Remote Backups Made Simple

Seth Kenlon

It's difficult to say what the most difficult part about backing up your data is; it could be the sheer magnitude of coordinating a good backup plan, finding a place to put the data, finding a good application to do the backup for you, or it could be remembering to backup regularly.

Happily, Fedora 15 deprecates both concerns with a simple backup application called Deja Dup. This application can be found the way you find any application in Fedora 15: go to the *Activities* (or Applications in fallback GNOME 3) menu in the upper left corner of the screen, and browse your application list for Deja Dup.

Clicking on the icon will launch Deja Dup and it might surprise you to see just how simple an application it is for such a seemingly complex task. Yes, Deja Dup has but two buttons: *Backup* and *Restore*.

Simply clicking on the *Backup* button will start the backup process, and step you through setting up a backup location and plan. The simplest plan would be to purchase a large harddrive (they're surprisingly inexpensive these days) and use that as a local backup drive. It's called a local backup because it co-exists with you and your computer. It's physically in the same place as you are.

For that same reason, it's a less secure and less safe backup; if your home computer is damaged, then quite possibly whatever damaged it will also damage your backup drive and you are left with no copies of your data. It's far safer to do "off site" backups, meaning that you are sending your data over the network to some remote location which, simply by being physically separate from the original copy of the data, decreases the likelihood that both copies might be damaged.

Figure 1. *Launching the Deja Dup application*

Configuring Deja Dup

You can do the configuration for remote backups by clicking the *Backup* button in the Deja Dup window, or you can set the *Preferences*, found in the *Edit* menu. To better cover all options, we'll look at the *Preferences*.

The first tab of the *Preferences* window is concerned with location; where do you want to send your backups? As is typical of Linux, there is no prejudice here; if it's an open or

reverse-engineered protocol, then Deja Dup will let you use it.

The most secure way to send data over a network is via SSH (secure shell). Happily, many servers provide SSH access with a basic account. For instance, *hostgator.com* provides SSH access at their most basic $4/month account, and features unlimited bandwidth and diskspace. Signing up with them is as simple as any normal online checkout process; you don't need to be a network engineer to secure some off site storage!

The nice thing about SSH is that it encrypts all of the network traffic between your computer and your storage location. This could be important if you have personal information on your computer that you'd like to backup and keep private. With SSH, the chances of anyone seeing bits of your data that you'd rather them not see are drastically reduced.

Choosing SSH as your backup option asks for the common SSH information; the location of the server (ie, the name of the server that you host your backups on), where on the server you wish to place the data (your home folder is fine), your username (this is assigned to you from your hosting company) and password. And that's it!

SSH is highly recommended for all of your network transactions, but if it is not available then you can always use FTP, webDAV, SAMBA, Rackspace, and much more. All of them essentially require the same information types; the name or IP address of the server you will save your data to, and the username and password that you use to access that server.

For example, FTP is an old but still common way of accessing servers. Configuring it may be slightly different from SSH settings, usually in the server name (rather than myserver.com you might use ftp.myserver.com) and username (sometimes instead of just username you'll need to use *username@myserver.com*). You will receive this information from the server when you sign up; all you'll need to do is enter the info into the *Preferences* window.

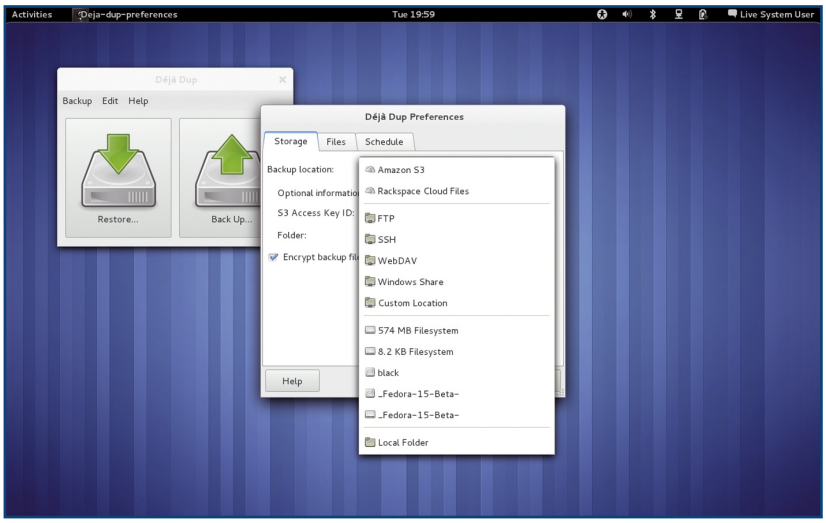

Figure 2. *If you have access to a remote server, you can probably use Deja Dup to backup to it*

Keep in mind that FTP does not encrypt your network traffic, so this is a less secure way to do your backups. However, it may be your only option if your server host does not offer SSH access in a price range that you can afford. Make sure you leave the "Encrypt Backup Files" turned on so that the backup files themselves are kept in an encrypted storage format.

