Effective Backup Methods for Ubuntu

Data loss can have a significant impact on home and business environments. Backing up files is crucial for safeguarding your data against loss due to hardware failures, accidental deletions, and malware attacks. Regular maintenance is vital to ensure that backups are stored securely and in a timeline fashion.

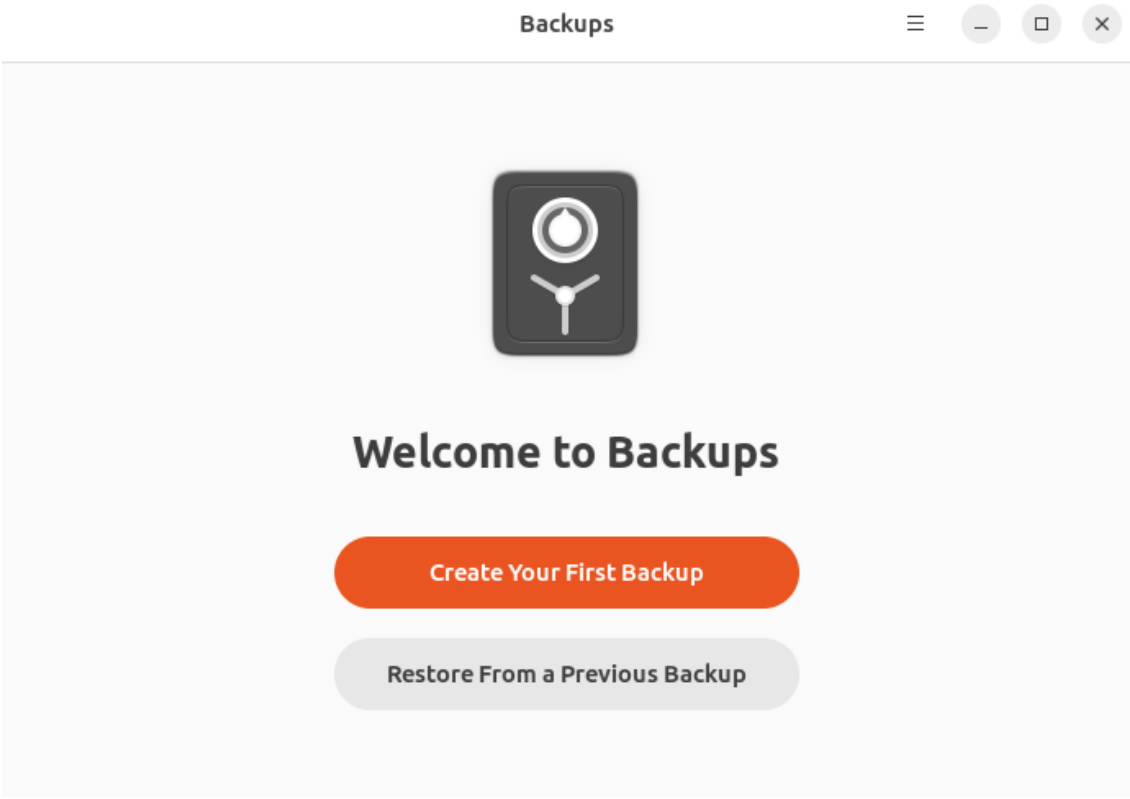
Deja Dup is a built-in utility in Ubuntu that is designed to be a user-friendly and is suitable for users, who prefer a simple backup solution with a graphical interface.

Here is a quick guide on how to setup Deja Dup.

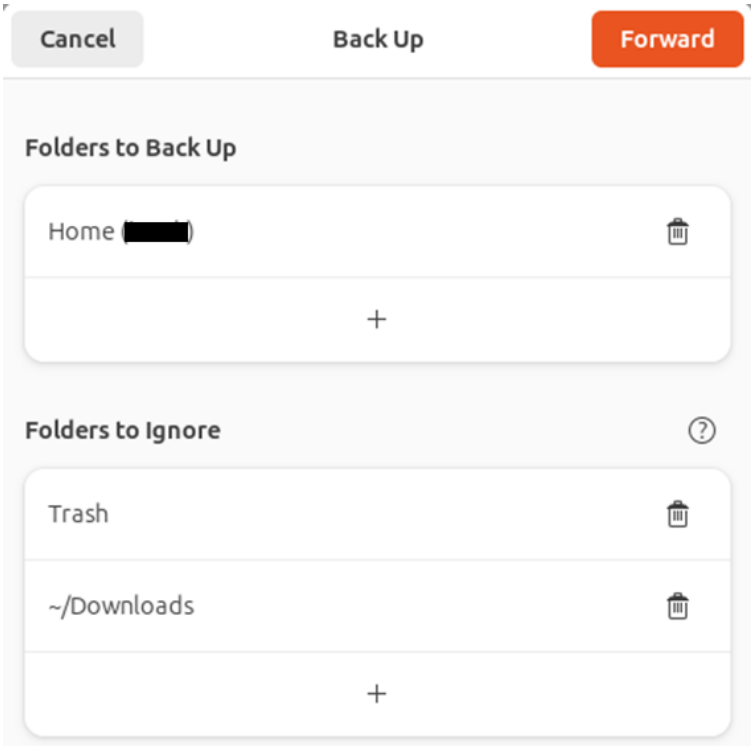
1. Even though Deja Dup is often installed on Ubuntu by default, the application can still be installed in Terminal via the following command line:

