

AUTHENTIFICATION VIA LE SERVEUR LDAP

Claude Lecommandeur@epfl.ch, SIC



*J*e vais vous parler de la pluie et du bottin.

Traditionnellement, les serveurs LDAP (Lightweight Directory Access Protocol) étaient utilisés pour ce qu'ils sont, c'est à dire des annuaires électroniques.

Le protocole LDAP, descendant direct de X.500 (voir le flash info 8/97 pour quelques croustillants détails historiques) est très puissant pour la gestion des annuaires et il est maintenant universellement adopté pour cette tâche.

Depuis quelques temps, une autre utilisation commence à voir le jour: l'authentification en réseau. Depuis toujours les serveurs LDAP disposent d'un système d'authentification pour leurs besoins propres. Chaque entrée de l'annuaire peut être munie d'un mot de passe. Ce mot de passe permet de se faire reconnaître du serveur et donc de disposer de droits spécifiques, comme par exemple modifier un attribut de l'entrée correspondante.

Des tas d'autres serveurs possèdent cette faculté, mais les voies de l'histoire de l'informatique sont impénétrables et c'est LDAP qui fut l'élu pour cette tâche d'authentification distribuée.

Un serveur LDAP supportant le bottin téléphonique de l'EPFL existe depuis la nuit des temps (environ 8 ans), mais la faculté d'authentification était volontairement fermée. Depuis l'avènement de GASPARE, nous disposons d'une infrastructure d'identification et authentification fiable et il a été décidé d'ouvrir l'authentification du serveur LDAP. Le mot de passe GASPARE permet de s'authentifier auprès du serveur LDAP.

Toute application qui se targue d'utiliser LDAP pour sa sécurisation peut donc utiliser notre serveur (ldap.epfl.ch) pour cette tâche.

Voyons le cas particulier du login sur les machines Unix.

Le système PAM (Pluggable Authentication Modules) de l'OSF (maintenant OpenGroup) est supporté par plusieurs Unix et permet de substituer un système d'authentification quelconque au traditionnel fichier `/etc/passwd`.

Cette information, ajoutée à celle qui précède ferait naître une idée dans la cervelle la plus poisseuse: existe-t-il un module PAM qui irait pêcher ses données d'authentification dans un serveur LDAP? Malheureusement, la réponse est non... Je blague, ce module existe et s'appelle `pam_ldap`. Il est gracieusement mis à notre disposition par PADL software.

L'installation et la configuration de ce module est très simple, il faut, bien sûr, installer `pam`, puis `pam_ldap`, et ensuite configurer `pam` pour qu'il utilise `pam_ldap` (`/etc/pam.conf` ou `/etc/pam.d/`, selon votre configuration).

A ma connaissance `pam` est utilisable sur Linux, Solaris et HP-UX/11. Je suis prêt à donner un coup de main aux hardis volontaires qui désireraient se lancer dans l'aventure.

L'intérêt de cette technique n'est pas évident dans le cas d'un poste de travail personnel. Par contre pour gérer une salle de stations, c'est très intéressant: plus de mot de passe à initialiser ou oublié, tout le monde sur Gaspar.

Saperlipopette, je m'aperçois que je n'ai pas encore parlé de la pluie et que je n'ai plus de place dans cette marge. Je le ferai donc dans un prochain article, promis.■