UFR : du SI autonome à l'intégration dans le SI université. Histoire et déboires

Gérard Milhaud
ESIL & CISCAM
ESIL – Luminy – Case 925 13288 Marseille Cedex 9
Gerard.Milhaud@univmed.fr

Dimitri Robert
ESIL – Luminy – Case 925 13288 Marseille Cedex 9
Dimitri.Robert@univmed.fr

Frédéric Bloise
ESIL – Luminy – Case 925 13288 Marseille Cedex 9
Frederic.Bloise@univmed.fr

Dominique Lalot
CISCAM, Université de la Méditerranée,
58, Bd Charles Livon - 13284 Marseille Cedex 07
Dominique.Lalot@univmed.fr

Résumé

Nous accompagnerons ici l'ESIL dans son parcours initiatique de première UFR de l'université de la Méditerranée à migrer depuis un SI autonome et ses bases d'utilisateurs locales indépendantes vers un SI s'appuyant totalement sur l'annuaire LDAP de l'université. Nous présenterons d'abord le contexte de la migration (université, CRI, UFR ESIL) pour en préciser l'enjeu, puis les caractéristiques respectives des systèmes avant et après la migration. Nous verrons les arguments qui nous ont poussés à migrer malgré le coût important de l'opération. Nous donnerons ensuite quelques précisions sur l'architecture technique choisie, puis nous nous intéresserons aux problèmes épineux (et non prévus) liés au flux d'information inter-services voire inter-universités, desquels le nouveau système nous rend fortement dépendant. Nous terminerons par une contribution au débat sur l'inévitable mutation du métier de l'informaticien d'UFR impliquée par la centralisation des services.

Mots clefs

Retour d'expérience, migration, LDAP, système d'information, Apogée, Harpège, ENT, UFR, centralisation, mutation du métier.

1 Introduction

Nombre d'universités en France disposent depuis quelques années d'un annuaire LDAP central intégrant tous les usagers de l'établissement. S'appuyant sur cette brique de base de leur SI, elles ont proposé de plus en plus de services, puis en ont globalisé l'accès au travers d'environnements numériques de travail aujourd'hui souvent très aboutis.

Dans ces conditions, une UFR a-t-elle encore le moindre intérêt à dupliquer nombre de services en maintenant un SI autonome ?

En 2006, nous – le service informatique de l'École Supérieure d'Ingénieurs de Luminy (ESIL) – avons décidé que non. Nous avons donc joué le dangereux rôle d'UFR pilote au sein de l'université de la Méditerranée en initiant un projet de migration de notre SI autonome vers un SI s'appuyant *totalement* sur l'annuaire de l'université.

Quels sont les problèmes techniques et logistiques d'une telle migration ? Quelles solutions leur avons-nous apportées ? Que devient l'informaticien d'UFR dans ce nouveau contexte dominant de centralisation des services ?

Nous nous proposons d'apporter quelques réponses à ces questions.

2 Contexte

Les modalités de la migration vont fortement dépendre du contexte dans lequel elle s'inscrit : organisation de l'université et du CRI, taille de l'UFR et contraintes techniques liées aux choix de conception de l'annuaire central.

2.1 L'université de la Méditerranée, son CRI et les services offerts

L'université de la Méditerranée est une des 3 universités du site Aix-Marseille[1]. Elle comporte 12 UFR réparties sur plus de 10 sites géographiques fortement dispersés. Elle accueille environ 20000 étudiants et 4000 personnels (hors CNRS et organismes similaires).

Le Centre de Ressources Informatiques, baptisé CISCAM[2], comprend 42 personnes entre les titulaires et les contractuels. Parmi elles, 17 sont à temps plein et 25, appelées correspondants d'UFR, à 20% pour le CISCAM et 80% pour leur UFR de rattachement.

Le CISCAM a commencé à mettre en place en 2001 un annuaire LDAP recensant l'ensemble des usagers université. Cet annuaire, clé de voûte du système d'information central, est pleinement opérationnel depuis 2003. Dans un premier temps, la messagerie des services centraux s'y est appuyée. Puis un service de webmel a été ajouté.

