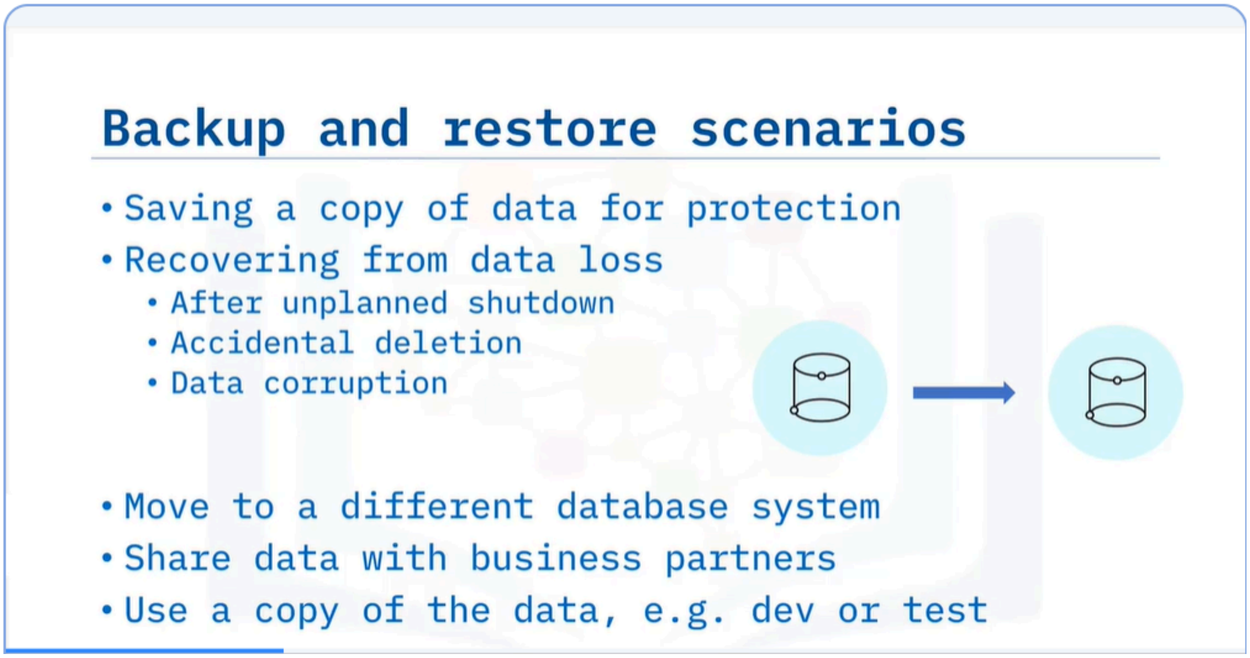
# Backup and Restore

Sure! Let's talk about the concept of **backup and restore** in databases.

Backup and restore is like having a safety net for your important data. Imagine you have a beautiful painting that you want to keep safe. You might take a photo of it (that's your backup) so that if something happens to the original, like it gets damaged or lost, you can recreate it from the photo (that's your restore). In the world of databases, backups protect your data from unexpected events like accidental deletions or system failures.

