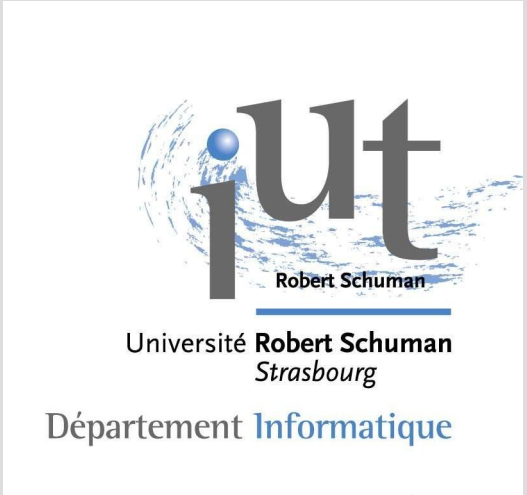
Authentifications dans un monde hétérogène

Emmanuel.Blindauer @ urs.u-strasbg.fr

IUT Robert Schuman

Département Informatique



X/STRA 2006

Problématique

Augmentation des services disponibles :

- Accès à un ordinateur
- Courrier électronique
- Accès intranet/extranet, wiki, blog
- Annuaires
- Accès réseau sans-fils

Problématique

Augmentation du nombre d'utilisateurs

- tous les étudiants
- tous les personnels
- ... même les personnes invités

Problématique

Augmentation du niveau de sécurité

- « *kiddies scripts* »
- Sisyphe: De nouvelles solutions à inventer lors de chaque nouveau péril
- authentification: la porte d'entrée

Problématique

Multiplication des Systèmes d'Exploitations

- Windows 95, 98, 2000, CE, 2003, XP, Vista
- MacOS 8, 9, MacOSX 10.2, 10.3, 10.4 ...
- Linux Debian, Mandriva, Fedora, ...
- FreeBSD, OpenBSD, ...
- Symbian, Zaurus, Palm ...

Problématique

Multiples authentifications et incompatibilités:

- Flat-file
- NIS, NIS+
- LDAP
- Kerberos
- Auth Web (Passport .NET, CAS, ...)

Problématique

Augmentation de l'attente des utilisateurs

- Cela doit être simple
- Aucun intérêt sur les problèmes techniques
- « Chez moi ca marche comme cela, ca doit être pareil ici »
- Trop de mots de passe à retenir

Problématique: une solution

La solution avec un compte par ordinateur :

- « toto » pour presque tous les services
- « C'est pas grave, j'ai rien d'important dessus »
- « Quel est mon mot de passe pour X,Y,Z ? »

Les systèmes actuels

Les authentifications dans le monde Windows:

- NTLM / NTLMv2
- SSPI (Kerberos)
- dur à modifier
- pas de garantie sur les implications
- pas de garantie sur le long terme (Kerberos?)

Les systèmes actuels

Les authentifications dans le monde MacOSX:

- flat file (/etc/passwd) (clients)
- OpenDirectory (LDAP / Kerberos) (server)
- autre : NIS, NTLMv2
- utilise PAM: *Pluggable Authentication Modules*
- orientation à long terme: Kerberos
- documentation assez complète

Les systèmes actuels

- Les authentifications dans le monde Linux:
- flat file (/etc/passwd)
- LDAP
- autre : NIS, NTLM, Kerberos
- utilise PAM: *Pluggable Authentication Modules*
- orientation à long terme : Libre
- documentation complète

Les solutions du passé

NTLM:

- stocke deux hash du mot de passe (NT et LM)
- peut être cassé par force brute et attaque offline
- le client ne peut pas identifier le serveur

Les solutions du passé

NIS:

- maître /esclave pour les fichiers d'authentification
- peut être cassé par force brute et attaque offline
- le client ne peut pas authentifier le serveur et inversement, appels RPC non sécurisés
- Combiné souvent avec NFS, toute usurpation d'identité sous le client est invisible

