Setting up Nextcloudpi (NCP) with an Encrypted Hard Drive

Posted on December 17,2018 by admin

The following tutorial is how you can setup an encrypted hard drive to work with Nextcloudpi. Please note that there are a few steps you will have to perform every time your pi goes down because the drive will require decrypting. Basic understanding of the command line will be required for this so if you don't have these skills locate someone who does. One step that should be complete before beginning is formatting your encrypted drive. We recommend following this tutorial for setting up your drive.

1. Flashing Nextcloudpi onto the SD Card using Etcher

Go and find Etcher. There are other ways to do it but Etcher works really well and fast. They seem to have deb packages now if you are Ubuntu/Debian

2. Download the appropriate NCP image

Here is the repository for the NCP downloads. Make sure to get the right one as there are different 'flavours' of raspberry pi's out there. Consider asking a community member. Generally it will be the generic RPi version if you are on a raspberry pi.

3. Extract the image from the downloaded archive

This extraction of the downloaded archive takes a bit more time than I expected so maybe get a coffee or play with your cat. Just saying. The extracted version is what you'll flash to the card in the next steps, however, I think Etcher can use the raw archive but I'm too lazy to research that…

4. Flash the NCP Image to the SD Card

The instructions are pretty hard to mess up with Etcher in terms of how to use it. Just do it, but read the next important note (seriously read it, that's why i put it bold and I'm mentioning it before you even read it)

Important usefule note!! It's very easy to create a tragedy when flashing an image onto an SD card since Etcher doesn't care that much what you are flashing on. I recommend physically removing any drive you don't want to screw up. If you don't it's possibe to accidentally flash this onto your drive and completely kill it. Again, physically remove the drives you don't want to kill and you'll be a happier person.

- Optional Step if you have previously attempted an Installation on this computer (clearly out your history)
  If you have already accessed a nextcloud server from Firefox and accessed it via ssh. While image is flashing onto the SD, remove historical garbage that will screw things up:
  - Remove cached stuff in Firefox (assuming Firefox)
    By going to settings and preferences / privacy & security / Cookies & Site data-Manage Data, then search IP address of your box and 'remove' and then 'save'. It will give a warning which you say ok to. Not doing this might prevent you from accessing your box on same IP address with new install
  - Remove 'known_hosts' from SSH.
    This makes sure your old SSH keys and such don't get in the way of a new SSH setup. In terminal go to /home/user(whatever it is) / .ssh.
    Now you are in the .ssh folder. Now type rm known_hosts.

5. Plug in Encrypted Drive

This step assumes you have already encrypted your drive. If you haven't or aren't sure if you have, don't continue but instead refer to comment in pre-amble above.

6. Put newly-etched SD card with NCP image on it, into your Raspberry Pi and plug it in.

About 2 minutes later you should be able to move to next step. If it hangs, you're too zealous… and chill. If you find the page won't load, perhaps you already tried an installation and you need to follow the 'optional steps' above?

7. Go to IP address of your Pi in your Browser

If you don't know the IP address of your Pi yet, you can get it from your router (if you know how) or you can use tools like nmap and zenmap to do this on your network. They scan to show what devices are there and their IP addresses. After entering your IP address into the browser URL (something like 192.168.x.xx), you will be prompted with an activation page. But righ before that you will be prompted to accept the not secure connection (which is fine for this part).

Save those passwords somewhere safe (note the convenient clipboard icon which automatically copies the long string to clipboard!) (I use KeepassX and 'activate' installation. Should take a minute or two. If it hangs on the activation page for more than 5 minutes, although unlikely, you may need to re-flash the image from Step 1 above as there could be a problem with the way the image flashed onto the card.

8. Enter user and password into the prompt box.

These are the passwords you saved from step 5. Specifically it will be the password for the top one (:4443). The user is 'ncp' and the password is that long string of gobbly gook you saved in Step 5 above. You may/will also need to confirm security exception here again (which is normal).

9. Skip the installation wizard when prompted

We are skipping this step since we are adding an encrypted drive. We'll do part of it later.

10. (Optional) Make Static IP

You can skipt this step, but I think it's smart for your future to make a static IP for your NCP at this point because some routers tend to change it etc, etc. Just go to the nc-static-IP option and type in what you like and what will work in your unique network config.

Power off and get back to this web admin area so that your router/network will have new static IP if you did this step. You can do this with the power button icon in the top right of NCP admin, too, but when it comes back remember you'll need to change the URL to the new IP in your browser.

11. Activate SSH in NCP admin

- On the left hand column you will see the SSH option in the NCP admin page. Go there and click the activate checkbox and enter an easy password. You can enter something as simple as 1234 here since it won't be your 'actual password'.
- Go to your terminal and do ssh pi@xxx.xxx.x.xx where the x's are your pi's IP address discovered in step 5 above.
- At the first prompt you enter the 1234 (easy password) you just made in the NCP admin page. This next part is a bit 'weird' if you haven't dont it because it will kick back a request for the same password again.
- Enter it again.
- NOW you enter a real and strong SSH password that you will use for actual access to your box. Make sure it's strong and you don't lose it.
- Once you enter that it will log you out of SSH again and force you to log in again with your new and real password.

Mastering this step is critical because you'll need SSH access to do encrypted drive stuff (such as decrypting it every time the power goes off) if something 'goes wrong' usually you can access your pi via SSH to try to fix it. Note: if you are prompted for the key fingerprint (should be) then answer 'yes'.

