

Authentification unifiée Unix/Windows

Benoit Métrot

Rencontres Mathrice - Octobre 2008

Plan

- 1 Contexte du laboratoire
- 2 Du côté Linux
- 3 Du côté Windows
- 4 Bilan et perspectives

Le laboratoire

- Laboratoire de Mathématiques et Applications
- Unité mixte de recherche (UMR-6086)
- Situé à Poitiers
- Environ 70 personnes

Le parc informatique

- Clients légers (Neoware)
- PCs fixes
- Ordinateurs portables (prêts pour exposés/séminaires)
- Les systèmes d'exploitation
 - Debian GNU/Linux
 - Quelques Windows XP (portables)

L'existant (mars 2008)

- Authentification des utilisateurs via un annuaire LDAP
 - Sessions interactives (SSH)
 - Messagerie électronique
 - Intranet
 - ...

L'existant (mars 2008)

- Authentification des utilisateurs via un annuaire LDAP
 - Sessions interactives (SSH)
 - Messagerie électronique
 - Intranet
 - ...
- Domaine SAMBA pour gérer les clients Windows et le serveur d'applications Windows (TSE)

Pourquoi changer ?

- Chaque modification dans l'annuaire LDAP impose une saisie de mot de passe
- Le mot de passe n'est pas complètement unifié (mot de passe Linux \neq mot de passe Windows)
- Les utilisateurs doivent saisir leur mot de passe à chaque accès à un serveur (noeud de calcul, dépôt des pages web)
- Pas de comptes individuels sur les portables (comptes génériques)

Objectifs

- Mettre en place une SSO transparente (sans clé SSH)
- Mise en place du nouveau serveur de fichiers avec sécurisation des montages NFS à destination des PCs Linux
- Pouvoir utiliser les fonctionnalités d'un domaine Windows pour l'administration des clients (GPO)
- Avoir un vrai mot de passe unique

Plan

- 1 Contexte du laboratoire
- 2 Du côté Linux**
- 3 Du côté Windows
- 4 Bilan et perspectives

Annuaire OpenLDAP

Base d'identification des utilisateurs (nom, prénom, login, attributs POSIX...) :

- Accès en anonyme via les bibliothèques NSS
- Chiffrage des communications avec SSL
- Réplication de l'annuaire via l'overlay d'OpenLDAP
- Authentification via Kerberos des replicas vis à vis du maître

L'arbre LDAP dc=labo,dc=prive est divisé en deux branches :

- ou=people pour les utilisateurs
- ou=groups pour les groupes

Kerberos

Qu'est ce donc ?

Kerberos est un protocole d'authentification réseau qui ne fait pas transiter les mots de passe sur le réseau, même cryptés.

Kerberos

Qu'est ce donc ?

Kerberos est un protocole d'authentification réseau qui ne fait pas transiter les mots de passe sur le réseau, même cryptés.

→ *Kerberos, the definitive guide* - Jason Garman - O'Reilly

Les fichiers utilisateurs

Les machines Linux montent le /home via NFSv4

- Montage authentifié par Kerberos (option `sec=krb5i`)
- Sécurité des données
- Root n'a pas accès au /home

Les fichiers utilisateurs

Les machines Linux montent le /home via NFSv4

- Montage authentifié par Kerberos (option `sec=krb5i`)
- Sécurité des données
- Root n'a pas accès au /home

→ Attention à l'expiration du ticket Kerberos

Configuration d'un client Linux

- 1 Création d'un *principal* Kerberos sur le KDC (host/machine.domain.tld@KRB-LABO.PRIVE)
- 2 Création d'une *keytab* depuis le KDC et copie dans /etc/krb5.keytab
- 3 Installation des bibliothèques Kerberos (MIT), du module pam_krb5.so, et modules GSSAPI (libsasl2-modules-gssapi-mit)
- 4 Définition des paramètres dans /etc/krb5.conf
 - Nom du royaume Kerberos
 - Adresses des KDC
 - Durée de vie et de renouvellement des tickets
- 5 Mise en place du montage NFSv4 pour /home (idmapd, rpc.gssd, fstab)

Plan

- 1 Contexte du laboratoire
- 2 Du côté Linux
- 3 Du côté Windows**
- 4 Bilan et perspectives

Domaine Active Directory

- Regroupe les machines et les utilisateurs du monde Windows
- Centralise l'authentification
- Permet d'appliquer des stratégies sur les postes (GPO)
- ...

