Kerberos: Linux, Windows et le SSO

Emmanuel.Blindauer @ urs.u-strasbg.fr

IUT Robert Schuman
Département Informatique

JRES 2005

Introduction

- Problématique
- Kerberos
- Windows 2000
- Linux et PAM
- Intégration dans les espaces numériques de travail (ENT)
- Perspectives

La problématique

- Multiplication des systèmes d'exploitation
- Multiplication des services disponibles
- Multiplication des utilisateurs
- Demande de simplification des authentifications :
  - Un seul login/pass
  - Ne pas re-demander quelque chose qui est évident : pas de ré-authentification inutile

La problématique

- Ne pas sacrifier la sécurité (pour les utilisateurs)
- Foisonnement de solutions d'authentification : unix, NIS, NIS+ Windows NT, Windows 2000, Kerberos, LDAP, auth. web (CAS, Passport .Net, ...) auth. SQL, etc

La problématique

- Obsolescence de certaines solutions: NIS
- Problème de sécurité : Facilité d'accès aux prises réseaux, PC de Troie...
- Incompatibilités, ou restrictions de certaines solutions d'authentification

Le But à la rentrée 2004

- Un seul login pour tous les services
- Un seul login pour tous les OS
- Une authentification avec une sécurité accrue
- Un vrai SSO : une seule authentification pour toute la durée du travail sur le poste
- Une forte recommandation d'avoir un domaine Active Directory (fonctionnalités complètes pour les outils Microsoft)

Plan

- Problématique
- Kerberos
- Windows 2000
- Linux et PAM
- Intégration dans les espaces numériques de travail (ENT)
- Perspectives

Le choix retenu

Kerberos :

- existe sur la plupart des plates formes
- est développé depuis des années
- répond à nos demandes de sécurité
- permet un vrai SSO
- Mais ... *semble* compliqué.

Kerberos - Introduction

- Développé au MIT dans les années 80 puis exporté et ré-implémenté dans différentes universités
- 3 implémentations répandues : MIT, Heimdal, Microsoft
- Principal but : ne plus faire transiter de mot de passe sur le réseau
- Architecture à tiers de confiance(AS,TGS)

Kerberos – Principe (1/2)

REALM : le domaine d'authentification

KDC : ensemble Authentification Server et Ticket Granting Server

Un utilisateur A souhaite accéder à un Service S :

- A s'identifie auprès de AS
- AS fourni un ticket (TGT) à A pour aller chez TGS
- A fourni le ticket TGT à TGS
- TGS vérifie le ticket TGS et émet un ticket T pour S
- A présente le ticket T à S et utilise les services

Kerberos – Principe (2/2)

- AS: Serveur

Plan

- Problématique
- Kerberos
- Windows 2000
- Linux et PAM
- Intégration dans les espaces numériques de travail (ENT)
- Perspectives

Windows 200X

- Bonne nouvelle : Windows 2000 sait gérer Kerberos
- Mieux : c'est le mode natif dans les domaines Active Directory
- Mais : on reste tributaire des changements qui peuvent s'opérer dans l'OS

Windows 200X

- Les Domain Controllers (DC) intègrent un KDC
- Obligation DNS = REALM
- Obligation d'un dDNS donc utilisation d'un DNS local pour tout le réseau local
- Réplication assez efficace des DC donc redondance et disponibilité

Windows 200X

- Pour les clients Windows

Plan

- Problématique
- Kerberos
- Windows 2000
- Linux et PAM
- Intégration dans les espaces numériques de travail (ENT)
- Perspectives

Configuration Linux

Séparation des problèmes :

- Authentification
- Gestion des autorisations

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 contrôleurs de domaine
- Attention aux types d'encodage des tickets

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

- Dans le cas de multiples stations : besoin d'une correspondance cohérente : Utilisation du backend LDAP ou RID
- Il faut rejoindre le poste unix au domaine AD : « net ads join » pour que winbind puisse faire des appels RPC
- Tests de winbind: « wbinfo -u »

