

Une Solution d'Authentification Unifiée dans un réseau hétérogène

Arnaud Antonelli, Samson Bisaro, Christian Maillard
Université Henri Poincaré - Nancy I

Mots clefs

Authentification, MySQL, OpenLDAP, PHP, IMP, *Active Directory*, Apogée

Résumé

L'authentification unique « rêve ou réalité »... Qui n'a pas rêvé de conquérir ce Saint Graal... Qui n'a pas, depuis l'avènement des deux mondes Windows et Unix, essayé de centraliser la gestion des comptes afin d'améliorer l'accès des utilisateurs et afin de faciliter l'administration par les ingénieurs systèmes. Nous avons tous testé les serveurs Windows NT et Windows 2000 pour unifier les environnements Microsoft, le protocole NIS pour unifier les environnements Unix et nous avons tous essayé d'unifier ces deux mondes opposés à coup de Samba, de LDAP, de Kerberos, de pGina... Mais la dure réalité du terrain montre que si un certain nombre de solutions fonctionnent, il est impossible de conserver toutes les fonctionnalités offertes par chacun des environnements si on privilégie un annuaire OpenLDAP unique ou un annuaire *Active Directory*. Dans notre cas, nous avons besoin de toutes les fonctionnalités offertes par les deux environnements. Après avoir testé plusieurs solutions, nous avons fait le choix d'avoir un *Active Directory* unique pour l'ensemble de l'Université afin de ne gérer qu'un seul annuaire d'authentification pour les postes Windows (actuellement le réseau comporte 19 serveurs, 850 postes de travail pour 17000 étudiants) et nous avons un annuaire OpenLDAP pour l'authentification Unix et l'authentification des applications web. Parallèlement à ce choix, nous avons développé une kyrielle de programmes pour assurer la création et la gestion de ces comptes tant sur le serveur OpenLDAP que sur le serveur *Active Directory*. Pour uniformiser les mots de passe, nous avons développé une interface web que les étudiants doivent obligatoirement utiliser pour valider leurs comptes ou pour modifier leurs mots de passe. L'étudiant dispose donc d'un compte virtuel unique (sésame) pour accéder à la totalité des moyens informatiques mis à disposition par l'Université. Ce n'est pas encore le Graal tel que nous l'avions espéré mais cette solution qui est en production depuis plus d'un an, nous donne l'impression d'avoir presque atteint notre rêve.