Retour d'expérience sur le déploiement de NFSv4-Kerberos à l'IMB

La Cellule Informatique de l'IMB

Mathrice - Orléans
10 octobre 2012

Laurent Facq, Sandrine Layrisse

Introduction

Retour d'expérience sur l'évolution de services informatiques en environnement mutualisé

Problématiques :

- Besoin de rationaliser & sécuriser le SI du laboratoire
- S'adapter aux réorganisations des tutelles & s'intégrer dans les changements structurels de leurs services informatiques

=> Évolution du SI d'un laboratoire dans son écosystème

Plan de la présentation

- Introduction
- Analyse de l'opération
  - Point de départ
  - Pourquoi migrer ? Quels objectifs ?
  - Les implications et les contraintes
  - Quelle démarche ? Comment s'y prendre ?
  - Vision technique
- Mise en œuvre technique
  - Surcharge d'attributs
  - Gérer l'authentification par service
  - Implémentation de Kerberos
  - Mise en œuvre de NFSv4 dans le royaume Kerberos
- Impact auprès des utilisateurs
- Conclusion

Analyse : Point de départ

L'IMB a toujours été un laboratoire autonome gérant ses propres moyens informatiques (généraux et de calcul) :

- Serveurs d'infrastructure (Messagerie, DNS, espace de stockage, …) et machines de calcul (clusters)
- Gestion de son Système d'Information (annuaires LDAP, appli « maison »)
  - Les fiches des membres permanents et temporaires du laboratoire = identification complète : statut, validité, équipe, ...
  - Les comptes informatiques rattachés à ses membres = identification et authentification : login/mot de passe)

Analyse : Pourquoi migrer ?

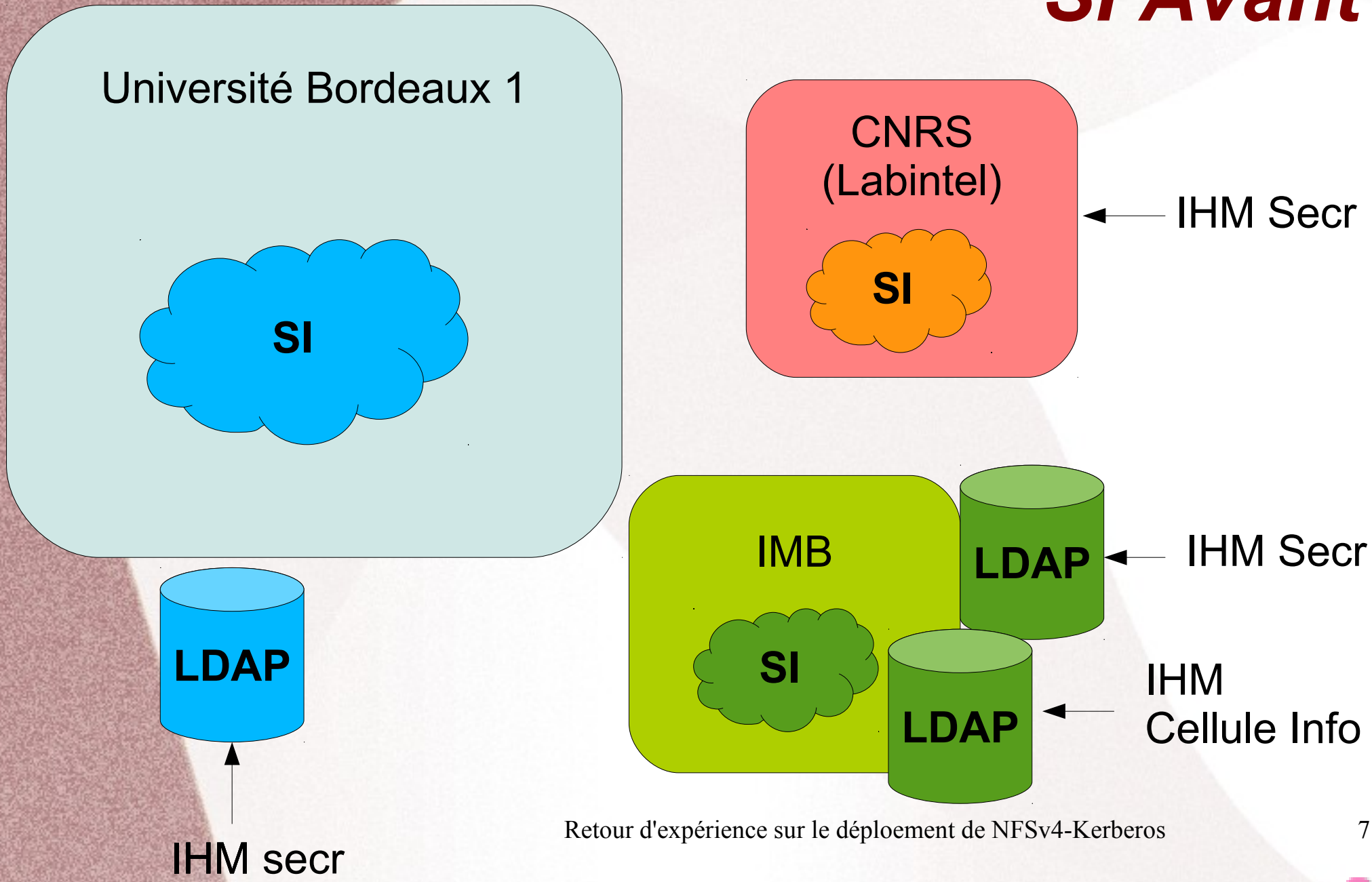
- Pas pour faire plaisir autour de nous ;-)
- Ni pour se lancer un nouveau challenge : tout casser pour voir !
- Partager : Le secrétariat du labo se retrouve détaché de la gestion administrative des comptes informatiques et de leur contrôle, aspects qui ne font pas partie du travail d'informaticien !
- Simplifier la tâche des secrétaires

