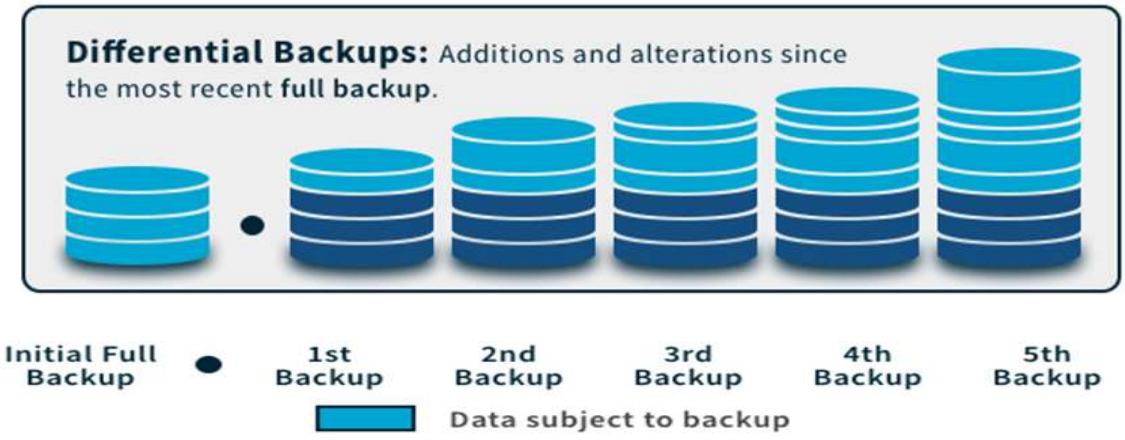



**Fig 2.3. Differential backup**

### 4. Mirror backups

A mirror backup is comparable to a full backup. This backup type creates an exact copy of the source data set, but only the latest data version is stored in the backup repository with no track of different versions of the files. The backup is a mirror of the source data. All the different backed up files are stored separately, like they are in the source.

One of the benefits of mirror backup is a fast data recovery time. It's also easy to access individual backed up files. Mirror backup is the fastest backup method because it copies files and folders to the destination without any compression.

One of the main drawbacks, though, is the amount of storage space required. It needs more storage space than any other backup type; password protection is not possible and cannot track different versions of files

With that extra storage, organizations should be wary of cost increases and maintenance needs. In addition, if there's a problem in the source data set, such as a corruption or deletion, the mirror backup experiences the same. As a result, it's a good idea not to rely on mirror backups for all your data protection needs, and to have other types of backup for the data. You'll want to follow the **3-2-1 rule** of backup, which includes three copies of data on two different media, with one copy off site.




Figure 2.5. The way mirror backup perform

### 2.2.2. Determining appropriate methods

To determine the type of backup strategy to be used there are different determinant factors such as overall business cost, performance, data protection levels, total amount of data retained and availability goals.

Do the right or appropriate backup for your organization. For organizations with small data sets, running a daily full backup provides a high level of protection without much additional storage space costs. Larger organizations or those with more data or server volume find that running a weekly full backup, coupled with either daily incremental backups or differential backups, provides a better option. Using differentials provides a higher level of data protection with less restore time for most scenarios and a small increase in storage capacity. For this reason, using a strategy of weekly full backups with daily differential backups is a good option for many organizations.

An organization must run a full backup at least once. For subsequent backups, it is possible to run either another full, an incremental or a differential backup. The first partial backup performed either a differential or incremental, will back up the same data. By the third backup operation, the data that is backed up with an incremental is limited to the changes since the last incremental. In comparison, the third backup with a differential will back up all changes since the first full backup, which was "Backup 1."

From these types of backup, it is possible to develop an approach for comprehensive data protection. An organization often uses one of the following backup settings:

- Full daily
- Full weekly + differential daily
- Full weekly + incremental daily

Performing a full backup daily requires the most amount of space, and will also take the most amount of time. However, more total copies of data are available, and fewer pieces of media are required to perform a restore operation. As a result, implementing this backup policy has a higher tolerance to disasters, and provides the least time to restore, since any piece of data required will be located on at most one backup set.

As an alternative, performing a full backup weekly, coupled with running incremental backups daily, will deliver the shortest backup time during weekdays and use the least amount of storage space. However, there are fewer copies of data available and restore time is the longest, since an organization may need to use six sets of media to recover the necessary information. If data is needed from data backed up on Wednesday, the Sunday full backup, plus the Monday, Tuesday and Wednesday incremental media sets, is required. This can dramatically increase recovery times, and requires that each media set work properly; a failure in one backup set can impact the entire restoration.

Running a weekly full backup plus daily differential backup's delivers results in between the other alternatives. Namely, more backup media sets are required to restore than with a daily full policy, although less than with a daily incremental policy. Also, the restore time is less than using daily incremental backups, and more than daily full backups. In order to restore data from a particular day, at most two media sets are required, diminishing the time needed to recover and the potential for problems with an unreadable backup set.

Most of the advanced types of backup such as synthetic full, mirror and continuous data protection require disk storage as the backup target. A synthetic full simply reconstructs the full backup image using all required incremental backups or the differential backup on disk. This synthetic full may then be stored to tape for offsite storage, with the advantage being reduced restoration time. Finally, continuous data protection enables a greater number of restoration points than traditional backup options.

## 2.3. Range of back-up and restoration

While each approach carries its own benefits and risks, organizations need to consider their need for performance, data protection, their total volume of data assets, and the cost of recovery. The following five factors can be used in making a decision about which backup schedule is right for you.

- **How active are your read/write activities?**

If your databases and applications are actively being updated with new data at a high rate, known to database specialists as "write activities", full backups could be more efficient. If you are primarily using your data assets for reference without updating them, known as "read activities," you may not need full backups on a very consistent basis.

- **What is your tolerance for recovery time?**

With a full backup on a daily basis, all of your assets are in a single set. While a full recovery isn't quite immediate, it can occur very quickly and doesn't require the combination of multiple types of backup files. If your tolerance to any downtime is zero, full backups represent the least risk.

- **How many of your data assets are actively being update?**

Unless all of your data assets, applications, and databases are "living," running full backups on a very consistent basis may take more storage space than necessary.

- **How much storage space can you dedicate?**

Running a full backup on a daily basis requires more than twice the storage space of differential or incremental in many cases. Assuming your business is actively using 25% of your data assets on a daily basis, running a full daily backup each weekday could require five times more storage space than a weekly full backup and a daily incremental or differential backup. At most organizations, the difference is significant.

- **How much data do you have?**

For some organizations, running a full backup daily is actually the most cost-effective approach. These are typically organizations with minimal data assets, which can be a product of their industry, products, services, or a lack of multimedia data assets. If cost and storage space factors are not prohibitive, a full backup represents the easiest and fastest recovery.