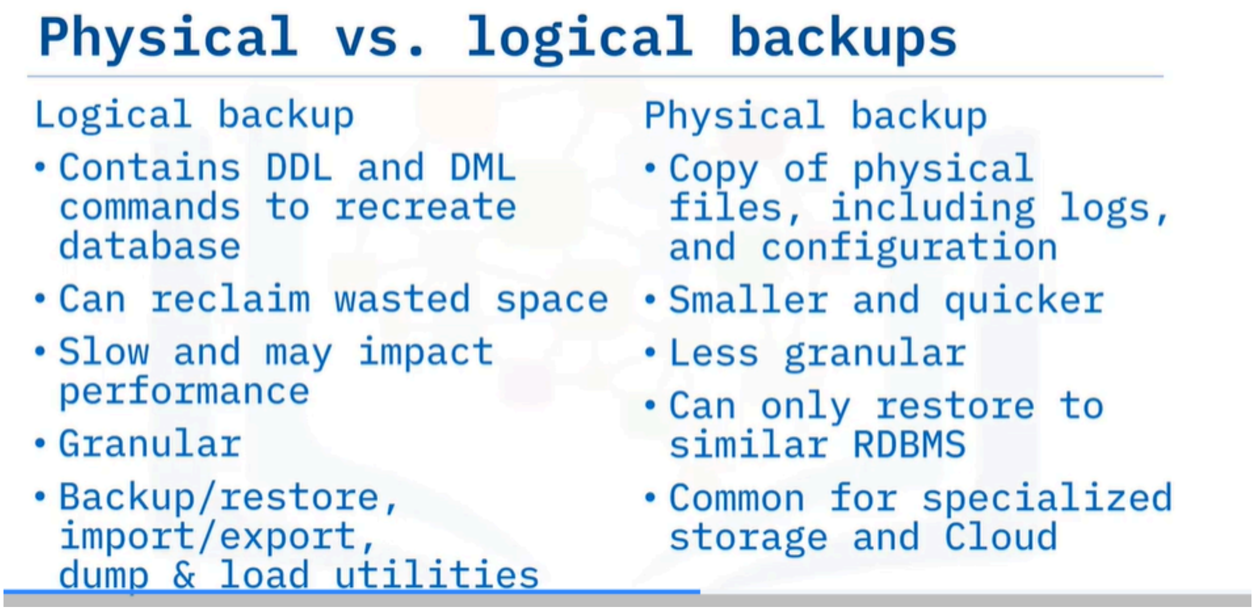
There are two main types of backups: **logical** and **physical**. A logical backup is like writing down the recipe for your favorite dish; it captures the steps and ingredients needed to recreate it. This means you can restore specific parts of your database, like a single table. On the other hand, a physical backup is like taking a snapshot of your entire kitchen, including all the ingredients and tools. This type is faster and captures everything, but it’s harder to pick out just one recipe from that snapshot.



## Backup and restore scenarios

- Saving a copy of data for protection
- Recovering from data loss
  - After unplanned shutdown
  - Accidental deletion
  - Data corruption
- Move to a different database system
- Share data with business partners
- Use a copy of the data, e.g. dev or test

- Backup and restore is a common phrase in database conversations and often used to refer to the process of backing up data for protection purposes- restoring it after data loss from an unplanned shutdown, accidental deletion, or data corruption. However, there are other scenarios when you might want to backup or restore your databases or objects within them. As a data engineer you are likely to perform data backup and restore operations to transfer data from one database to another. This may be to facilitate a change of RDBMS, to share data with or load data from a business partner, or to create a copy of the data for use in another location or system, such as development or test.



## Physical vs. logical backups

Logical backup

- Contains DDL and DML commands to recreate database
- Can reclaim wasted space
- Slow and may impact performance
- Granular
- Backup/restore, import/export, dump & load utilities