En 2005, après installation d'un serveur de SSO CAS, ces services ont été généralisés, et le CISCAM a pu fournir à l'ensemble des usagers université une adresse e-mail en @univmed.fr (avec la possibilité de l'écrire @nom_ufr.univmed.fr pour préserver les susceptibilités et favoriser l'adoption...) pour les personnels, et en @etumel.univmed.fr pour les étudiants. Les UFR proposent aussi des adresses e-mail locales, mais un souhait *très* appuyé du président est de pouvoir joindre tout usager de l'université à partir des adresses centrales...

En 2006, un ENT basé sur ESUP-Portal est passé en production après 4 mois de prototypage. Les services, accessibles en fonction du profil LDAP, sont nombreux. On peut citer, sans être exhaustif : webmel (IMP/horde avec filtre antispam, absence, etc.), agenda partageable, partage de documents, accès au serveur de listes Sympa (inscription automatique à certaines listes en fonction des données LDAP), aux documents de son compte personnel

1 Bientôt plus qu'une ?... Fusion annoncée pour 2009.
2 Centre Informatique et Systèmes de Communication d'Aix-Marseille

dans l'UFR (canal de stockage), à ses informations DRH (carrière, avancement, etc.), aux applications de gestion (NabuccoWeb, fiche de poste, etc.), au service de gestion de demandes de son UFR (canal Helpdesk), à un intranet (pour les personnels) pour le partage de documents et un certain nombre de tâches administratives.

Une plateforme pédagogique basée sur le produit Moodle[3] a été mise en place à la rentrée 2006. Des emplois (CDD) ont été créés par l'université pour aider les enseignants volontaires à diffuser leur cours sur cette plateforme.

D'évidence, la multiplication des services fournis en central, associé à un véritable effort de la gouvernance dans ce sens, donne à l'ENT un aspect de plus en plus attractif et incontournable. Il existe une volonté affichée, au plus haut niveau, de faire en sorte qu'un usager informatique, quelle que soit son UFR, soit avant tout un membre de l'université : mobilité facilitée (*login*/mot de passe unique pour tous les services proposés, solution WIFI unique avec gestion centralisée (ARUBA) déployée dans toutes les UFR, serveur de VPN central...), adresse e-mail en @univmed.fr pour tout le monde, communication directe vers tous les utilisateurs via l'ENT.

2.2 Les UFR

Historiquement et comme dans bien des établissements, les UFR sont totalement autonomes quant à leur système d'information qui est géré en interne. Dans la plupart des cas, le responsable informatique de l'UFR fait partie des personnels affectés pour 20% de leur temps au CISCAM.

Les UFR ont donc un SI existant antérieur à la naissance de l'annuaire central (et bien souvent antérieur à l'époque où le terme système d'information est devenu courant...).

La problématique de la migration est fixée : d'un côté une volonté marquée de l'université de développer des services numériques et un ENT toujours plus présent qui tendent à rendre déplacé la maintenance d'un système d'information local indépendant, de l'autre un existant autonome qui fonctionne et très souvent peu de moyens humains pour se lancer dans un processus de changement assez lourd...

Il est nécessaire à ce stade de fixer clairement les idées sur la signification exacte que nous donnons au terme migration dans cet article : il s'agit essentiellement de l'adoption de l'annuaire central comme référentiel unique, en supprimant toute base d'utilisateurs locale et indépendante, accompagné d'un hébergement du mail par le système central.

2.3 L'ESIL

L'UFR en quelques chiffres clés afin de mieux percevoir les enjeux de la migration :

- 5 filières d'ingénieurs, une licence professionnelle, une option de Master Recherche et une de Master Pro ;
- 5 laboratoires hébergés, surtout composés de personnels non université donc non présents dans Harpège...
- 644 utilisateurs dont 451 étudiants et 193 personnels ;
- 4 bâtiments (11000 m2), 3 locaux de brassage et 2 salles machines ;
- 25 salles informatiques pédagogiques dont 18 en libre-service ;
- 420 machines, dont 26 serveurs (de CPU ou d'infrastructure) ;
- un service informatique de... 2 titulaires (IGR correspondant CISCAM + IGE) + 1 contractuel (technicien).