AuthN / AuthZ

- AuthN : AuthentificatioN
- AuthZ : AuthoriZation
- Séparation de l'identification de l'utilisateur et du choix de l'autoriser à utiliser tel service
- Séparer pour mieux déléguer: AuthN sur un annuaire métropolitain et authZ dans ses locaux

Choix

Kerberos :

- ne nécessite pas de modification à Windows
- fonctionne sur les autres systèmes
- est une technologie Unix qui a fait ses preuves
- nécessitait quelques connaissances.
- permet le Single Sign On (SSO)

Kerberos

- Développé au MIT dans les années 80
- Krb5: RFC 1510
- 3 implémentations majeures dans le monde: MIT, Heimdal, Microsoft
- But principal: ne plus faire transiter d'informations sensible sur le réseau, même chiffrée.
- Architecture à tiers de confiances (AS, TGS)

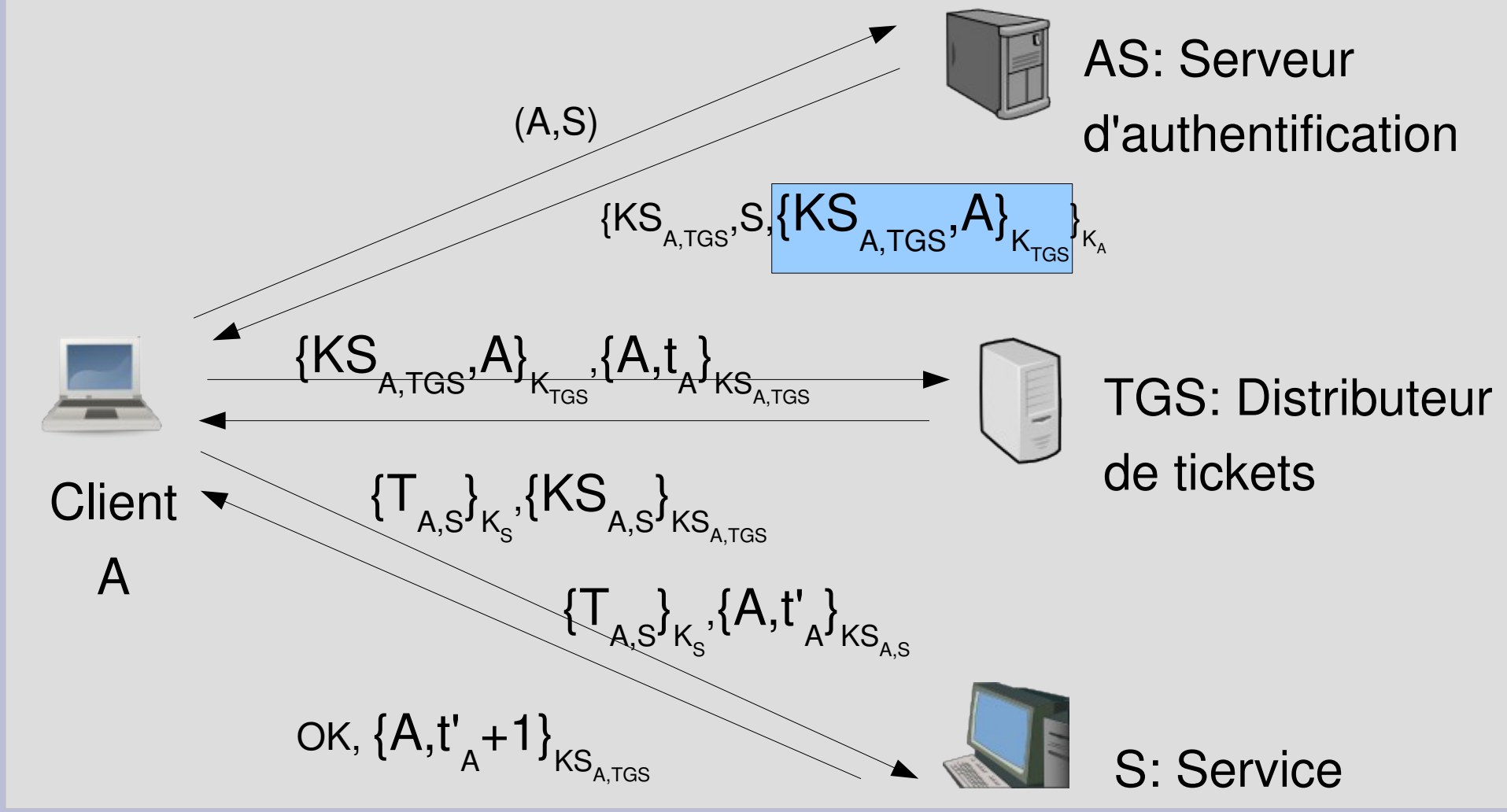
Kerberos - Glossaire

- REALM : domaine d'authentification
- Principal : utilisateur , service « login@REALM » ou « nfs/hostname@REALM »