Table 2.1. Comparison of backup type

| | Full | Differential | Incremental |
|---|---|---|---|
| **Storage Space** | High | Medium to High | Low |
| **Backup Speed** | Slowest | Fast | Fastest |
| **Restoration Speed** | Fastest | Fast | Slowest |
| **Media Required for Recovery** | Most recent backup only | Most recent full backup & most recent differential backup | Most recent full backup & all incremental backups since full backup |
| **Duplication** | Stores a lot of duplicate files | Stores duplicate files | No duplicate files |

- **The advantages and disadvantages of each backup type**
  - Pros of Full Backups
    - ✓ Potential for fast, total recovery of data assets.
    - ✓ Simple access to the most recent backup version.
    - ✓ All back-ups are contained in a single version.
    - ✓ Minimal time needed to restore business operations.
  - Cons of Full Backups
    - ✓ Requires the most storage space.
    - ✓ Demands the most bandwidth.
    - ✓ Relatively time-consuming to complete the backup process
  - Pros of Incremental Backups
    - ✓ Minimal time to complete backup.
    - ✓ Requires the least storage space.
    - ✓ Demands the least bandwidth.
  - Cons of Incremental Backups
    - ✓ Recovery time may be slower.
    - ✓ Requires a full backup in addition to incremental backups for complete recovery.
    - ✓ Recovery requires the piecing together of data from multiple backup sets.
    - ✓ Small potential for incomplete data recovery if one or more backup sets has failed.
  - Pros of Differential Backups

- ✓ Requires less storage space than full backups.
- ✓ Only two backups (last full and most recent incremental) are required for recovery.

➢ Cons of Differential Backups

- ✓ Slower than incremental.
- ✓ Requires an initial full backup for complete recovery.
- ✓ IT will need to piece together two backup sets.
- ✓ Potential for failed recovery if one or more backups is incomplete

## 2.4. Off-line back-ups

Off-line backup is also called cold backup or static backup. It is a database backup during which the database is offline and not accessible to update or the database operations are entirely stopped, and then the backup is performed. While the backup is in progress, no business operations can be performed. This requires the data access to be completely shut off from the front-end and neither online users nor background processes can access the database for the duration of the backup.

It is mostly accomplished before the beginning of the day or at the end of the day. Here a single backup version is made. Since no new data is added to this in real-time, the backup is performed swiftly and only once.

Cold backups consume fewer resources but have a limitation. The database cannot be accessed when the backup operation is in progress.

The advantage of this method is that users are still able to access the system during the backup. However, if the server crashes, the backup will also be gone. The risk that comes with a hot backup is that the data may be modified during the process, resulting in inconsistent data.

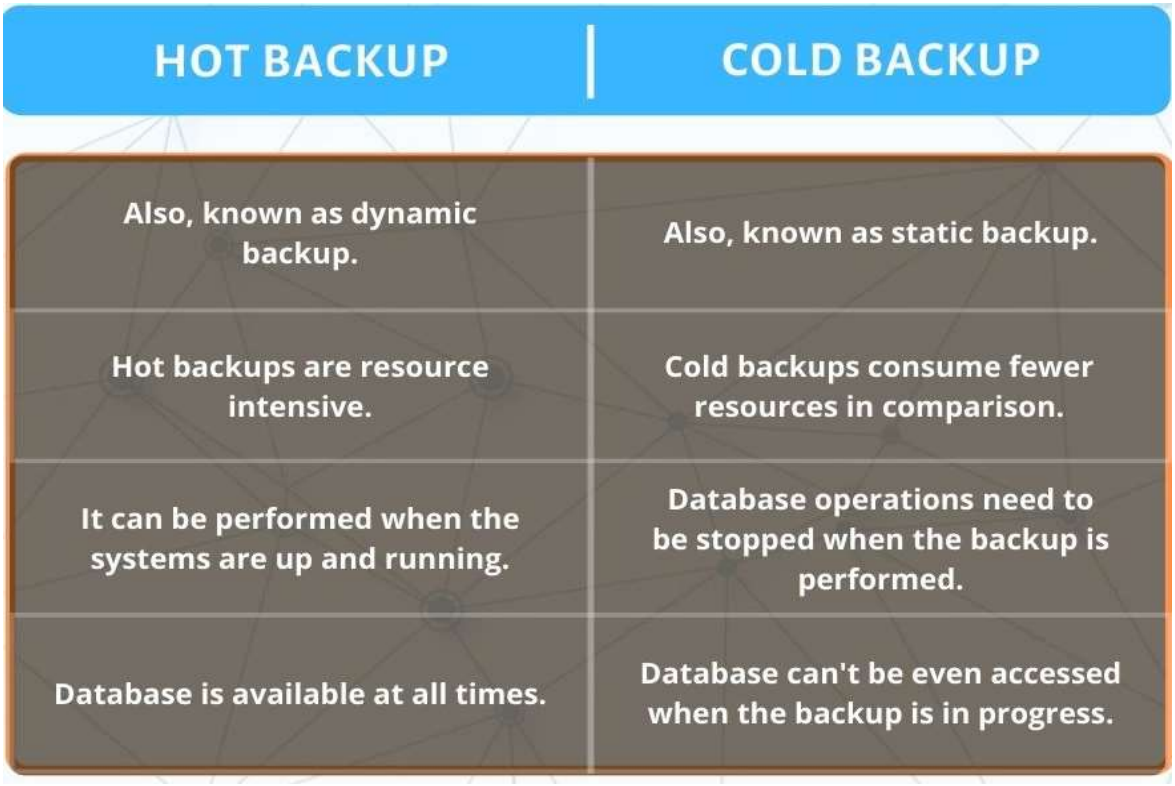
## 2.5. On-line file back-ups

It is also called a hot backup or dynamic backup. A hot backup is a backup performed while the database is open and available for use (read and write activity). It is performed in near real-time when the systems are up and running, and new data is continuously generated or captured.

In a hot backup, there is a time parameter involved as to when to perform a backup. This can range from seconds to minutes. The entire data is copied on the secondary location, and hence the relevant changes reflect in the new backup. Hot backups are a bit resource intensive as there are multiple iterations stored at a time. This allows the user to restore the backup to a required point.

The most important advantage here is the capability to continue business operations while the backup is in progress. The database is available at all times, and hence the business can continue as usual.

Table 2.2. Comparison of Hot Backup and Cold Backup




If you are an organization with business operations working around the clock and cannot afford any disturbance or downtime, then hot backup is the one for you.

This way, you can safeguard your data and keep your business applications and operations running. If you are an organization that has fixed working hours, then cold backup is better for

you. The data which has been updated through the working day will be easily copied over without any hindrances.

## 2.6. Disk mirroring

Disk mirroring, also known as RAID 1, is the replication of data to two or more disks. Disk mirroring is a strong option for data that needs high availability because of its quick recovery time. It's also helpful for disaster recovery because of its immediate failover capability. Disk mirroring requires at least two physical drives. If one hard drive fails, an organization can use the mirror copy. While disk mirroring offers comprehensive data protection, it requires a lot of storage capacity.

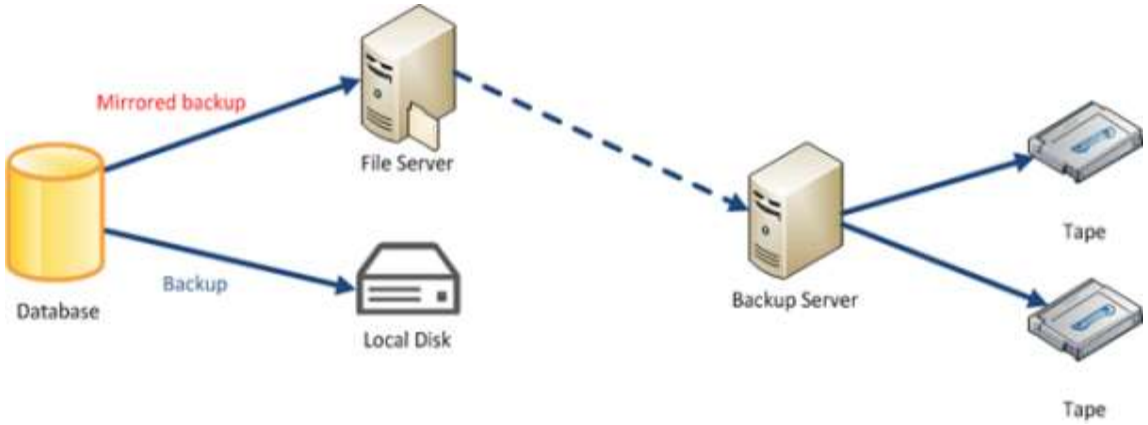



Figure 2.6. Database mirroring

## 2.7. RAID

RAID refers to redundancy array of the independent disk. It is a technology which is used to connect multiple secondary storage devices for increased performance, data redundancy or both. It gives the ability to survive one or more drive failure depending upon the RAID level used.