2.4 L'annuaire LDAP université et ses contraintes

L'annuaire, basé sur OpenLDAP, est alimenté par les bases métiers Harpège et Apogée via des scripts Perl. Il respecte la norme Supann, complétée par un schéma additionnel lié à certains besoins spécifiques de l'université.

Les *login* (champ LDAP *uid*) respectent les conventions suivantes :

- pour les personnels : *uid* = Nom pour le premier utilisateur de nom « Nom » inséré dans l'annuaire ; *uid* = Nom.n pour le n^{ième} ;
- pour les étudiants : *uid* = première lettre du nom suivie des 6 chiffres du code étudiant (inscrit sur la carte étudiant).

Les administrateurs d'UFR disposent d'un accès en écriture restreint aux fiches de leur UFR, dont ils peuvent modifier une partie des champs (téléphone, mot de passe, reroutage de courrier). Cet accès est de plus limité à une interface web (application PHP interne *casifiée*) : aucune possibilité d'écriture dans l'annuaire par script pour les UFR.

L'interface permet l'ajout et la destruction (une par une...) de fiches déconnectées de la base Harpège pour gérer les personnels non université. Pour les étudiants, en revanche, aucun ajout hors Apogée n'est possible. Enfin, les fiches issues d'Harpège ou Apogée ne peuvent être détruites au niveau de l'UFR.

3 La migration ESIL

3.1 Le SI ESIL d'avant...

Comme bon nombre de structures, nous continuions à faire fonctionner une architecture classique, éprouvée mais dépassée. Nous en présentons ici les caractéristiques impactées par la migration :

- un serveur mail (SMTP(postfix + postgrey + SpamAssassin)/IMAPS) gérant le domaine de messagerie @esil.univ-mrs.fr ;
- un webmail IMP/Horde ;
- 2 serveur NIS (master/esclave) pour gérer le monde Unix ;
- un PDC et un BDC NT4 pour le monde Windows ;
- 2 bases d'utilisateurs disjointes pour Windows et Unix (avec les mêmes *logins*), indépendantes de l'annuaire LDAP central ;
- utilisation de comptes utilisateurs non-nominatifs pour les groupes de travail (ex. *forumbio2007*, *bde*, *gala*) ;
- synchronisation des mots de passe Unix et Windows par script ; modification par interface web dédiée. Mots de passe initiaux à fournir à chacun par contact direct ;
- profils Windows itinérants hébergés sur le PDC NT4 ;
- imprimantes gérées pour Windows par le BDC NT4 et pour Unix par un serveur CUPS ;
- données centralisées sur un serveur NFS+SAMBA.

3 http://fr.wikipedia.org/wiki/Moodle

3.2 Le SI ESIL tel qu'on le souhaite, et le coût prévisible

Le fonctionnement visé est le suivant :

- passage au *uid* (*logins*) et *uidnumber* centraux, tels que définis dans l'annuaire LDAP ;
- passage aux adresses mail @univmed.fr et @etumel.univmed.fr, avec utilisation des serveurs SMTP/ IMAP/webmail centraux ;
- unique serveur SAMBA/LDAP pour gérer les utilisateurs Windows et Unix, avec synchronisation permanente des données de l'annuaire LDAP central vers le local ;
- mot de passe unique Windows/Unix, modifiable par l'interface web de l'annuaire central. Mode d'initialisation des mots de passe *étudiants* évitant d'avoir à leur fournir par contact direct[4] ;
- profils Windows itinérants hébergés dans le *homedir* ;
- plus aucun compte utilisateur non nominatif ;
- imprimantes gérées par le serveur CUPS pour Windows et pour Unix, et partagées pour Windows via SAMBA ;
- données centralisées sur un NetAPP FAS 250, acheté pour l'occasion.