   sudo apt install deja-dup

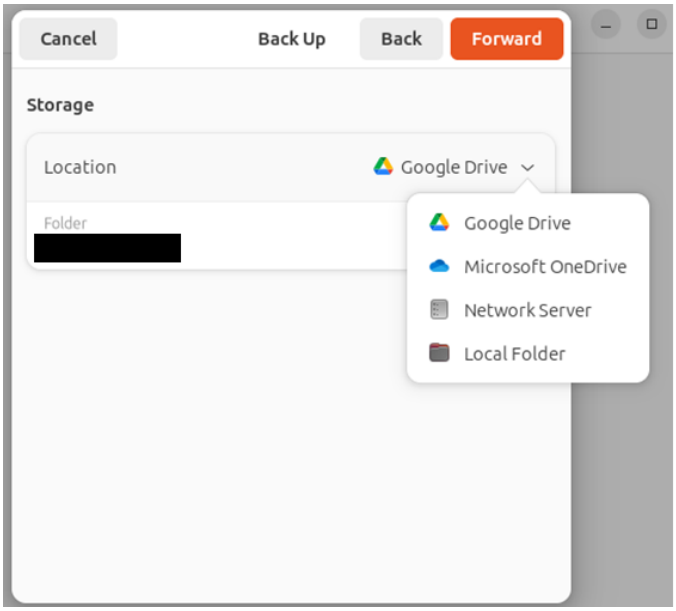
2. In the Applications menu, proceed to open **Deja Dup**. Alternatively, search for “Backup” or Deja Dup” and open the application.



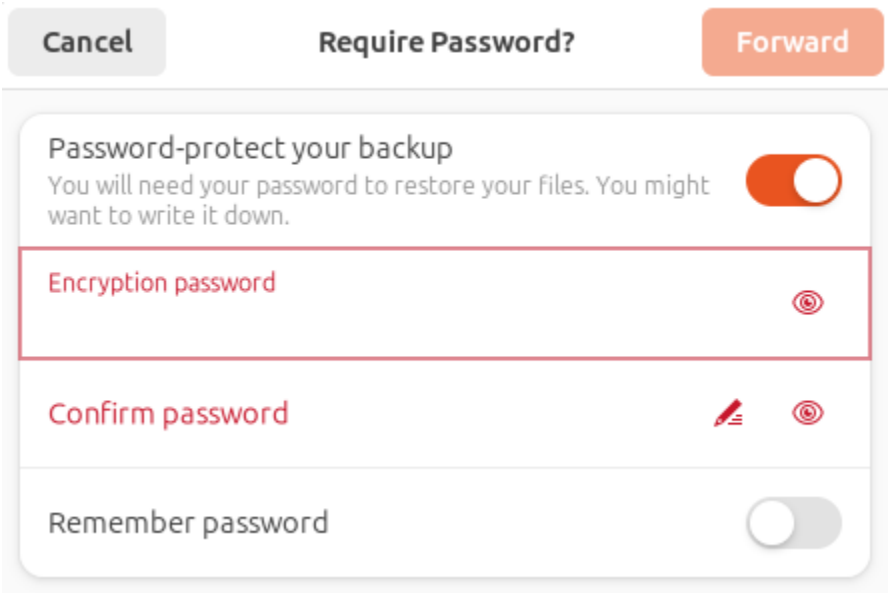
3. Once Deja Dup is opened, proceed to configure the backup settings. There are options for your backup location, schedule, and other preferences. The storage location can be local, network or cloud. Specify the desired folders to be included or excluded from backups.



When selecting **Forward**, in Location, there are options to save files to Google Drive, Microsoft OneDrive, Network Server and Local Folder. An external hard drive, USC Thumb Drive, or a WD My Cloud Home, Synology or Qnap NAS are also viable options for backup.



4. **Set Encryption** (Optional) -> for added security, you have the option to encrypt your backup for added security. Be sure to remember the password. Click on **Forward** to complete the process.



Password Manager Software
Consider using a password manager application for saving passwords. Popular password applications include LastPass, NordPass and Bitwarden. This list is not exhaustive, and alternatives can be found online.

Backup Media
When selecting an encrypted USB drive, consider factors such as encryption strength, ease of use, durability, and the level of certification. Kingston, SanDisk, Verbatim, Lexar are a few popular brand names. Always check reviews and features online. External hard drives with password encryption are recommended. Synology and Qnap does offer excellent Network-Attached Storage (NAS) devices that are ideal for home and business uses.