It consists of an array of disks in which multiple disks are connected to achieve different goals. There are 7 levels of RAID schemes. These schemas are as RAID 0, RAID 1, ...., RAID 6.

These levels contain the following characteristics:

- It contains a set of physical disk drives.
- The operating system views these separate disks as a single logical disk.

- In this technology, data is distributed across the physical drives of the array.
- Redundancy disk capacity is used to store parity information.
- In case of disk failure, the parity information can be helped to recover the data.

### 2.7.1. RAID 0

RAID level 0 provides data stripping, i.e., a data can place across multiple disks. It is based on stripping that means if one disk fails then all data in the array is lost. This level doesn't provide fault tolerance but increases the system performance.

**Pros of RAID 0:**

- In this level, throughput is increased because multiple data requests probably not on the same disk.
- This level full utilizes the disk space and provides high performance.
- It requires minimum 2 drives.

**Cons of RAID 0:**

- It doesn't contain any error detection mechanism.
- The RAID 0 is not a true RAID because it is not fault-tolerance.
- In this level, failure of either disk results in complete data loss in respective array.

### 2.7.2. RAID 1

This level is called mirroring of data as it copies the data from drive 1 to drive 2. It provides 100% redundancy in case of a failure. Only half space of the drive is used to store the data. The other half of drive is just a mirror to the already stored data.

**Pros of RAID 1:**

- The main advantage of RAID 1 is fault tolerance. In this level, if one disk fails, then the other automatically takes over.
- In this level, the array will function even if any one of the drives fails.

**Cons of RAID 1:**

- In this level, one extra drive is required per drive for mirroring, so the expense is higher.

### 2.7.3. RAID 2

RAID 2 consists of bit-level striping using hamming code parity. In this level, each data bit in a word is recorded on a separate disk and ECC code of data words is stored on different set disks. Due to its high cost and complex structure, this level is not commercially used. The same performance can be achieved by RAID 3 at a lower cost.

**Pros of RAID 2:**

- This level uses one designated drive to store parity.
- It uses the hamming code for error detection.

**Cons of RAID 2:**

- It requires an additional drive for error detection.

### 2.7.4. RAID 3

RAID 3 consists of byte-level striping with dedicated parity. In this level, the parity information is stored for each disk section and written to a dedicated parity drive. In case of drive failure, the parity drive is accessed, and data is reconstructed from the remaining devices. Once the failed drive is replaced, the missing data can be restored on the new drive. In this level, data can be transferred in bulk. Thus high-speed data transmission is possible.

**Pros of RAID 3:**

- In this level, data is regenerated using parity drive.
- It contains high data transfer rates.
- In this level, data is accessed in parallel.

**Cons of RAID 3:**

- It required an additional drive for parity.
- It gives a slow performance for operating on small sized files.

### 2.7.5. RAID 4

RAID 4 consists of block-level stripping with a parity disk. Instead of duplicating data, the RAID 4 adopts a parity-based approach. This level allows recovery of at most 1 disk failure

due to the way parity works. In this level, if more than one disk fails, then there is no way to recover the data. Level 3 and level 4 both are required at least three disks to implement RAID.

In this level, parity can be calculated using an XOR function. If the data bits are 0,0,0,1 then the parity bits is XOR (0,1,0,0) = 1. If the parity bits are 0,0,1,1 then the parity bit is XOR (0,0,1,1)= 0. That means, even number of one results in parity 0 and an odd number of one results in parity 1.

This level allows us to recover lost data.

### 2.7.6. RAID 5

RAID 5 is a slight modification of the RAID 4 system. The only difference is that in RAID 5, the parity rotates among the drives. It consists of block-level striping with DISTRIBUTED parity. Same as RAID 4, this level allows recovery of at most 1 disk failure. If more than one disk fails, then there is no way for data recovery. This level was introduced to make the random write performance better.

**Pros of RAID 5:**

- This level is cost effective and provides high performance.
- In this level, parity is distributed across the disks in an array.
- It is used to make the random write performance better.

**Cons of RAID 5:**

- In this level, disk failure recovery takes longer time as parity has to be calculated from all available drives.
- This level cannot survive in concurrent drive failure.

### 2.7.7. RAID 6

This level is an extension of RAID 5. It contains block-level stripping with 2 parity bits. In RAID 6, you can survive 2 concurrent disk failures. Suppose you are using RAID 5, and RAID 1. When your disks fail, you need to replace the failed disk because if simultaneously another disk fails then you won't be able to recover any of the data, so in this case RAID 6 plays its part where you can survive two concurrent disk failures before you run out of options.

**Pros of RAID 6:**

- This level performs RAID 0 to strip data and RAID 1 to mirror. In this level, stripping is performed before mirroring.
- In this level, drives required should be multiple of 2.

**Cons of RAID 6:**

- It is not utilized 100% disk capability as half is used for mirroring.
- It contains very limited scalability.

## 2.8. Off-site back-up files

Offsite backup is the replication of the data to a server which is separated geographically from a production systems site. Offsite data backup may also be done via direct access, over Wide Area Network (WAN). An offsite backup is a backup process or facility that stores backup data or applications external to the organization or core IT environment.
It is similar to a standard backup process, but uses a facility or storage media that is not physically located within the organization's core infrastructure.

Offsite backups are primarily is used in data backup and disaster-recovery measures. The core objective behind storing and maintaining data at a backup facility is to:

- Secure data from malicious attacks
- Keep a backup copy of data in case the primary site is damaged or destroyed

Cloud backup, online backup or managed backup are examples of offsite backup solutions that enable an individual or organization to store data at facilities that are geographically and logically external.

- **Advantages and disadvantages Offsite Storage**

**Advantages**

Offsite storage has several major advantages. Some of them are;

- **Scalability:**. The cloud provider or managed service provider is responsible for offering storage that can be expanded on demand.
- **Cost & Value:** Offsite and cloud storage is extremely affordable; in most circumstances, you only pay for what you use. There is no initial outlay for expensive storage platforms and no additional maintenance or support contracts.
- **Fast Deployment:** With offsite cloud storage, the infrastructure is already in place, and the platform is already available to use. There is no waiting for purchasing and installation of hardware and the client can simply plug into the cloud storage and get started immediately.
- **Managed Storage Service:** The cloud provider will usually have a team of storage experts and subject matter experts who own the solution and manage the service for its clients. Many providers offer automated object storage deployment, where blobs of data storage can be assigned and removed when needed.
- **Connectivity:** Offsite storage can be made available over an internet connection or a dedicated virtual private network for added security. This flexible approach to connectivity is great for clients, as it makes accessing data extremely easy. Dedicated network links can provide high-speed data pipes between the clients and the storage for ultra-fast connectivity.
- **Performance:** Offsite storage performance has gotten significantly faster in recent years. Network improvements have boosted the performance of storage and, in most circumstances, provide near real-time response rates.