Une telle migration implique forcément un important travail en amont, plus encore dans notre situation d'UFR pilote... 6 mois de préparation nous ont été nécessaires :

- réflexion sur l'architecture à adopter ;
- achat de nouveau matériel : serveurs LDAP, NetAPP. Au coût direct des équipements, il faut ajouter le temps nécessaire aux achats publics correspondants : montage de MAPA... ;
- acquisition des nouvelles connaissances (OpenLDAP, NetApp, API LDAP Perl, heartbeat/DRBD) ;
- mise en place du serveur LDAP/SAMBA tel qu'il sera en production ;
- développement de la suite de scripts Perl nécessaires pour la synchronisation des annuaires, la gestion les groupes d'utilisateurs UNIX et Windows, des partages associés aux groupes de travail (anciens comptes non nominatifs), l'ajout/destruction des utilisateurs locaux ;
- création de nouvelles images disques pour les postes Windows et Unix car changement de mode d'authentification et de domaine Windows (merci JeDDLaJ[5]) ;
- vérification de la présence dans l'annuaire central de tous les personnels université et de la pertinence des données entrées (bonne UFR, bon code Labo Harpège...) ;
- ajout dans l'annuaire central, à la main et un par un via l'interface dédiée (cf. 2.4), de tous les personnels non présents dans Harpège (5 laboratoires non université...) ;
- préparation du serveur CUPS unique ;
- préparation des serveurs Unix pour le passage à l'authentification et la gestion des utilisateurs via LDAP ;
- préparation du nouveau fichier de préférences thunderbird permettant à chacun l'accès au nouveau compte @univmed ET à l'ancien @esil.univ-mrs.fr pour permettre le déplacement des mails par l'utilisateur ;
- tests, tests, tests...
- quelques jours avant la migration effective, lancement d'un rsync des données utilisateurs du serveur NFS vers le NetAPP pour minimiser le temps de copie le jour J ;
- communication vers la direction pour présenter/expliquer le projet et ses implications ;
- *forte* communication vers les utilisateurs pour leur indiquer ce qui va changer et quel sera leur rôle actif dans la migration, en particulier la copie des mails locaux vers leur compte univmed ; leur expliquer en quoi ce changement pénible va leur être bénéfique... Développement de vidéos[6] de capture d'écran pour détailler certaines opérations à effectuer (par exemple le déplacement des mails), un mode de communication qui s'est avéré très apprécié.

Il faut également prévoir pour la migration *effective*, un arrêt total du SI. Malgré la préparation, un week-end entier sans notion claire de jour et nuit n'a pas été de trop pour nous... Les étapes les plus significatives :

- passage de NIS à LDAP sur tous les serveurs UNIX ;
- arrêt des contrôleurs de domaines Windows après avoir copié les logonscripts sur le serveur SAMBA. Sacrifice (annoncé) des profils itinérants qui ne contiennent chez nous pas de données ;
- réinstallation de TOUS les postes Windows et Unix à partir des nouvelles images préparées (re-merci JeDDLaJ) ;
- *rsync* des données utilisateurs pour parachever la copie initiée quelques jours auparavant ;
- renommage et association de nouveaux droits pour tous les *homedirs*. Modification des fichiers de configuration des applications pour qu'ils reflètent les nouveaux *login* et *homedir* ;
- copie, dans tous les comptes, du nouveau fichier de préférences thunderbird ;
- lancement en cron de la synchronisation des annuaires.

Outre la charge de travail considérable, la migration a aussi un coût en termes de disponibilité et de maîtrise du SI, puisque l'UFR dépend désormais beaucoup plus du SI central distant. On peut citer quelques exemples significatifs.

L'intervention sur les données utilisateurs ne peut pas toujours être faite directement par l'UFR, ce qui induit un délai pour les modifications/corrections.

Toute possibilité de réglage ad-hoc pour l'UFR des services disparaît avec leur centralisation.

Il faut prévoir un traitement spécial avec désynchronisation des annuaires pour les utilisateurs que l'on souhaiterait garder pour une raison ou une autre après leur suppression automatique en central. Dans tous les cas, ils perdront leur compte mail et l'accès à tous les services liés à l'existence dans l'annuaire central : accès ENT, WIFI, VPN, etc.

Les utilisateurs LDAP locaux, créés indépendamment de l'annuaire central seront dans le même cas.

