

Utilisation de LDAP pour les ACOMPTES UNIX



CLAUDE.LECOMMANDEUR[AT]epfl.ch, SIC

INTRODUCTION

Depuis quelques mois, notre serveur LDAP met à disposition les informations d'authentification de GASPARG (voir Authentification via le serveur LDAP – <http://sic.epfl.ch/publications/FI01/fi-9-1/9-1-page5.html>). Ces informations permettent à différentes applications de déléguer directement l'authentification de leurs utilisateurs à ce serveur. Cette méthode est largement utilisée et de nombreux outils devant authentifier leurs utilisateurs fournissent une interface LDAP en standard. Le login Unix (Linux, Solaris et bien d'autres) peut ainsi être confié à un serveur LDAP par l'intermédiaire de l'interface PAM (Pluggable Access Module).

De même Samba – <http://www.samba.org> (voir à ce sujet l'excellent article de Pascal Jermini et Vittoria Rezzonico[2] – <http://sic.epfl.ch/publications/FI02/fi-2-2/2-2-page8.html>, sendmail, qmail et une multitude d'autres outils à accès restreints utilisent ce mécanisme.

Nous allons dans cet article ajouter une brique à cet édifice. L'authentification est traditionnellement à la charge du fichier local `/etc/passwd` sur les machines Unix. L'utilisation de LDAP délègue cette charge à un serveur central. Ceci permet d'avoir un mot de passe unique sur plusieurs machines.

On peut alors imaginer de déléguer le reste du contenu de ce fichier à un serveur central. C'est ce que fait NIS. Mais il existe sur les différents Unix (parmi lesquels Linux) un service appelé *Name Service Switch* (NSS), dont l'idée originale provient de Sun Microsystems, comme beaucoup d'autres, et nous les en remercions grandement.

Ce service permet justement de déléguer tout ce qui se trouve dans le fichier local `/etc/passwd` à un serveur quelconque. Et bien entendu, il existe une interface NSS --> LDAP. Un module implémentant cette interface, `nss_ldap` – http://www.padl.com/nss_ldap.html, nous est fourni gracieusement par PADL Software – <http://www.padl.com/>. Comme nous est d'ailleurs fourni le module `pam_ldap` – http://www.padl.com/pam_ldap.html.

SUPPORT DU SERVEUR LDAP

Le rfc 2307 – <http://www.cis.ohio-state.edu/cgi-bin/rfc/rfc2307.html> – décrit (en particulier) le support que doit apporter le service LDAP pour permettre à un service NSS de fonctionner.

Notre serveur `ldap.epfl.ch` place chaque personne (étudiant et personnel) dans une classe `posixAccount`, c'est à dire que les champs suivants sont renseignés:

- le UID (User ID).
- `gidNumber`
 - le GID (Group ID).
- `gecos`
 - champ GECOS (description).
- `homeDirectory`
 - répertoire principal
- `loginShell`
 - Shell.
- `uid`
 - le username.

Ceux-ci correspondent champ pour champ à ceux d'un fichier `passwd` (faire *man 5 passwd* pour une description de ces champs sous Unix).

Bien sûr, la question s'est posée: que mettre dans ces champs qui puisse avoir le maximum d'utilité pour les gestionnaires de machines Unix?

Examinons ces champs en détail.

EXAMEN DES CHAMPS DE `posixAccount`

`uid`

C'est le username. Il est automatiquement attribué dès qu'une personne apparaît soit dans la liste du personnel, soit dans la liste des étudiants. En général, c'est le nom de la personne. Bien sûr, ce nom est souvent déjà pris: on accole alors la première lettre de prénom au début du nom, etc. Pour les curieux, l'algorithme utilisé est visible ici – http://cognac1.epfl.ch/alloc_user.txt (mais est susceptible de changer sans préavis). C'est le même username qui est utilisé pour les comptes IMAP – <http://mailbox.epfl.ch/>.

`uidNUMBER`

Comme le username, l'UID est attribué à l'apparition d'une personne sur le site (personnel ou étudiant). L'algorithme d'attribution est le suivant: c'est le numéro SCIPER (alias CAMIPRO, celui qui se trouve sur votre carte éponyme) auquel on soustrait 99000. Si ce numéro est déjà pris, on cherche séquentiellement un numéro libre à partir de 1025.

`gidNUMBER`

Ça se complique. Chaque unité de l'école, aussi bien pour le personnel (institut, laboratoire, chaires, etc...) que pour les étudiants (Sections) se voit attribué à sa création un numéro unique, dans la tranche des GID Unix valides (0..65534). Le GID d'une personne est ce numéro pour l'unité principale de rattachement de cette personne.

C'est encore un peu compliqué pour les étudiants. De façon à ce que ceux-ci ne changent pas de GID chaque année, voire chaque trimestre, les GID sont attribués par couples (Section, Année début d'étude). Par exemple : (dans le format d'un fichier */etc/group*)

```
ar-1997:Architecture - Année début 1997:30000:
ar-1998:Architecture - Année début 1998:30001:
ar-1999:Architecture - Année début 1999:30002:
ar-2000:Architecture - Année début 2000:30003:
ar-2001:Architecture - Année début 2001:30004:
ch-1997:Chimie - Année début 1997:30100:
ch-1998:Chimie - Année début 1998:30101:
ch-1999:Chimie - Année début 1999:30102:
ch-2000:Chimie - Année début 2000:30103:
ch-2001:Chimie - Année début 2001:30104:
```

Ainsi, un étudiant qui suit une scolarité normale ne changera pas de GID au cours de cette scolarité.

GECOS

Ce champ contient une courte description de la personne

- pour le personnel: *prénom nom, bureau, téléphone.*
- pour les étudiants: *prénom nom, section - semestre semestre.*

HOME DIRECTORY

Pour l'instant: */home/username*. Dans le futur il faudra sans doute prévoir des outils pour une gestion plus fine.

loginShell

Pour l'instant: */bin/tcsh*, mais de même que pour le champ *homeDirectory*, il faudra retravailler la chose. Sans doute une interface de gestion basée sur GASPARE.

CONSULTATION DE CES DONNÉES DANS L'ANNUAIRE

En standard, le username est donné dans l'interface LDAP/WWW – <http://www.epfl.ch/cgi-bin/csoldap2002>. Pour avoir tous les champs de la classe *posixAccount*, utiliser l'URL avec */all* – <http://www.epfl.ch/cgi-bin/csoldap2002/all>. De même, pour avoir le GID d'une unité, utilisez le suffixe */all*.

QUELQUES RÉFÉRENCES

- [1] Authentification via le serveur LDAP – <http://sic.epfl.ch/publications/FI01/fi-9-1/9-1-page5.html>
- [2] Avoir une identité unique dans un réseau hétérogène LDAP et Linux à la rescousse! – <http://sic.epfl.ch/publications/FI02/fi-2-2/2-2-page8.html>
- [3] Configuring Your System to Authenticate Using OpenLDAP – <http://linuxline.epfl.ch/Doc/rhl-rg-en-7.2/s1-ldap-redhattips.html>
- [4] System Databases and Name Service Switch – http://www.gnu.org/manual/glibc-2.2.3/html_chapter/libc_28.html
- [5] rfc2307 – <http://www.cis.obio-state.edu/cgi-bin/rfc/rfc2307.html>
- [6] NSS LDAP Module – http://www.padl.com/nss_ldap.html ■