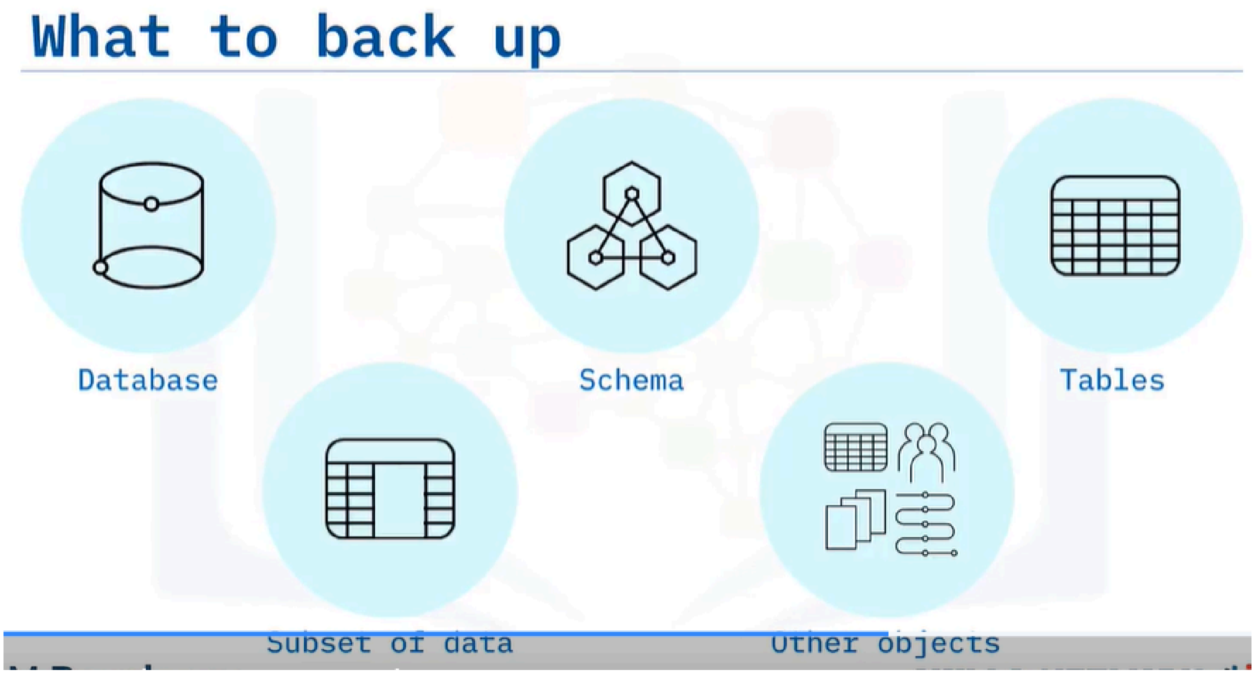
Physical backup

- Copy of physical files, including logs, and configuration
- Smaller and quicker
- Less granular
- Can only restore to similar RDBMS
- Common for specialized storage and Cloud

- When backing up databases, you can perform either logical or physical backups. A logical backup creates a file containing DDL (such as create table) and DML commands (such as insert) that recreate the objects and data in the database. As such, you can use this file to recreate the database on the same or another system. Generally, when you perform a logical backup and restore, you reclaim any wasted space from the original database because the restore process creates a clean version of the tables.
- Generating logical backups can take a long time for large databases and may impact the performance of other queries that are concurrently running. Logical backups enable you to backup granular objects. For example, you can back up

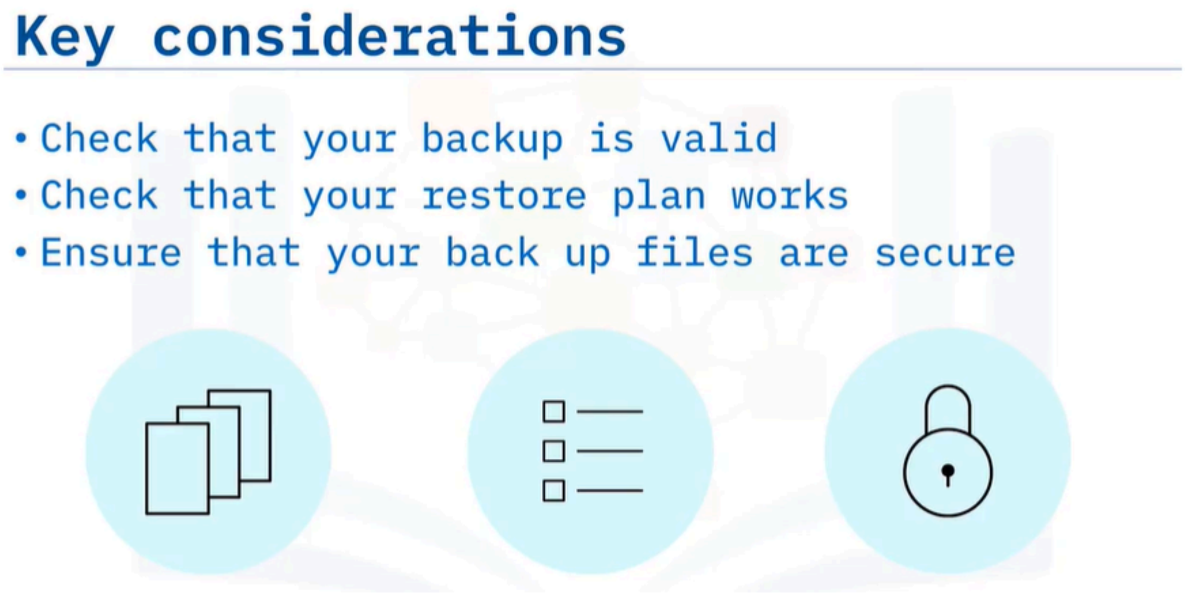
an individual database or table; however, you cannot use it to backup log files or database configuration settings. You typically use import, export, dump, and load utilities to perform logical backups.