In the second and third tabs of Deja Dup's Preferences window, you can set which files you do and you do not want to backup. Linux stores all of your personal data in one place so it's easy to choose what you want to backup. Just choose your Home Folder, and you can rest assured that it contains all of your personal data. You can also exclude certain folders from being backed up; you might exclude a Work folder that contains data that you have on another computer anyway, and the *Trash* folder and *Downloads* folder, and so on.

One of the keys to making backups work for you is to make it automatic. Even the most ardent fan of backing up can't remember to backup as consistently and dutifully as a computer can. This is the third tab in the *Preferences* window; you can schedule how often you wish to make backups (weekly is strongly suggested, if not more), and also how long the remote server should keep your files.

Some people like the comfort of knowing that they can go back a year and find old files, while other people only give themselves three months or so.

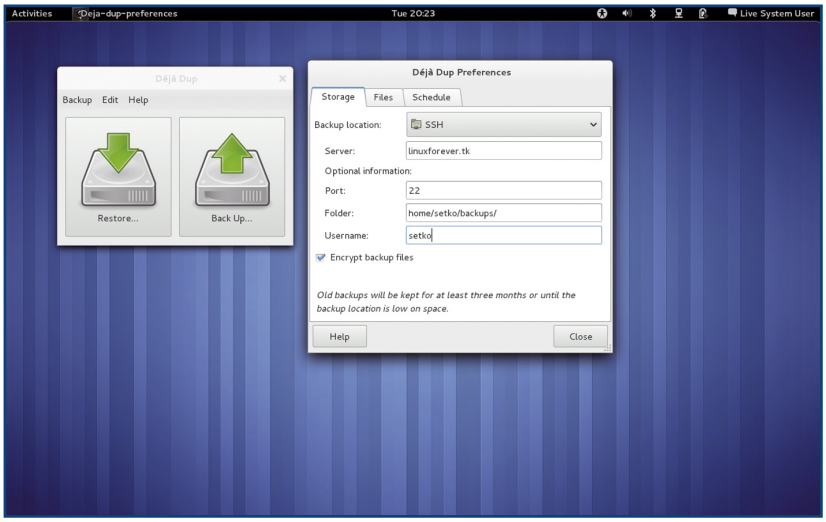

Figure 3. *Setting up remote backup via a Secure Shell (SSH)*

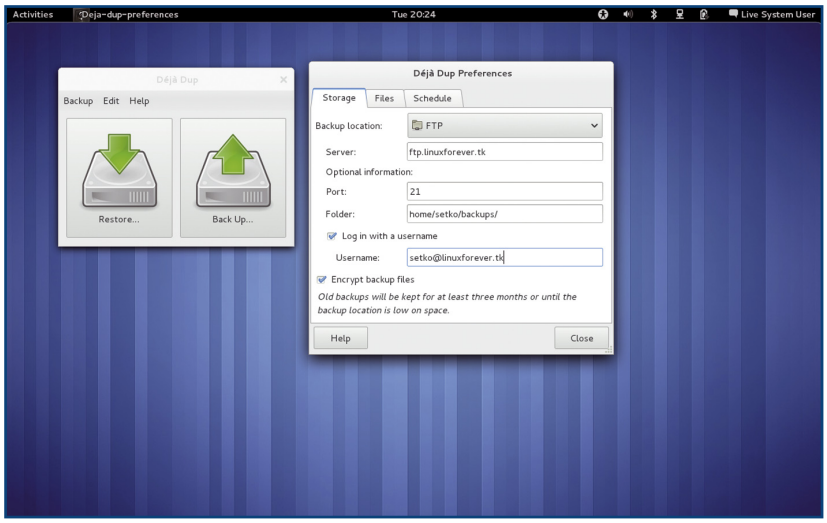

Figure 4. *Configuring an FTP login if SSH is not available*

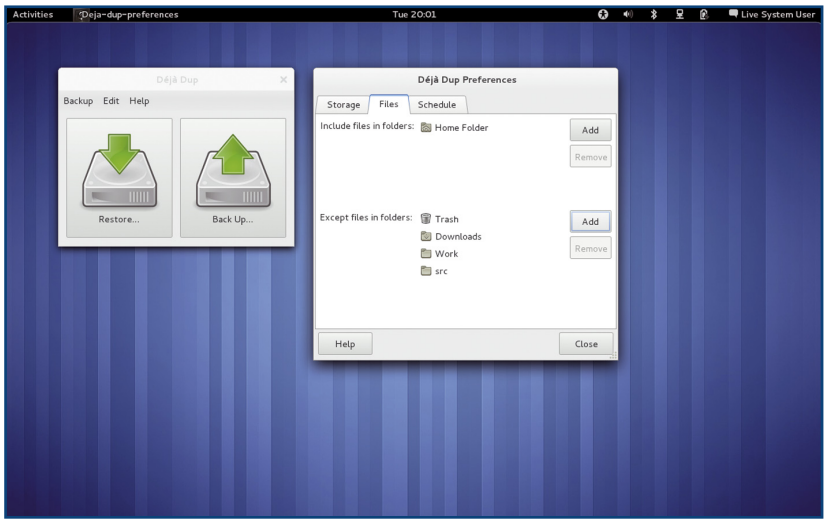

Figure 5. *Exclude files you don't want backed up in the Preferences*

Backing Up

All that's left now is to backup your data. Click the *Back Up* button in Deja Dup and confirm that the settings are correct to access the server. Click through until you are prompted for an encryption password; this is a password you should invent as the key to your encrypted backups. You may choose not to encrypt the data, but then your data will be sitting unencrypted on your remote server, which is an added risk to your privacy. So invent a password and file it away in the event that you ever need to restore from your backup.

Deja Dup will then contact the remote server and push all of your data to your remote storage. If you're backing up a lot of data for the first time, count on this process taking quite a while; possibly overnight. Later, when the process is intermediate, the backups will happen much faster.

