Debian: Problème causé par OpenLDAP et NSS (et Udevd)

Si on installe un service OpenLDAP et qu'on configure le serveur pour résoudre les noms d'utilisateurs et de groups sur la base LDAP (gràce à NSS via /etc/nsswitch.conf), il apparait des erreurs au cours du démarrage de la machine. Même si le service LDAP fonctionne parfaitement.

Du genre (extraits de logs pris au hasard):

> udevd[xxx]: nss_ldap: failed to bind to LDAP server ldap://127.0.0.1: Can't contact LDAP server
> udevd[xxx]: nss_ldap: could not search LDAP server - server is unavailable
> udevd[xxx]: nss_ldap: reconnecting to LDAP server (sleeping 1 seconds)
> udevd[xxx]: nss_ldap: could not search LDAP server - Can’t contact LDAP server
> udevd[xxx]: lookup_group: error resolving group 'xxx': illegal seek

Ce problème apparait sur une Debian Etch, une Lenny, et je pense que c'est identique sous Ubuntu.

Ci-dessous voici comment j'ai résolu le problème.

En regardant les traces ci-dessus, on voit que les messages sont générés par udevd.

Udev est démarré au niveau single, donc très tôt. Son rôle est de occuper de l'identification des périphériques sous /dev, du chargement des modules des pilotes correspondants. Le souci vient du fait qu'il change la propriété group du device par rapport à des règles définies sous /etc/udev/permissions.rules.

Voilà ou est le problème: l'appel "lookup_group" provoque une résolution du nom du groupe. Qui conformément à la configuration NSS (/etc/nsswitch.conf) essaie de le résoudre sur ldap.
Mais les couches réseaux sont pas encore montées (script "/etc/init.d/networking"),et à fortiori le serveur openLdap ne l'est pas.

Il est évident qu'on ne peux pas avancer le networking avant le montage des devices.

donc comme solution on peut dans un premier temps:

rajouter "bind_policy soft" dans le fichier /etc/libnss-ldap.conf. ca indique au module ldap de nss de ne pas rééssayer plusieurs fois la connection au serveur LDAP.

La vraie solution de contournement:

udev fait un appel à la fonction lookup_group, qui recherche le nom dans le fichier local /etc/groups puis sur la base LDAP s'il ne l'y trouve pas (ceci si on a mis "group: files ldap" dans nsswitch.conf).

Donc la solution c'est de créer en local les groupes qui sont recherchés par udev. Il faut le faire pour tous les messages "lookup_group: error resolving group 'xxx'".

Voici ceux qui sont recherchés sous Etch, et les commandes pour les créer.

{mostip}
addgroup --system scanner
addgroup --system nvram
addgroup --system tss
addgroup --system fuse
addgroup --system kvm
addgroup --system rdma
adduser --system --no-create-home --ingroup tss tss
{/mostip}

La dernière commande ajoute un utilisateur, necessaire pour tss.

C'est la seule possibilité que je vois sans modifier la configuration système:

- on pourrait modifier les fichiers permissions sous /etc/udev/permissions.rules et sous rules.d, mais les effets peuvent être hasardeux
- sinon la seule vraie possibilité serait de modifier le code source de udev pour qu'il teste avant de faire la résolution de nom dans les fichiers locaux, où qu'il la fasse en direct, car ce n'est que là que les groupes pour les devices peuvent se trouver finalement ;-)