Extract from: http://guficulo.blogspot.de/2015/04/backup-your-raspberry-pi-automatically.html

First we need to ensure that the Raspberry Pi allows SSH logins from the Synology's root account via public key authentication.

Doing this from scratch means that we first have to allow root to login via password on the Pi (temporarily). By default (in Raspbian at least) it does not. Password authentication is only needed long enough to push a public SSH key from the Synology server to the Raspberry Pi so that SSH key authentication will be allowed for root logins in the future. You can remove the root password thereafter (see Step 4).

1. Open up two SSH (PuTTY or equivalent) sessions, one to the Pi (login as your standard account, e.g. "pi") and one to the Synology server (login as "root" -- unless you've changed it, the root password is the same as the one you configured for the "admin" account)

2. From the Pi session, run

```
sudo passwd root
```

Then enter your desired password for the root account. This is only temporary and will be deleted as soon as we're finished transferring the SSH key (unless you want to make it permanent).

3. From the Synology session:

- Confirm that SSH keys are already present by running

```
ls ~/.ssh
```

If you see a file called `id_rsa.pub` there (assuming you've already been through this once and are setting up a new Pi to be backed up) you can skip the next step

- If no keys are found, run

```
ssh-keygen -t rsa -C root@<Your Synology server's name>
```

- When prompted for the file in which to save the key, accept the default (hit `<Enter>`)

- When prompted for a passphrase hit `<Enter>` (no passphrase)

- Push the public key to the Raspberry Pi (this is why we need the Pi to briefly allow password logins on the root account, because until the public key exists on the destination server, you will be prompted for a password when you run this command):

```
 cat ~/.ssh/id_rsa.pub | ssh root@<your Pi's IP address>
'cat >> .ssh/authorized_keys'
```

- Enter the password you created in Step 2 when prompted

- Confirm that SSH key logins are now accepted by the Raspberry Pi by running this command *(still from the Synology session, don't toggle back to the Pi session yet*:)

```
ssh root@<Your Pi's IP Address>
```

- If the connection succeeds, you can close the Synology session's terminal window

4. Return to the Pi session:

- If there was any problem connecting via SSH key above, first `logout` of the "pi" session, log back in as "root" (using the password you created in Step 2), then confirm that the SSH key was accepted by running:

```
cat ~/.ssh/authorized_keys
```

- You should see an entry in that file having "root@<Your Synology server's name>" at the end. If not, repeat Step 3 above.

- If the key was accepted, you're good to go with Step 5. Optionally, at this point, if you don't want to allow password logins to the Pi's root account any longer, you can disable root password logins to the Pi via password by running:

```
passwd -d root
```

MAKE ABSOLUTELY CERTAIN THAT YOU ONLY RUN THE ABOVE COMMAND FROM THE RASPBERRY PI SESSION, NOT FROM THE

SYNOLOGY SESSION! Removing the root password from your Synology server can cause major problems.

5. We're done with the PuTTY/terminal stuff now. Close both of those sessions if you haven't already. Everything else can be done from the Synology Web (DSM) UI. Open that and login as "admin".

Assuming this is the first Pi that you're backing up on the Synology server, you'll need to create a backup script, covered in Steps 6-8. If you've already created the `backup_target.sh` file, and you're just setting up another Pi to be backed up, you can skip to Step 9.