Restoring Everything From Backups

A system restore, hopefully, will rarely, if ever, be needed. Hopefully your data remains in tact and safe, and you'll never need to restore. Of course, it's for those times that something bad does happen to your data that you are backing up at all, so let's go over how to get your data back should something happen to it.

Note that this is a full system restore. This will NOT allow you to cherry-pick through your backed up files and choose one or two files that may have been accidentally changed or deleted. The restore option is meant for full data loss, and all of your user data is indescriminantly copied from the server to your home directory, even if it means overwriting more up-to-date files on your computer. This is a backup application, not a versioning control system!

However, if the need does arise to restore without overwriting your current data, you can choose to restore files to a different location. However, Deja Dup will restore everything, so if you rely on this to bail you out of an accidental deletion of one small text file, you might find yourself pulling gigabytes of backups just to recover a few kilobytes.

Restoring your data from Deja Dup is straight-forward. Click the *Restore* button, confirm the settings as needed, choose the date from which you wish to restore, and the backup files from the remote location will be copied back onto your machine.

The restore process will take quite some time, since all of the data you had backed up will be pulled over the network and copied onto the new computer or harddrive you are restoring to. But it's a very accurate job; once finished, log out of your computer and then back in, and you will see that everything will be exactly as you'd left it.

Safety First

Obviously, backing up is not as complex or mysterious as it might first seem; get a server account with SSH access from a reliable host, set up Deja Dup with a good backup policy, and you can be confident that your digital life is safe from mishap.

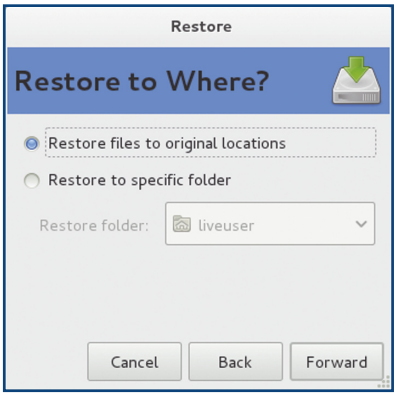

Figure 6. *Restoring your data is simple with Deja Dup*