- Authentication Server AS : AuthN
- Ticket-granting Server TGS: distributeur
- KDC: (AS) + (TGS)
- Tickets: tgt, tgs

Kerberos

- Un utilisateur A souhaite accéder à un service S
- A s'identifie auprès de AS avec son login/pass
- AS fourni un ticket initial pour acceder à TGS
- A fourni le ticket à TGS qui pourra s'assurer de l'identitée de A.
- TGS génère alors un ticket tgs pour que A puisse acceder à S
- A fourni le tgs à S (seul S peut le déchiffer)

Kerberos – Principe (2/2)



Kerberos - Windows

Où trouver Kerberos ?

- Active Directory en mode mixte au moins
- Utilisé par tout compte créé ou mot de passe modifié
- Est l'implémentation sous-jacente à SSPI
- Disponible dans le framework .NET

Kerberos - Windows

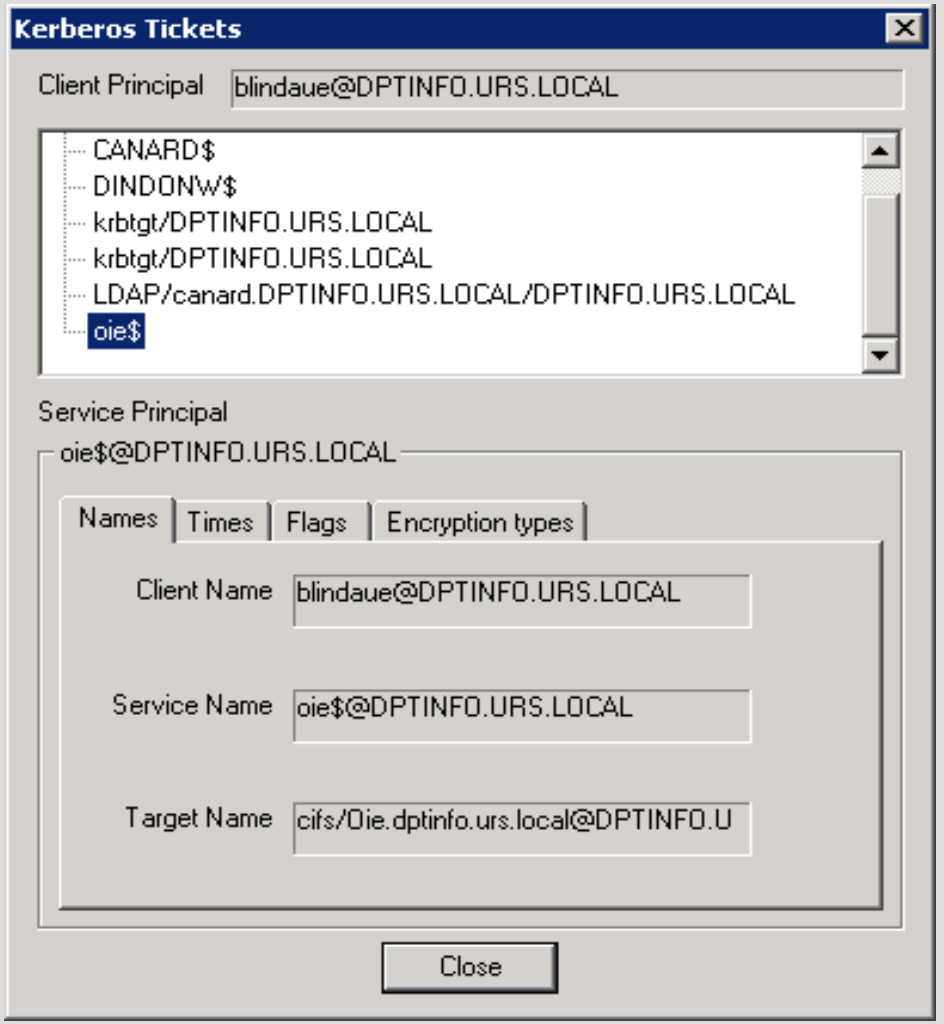
- Tout client 2000 authentifiant un utilisateur AD passe par kerberos
- Ce n'est pas le cas avec les comptes locaux