- **Disadvantages**

Some disadvantages of offsite storage include;

- **It can be difficult to access** the data when it is needed. For example, some of the offsite data servers will be routinely taken offline in order to perform preventive maintenance. During that time period, access to the offsite data will either be severely limited or

completely cut off. In most cases, clients who use offsite storage are given plenty of notice when a site is going down for maintenance or repair.

- **Security and Privacy:** One of the major concerns with offsite cloud storage is the security and integrity of data. Data protection and privacy are extremely important for business organizations. If you choose to move data to an offsite storage provider, consideration must be given to compliance as well as the security measures in place to protect the data. Offsite storage must be protected from unauthorized access and should always be encrypted.
- **Compliance and Data Governance:** there are complex compliance and governance rules which must be adhered to when securing or destroying data.
- **Lifetime Costs**: Offsite storage is often affordable; however, there may be a risk of vendor lock-in when an organization is reliant on the provider's organization. This may result in a lifetime of monthly charges for data usage, so it's important to weigh up if the overall costs and benefits outweigh implementing local storage.

**Speed:** Although cloud/offsite performance is generally very good, some data-intense applications may perform better using local storage. Even if dedicated express routes are used, latency and network bottlenecks may impact performance.

**Noisy Neighbours:** When choosing offsite storage, it's important to understand whether you will be leveraging dedicated offsite storage or if you will be using shared storage.

## 2.9. Onsite Backup

In onsite storage, data and storage hardware are geographically located internally to your business or organization. You may have a computer room or data center onsite where the storage arrays are securely located. All your internal systems will have direct access to the storage within the same building or organization, usually over an internal Local Area Network (LAN).

Organizations supporting databases with a high data change rate will often employ an onsite backup strategy for quick recovery in the event of a failure.

Onsite storage usually entails storing important data on a periodic basis on local storage devices, such as hard drives, DVDs, magnetic tapes, or CDs. Offsite storage requires storing important data on a remote server, usually via the Internet, although it can also be done via direct access.

- **Advantages of onsite storage:**
  - Immediate access to data
  - Less expensive
  - Internet access not needed
  - Control of your own data security
  - Performance improvement
- **Disadvantage of onsite storage;**

- In the event of a catastrophic event, onsite data storage can be destroyed. For example, if there is a fire in the building, or a water main bursts, the onsite servers can lose all the data that has been collected on them. In addition, onsite storage units can also be stolen, resulting in a loss of time, money, and data.
- Storage can be extremely expensive depending on the size of the storage array.
- Storage device will need to be managed, maintained, and upgraded in-house.

## 2.10. Hybrid storage

This section will focus on onsite and offsite storage advantages and disadvantages; however, for the benefit of completeness, it's important mention hybrid storage. Hybrid storage is a mix of offsite and onsite storage approaches. A typical hybrid setup could be a local storage array at a head office which replicates data to an external cloud-based location; such a setup could be for backups or data integrity reasons.

# Self-check 2

**Part-I multiple choice**

1. Backing up the data to a server which is geographically separated from a production systems.
   A. Online B. Offline C. Offsite D. Onsite
2. A mix of offsite and onsite storage approaches for the benefit of completeness.
   A. Dynamic B. Hybrid C. Cloud D. Cold
3. One is not the advantages of onsite backup
   A. May be destroyed during a catastrophic event C. Control of your own data security
   B. Immediate access to data D. Less expensive
4. Which RAID level is called a mirroring of data?
   A.RAID 0 B. RAID 1 C. RAID 2 D. RAID 7 E. All level
5. How many disk drives are required to implement disk mirroring?
   A. At least two physical drives.
   B. At least one disk drive and two logical drives
   C. At least two logical drives
   D. None
6. Which one of the following statement is incorrect about RAID?
   B. It contains a set of physical disk drives.
   C. The operating system views these separate disks as a single logical disk.
   D. Data is distributed across the physical drives of the array.
   E. None

**Part-II Give short answer**

1. List and explain Types of backup?
2. Write the difference between hot and cold backup?
3. List the Advantages and Dis advantages of Full backup

# Operation sheet 2.1 Take backup

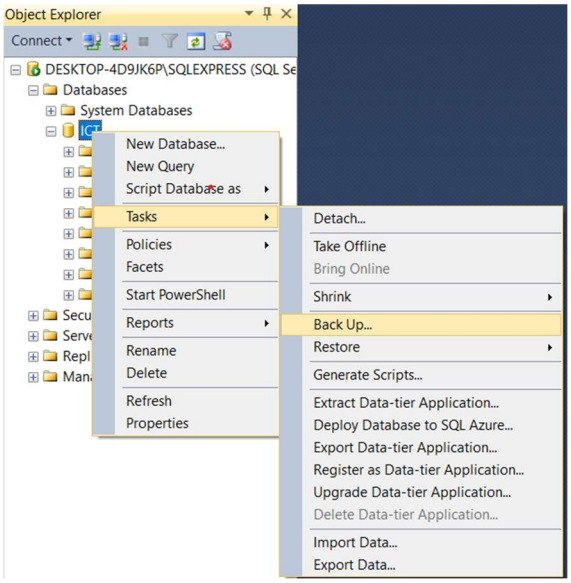
**Operation title:** Take backup

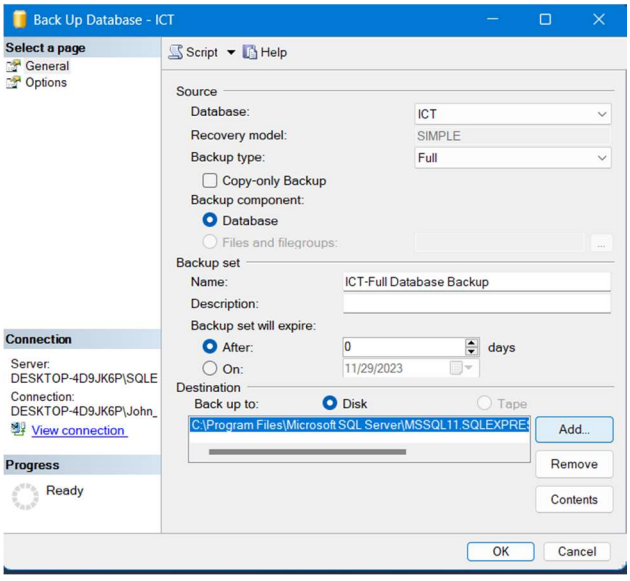
**Purpose:** Take database Backup Using SSMS