  triple saisie des fiches : IMB, Bx1, CNRS(Labintel)
  avec les divergences inévitables

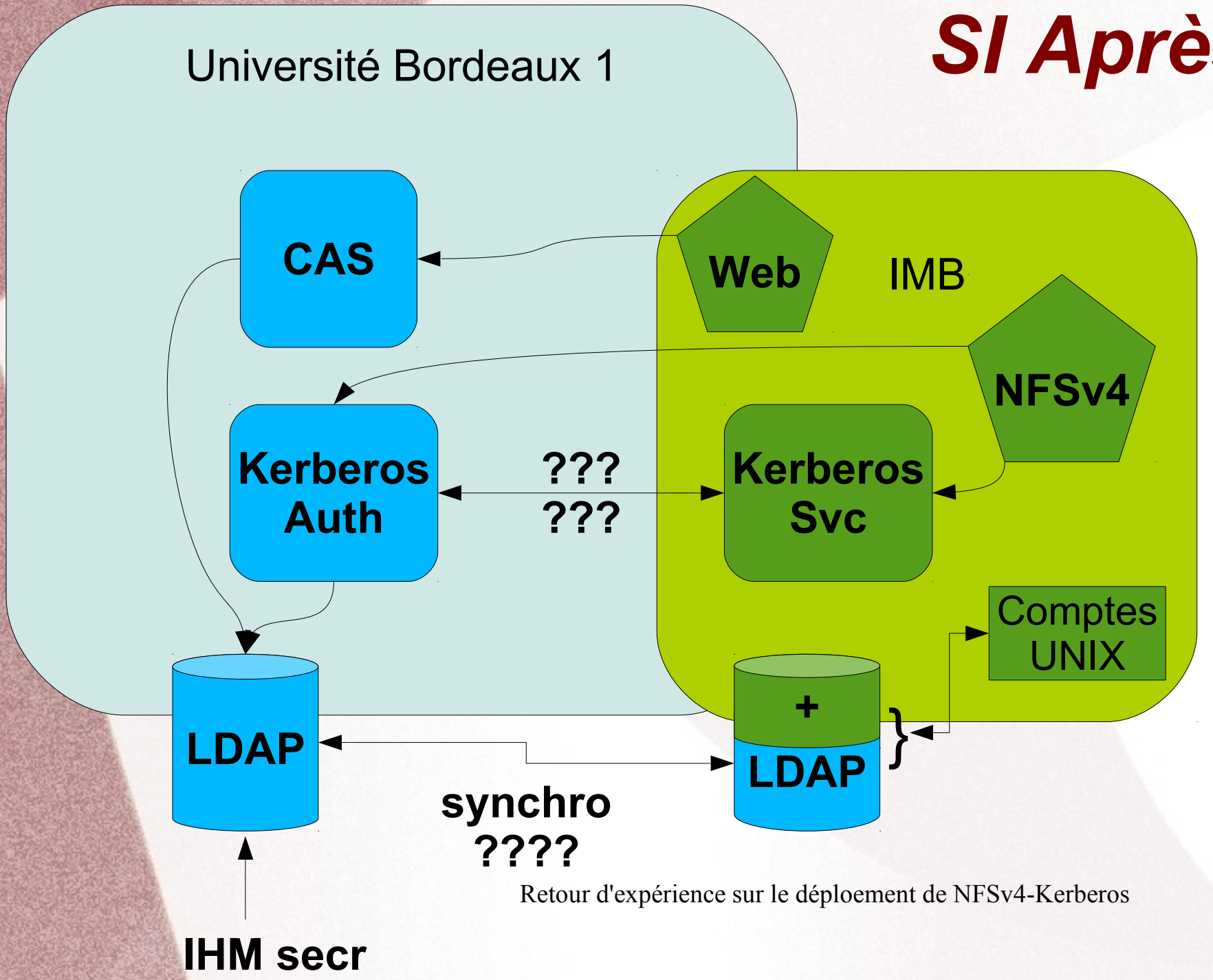
Analyse : perspectives

- S'appuyer sur l'authentification de Bordeaux 1 récemment mise en place dans le nouveau SI de l'université (SSO : kerberos/CAS) => le royaume Kerberos local gérerait les services
- Aller dans le sens de la mutualisation des moyens, mais en conservant la maîtrise des informations
- Renforcer la sécurité informatique : intégrité,confidentialité (NFSv4, services kerbérisés, CASsifiés)
- Avantage pour les usagers : Un login/mot de passe en moins pour les membres du laboratoire (plus que Labo/Bx1, Plateforme de calculs, Mathrice, INRIA, …)

SI Avant


Université Bordeaux 1
SI
LDAP
IHM secr
CNRS
(Labintel)
SI
IHM Secr
IMB
SI
LDAP
IHM Secr
LDAP
IHM
Cellule Info

SI Après ?


Université Bordeaux 1
CAS
Web
IMB
NFSv4
Kerberos Auth
???
???
Kerberos Svc
Comptes UNIX
LDAP
+
LDAP
synchro
????
IHM secr

Analyse : Implications et contraintes

- Dans la démarche, le laboratoire se positionne comme « pilote ». Avant de se lancer :
  - discussions avec labo voisins sur leurs intentions, leurs perspectives
  - discussions avec la DI Bx1
- Définition d'un contrat de service (cadrage) avec la DI Bx1: réunions régulières, mise en place de procédures, contacts privilégiés
- Toujours répondre aux besoins spécifiques « justifiés » (comptes hors gestion classique comme les invités/visiteurs, adaptation des cycles de vie des comptes)
- Recherche de souplesse : rester autonome pour le déploiement des services