Kerberos – Windows - Détails

- Obligation domaine DNS et REALM identique
- Obligation serveur DNS en local
- Intégration du KDC à un contrôleur de domaine
- Réplication Multi-maître

Kerberos - Windows

- Pour les clients : les mettre dans le domaine
- Possibilité de voir les tickets avec klist.exe ou kerbtray.exe
- Renouvellement automatique des tickets



Kerberos - Windows

- Possibilité d'utiliser ktutil.exe pour générer des keytab: des tickets pour authentifier des services
- Une entrée par service: HTTP, HOST, CIFS..
- Regrouper des principals sur un seul principal: setspn.exe

Configuration Linux

Séparation des problèmes dans PAM:

- Authentification (section « auth » dans PAM)
- Gestion des autorisations (section « account » et « session » dans PAM)

Linux - Authentification

Authentification :

- Configuration classique Kerberos (/etc/krb5.conf)
- Utiliser le REALM du domaine Windows (nom DNS complet)
- Les serveurs de mots de passe sont les DC
- Attention aux types d'encodage des tickets (CRC-CBC-MD5)

Linux - Authentification

- Vérification de la configuration:

  « kinit user ; klist »

- Rajouter ntpd pour synchroniser les horloges (utilisation de la date dans les tickets)

Linux - Autorisations

- Besoin de uid, gid, GECOS, $shell, $home
- Utilisation de winbind pour chercher certains paramètres dans les DC (uid, gid, GECOS) par appel RPC
- Winbind maintient une correspondance entre uid/gid unix et SID Windows

Linux - Autorisations

- Backend winbind :
- winbind_ldap : stockage du mapping uid/SID dans un serveur LDAP
- winbind_rid : dérivation reproductible de l'uid depuis le SID (un seul domaine)
- winbind_sfu : stockage complet du mapping dans AD modifié avec SFU (avantage: permet de changer HOME, ou SHELL par ex.)