Domaine Active Directory

- Regroupe les machines et les utilisateurs du monde Windows
- Centralise l'authentification
- Permet d'appliquer des stratégies sur les postes (GPO)
- ...

Bref, c'est censé faciliter l'administration d'un parc Windows

Configuration du domaine Active Directory

DNS

Pour éviter de polluer le *vrai* DNS, le contrôleur de domaine fait office de serveur DNS. Un nom de domaine privé (du type 2003-labo.prive) est utilisé pour éviter les conflits.

Approbation de domaines

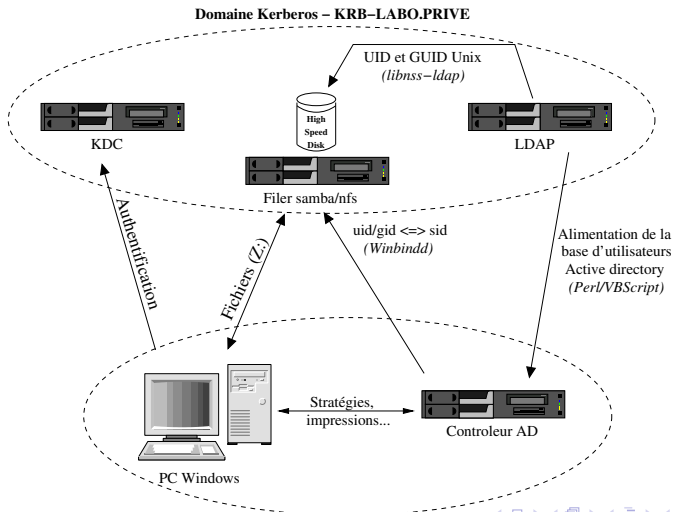
L'approbation de domaines permet aux utilisateurs Kerberos d'ouvrir une session sur le domaine Windows. Cependant, chaque *principal* Kerberos doit être mappé avec un compte utilisateur d'Active Directory.

Les fichiers

- Hébergés sur le NAS du Labo
- Distribués par SAMBA qui est intégré au domaine
- Correspondance des UID Linux et SID Windows par *Winbindd*

→ Création d'une partition dans Active Directory pour stocker cette correspondance

Schéma global d'intégration



Contrainte supplémentaire

Toutes les machines du domaines doivent avoir la connaissance du royaume Kerberos et notamment du KDC.

Commande *ksetup.exe*¹ :

```
ksetup.exe /AddKdc KRB-LABO.PRIVE  
kdc.priv.domain.tld
```

¹Inclus dans les Supports Tools pour Microsoft XP

Plan

- 1 Contexte du laboratoire
- 2 Du côté Linux
- 3 Du côté Windows
- 4 Bilan et perspectives**

Création d'un compte

- 1 Création d'une fiche dans l'annuaire LDAP
- 2 Création du *principal* Kerberos dans le KDC
- 3 Création du home directory sur le NAS
- 4 Création d'un utilisateur dans Active Directory avec un mot de passe aléatoire
- 5 Mappage du principal Kerberos avec le compte Active Directory
- 6 Enregistrement de la correspondance uidNumber/SID

Création d'un compte

- 1 Création d'une fiche dans l'annuaire LDAP
- 2 Création du *principal* Kerberos dans le KDC
- 3 Création du home directory sur le NAS
- 4 Création d'un utilisateur dans Active Directory avec un mot de passe aléatoire
- 5 Mappage du principal Kerberos avec le compte Active Directory
- 6 Enregistrement de la correspondance uidNumber/SID

→ Scriptable avec Perl et VBScript

Ce que cela apporte

- Un vrai mot de passe unique
- Les premières briques d'une SSO
- L'usage des comptes utilisateurs sur les portables hors-connexion (Sous Windows avec un profil temporaire)
- L'usage des GPO sous Windows et notamment la redirection des dossiers pour diminuer la taille des profils itinérants
- Un montage NFS du /home sécurisé sur les clients Linux

Difficultés rencontrées

- Transfert des mots de passe de l'annuaire LDAP dans Kerberos
- Mise en route de Kerberos et intégration du NAS au domaine AD
- Changement du SID lors de la migration domaine SAMBA → Active Directory (ruche NTUSER.DAT)

Il reste à...

- Automatiser la création des comptes Active Directory
- Trouver un moyen de rendre inactif l'ouverture de session avec les comptes Active Directory
- Rendre disponible hors-connexion l'accès aux comptes utilisateurs sous Linux
- Déployer une SSO complète : services WEB, messagerie