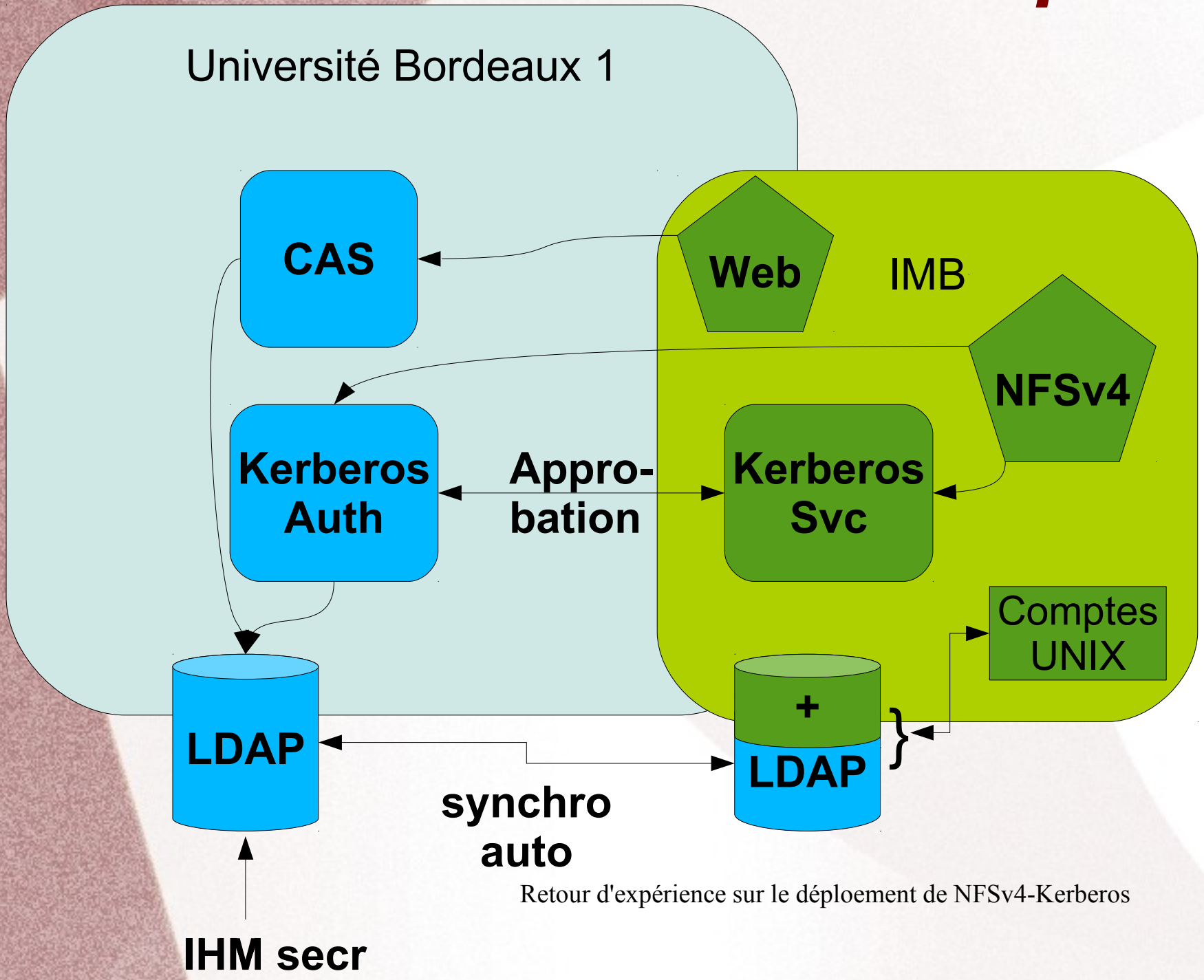
Analyse : Quelle démarche ?

- >1 an de discussion avec la Direction Informatique Bx1
- Démarche initiale :
  - maquettage de l'ensemble pour bascule « big bang » en juin ou au pire fin août
  - spécificités techniques : non triviales
    - kerberos CROSS-REALM
    - overlay ldap (Translucent)
- Après réflexion suite au maquettage : migration progressive des services (période de rentrée non propice au changement)
- Et un jour d'octobre, on s'est lancé ! => Migration du serveur de messagerie (kerberos sur PAM) : bon choix (impact sur un seul service)

Analyse : Compatibilité des SI

- Besoin d'enrichir l'annuaire de l'université Bx1 avec infos locales au labo :
  - Comptes & groupes UNIX, n° bureau, …
- Recherche d'une démarche technique « propre »
  - Éviter les import/export via cron ou autre mécanismes
  - Privilégier un moyen natif de surcharge des attributs