Linux - Autorisations

- Il faut rejoindre le poste unix au domaine AD : « net ads join » pour que winbind puisse faire des appels RPC
- Tests de winbind: « wbinfo -t » pour verifier les appels RPC, « wbinfo -u » pour avoir la liste des utilisateurs

Linux - Intégration

- Modifier PAM pour faire l'authentification via kerberos : utiliser pam_krb5 (possiblité d'utiliser pam_winbind, cached credentials 3.2)
- Modifier nsswitch.conf pour utiliser les uid, gid, etc :

  « passwd: files, winbind »
- Test final : « getent passwd »

Postes en boot double

- Chaque poste a un identifiant unique
- Mais le nom court (hostname) doit également être unique

Services supplémentaires

Utiliser kerberos via ssh:

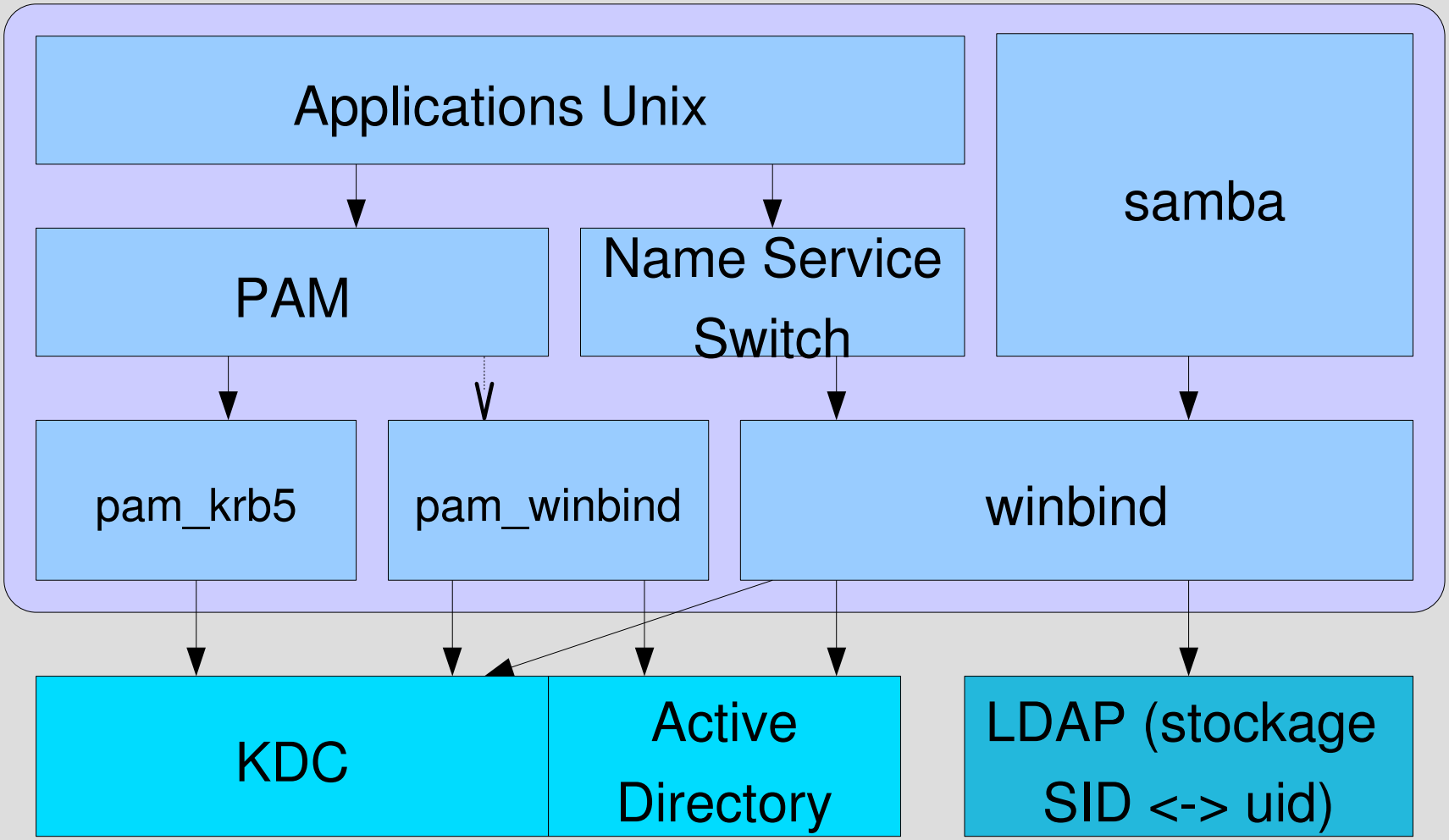
- Activer GSSAPI pour les clients et serveurs
- Rajouter une entrée dans le keytab pour le SPN (servicePrincipalName)
  « HOST/hostname@REALM »
- Plus besoin de taper son mot de passe