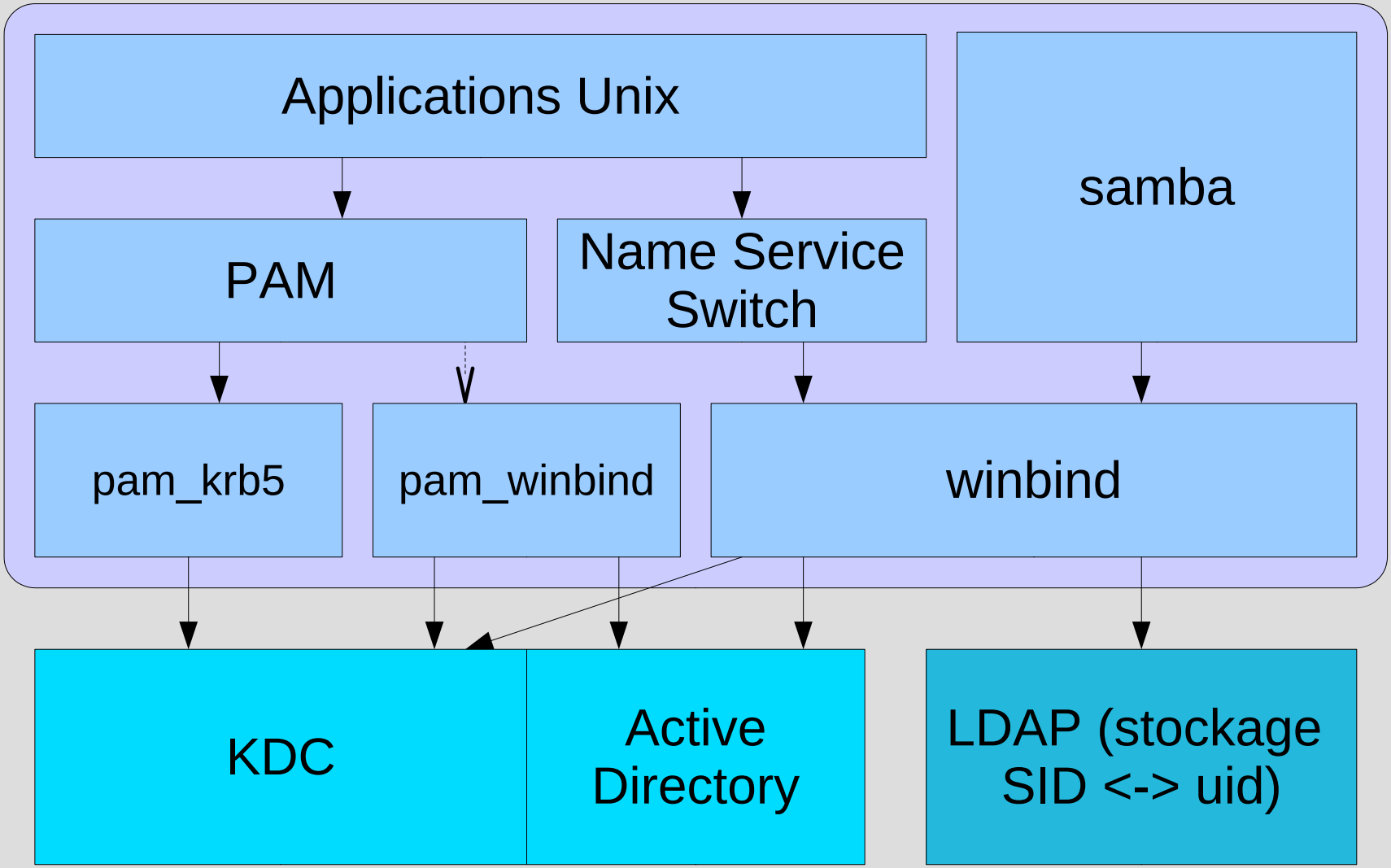
Linux - Intégration

- 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

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

Plan

- Problématique
- Kerberos
- Windows 2000
- Linux et PAM
- Intégration dans les espaces numériques de travail (ENT)
- Perspectives

Intégration dans les ENT

- Projets nationaux qui vont s'implanter
- Volet authentification : CAS avec backend au choix, utilisation de LDAP dans les 4 projets retenus
- L'utilisateur : un seul login!

Intégration dans EPPUN

EPPUN: Serveur openLDAP, réplicat local

Idée: modifier la GiNA :

- Faire l'authentification LDAP
- Forcer le mot de passe du domaine
- Faire l'authentification dans le domaine
- En cas d'échec LDAP, basculer sur l'authentification classique domaine

Intégration dans EPPUN

- Utilisation de pGina
- Domaine AD en mode mixte pour autoriser les appels RPC
- Utilisation du plugin LDAP
- Pré-création des comptes étudiants besoin d'accès aux PC pour créer leurs comptes dans EPPUN

Pgina / Plugin LDAP

Pgina / Interaction AD

Intégration dans EPPUN

Au final la mire est devenue:

Plan

- Problématique
- Kerberos
- Windows 2000
- Linux et PAM
- Intégration dans les espaces numériques de travail (ENT)
- Perspectives

Problèmes

- 80% : le DNS configuré dans la station n'est pas un des DC
- 5% : le PC a plus de 5 minutes de décalage: refus des tickets kerberos
- 15% : Les mises à jour Windows ont changé quelquechose dans les appels RPC ou dans Kerberos

Améliorations

- Utilisation de pGina en mode AD natif
- Utiliser un KDC Unix

Conclusions

- Enfin une solution qui réunit l'authentification Windows et linux, sans modifier les serveurs windows
- Plus de « j'ai oublié mon mot de passe pour XXXXX »
- Une seule base d'utilisateurs
- Un vrai SSO
- Les systèmes et applications ouverts sont un avantage pour l'intégration