Schéma Technique Final



Mise en œuvre technique : annuaireS LDAP

1) Base : réplication partielle de l'annuaire de l'université

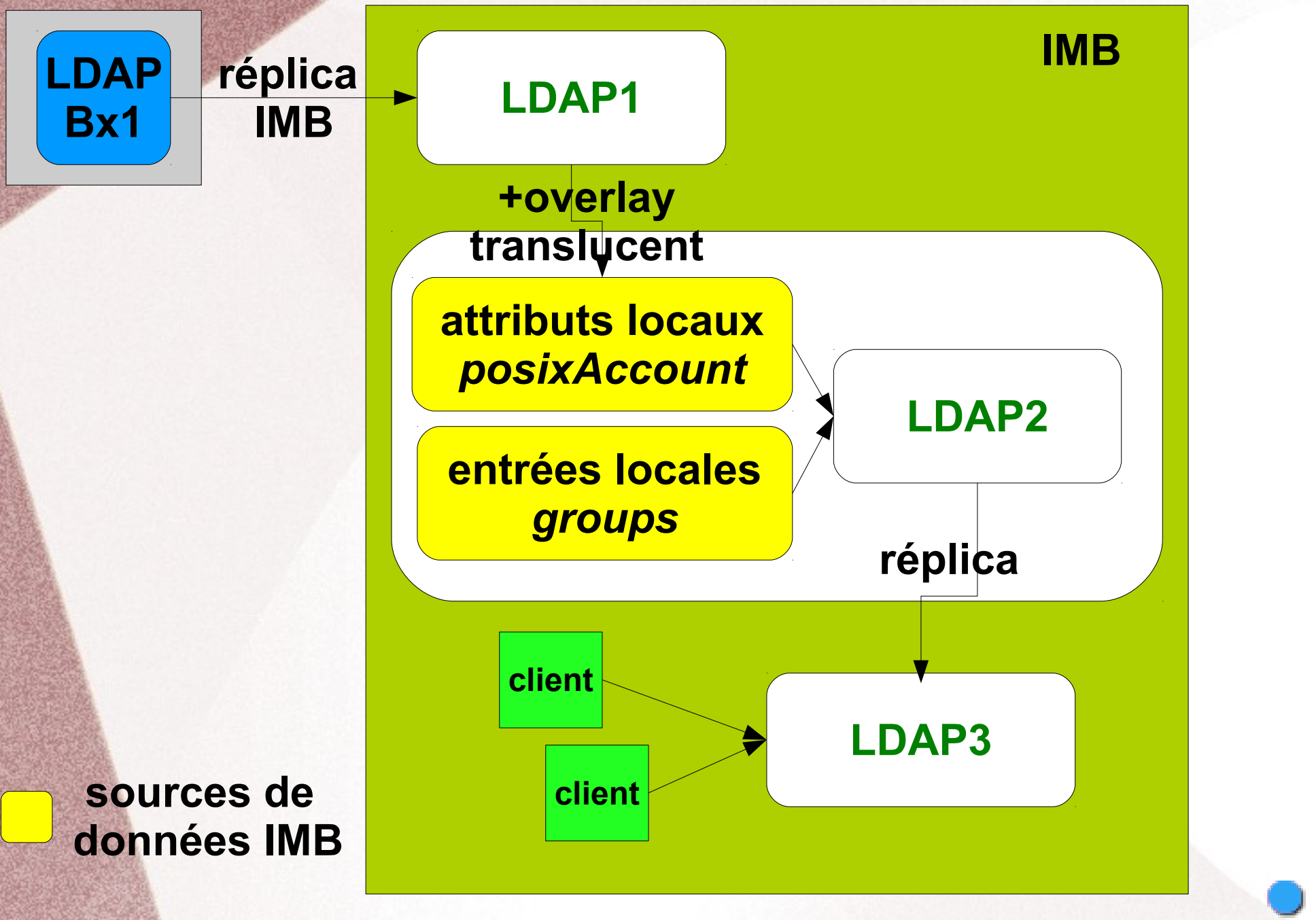
2) Pour l'ajout et la surcharge d'attributs :

- LDAP Transluscent répond nativement.
- *Délicat à maîtriser => quelques surprises !*
  Ex : impossible d'interroger directement les attributs ajoutés

3) Deuxième réplication pour « tout aplatir »

Quelques problèmes de synchronisation, nécessitent parfois de forcer une re-génération

Implémentation LDAP



Mise en œuvre technique : Kerberos ?