Services supplémentaires

Utiliser un serveur apache et kerberos :

- Utiliser le module mod_auth_kerb5
- Rajouter une entrée dans le keytab pour le SPN (servicePrincipalName)
  « HTTP/hostname@REALM »
- Plus besoin de taper son mot de passe

Récapitulatif



Services SSO

Enormément d'applications Windows !

- Utilisations de partages réseaux
- Authentification SQL Server
- Applications basées sur framework .NET
- IIS
- putty

Services SSO

- Apache + mod_auth_krb5
- Samba
- Openssh
- Mozilla, konqueror
- Cyrus Imap
- NFS v4

Services SSO

Concrètement, ce qui est en place :

- Une seule authentification lors de la connexion de l'utilisateur.
- Ouverture avec le bon profil de l'extranet
- Sans avoir à stocker de mot de passe
- Tous les services Windows fonctionnels

KDC Unix - Workstation

- Possibilité d'utiliser un KDC Unix pour plus de sécurité et stabilité
- Ne fonctionne que en dehors d'un domaine
- Chaque poste doit être configuré pour authentifier sur le KDC, mais les comptes doivent être locaux (gestion des comptes via la SAM): on ne délègue que AuthN

Kerberos - Trust AD / KDC Unix

- Possibilité d'utiliser un KDC Unix pour plus de sécurité et stabilité
- Un autre REALM doit être défini
- Le domaine AD doit definir une bijection entre les SPN AD et ceux du REALM
- Chaque poste doit être configuré pour approuver le REALM
- Les utilisateurs s'identifient sur le KDC et utilisent leur compte AD

L'autre solution : LDAP

- Concept plus simple: flat-file centralisé
- Enormement de support
- Permet de stocker des annuaires
- Mais ne contient pas de solution de SSO
- Définition des entrées modulable, par « schema »

LDAP coté serveur

- Gestion des réplications
- Facile à mettre en oeuvre pour les petits serveurs
- Réplication multimaitre peu courante
- Gestion des ACL un peu complexe
- Usage courant avec Samba pour gérer un domaine Windows

LDAP coté client

Sous linux, peu de problème:

- Utilisation de pam_ldap pour AuthN et AuthZ
- Possibilité de mixer Kerberos/LDAP
- /etc/ldap.conf pour dire quel serveur utiliser et quelles branches parcourir.

LDAP coté Windows

Dans le cas d'un domaine samba 3

- Rejoindre le poste dans le domaine (créer le compte machine au besoin)
- L'authentification se fait sur le couplet NTLMv2
- Pas de SSO
- Suffisant dans 90% des cas

LDAP coté Windows AD

Dans le cas d'un domaine AD

- Problématique : il n'y a qu'un seul référenciel dans le monde Microsoft, c'est Microsoft et le reste n'existe pas
- Si on modifie, quels seront les impacts ?

