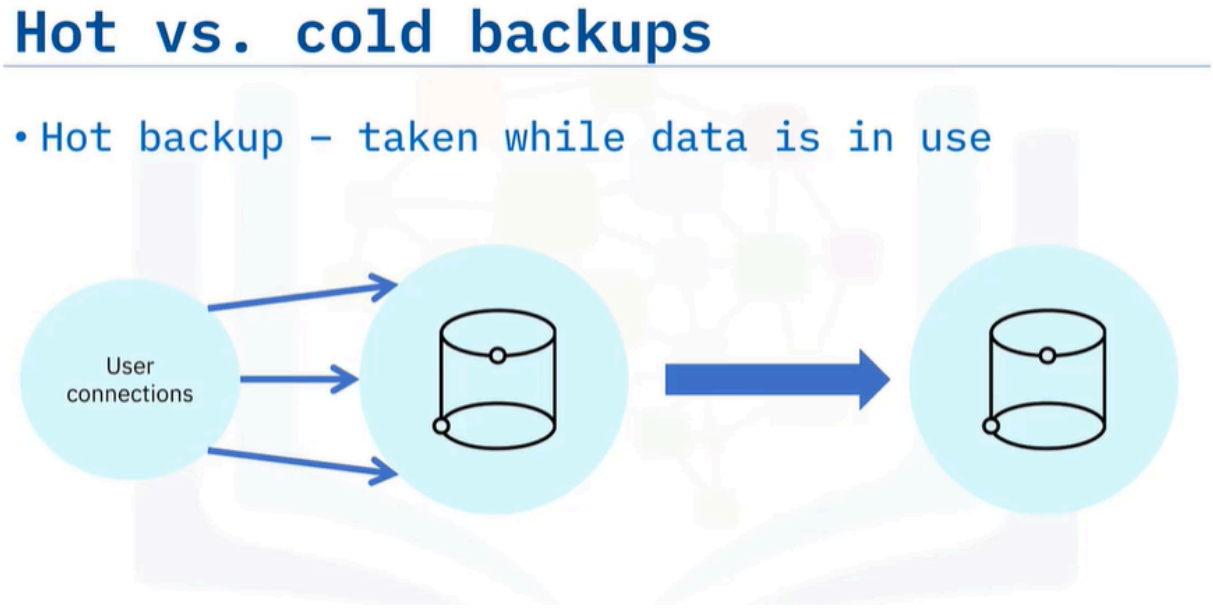
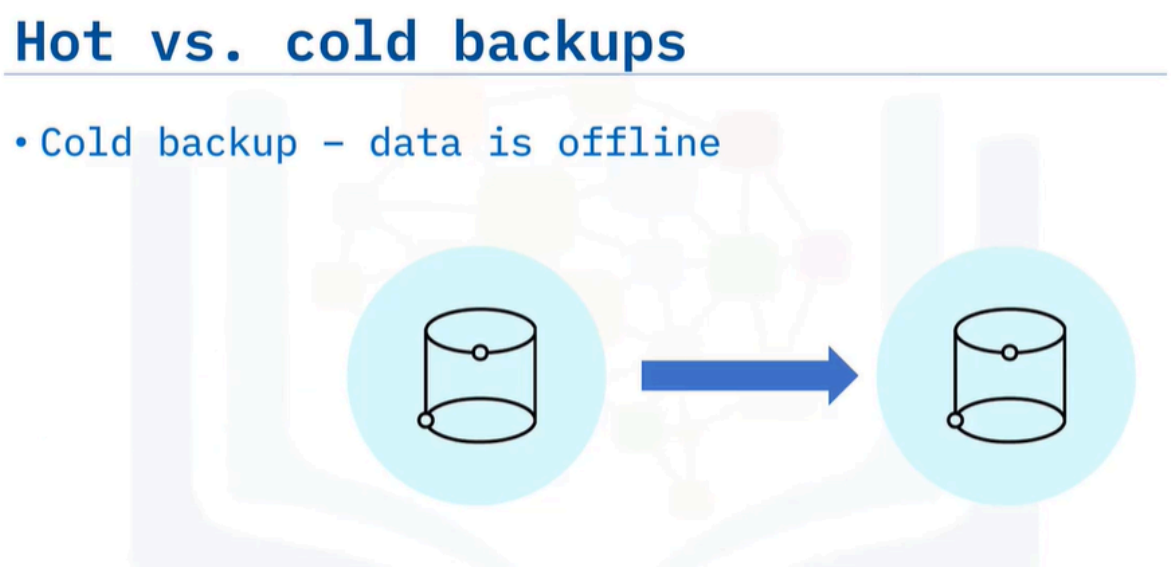
Backup Policies