**Tools and equipment:** SQL server installed computer

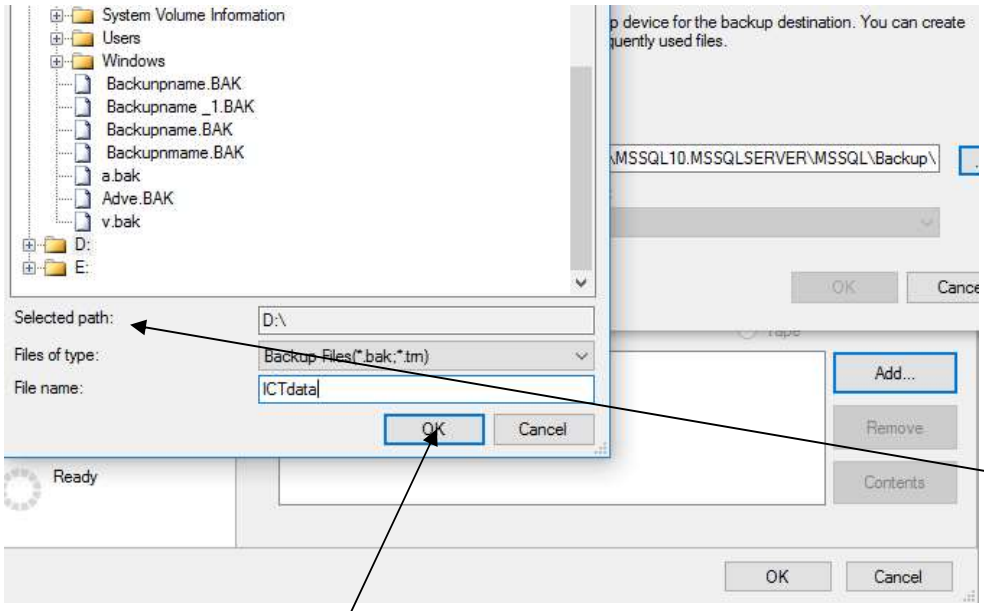
**Steps by doing tasks:**

1. Open SQL Server 2008
2. Connect the Server and point to your database
3. Make right click on your database and Select Task→ click on Backup

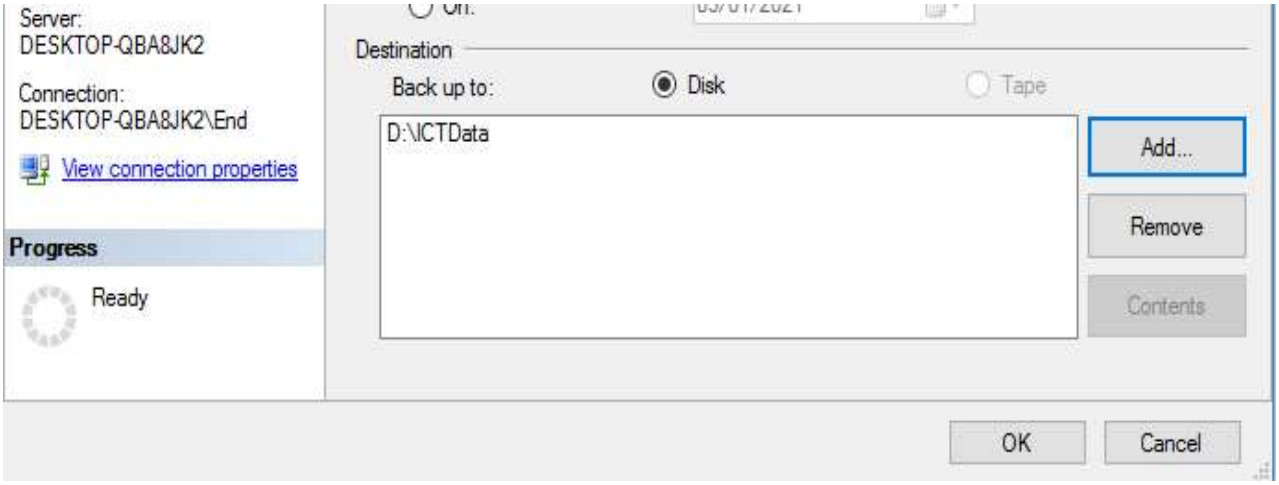


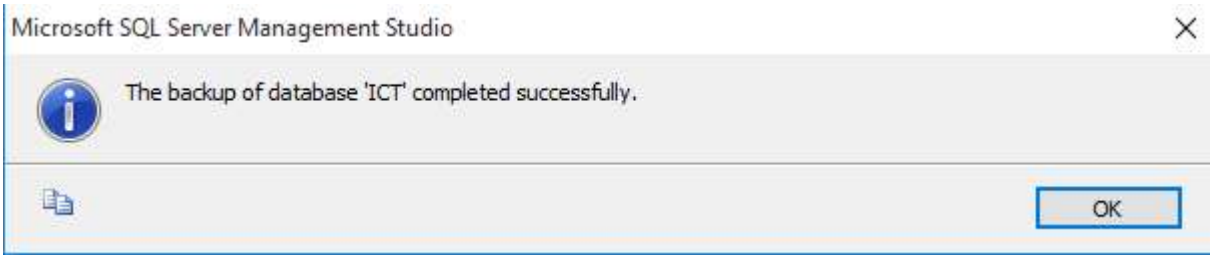

4. Select the backup destination and write the backup name(Add)




5. Click on OK button




6. Click on OK button



# Operation sheet 2.2 Taking Database Offline

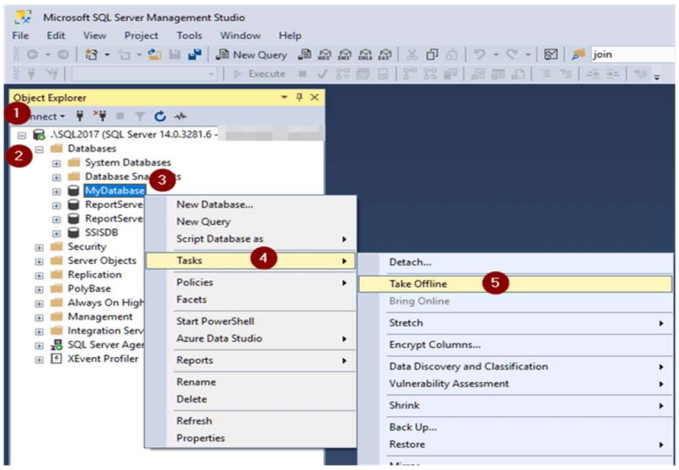
**Operation title:** Taking Database Offline

**Purpose:** Taking Database Offline using SSMS (SQL Server Management Studio) and T-SQL

**Tools and Equipment**: computer and SQL server

**Steps by doing tasks:**

1. Login to SQL Server Management Studio.
2. In the Object Explorer, select the **database** you want to **take offline** and right-click.
3. In the right-click menu go to Tasks >> **Take Offline**.
4. In the pop-up window, choose the check box under the Drop All Active Connections and click OK




5. After Opening SQL Server Management Studio and open a Query Editor pane. Enter and execute the following code:

```
USE DB_name;

GO

ALTER DATABASE <<Database-name>>  SET OFFLINE
```

# Operation sheet 2.3 Take Full backup

**Operation title:** Take Full backup

**Purpose:** Back Up the Database Using T-SQL

**Tools And Equipment**: computer and SQL server

**Steps by doing tasks:**

1. After Opening SQL Server Management Studio and open a Query Editor pane. Enter and execute the following code:

```
BACKUP DATABASE << databaseName >> TO DISK = 'C:\Backupname.BAK'
```

The command is BACKUP DATABASE databaseName. The "TO DISK" option specifies that the backup should be written to disk and the location and filename to create the backup is specified.

2. Create a full SQL Server backup with a password

```
BACKUP DATABASE << databaseName >>
TO DISK = 'C:\ Backupname.BAK'
WITH PASSWORD = 'Q!W@E#R$'
GO
```

# LAP Tests

**Instructions:** Given necessary templates, tools and materials you are required to perform the following tasks accordingly.

**Task 1:** To do the following tasks use database Backup Using SSMS and T-SQL

**Task2:** Create a database named TVET.

**Task 3:** Create a folder named "**Data**" on the desktop and take the backup of your database in **Data** folder using "SSMSbackup" and "TSQLbackup" as a backup name using both SSMS and T-SQL respectively.