LDAP coté Windows AD

- `msgina.dll` responsable de l'authentification
- Documentation existante sur cette partie
- pGina : une dll vient en remplacer une autre
- Multiples possibilités avec pGina: authN vers LDAP, PAM, ssh, SQL, Radius, web, imap,...
- Ne pas perdre les avantages de AD, sinon, samba 3 presque suffisant

LDAP coté Windows AD

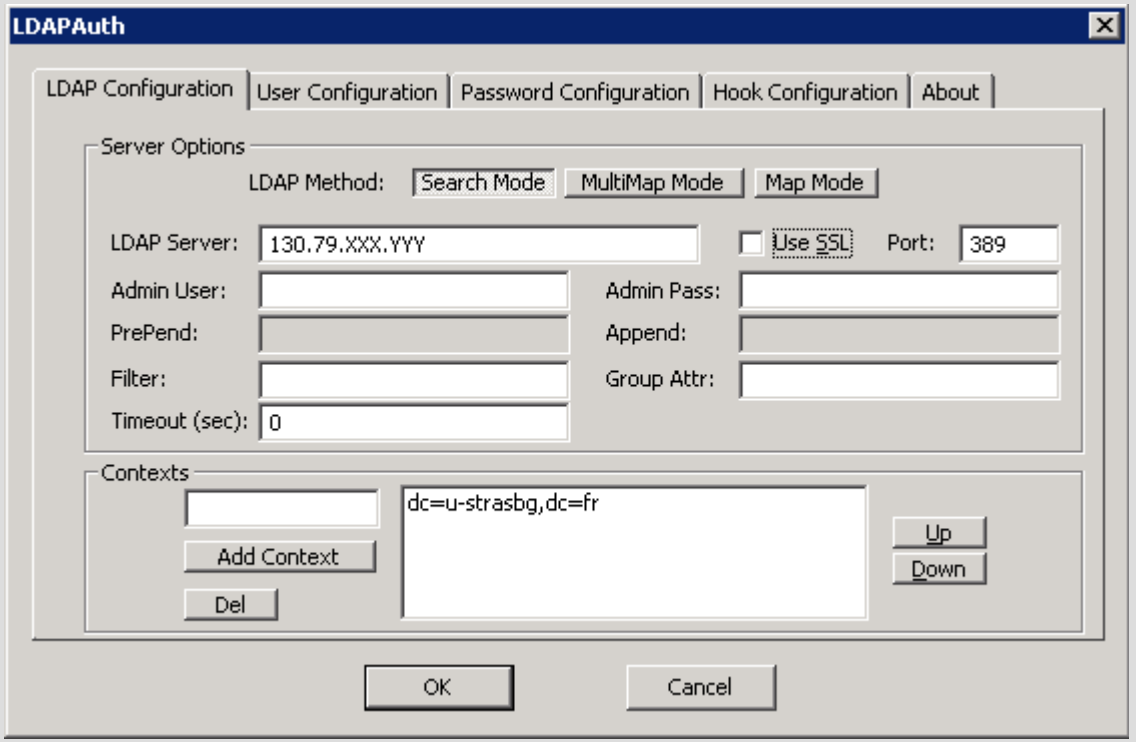
Idée : cumuler authN LDAP et authN AD

- Même login/pass : enchainer les authentifications
- AuthN AD : permet d'utiliser Kerberos
- Il faut les mêmes login (facile)
- Il faut les mêmes mots de passe (dur, on ne peut pas déchiffer un mot de passe, ...)
- Choix: référentiel des mots de passe : LDAP

