Ces fichiers ne sont normalement pas à éditer. Passez au III.

fichier /etc/nslcd.conf

```
uid nslcd
gid nslcd
uri ldap://172.16.0.253
base dc=kwartz,dc=dom
#SSL options
#ssl off
#tls_reqcert never
#tls_cacertfile /etc/ssl/certs/ca-certificates.crt
#base passwd OU=Users,DC=kwartz,DC=dom
#base group OU=Groups,DC=kwartz,DC=dom
```

Ce fichier ne semble plus présent :

fichier etc/pam_ldap.conf

```
host 172.16.0.253
uri ldap://172.16.0.253
ldap_version 3
pam_password crypt
```

/etc/nsswitch.conf (Ne pas ajouter `systemd` sur Raspberry)

```
passwd: files systemd ldap
group: files systemd ldap
shadow: files ldap

gshadow: files
hosts: files mdns4_minimal [NOTFOUND=return] dns myhostname

networks: files
protocols: db files
services: db files
ethers: db files
rpc: db files

netgroup: nis
```

Pour information:

- ldap version
  3
- ldap account for root
  {laisser vide}
- ldap root account password
  {laisser vide}

Fichier /etc/pam.d/common-session

```
# /etc/pam.d/common-session - session-related modules common to all services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of modules that define tasks to be performed
# at the start and end of interactive sessions.
#
# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules.  See
# pam-auth-update(8) for details.

# here are the per-package modules (the "Primary" block)
session [default=1]                     pam_permit.so
# here's the fallback if no module succeeds
session requisite                       pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
session required                        pam_permit.so
# The pam_umask module will set the umask according to the system default in
# /etc/login.defs and user settings, solving the problem of different
# umask settings with different shells, display managers, remote sessions etc.
# See "man pam_umask".
session optional                        pam_umask.so
# and here are more per-package modules (the "Additional" block)
session required        pam_unix.so
session optional        pam_mount.so
session [success=ok default=ignore]     pam_ldap.so minimum_uid=1000
session optional        pam_systemd.so
session optional        pam_ecryptfs.so unwrap
session required        pam_mkhomedir.so
# end of pam-auth-update config
```