**Task 4:** Create a mirrored SQL Server backup

**Task 5:** Create a full SQL Server backup with progress stats

# Unit Three: Database Recovery Points & Procedures

This unit is developed to provide you the necessary information regarding the following content coverage and topics:

- Database Recovery Points
- Restore Process
- Point-of-Failure Database Restoration

This unit will also assist you to attain the learning outcomes stated in the cover page. Specifically, upon completion of this learning guide, you will be able to:

- Identify strategic recovery points based on backup arrangements and organizational guidelines.
- Develop a comprehensive test plan for the restore process
- Minimize downtime during the testing process and address any issues promptly
- Understand the steps involved in point-of-failure restoration

## 3.1.Database recovery point

Database recovery is the process of restoring the database to a correct (consistent) state in the event of a failure. In other words, it is the process of restoring the database to the most recent consistent state that existed shortly before the time of system failure.

There are many situations in which a transaction may not reach a commit or abort point. Some of them include;

An operating system crash can terminate the DBMS processes

- The DBMS can crash
  - System failure(e.g. power outage)
    - ✓ Affects all transactions currently in progress but does not physically damage the data (softcrash)
  - Media failures(e.g. Head crash on the disk)
    - ✓ damage to the database (hard crash)
    - ✓ need backup data
  - The system might lose power
  - Human error can result in deletion of critical data.

In any of these situations, data in the database may become inconsistent or lost.

When a DBMS recovers from a crash, it should maintain the following

- It should check the states of all the transactions, which were being executed.
- A transaction may be in the middle of some operation; the DBMS must ensure the atomicity of the transaction in this case.
- It should check whether the transaction can be completed now or it needs to be rolled back.
- No transactions would be allowed to leave the DBMS in an inconsistent state.

In case of any type of failures, a transaction must either be aborted or committed to maintain data integrity.

Transaction log plays an important role for database recovery and bringing the database in a consistent state in the event of failure. Transactions represent the basic unit of recovery in a database system. The recovery manager guarantees the atomicity and durability properties of transactions in the event of failures. During recovery from failure, the recovery manager ensures that either all the effects of a given transaction are permanently recorded in the database or none of them are recorded. A transaction begins with successful execution of a <T, BEGIN>" (begin transaction) statement.

### 3.1.1. Database Recovery Techniques

- For fast restoration or recovery of data, the database must hold tools which recover the data efficiently. It should have atomicity means either the transactions showing the consequence of successful accomplishment perpetually in the database or the transaction must have no sign of accomplishment consequence in the database.

- So, recovery techniques which are based on deferred update and immediate update or backing up data can be used to stop loss in the database.

- **Immediate Update**: As soon as a data item is modified in cache, the disk copy is updated.

- **Deferred Update**: All modified data items in the cache are written either after a transaction ends its execution or after a fixed number of transactions have completed their execution.

- **Shadow update:** The modified version of a data item does not overwrite its disk copy but is written at a separate disk location.

- **In-place update**: The disk version of the data item is overwritten by the cache version.

### 3.1.2. Two approaches of Recovery

- **Manual Reprocessing**

In a Manual Reprocessing recovery approach, the database is periodically backed up (a database *save*) and all transactions applied since the last save are recorded

If the system crashes, the latest database backup set is restored and all of the transactions are re-applied (by users) to bring the database back up to the point just before the crash.

- Several shortcomings to the Manual Reprocessing approach:
  - ✓ Time required to re-apply transactions
  - ✓ Transactions might have other (physical) consequences
  - ✓ Re-applying concurrent transactions in the same original sequence may not be possible.

- **Automated Recovery with Rollback / Roll forward**
  - Introduce a Log file – this is a file separate from the data that records all of the changes made to the database by transactions. Also referred to as a Journal.
  - This *transaction log* Includes information helpful to the recovery process such as: A transaction identifier, the date and time, the user running the transaction, *before images* and *after images.*
    - ✓ **Before Image**: A copy of the table record (or data item) before it was changed by the transaction.
    - ✓ **After Image**: A copy of the table record (or data item) after it was changed by the transaction.
  - The Automated Recovery process uses both rollback and roll forward to restore the database.

- ✓ **Rollback**: Undo any partially completed transactions (ones in progress when the crash occurred) by applying the *before images* to the database. **UNDO** the transactions in progress at the time of failure.
- ✓ **Roll forward**: Redo the transactions by applying the *after images* to the database. This is done for transactions that were committed before the crash. **REDO** the transactions that successfully complete but did not write to the physical disk.
- ✓ **Checkpoint** is a mechanism where all the previous logs are removed from the system and stored permanently in a storage disk. **Checkpoint** declares a **point** before which the **DBMS** was in consistent state, and all the transactions were committed. **Checkpoints** can also be taken (less time consuming) in between database saves.

- ➢ The DBMS flushes all pending transactions and writes all data to disk and transaction log.
- ➢ Database can be recovered from the last checkpoint in much less time.

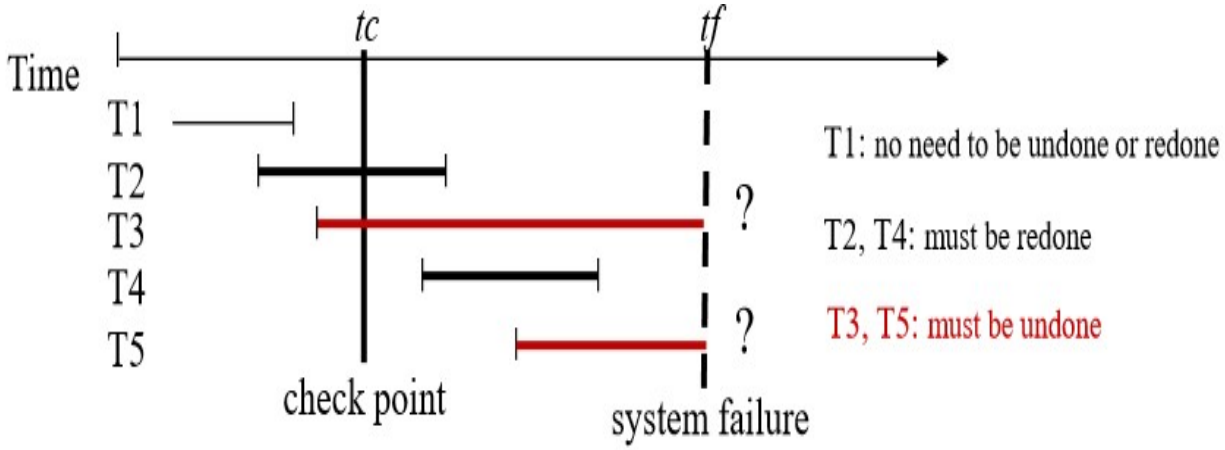



Figure 1.1. Recovery with Rollback / Roll forward

For example in the figure above;

STEP1: UNDO-list = list of transactions given in the checkpoint record = {T2, T3}

REDO-list = { }

STEP2: Search forward through the log, starting from the checkpoint, to the end of log:

• If a 'BEGIN TRANSACTION' is found => add to UNDO-list {T2, T3, T4, T5}

• If a 'COMMIT' is found => remove from UNDO-list to REDO-list

UNDO-list = {T3, T5} (System works backward through the log, undoing the UNDO-List.)

REDO-list = {T2, T4} (System then works forward through the log, redoing the REDO-List)

## 3.2.Testing restore process

Test Database recovery testing is used to ensure that the database is recovered. Recovery testing allows you to find out whether the application is running properly and to check retrieving invaluable data that would have been lost if your recovery method is not properly setup.