- A physical or raw backup creates a copy of all the physical storage files and directories that belong to a table, database, or other objects, including the data files, configuration files, and log files to aid point-in-time recovery. Physical backups are often smaller and quicker than logical backups; they are useful for large or important databases that require fast recovery times. They are similar to backing up any other types of files on your physical system; however, this means you won’t be able to easily recover individual tables or database objects if a physical file contains data for more than one object. Because the backup file is specific to the RDBMS, you can only restore it to a similar system. This approach of taking storage level snapshots is common for databases utilizing specialized storage systems and on Cloud.



What to back up

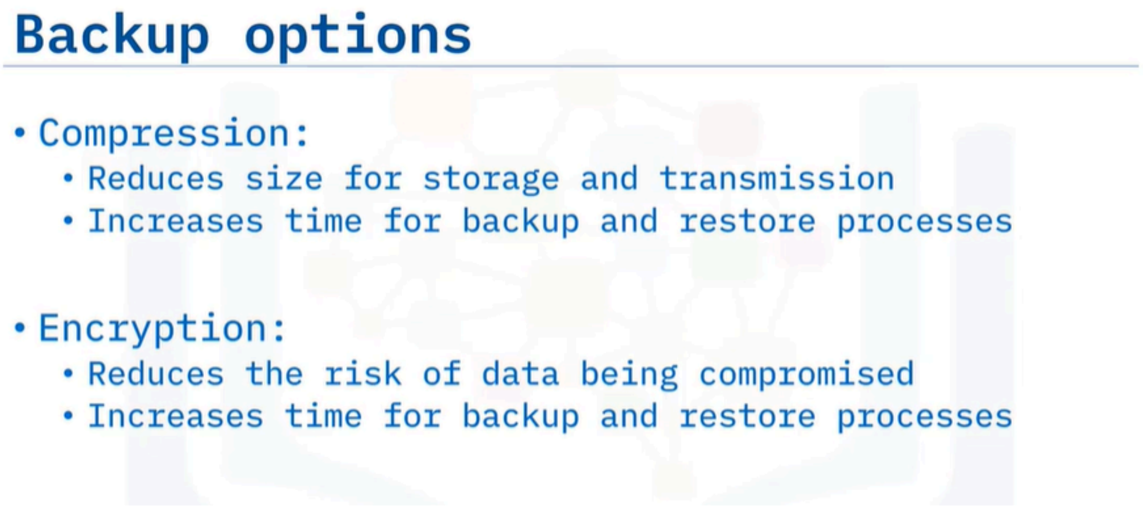
- You can choose exactly which parts of a database you want to backup. Depending on the RDBMS you are using and type of backup you are performing, you can back up a whole database, the contents of a schema, one or more tables from a database, a subset of data from one or more tables in a database, or a collection of other objects in the database. Because you can also choose the regularity and type of backup you perform, you can customize your backup policies to exactly meet your needs.