- protocole d'authentification multi-plateforme
- système de demande d'identification unique
- permet de contacter ensuite autant de services que souhaité (SSO)
- protocole sécurisé : ne transmet jamais de mot de passe en clair sur le réseau (tickets cryptés à durée de vie limitée)

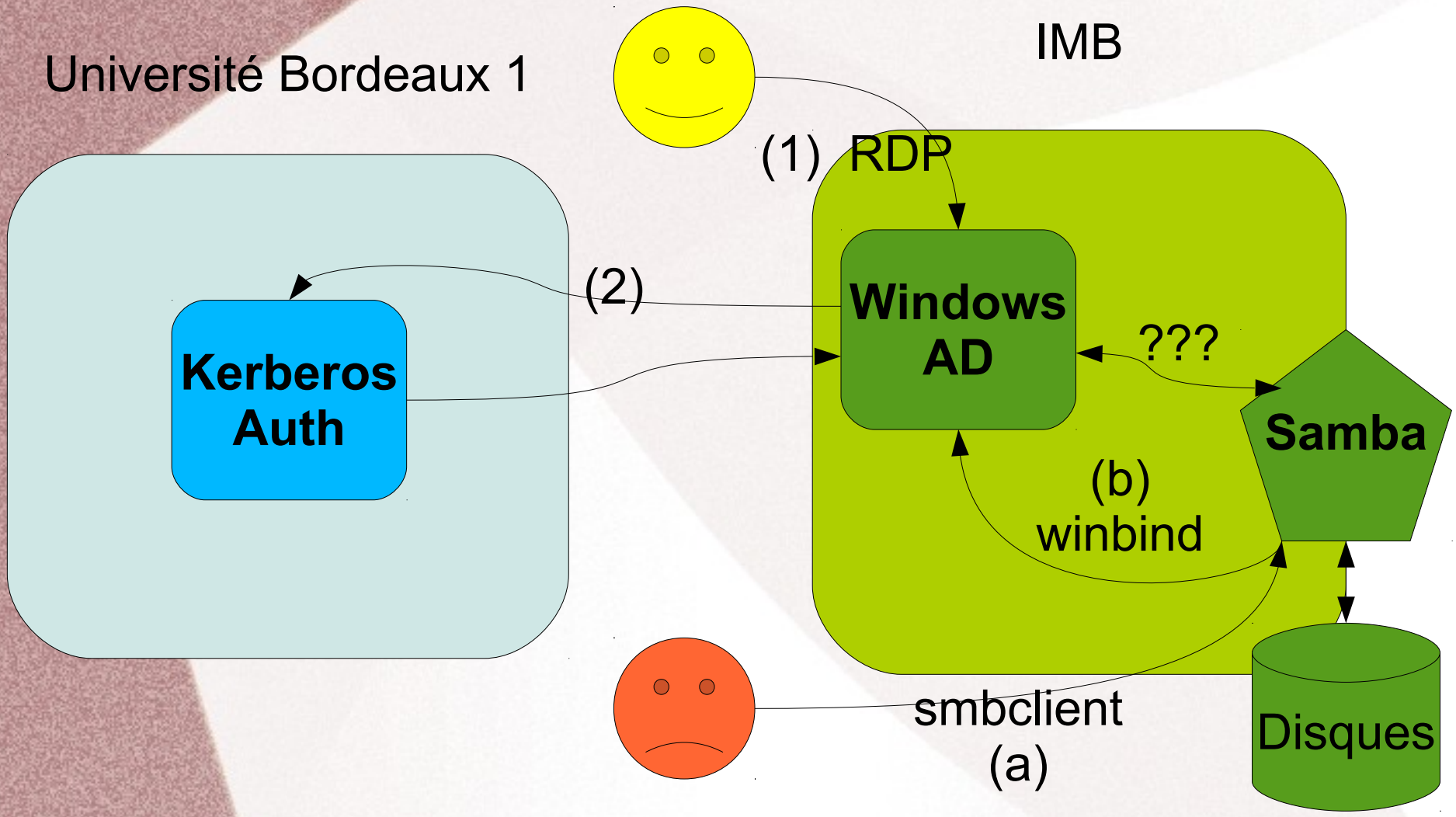
Mise en œuvre technique : Implémentation de Kerberos

- Création d'un royaume local pour le labo : choix Heimdal (idem Bx1)
- Approbation du royaume local avec le royaume de l'université (pour l'authentification en CROSS-REALM)
- Déclaration des services dans le royaume local (host/, nfs/, http/, ...)

