Authentification centralisé

Jeudi 23 septembre 2010

Emmanuel Blindauer
e.blindauer (at) unistra.fr
IUT R.Schuman
Université de Strasbourg

Plan

- Introduction
- Les possibilités
- Configurations du serveur Kerberos
- Configurations des clients Linux
- Configurations des clients MacOSX
- Configurations pour Active Directory
- Problèmes possibles
- Conclusion

Introduction 1/2

- Authentifier : Vérifier si une personne est ce qu'elle dit être.
  - Via login/pass
  - Via carte à puce
  - Via toute connaissance personnelle...
- Autoriser : Vérifier si la personne authentifiée à accès aux ressources
  - Restriction de certains serveurs à certains groupes
  - Vérification de liste noires

Introduction 2/2

- Utilisateur :
  - Services multiples
  - Devient exigent
  - « A la maison, ca marche »
  - Ne comprend pas le risque au travail
- L'administrateur :
  - Simplifier les outils
  - Augmenter la sécurité
  - Multiplications des systèmes

Plan

- Introduction
- Les possibilités
- Configurations du serveur Kerberos
- Configurations des clients Linux
- Configurations des clients MacOSX
- Configurations pour Active Directory
- Problèmes possibles
- Conclusion

Les possibilités

- Où stocker l'authentification pour l'utilisateur ?
  - Flat file, shadow, NIS, NYS, Hesiod, Kerberos, openId, LDAP, SASL, MySQL, SAM, NTHASH, LMHASH, OTP, Active Directory, OpenDirectory, Radius, CAS, certificats, shibboleth, …
  - Lequel choisir ?

Les possibilités

- Choisir … celui qui s'adapte le mieux votre environnement
- Quels type d'architecture est le plus répandu ?
- Les grandes familles
  - Active Directory (ldap + kerberos + proprio)
  - OpenDirectory (ldap + kerberos + pas souple)
- Dans tous les cas, chaque système pense être au centre du monde

Plan

- Introduction
- Les possibilités
- Configurations du serveur Kerberos
- Configurations des clients Linux
- Configurations des clients MacOSX
- Configurations pour Active Directory
- Problèmes possibles
- Conclusion

Kerberos 1/3

- Authentifications des systèmes sur le marché
  - Facteur commun : OpenDirectory, Active Directory, etc
  - Stabilité de la solution
  - Pérénité : Choix des acteurs, licences des logiciels

Kerberos 2/3

- TGT : Ticket initial donné après authentification (mot de passe, certificat, …) (Ticket Granting Ticket)
- TGS : Un ticket par service, obtenu grace au TGT (Ticket Granting Service)
- En pratique, pour un utilisateur
  - Un TGT obtenu lors de sa connexion sur son poste
  - Plusieurs TGS, un par service accédé, obtenu automagiquement
  - Une durée initiale de validité des tickets de 10h

Kerberos 3/3

- Avantages
  - Le mot de passe n'est demandé qu'une seule fois (TGT)
  - Les accès à d'autres services se font via des « TGS » automatiquement attribué
  - Les TGS permettent l'identification de l'utilisateur
  - D'un point de vue utilisateur, on s'authentifie avec un login/pass la première fois
- Inconvénients
  - Pas d'identité multiple simultanément

Configuration serveur

- Choix du serveur :
  - MIT ou Heimdal
  - Virtualisation possible (pas de charge importante)
  - Faire des choses simple : base de donnée locale (BDB)
  - Se configure une seule fois : « créer la base initiale »

Exploitation serveur

- Outil principal: « kadmin » sous forme de shell
  - Ajouter un utilisateur : **`kadmin> add user1`**
  - Changer un mot de passe : **`kadmin> passwd user1`**
  - Lister les comptes : **`kadmin> list`**
  - Effacer un compte : **`kadmin> delete user1`**
- Possibilités de qualité de mots de passe, expiration, etc..
- Sauvegarde par copie de deux fichiers !