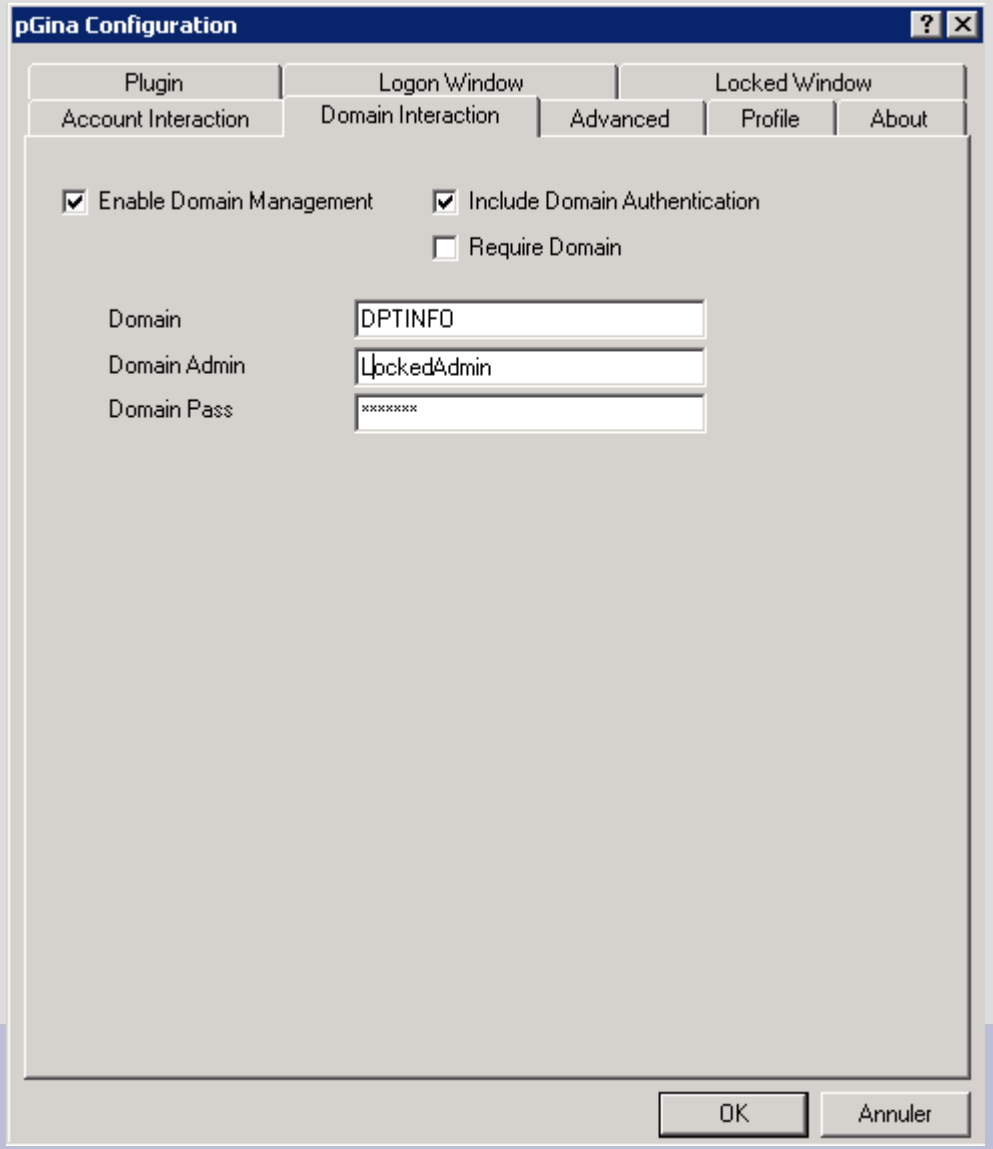
LDAP coté Windows AD

- pGina permet tout cela : Cumuler les authentifications
- On garde 100% des fonctions AD
- AuthN sur LDAP
- Besoin d'avoir le domaine en mode mixte, pour forcer les mots de passe et créer les comptes à la volée (pourrait être changé)

Pgina / Plugin LDAP



Pgina / Interaction AD



LDAP ou/et Kerberos

Que choisir ?

- LDAP pur : pas de SSO
- LDAP + Kerberos : difficulté de la mise en oeuvre, replication
- Kerberos : toutes les appli presque compatible (GSSAPI / SASL)
- AD pur : Dépendance Microsoft
- OpenDirectory : uniquement pour MacOSX
- Samba-4 en bonne voie (disparition de AD4Unix)

Conclusion

- Kerberos: concept d'il y a 20 ans, mais pourtant repris dans Windows
- Permet un SSO facile
- Augmente la sécurité
- Unification des authentifications
- Plein de solutions pour faire presque ce que l'on veut