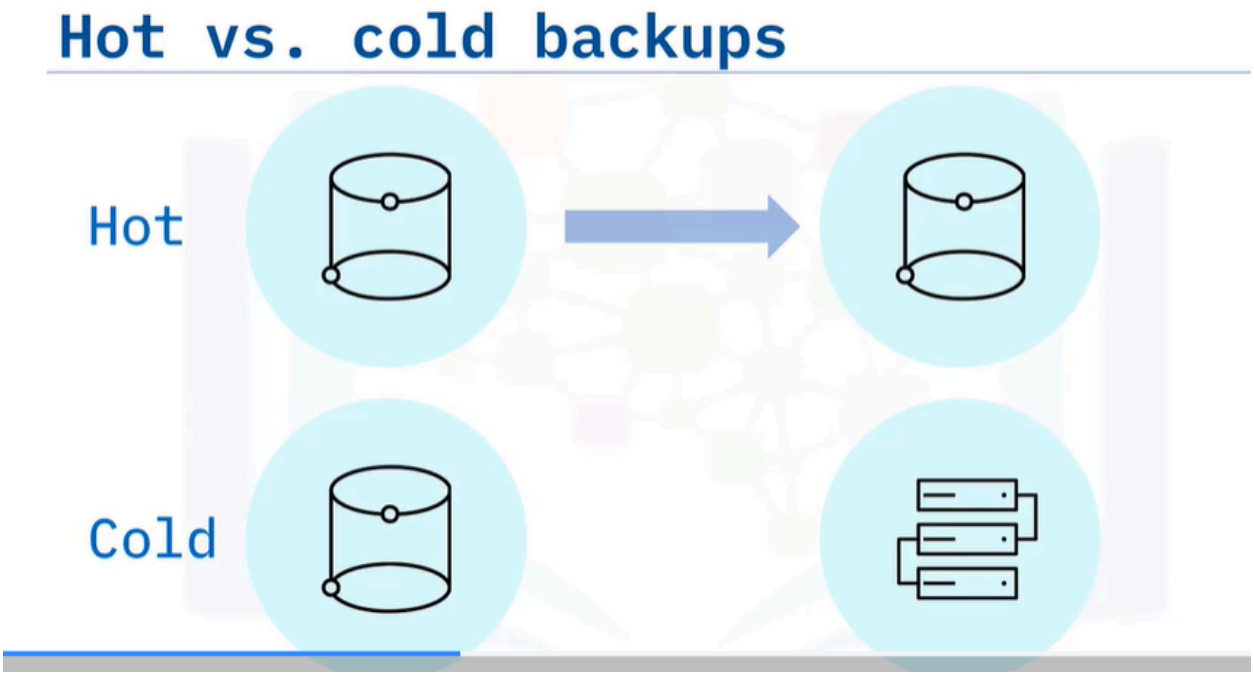




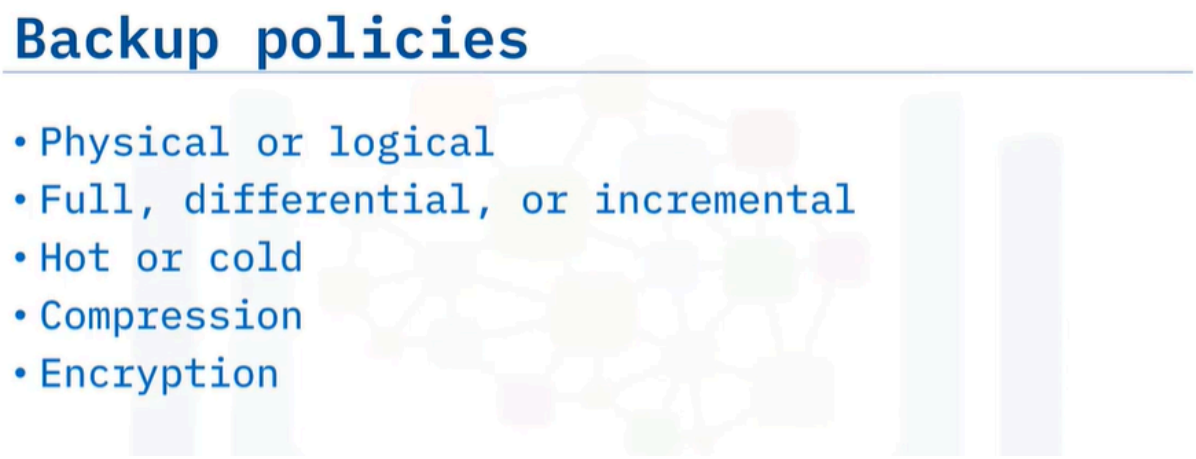
- Hot backups, or online backups, are those performed on data when it is in use. The advantage of hot backups is that they have no impact on availability and users can continue with their activities throughout the backup period. However, hot backups can result in performance degradation for users while

the backup is running and can impact on data integrity if data changes during the backup process.

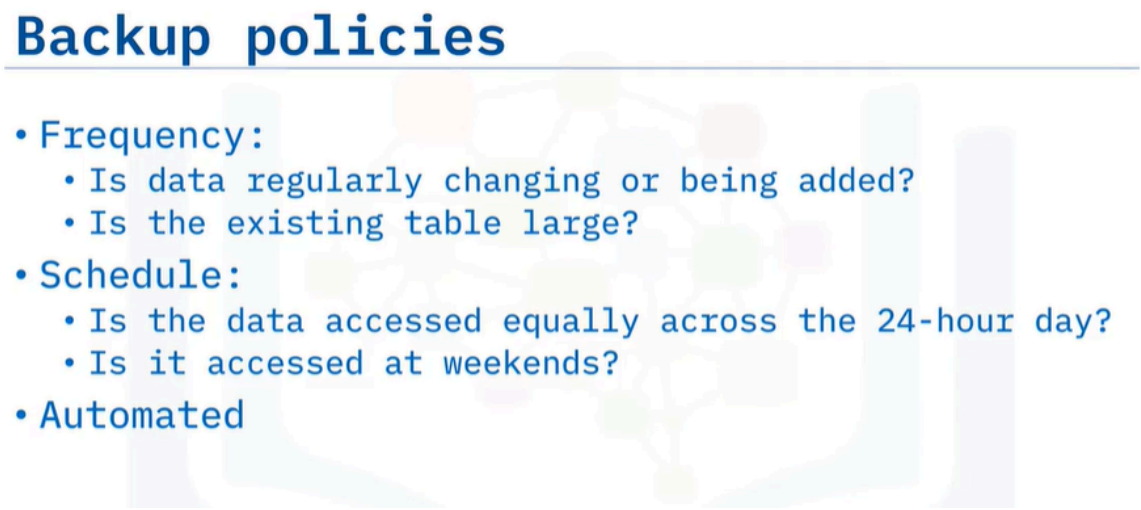
- The alternative to hot backups is to take the database offline while the backup is run. This is known as a cold, or offline, backups. This eliminates the data integrity risks associated with hot backups, but has a greater impact on user availability and cannot be used in 24/7 environments.



- Hot backups are generally stored on an available server and often receive regular updates from the production database. This enables them to be brought online should the production server fail, to ensure continuing availability to users.
- Cold backups tend to be stored on external drives or on servers that are shut down between back up operations. This can provide greater data safety, but does mean that the recovery process will take longer than that of a hot backup.