Plan

- Introduction
- Les possibilités
- Configurations du serveur Kerberos
- Configurations des clients Linux
- Configurations des clients MacOSX
- Configurations pour Active Directory
- Problèmes possibles
- Conclusion

Configuration clients 1/3

- Linux : Pluggable Authentication Modules
  - /etc/pam.d/*
  - Utilisé par toutes les applications (sauf openssh)
  - Sert à savoir comment :
    - *Vérifier l'identité (`auth`)*
    - Changer un mot de passe (`password`)
    - Qui peut accéder aux application (`account`)
    - Ce qui doit être fait avant de démarrer une session (`session`)
  - Permet d'utiliser plusieurs sources :
    - Vérifier sur un serveur Kerberos ou un serveur LDAP ou un serveur radius

Configuration clients 2/3

- Exemple qui cumule deux authentifications Kerberos et une authentification avec /etc/passwd

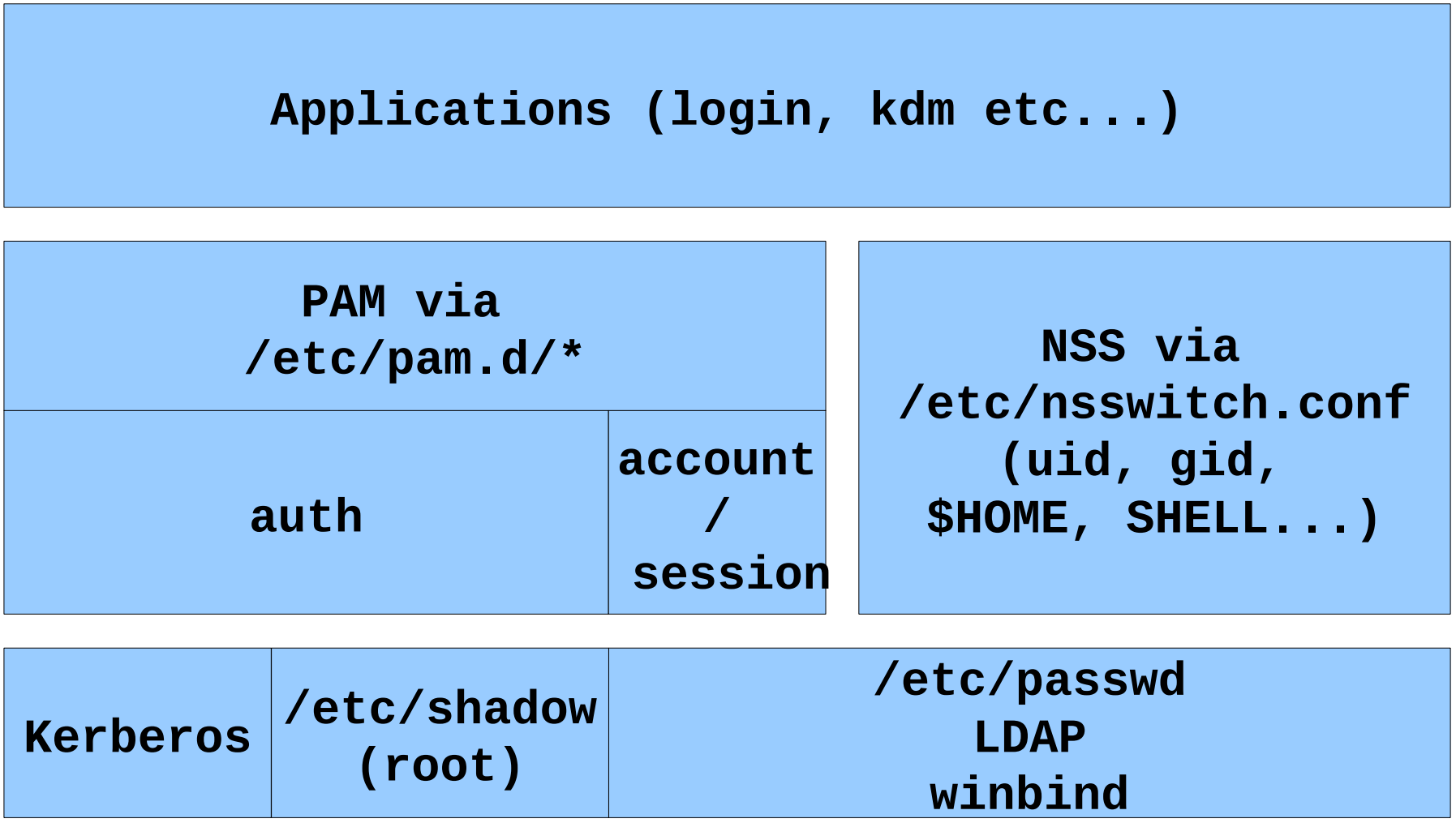
```
auth  sufficient   pam_krb5.so realm=UNISTRA.FR
auth  sufficient   pam_krb5.so realm=DPTINFO.URS.LOCAL use_first_pass
auth  [success=1 default=ignore] pam_unix.so try_first_pass
auth  requisite    pam_deny.so
```