12. Update your Pi-kages

This is to make sure you have the packages required to do useful stuff such as encrypt your drive. The cryptsetup package is in here so if ou want to do steps 11 below you better run these two:

sudo apt update
sudo apt upgrade

9. Do an NCP Update

Log in again with ssh pi@xxx.xxx.x.xx and run this command below. This is to make sure that your packages includ the 'cryptsetup' package and also makes sure that your box is up to date:

sudo ncp-update

10. Make Apache2 not start on boot.

Making apache2 not start on boot lets you decrypt your encrypted drive before the system starts up. If/when your pi goes down, you will need to later go in and manually mount the drive each time (instructions to follow):

sudo update-rc.d apache2 disable

Remember: when the power goes off your Nextcloud will not work until you go in with SSH, decrypt drive, and restart apache2. More on this later…

11. Pre-Mounting of the Encrypted Drive

From this point we assume your drive is already encrypted in Luks format. If it's not refer to [this page](link to come) for those instructions

- a) Install the encryption toolset so you can decrypt your drive on NCP sudo apt install cryptsetup
- b) Check your pi to make sure the drive is showing up at least sudo lsblk

Mine shows up as 'sda' but yours might be different. Look at profile of it and make sure it's at least there.

- c) Key step: --> make sure contents of encypted drive are EMPTY…..
- d) Decrypt the drive so it's usable by Nextcloud. You'll need your drive de-cryption password here (and every single time you reboot your NCP…so get used to this step…): sudo cryptsetup luksOpen /dev/sda gcw2
- e) Check again to make sure drive is looking right sudo lsblk
  Mine looks like this:

```
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
sda 8:0 0 232.9G 0 disk
??gcw2 254:0 0 232.9G 0 crypt
```

12. Start apache

This makes your nextcloud stuff work so you can reach it in a browser

sudo /etc/init.d/apache2 start

13. Run the NCP Installation Wizard to Move Files to Encrypted Drive

- Go to the address of your pi in your browser with :4443/wizard at the end to access the first run wizard in NCP https://xxx.xxx.x.xx:4443/wizard
- "Do you want to save Nextcloud data in a USB drive?" Yes.
- "Plug in the USB drive and hit continue." --> it's plugged in so 'continue'
- "If you want to prepare the USB drive to be used with NextCloudPi hit Format USB. Skip if already formated as ext4 or BTRFS. Attention! This will format your USB drive as BTRFS and will destroy any current data." --> Skip formatting of drive because it's encrypted and you want to keep it that way
- Move data to USB --> click the button
- Go through the 'external access' wizard however you like. I do mine manually in router
- For DDNS, I skip and do mine manually in router as well with No-ip but you can try this if you want. This is not the point of this tutorial This should make your nc-datadir point to your drive meaning that your hard files will now save to the encrypted USB drive instead of to the stock SD card which is by default where they would go. You will know if this part was successful because nc-automount and nc-datadir should will change from an orange colour to a green colour in the bottom right side of your browser screen.
- Go back to web admin panel from there

14. Run the nc-database move feature in the NCP admin panel

Again, make sure the hard drive is completely clear at this point. It's probably possible to move a previous existing database here, but it's out of the scope of my ability or this tutorial. You can investigate it yourself but this is assuming you have a clear drive.

Bonus section you hopefully won't need

If you got a green light above in the last step don't even read this section and skip to Step 15. If you have a problem where you try to do the above step and it gives you a permission So what happens here with encryption is a 'symlink' is created so it's this symlink that needs to get the right permissions or NCP can't do it's thing with the step above. This may be a bug that no one else sees, but I'm leaving a few hints here in case we need it later:

In the next steps you have to in your terminal go to your /media/ folder and correct a permission manually before you are able to use the NCP ncdatabase function. if you have done previous nextcloud installations with their default directories on this drive, you will need to wipe out whatever is there before you move forward.

sudo chmod o+xr /media/gcw-ssd

(gcw-ssd is the name of the symlink created on your drive that points to USBdrive in Nextcloud)

Now go back to your NCP web area and do the nc-database move and it should work.

Command to empty your folders complete are as follow (use with caution, of course because this will ruin your day if you do it to the wrong dir!)

(if it's not empty run: sudo rm -rf /media/USBdrive/ncdatabase)

You might also like to keep this command handy to check permissions if someone asks:
sudo ls -ld

15. LetsEncrypt - nice and easy.

This is a good chance to relax and do some Lets Encrypt since it's easy and satisfying. Go to the left panel of web admin find letsencrypt, fill in the blanks, and press go. Now you should be able to find your box from the internets with secure connection too. You'll need your dynamic dns url at this point to make it all work so go and do that at no-ip.com or whatever you like. S

16. Reboot system to make sure things are working as they ought

- Shut down your box with command:
  sudo reboot
- To be sure it's back up you can ping xxx.xxx.x.xx (your box). When it starts responding you should be ready to ssh in
- SSH in (see instructions above in Step 8) At this point, because you made apache2 not start on reboot, neither your NCP admin pages nor your nextcloud instance will be accessible. We will proceed with a new section now which will be your process to get it back up each time the power goes down or it's rebooted.

17. Getting things back up after a reboot:

- Unlock/decrypt drive. Note: yours will not be 'gcw2' - that's just my example. Can be whatever you like.
- sudo cryptsetup luksOpen /dev/sda gcw2
- Enter your decryption password for drive
- Restart apache (see above)
- sudo /etc/init.d/apache2 start

Celebrate if it's working! Try again if it's not!

Special thanks to Tobias, Nachoparker and Kevin for all your hard work with me getting it this far!

Posted in:Technology,Tutorial,Ubuntu | Tagged:Freedom,Ncp,Nextcloud,Nextcloudpi,Privacy,Ubuntu | With 0 comments