You also check if several critical processes are running smooth to ensure that the data recovery will pass smoothly through the testing phase.

The key aim of backup testing is to ensure the business can retrieve its data and continue operations. Businesses should test that they can restore files, folders and volumes from backups on a storage volume, user and application basis. Backup testing should be regular and routine. In an ideal world, businesses would test every backup, but that is rarely practical.

- **Common Steps in Database Backup and Recovery Testing**

In database recovery testing, you need to run the test in the actual environment to check if the system or the data can actually be recovered in case of any disasters and any other unforeseen events in the business environment.

- The common actions performed in Database Recovery Testing:

- Testing of database system
- Testing of the SQL files
- Testing of partial files
- Testing of data backup
- Testing of Backup tool
- Testing log backups

These policies should set out the recovery point objective (RPO) and the recovery time objective (RTO).

The RPO sets out how old the most recent backup can be, or put another way, the amount of data loss the organization can tolerate and still operate. The RTO specifies how quickly systems must be recovered. Unless the business tests recovery, CIOs will not know if they can meet the RTO and RPO, or if recovery works at all.

## 3.3.Restore a database to a point in time

A point-in-time recovery can be used to return the database data and database object to its functional state prior to detrimental action has been performed.

The ability to perform this kind of recovery depends on a recovery model set for the database. The database must be in either the Full or Bulk-Logged recovery model. In case the Simple recovery mode was used, this recovery method is not possible.

In case of using the Bulk-Logged recovery model some errors may occur and recovery to a point in time might fail. An error will be thrown in case when any bulk-logged operations were performed. As such operations are minimally logged; there is not sufficient data in a particular transaction log.

When you issue a RESTORE DATABASE or RESTORE LOG command the WITH RECOVERY option is used by default.

If you restore a "Full" backup the default setting it to RESTORE WITH RECOVERY, so after the database has been restored it can then be used by your end users.

If you are restoring a database using multiple backup files, you would use the WITH NORECOVERY option for each restore except the last.

If your database is still in the restoring state and you want to recover it without restoring additional backups you can issue a RESTORE DATABASE. WITH RECOVERY to bring the database online for users to use.

The RESTORE ... WITH NORECOVERY option puts the database into a "restoring" state, so additional backups can be restored. When the database is in a "restoring" state no users can access the database or the database contents.

When you issue a RESTORE DATABASE or RESTORE LOG command; the WITH NORECOVERY option allows you to restore additional backup files before recovering the database. This therefore allows you to get the database as current as possible before letting your end users access the data.

This option is not on by default, so if you need to recover a database by restoring multiple backup files and forget to use this option you have to start the backup process all over again.

The most common example of this would be to restore a "Full" backup and one or more "Transaction Log" backups.

### 3.3.1. Restore a database using T-SQL

- **Restore full backup and one transaction log backup**

The first command does the restore and leaves the database in a restoring state and second command restores the transaction log backup and then makes the database useable.

```
RESTORE DATABASE <<DatabaseName>>FROM DISK = 'C:\BackupName.BAK'
WITH NORECOVERY
GO
RESTORE LOG <<DatabaseName>> FROM DISK = 'C:\BackupName.TRN'
WITH RECOVERY
GO
```

- **Restore full backup and two transaction log backups**

This restores the first two backups using NORECOVERY and then RECOVERY for the last restore.

```
RESTORE DATABASE <<DatabaseName>>  FROM DISK = 'C:\ BackupName.BAK'
WITH NORECOVERY
GO
RESTORE LOG <<DatabaseName>>  FROM DISK = 'C:\ BackupName.TRN'
WITH NORECOVERY
GO
RESTORE LOG <<DatabaseName>>  FROM DISK = 'C:\ BackupName1.TRN'
WITH RECOVERY
GO
```

- **Restore full backup, latest differential and two transaction log backups**

This restores the first three backups using NORECOVERY and then RECOVERY for the last restore.

```
RESTORE DATABASE <<DatabaseName>>   FROM DISK = 'C:\ BackupName.BAK'
WITH NORECOVERY
GO
RESTORE DATABASE <<DatabaseName>>   FROM DISK = 'C:\ BackupName.DIF'
WITH NORECOVERY
GO
RESTORE LOG <<Database Name>>   FROM DISK = 'C:\ BackupName.TRN'
WITH NORECOVERY
GO
RESTORE LOG <<DatabaseName>>   FROM DISK = 'C:\ BackupName1.TRN'
WITH RECOVERY
GO
```

# Self-check 3

**Part-I multiple choice**

1. _____the process of restoring the database to the consistent state in the event of a failure.

   A. Restore B. Attach C. Recovery D. All

2. A process by which DBMS REDO the transactions that successfully complete before failure but did not write to the physical disk.

   B. Recover B. Roll Forward C. Rollback D. Restore

3. A recovery method by which the modified version of a data item is written at a separate disk location.

   A. Differed Update
   B. Shadow update
   C. Immediate update
   D. None

4. Factors that enforce the transaction not to reach a commit or abort point.

   A. Human error
   B. operating system crash
   C. DBMS crash
   D. All

## Part-II Give short Answer

1. Write and explain recovery approaches
2. Explain Rollback and commit

# Operation sheet 3.1

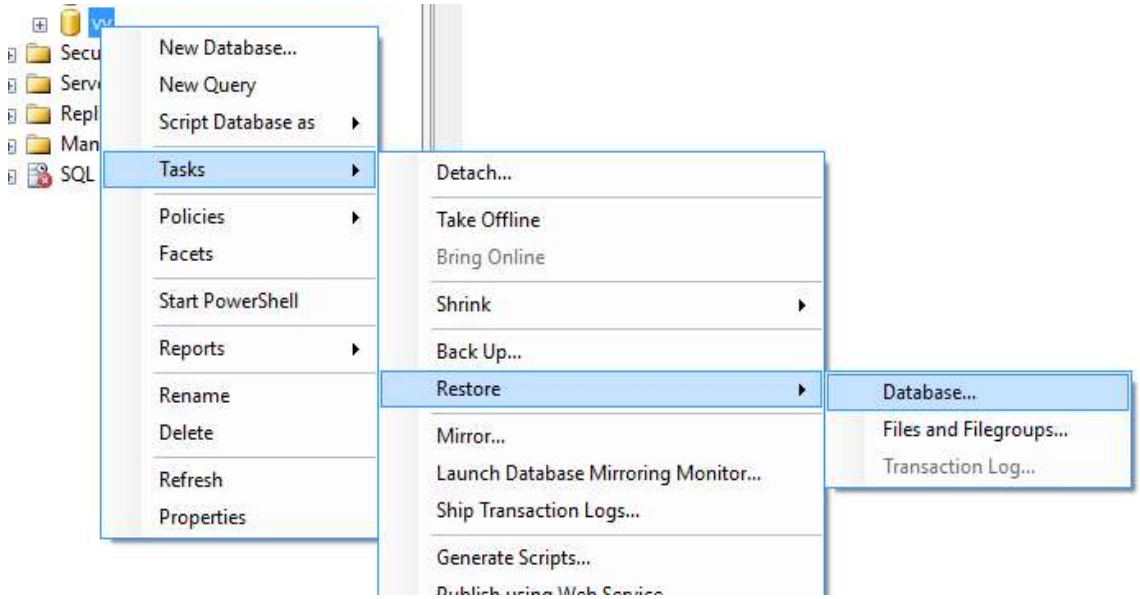
Operation title: Restoring Database from the backup