Configuration clients 3/3

- Le fichier de configuration pour Kerberos
  `/etc/krb5.conf`

```
[libdefaults]
     default_realm = UNISTRA.FR
     allow_weak_crypto = true #(pour les ubuntu 10.04 et +)

[realms]
     UNISTRA.FR = {
             kdc = krb.unistra.fr
             kdc = krb2.unistra.fr
     }
```


Applications (login, kdm etc...)
PAM via /etc/pam.d/*
auth
account / session
NSS via /etc/nsswitch.conf (uid, gid, $HOME, SHELL...)
Kerberos
/etc/shadow (root)
/etc/passwd LDAP winbind

Plan

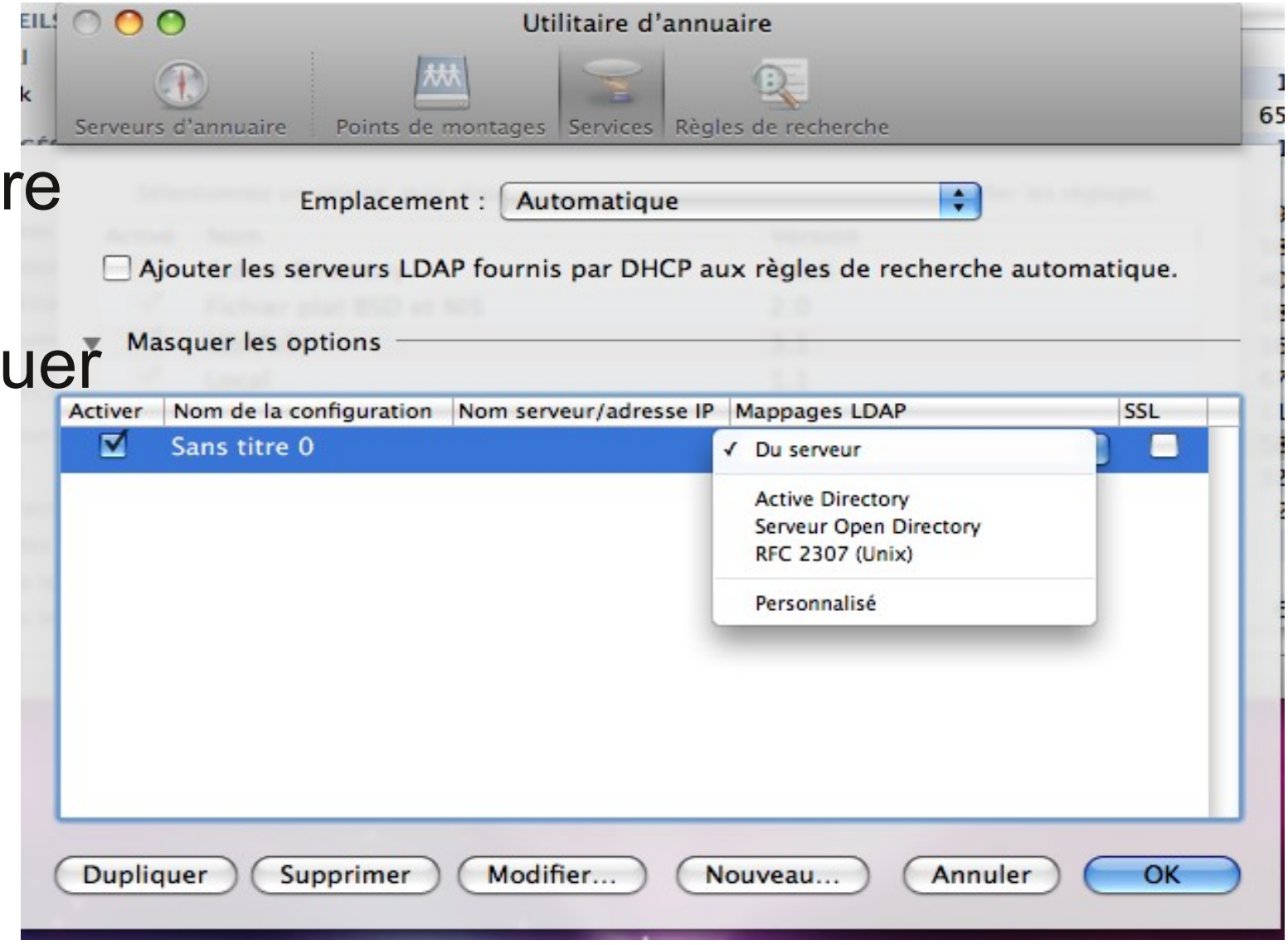
- Introduction
- Les possibilités
- Configurations du serveur Kerberos
- Configurations des clients Linux
- Configurations des clients MacOSX
- Configurations pour Active Directory
- Problèmes possibles
- Conclusion