Mise en œuvre technique : Gérer l'authentification par service

- SSO pour presque tous les services :
  - CAS pour les services Web
  - Kerberos pour le reste
- 2 points durs :
  - USVN (auth dans le code PHP) => LDAP
  - SAMBA : via Active Directory mais auth en CROSS-REALM non résolue (synchro des mots de passe kerberos/AD pas propre)

Mise en œuvre technique : Pb avec samba RDP OK / smbclient KO



Mise en œuvre technique : NFSv4 ?

Fonctionnalités	NFSv3	NFSv4
Mode	Sans état	Avec état (+ perf)
Environnement	UNIX	UNIX + Mac + Windows
Sécurité	Faible	**Forte (Kerberos) Intégrité, Confidentialité**
Transport	UDP & TCP	TCP, RDMA
I18N	-	UTF8
...	...	...

Mise en œuvre technique : NFSv4 + Kerberos

- Déclaration du serveur NFS dans le royaume local
- Côté serveur de « home » (Solaris 10 => MIT) :
  - krb5.conf et krb5.keytab
  - Export NFS des ZFS
- Côté client (Linux compatibilité MIT/Heimdal) :
  - krb5.conf et krb5.keytab client
    (Sur diskless : host/*.math.... magique !)
  - rpc.idmapd, rpc.gssd, pam_krb, ldap.conf, ...

Mise en œuvre technique : Problèmes

- Connexion par bi-clé sur les machines sas plus possible : choisir entre sécurité ou confort
  - le confort est choisi => nfsv4 en « sec=sys » sur 2 machines (mais surveillance renforcée)
- Renouvellement « automatique » des tickets kerberos
  - impose d'activer le verrouillage écran (ressaisie mdp) sur les postes utilisateurs
  - lifetime et renew_lifetime ajustés : 24h et 2 mois (idem sur KDC des services - ex : NFS)

Impacts utilisateurs : les difficultés rencontrées

- Changement de login (pour 70% des anciens) et de mot de passe (un de moins)
- Délai aléatoire sur les opérations annuaire Bx1 car difficile d'anticiper tous les cas particuliers (mais en cours d'amélioration):
  - doctorants non réinscrits qui soutiennent avant décembre,
  - stagiaires de Bordeaux 1,
  - suivi des invités “longue durée, invités réguliers,
  - jeunes retraités,
  - doublons lors des changements de statuts ...

Impact utilisateurs : les solutions

- Envoi de mail aux usagers 2 à 3 mois avant expiration du compte (secrétariat)
- Pas de date d'expiration pendant les vacances
- Script quotidien qui extrait la liste des comptes proche de l'expiration
- Comprendre le cycle de vie des comptes (DI, DRH, scolarité, …) et s'y adapter
- … et gestion téléphonique des exceptions !

Conclusion : bilan technique

- Important travail de collaboration avec la DI-BX1 pour :
  - trouver des solutions puis les tester, …
  - Comprendre leurs flux de traitement
- Découverte de bugs ou points durs techniques
- Mais au final, opérationnelle et techniquement satisfaisante

Conclusion : bilan humain & organisationnel

- Le contrat de coordination DI-IMB prend tout son sens avec cette opération
  - renforcement de la coopération entre services
- Importance de la communication :
  - utilisateurs : page web + accompagnement
  - direction : soutien et arbitrage
- Satisfaction globale :
  - cellule info et secrétariat : rationalisation
  - utilisateurs : simplification

Perspectives

- Cette opération d'unification préfigure d'autres réorganisations à venir :
  - Fusion des universités en une seule : Nouvelle Université de Bordeaux (référentiel unique)
  - MATHRICE : évolution vers fédération d'identités
  - Centre de calcul nationaux ?
- Reproductibilité de l'opération ?

Vos questions ?