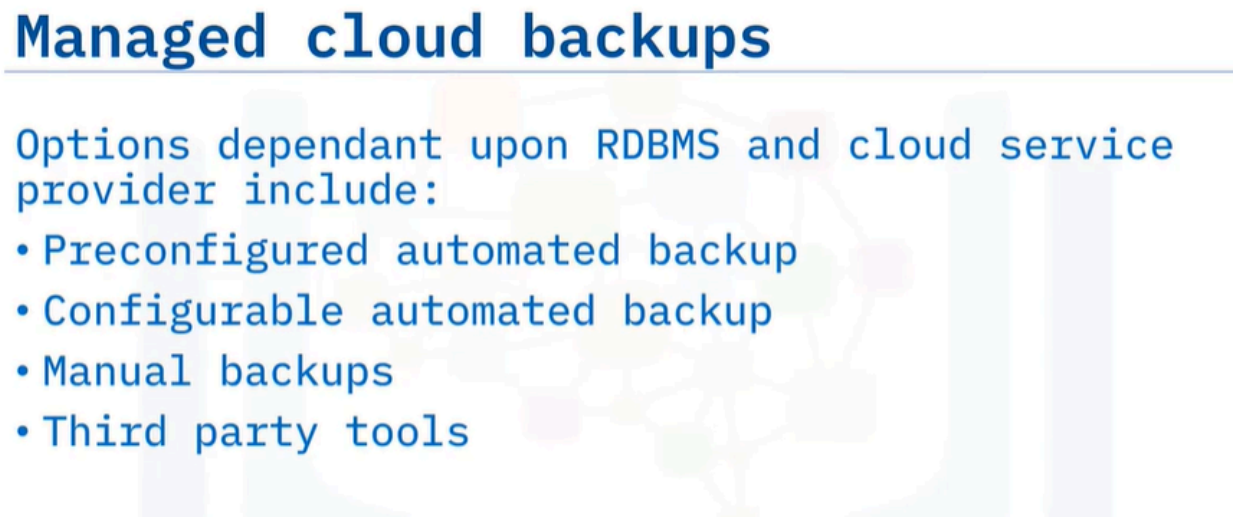


- You have already seen that there are many decisions that you must make about how to implement your backup and restore policy: physical or logical backups, type of backup, hot or cold backup, compression, and encryption. You also need to consider how often you need to back up your data.



- This is dependent on the impact that any data loss would have on your business operations and how frequently your data is changing. For example, a table containing product information is likely to change less frequently than a table containing customer orders, so you could back that up less regularly than the orders table. But if your orders table already contains a large amount of data, you won't want to be performing frequent full backups, so should

consider using differential or incremental backups for it. You also need to consider when to perform your backups. If your data is mainly accessed during the working day in one time zone, you should schedule your backup outside of those hours. However, if it is accessed across the whole day, you could consider implementing full backups at a weekend and incremental or differential backups on a daily basis. Because backups will be a regular task, if your RDBMS provides the ability to schedule or automate your backups, you should consider using it.



- It is equally important to consider backing up your cloud databases. Depending on the RDBMS that you are using, backups might run automatically, you may need to enable automated backups, you may need to run manual backups, or you may be able to use the techniques you have learned about in this video to run your own backup strategy. For example, the paid plans of Db2 on Cloud run an encrypted backup every day and with the Enterprise or Standard plans, you can also run manual backups and perform point-in-time restores. And when using Google Cloud SQL for MySQL, Postgres, and SQL Server, you can enable automated incremental backups or perform on-demand backups. If you find that your combination of RDBMS and cloud provider does not support any of these options, there are third party backup tools available to purchase.

Summary

In this video, you learned that:

- **Hot** backups allow data to be backed up while the database is active
- **Cold** backups require the database to be offline
- Your backup policy should be determined from your recovery needs and your data usage
- Most managed cloud databases provide automated backup functionality