Configuration clients 1/2 MacOSX

- /Library/Preferences/edu.mit.Kerberos
  - Contenu identique qu'un krb5.conf classique
- /private/etc/authorization
  Modifier la clef « *mechanism* » de
  « *system.login.console* » par :
  <string>builtin:krb5authnoverify,privileged</string>

Configuration clients 2/2 MacOSX

- Utilisation du service d'anuaire LDAP rfc2307
- On peut continuer à utiliser OpenDirectory pour la gestion des postes



Plan

- Introduction
- Les possibilités
- Configurations du serveur Kerberos
- Configurations des clients Linux
- Configurations des clients MacOSX
- Configurations pour Active Directory
- Problèmes possibles
- Conclusion

Configuration AD 1/3

- Relation de confiance :
  - Un ticket d'un royaume A est valide dans un royaume B
  - Active Directory intègre un royaume Kerberos
  - L'approbation entre royaume Kerberos UNIX et Active Directory est prévue
  - On peut avoir plusieurs Active Directory ayant confiance en un royaume Kerberos Unix
  - Mise en place aisée

Configuration AD 2/3

- Utilisation de comptes supports :
  - Un utilisateur *totobis* du domaine AD
  - Il est « support » pour *toto* qui existe dans le domaine Kerberos Unix
  - A la connexion
    - Vérification du mot de passe pour *toto*
    - Attribution d'un TGT pour *toto*
  - On travaille ensuite avec le user *totobis*, tout en montrant le TGT de *toto*
  - Tous les services reconnaissent les TGS issues pour ce TGT (relation de confiance)

Configuration AD 3/3

- Relier un compte Kerberos à un compte Active Directory : attribut LDAP altSecurityIdentities
- Indiquer les serveurs Kerberos aux clients Windows (Base de registre, gpo ou script, car eux pas comprendre /etc/krb5.conf)
- Windows 2008, Windows 7 : Limiter les types de chiffrements si nécessaire

Configuration AD : Résultat

Plan

- Introduction
- Les possibilités
- Configurations du serveur Kerberos
- Configurations des clients Linux
- Configurations des clients MacOSX
- Configurations pour Active Directory
- Problèmes possibles
- Conclusion

Les problèmes … divers

- Samba (ou NT4) en contrôleur de domaine → samba4
- MacOSX : Fâcheuse tendance à écraser les configurations fichiers
- Workgroup de postes windows : des solutions existent, cf. le Technet Microsoft, le principe reste le même
- Problème avec Active Directory ? : Wireshark est le meilleur moyen de savoir ce qui se passe

Les problèmes lors de la mise en place

- Bien différencier authentification et autorisation
  - « **`kinit user@REALM`** » permet une vérification rapide que la partie Kerberos est OK
  - Les logs coté serveur KDC sont explicites.
- « **`pam.d`** » permet de configurer la partie authentification et autorisation, mais c'est **`/etc/nsswitch.conf`** qui dit où chercher l'information:)
- Généralement on utilise libnss-ldap
  - Pour être sur que la partie « compte » fonctionne, utiliser « **`getent passwd`** » pour voir la liste des comptes visibles

Plan

- Introduction
- Les possibilités
- Configurations du serveur Kerberos
- Configurations des clients Linux
- Configurations des clients MacOSX
- Configurations pour Active Directory
- Problèmes possibles
- Conclusion

Conclusion

- Ca marche
- Déploiement réalisé sans problème pour un département de l'IUT, et en cours pour le département Math-info
- Permet de bien décomposer les éléments relatifs aux utilisateurs

Conclusion

- Gain pour l'administrateur :
  - un référentiel unique des comptes
  - Une sécurité accrue
  - Les trois grandes familles peuvent exploiter la même base de mots de passe
- Gain pour l'utilisateur : Avec du SSO, il y aura un seul et unique moment pour donner le couplet login/password

Questions ?