Key considerations

- Check that your backup is valid
- Check that your restore plan works
- Ensure that your back up files are secure

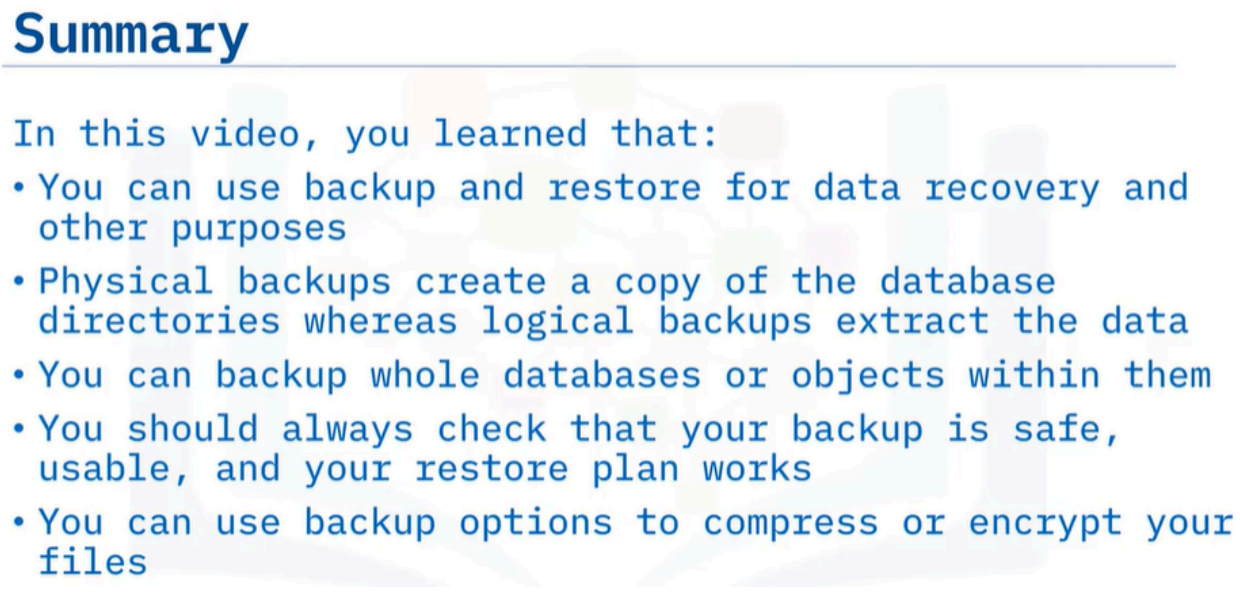
- When using backup and restore, you should remember to check that your back up file or files are valid and that you can use your restore plan to restore them successfully. It is essential to check these when using backup and restore as part of your disaster recovery plans, as an invalid back up or an inability to restore can result in data loss. You should also ensure that you secure the transfer and storage location of your back up files at the same level that you secure the data in your database.



## Backup options

- Compression:
  - Reduces size for storage and transmission
  - Increases time for backup and restore processes
- Encryption:
  - Reduces the risk of data being compromised
  - Increases time for backup and restore processes

- When performing backups, some RDBMSs support additional options that you can use: You may be able to configure a compression level for the backup files. Compressing the files will reduce the output file size which can be useful for large databases or if you are backing up to a remote location; however, it comes at a cost of time taken to perform the backup and the restore procedures. You may also be able to encrypt the backup files, to reduce the risk of any data being compromised. But again, this will increase the time taken for the backup and restore.



## Summary

In this video, you learned that:

- You can use backup and restore for data recovery and other purposes
- Physical backups create a copy of the database directories whereas logical backups extract the data
- You can backup whole databases or objects within them
- You should always check that your backup is safe, usable, and your restore plan works
- You can use backup options to compress or encrypt your files