Purpose: Restore Database from the backup

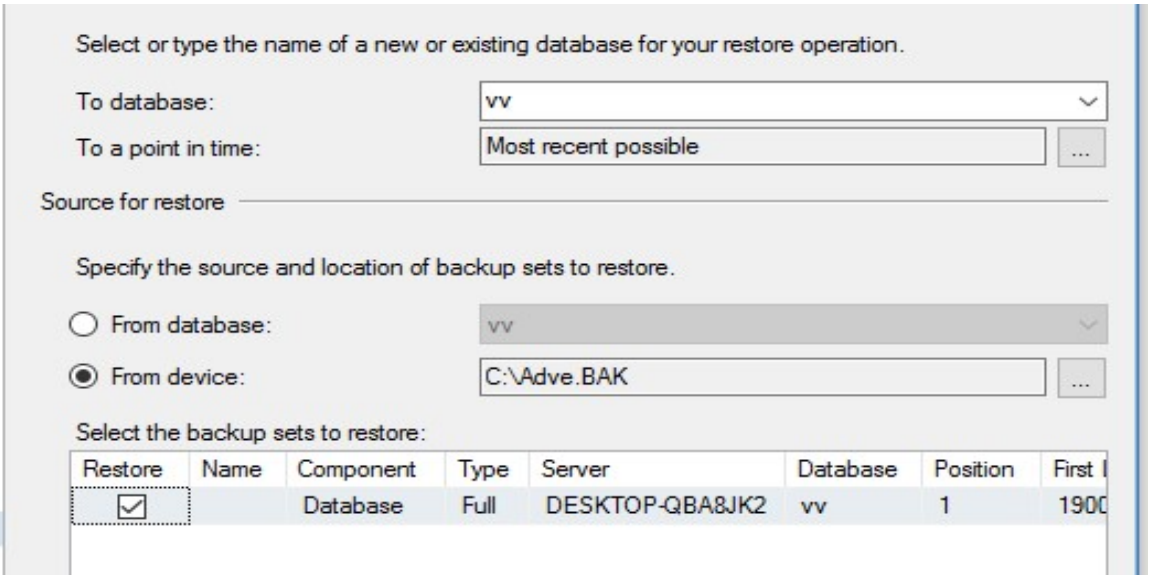
Material: computer and SQL server

**Steps**

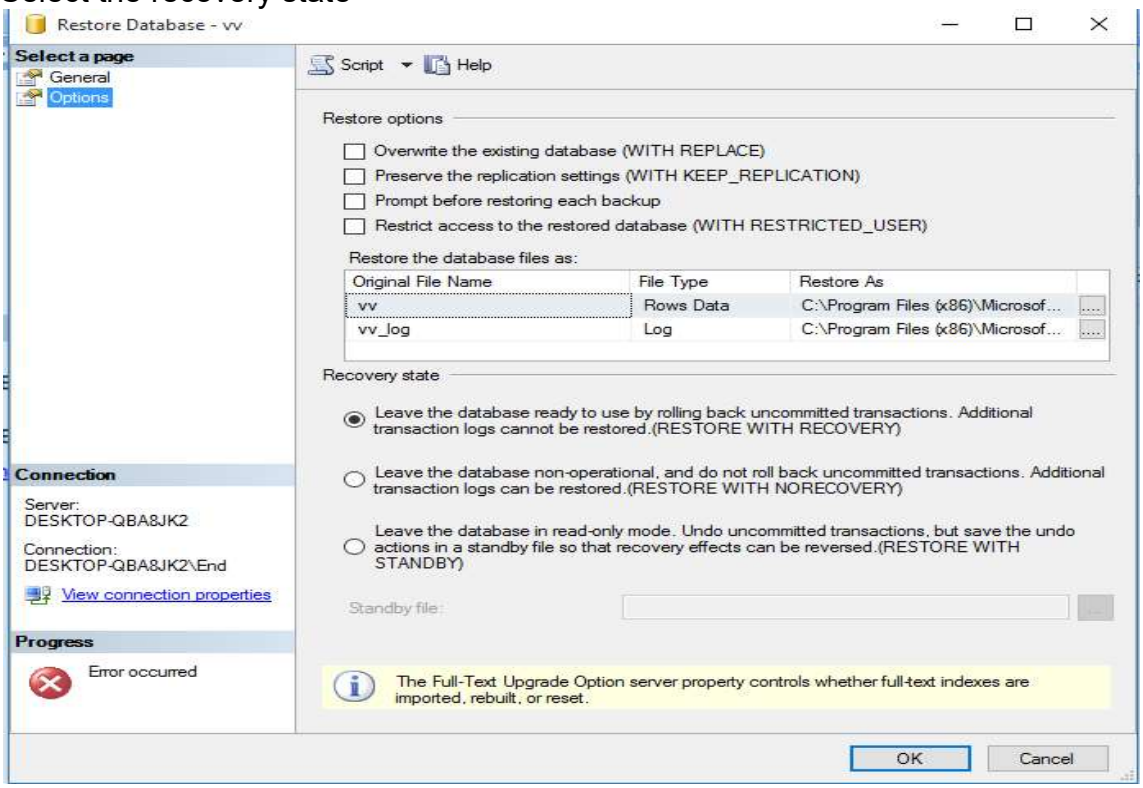
1. Open SQL Server 2008
2. Select the Master database
3. Make right click your database (VV)
4. Point on Tasks→Restore→click on Database




5. Specify the location of your backup




6. Select the recovery state




7. Click OK button

# LAP Test

Instructions: Given necessary templates, tools and materials you are required to perform the

Task 1: backup Database using T-SQL?

Task 2 Restoring Database from the backup by using T-SQL?

# References

## Books

Database Backup & Recovery B.H.GARDI COLLEGE OF ENGINEERING & TECHNOLOGY

## URL

https://www.guru99.com/dbms-architecture.html

https://learn.org/articles/What_is_Database_Architecture.html

https://www.javatpoint.com/dbms-architecture

https://searchdatabackup.techtarget.com/feature/Full-incremental-or-differential-How-to-choose-the-correct-backup-type

https://www.datto.com/blog/data-backup-and-recovery-methods-the-basics-you-need-to-know

https://www.backup4all.com/mirror-backup-kb.html

https://www.mssqltips.com/sqlservertutorial/112/recovering-a-sql-server-database-that-is-in-the-restoring-state/

https://www.tutorialspoint.com/dbms/dbms_data_recovery.htm

‘

# Developer's Profile

| No | Name | Qualification | Field of Study | Organization/ Institution | Mobile number | E-mail |
|---|---|---|---|---|---|---|
| 1 | Frew Atkilt | M-Tech | Network & Information Security | Bishoftu Polytechnic College | 0911787374 | frew.frikii@gmail.com |
| 2 | Gari Lencha | MSc | ICT Managment | Gimbi Polytechnic | 0917819599 | Garilencha12@gmail.com |
| 3 | Kalkidan Daniel | BSc | Computer Science | Entoto Polytechnic | 0978336988 | kalkidaniel08@gmail.com |
| 4 | Solomon Melese | M-Tech | Computer Engineering | M/G /M/Polytechnic College | 0918578631 | solomonmelese6@gmail.com |
| 5 | Tewodros Girma | MSc | Information system | Sheno Polytechnic College | 0912068479 | girmatewodiros @gmail.com |
| 6 | Yohannes Gebeyehu | BSc | Computer Science | Entoto Polytechnic College | 0923221273 | yohannesgebeyehu73@gmail.com |