03 - patch saslauthd

Une alternative plus simple est d'utiliser la fonctionnalité "cacheDirectory" de la dernière version de esup-pam-cas.

Un patch du démon saslauthd est proposé par Dominique LALOT (Université de la Méditerranée - Aix Marseille 2).

Ce patch permet d'optimiser le fonctionnement de saslauthd avec pam_cas ; il corrige également un bug du démon. Nous recommandons son utilisation, en particulier dans le cadre de son utilisation avec un webmail.

Par défaut, saslauthd met en cache le mot de passe des utilisateurs pour les différents protocoles utilisés (pop, imap, ...).

Le patch proposé permet à saslauthd de mémoriser plusieurs mots de passe éventuels pour un même utilisateur.

Le cas d'utilisation exposé ci-après permet de comprendre l'intérêt de ceci.

Utilisation canal imap et webmail horde imp

On suppose un ent esup-portail utilisant le canal imap et le webmail horde.

Le canal imap et le webmail sont tous 2 des proxy-CAS.

Afin d'éviter de redérouler tout le processus d'authentification CAS pour chaque connexion IMAP, ces deux 'applications' ont été programmées ainsi :

- Première connexion imap pour un utilisateur :
  L'application requiert un proxy ticket (PT) pour cet utilisateur et le service imap. Il utilise ce PT pout initialiser la connexion.
  Dans le protocole CAS, le PT ne peut servir qu'une seule fois.
  A des fins d'optimisation, l'application conserve le PT pour le rejouer ultérieurement, ce qui n'est pas autorisé par le serveur CAS.
- Nouvelle connexion imap pour le même utilisateur :
  L'application tente une nouvelle connexion avec l'ancien PT, en espérant que le cache saslauthd l'ai conservé en mémoire.
  - Si le PT est dans le cache saslauthd, la connexion est acceptée
  - Sinon, la connexion est refusée (bad password).
    L'application est alors programmée pour redemander un nouveau PT auprès du serveur CAS, et tenter à nouveau la connexion.

Ce processus de cache fonctionne très bien et de manière optimisée avec un démon saslauthd non patché.

Mais dans le schéma proposé avec un canal imap et le webmail horde :

- L'utilisateur clique sur le canal imap ; celui-ci réclame un PT et le joue. Le PT du canal imap est caché dans saslauthd
- Il rebondi sur le webmail ; celui-ci réclame un PT et le joue. Le PT du webmail est alors caché dans saslauthd à la place du précédent
- Et ainsi de suite

On voit dans cet exemple qu'on perd une partie du bénéfice du cache de mot de passe sanslauthd dans ce cas.

Un cas similaire peut être l'utilisation du webmail en parallèle avec un client de mail lourd.