---

4 login/password déductibles à partir des données de la carte étudiant

5 **Je D**éploie **D**ans **la J**oie - http://la.firme.perso.esil.univmed.fr/JeDDLaJ

6 Utilisation du freeware Wink - http://www.debugmode.com/wink/ ; exemples : http://la.firme.perso.esil.univmed.fr/video/

3.3 Pourquoi finalement choisir de migrer ?

C'est une question légitime car, comme le dit le célèbre dicton, « L'informatique qui *marche*, c'est l'informatique qui *a marché* ». De plus, on l'a vu, la migration va demander beaucoup de travail à un service informatique la plupart du temps déjà débordé, et comporte en outre quelques inconvénients.

Néanmoins, les arguments suivants nous semblent légitimer le risque du changement :

- diminution du nombre de services à maintenir par l'UFR qui manque de ressources humaines ;
- notre architecture informatique est vieillissante. C'est l'occasion d'en améliorer les performances... et la sécurité en se débarrassant de NIS, couramment surnommé « *Network Intruder Service* »... On en profite également pour supprimer les serveurs Windows... ;
- simplification de la gestion des comptes utilisateurs : on les aspire automatiquement. Plus de création de *login* ni de gestion des doublons, plus de traitement des listes d'étudiants Excel des secrétariats, etc. ;
- forte simplification de l'environnement de l'utilisateur : un seul *login*/mot de passe, meilleure proximité avec l'ENT et tous les services centraux ;
- amélioration des services fournis grâce entre autres aux possibilités de DB de LDAP, qui permet de stocker des données plus précises/complètes sur les utilisateurs : annuaire interne WEB, aiguillage dynamique vers les bons groupes, les bonnes listes de mail, les bons accès aux ressources partagées, ... ;
- gain de temps à moyen terme grâce à la standardisation du SI. LDAP est devenu une norme de fait et profite donc d'un important effort d'intégration de tout le monde informatique (logiciels, langage de programmation, boîtiers divers...), d'un déploiement massif et d'une communauté active : l'évolution et la maintenance du SI en seront facilitées ;
- meilleure utilisation des ressources humaines au niveau de l'université : on minimise la duplication des services ;
- acquisition des nouvelles compétences en se lançant dans un projet motivant.

3.4 Détails techniques et argumentation sur l'architecture choisie

Le serveur LDAP

La technologie choisie est OpenLDAP, qui est libre, ouverte et utilisée pour le serveur central, donc bien maîtrisée par le CISCAM.

Nous avons opté pour un serveur maître (alimenté par une extraction de l'annuaire central restreinte à l'UFR, et synchronisé toutes les heures). Un réplica aurait certes été moins lourd à administrer mais nous avions besoin d'un *vrai* serveur, c'est-à-dire dans lequel on puisse *écrire*, pour les raisons suivantes :

- certains des champs des fiches centrales, dont nous avons besoin pour l'exploitation (*homedir*, *loginShell*,...), sont renseignés par des valeurs génériques sans objet pour l'ESIL. Certains autres champs, par exemple la plupart de ceux liés à SAMBA, ne sont pas présents en central. Il nous faut donc pouvoir, à la volée lors de la synchronisation, modifier/ajouter des champs de façon pertinente pour l'ESIL ;
- nous avons souhaité, classiquement, que le serveur SAMBA PDC utilise LDAP comme *backend* pour gérer les machines du domaine. Une branche *machine*, non présente sur le serveur central, nous est donc nécessaire ;
- les groupes Windows et Unix locaux de l'ESIL sont aussi gérés via LDAP. Une branche *groupe*, déconnectée de son homologue centrale, est donc également nécessaire ;
- un serveur local permet de gérer des utilisateurs non présents en central. Nous voulions disposer de cette souplesse, par exemple pour des intervenants très ponctuels pour lesquels une création en central, et donc un accès à l'ENT, n'est pas forcément souhaitable ;
- enfin, un serveur local sur lequel nous maîtrisons la synchronisation avec le central permet de disposer d'un « tampon » en cas d'ajout/suppression/modification d'utilisateurs en central que l'on ne souhaite pas, pour une raison ou une autre, répercuter immédiatement.

L'architecture choisie pour le serveur OpenLDAP consiste en un cluster de 2 machines Debian Linux en Heartbeat/DRBD/Mon (solution libre de haute disponibilité très bien exposée dans [1]). Tous les fichiers de données des services en haute disponibilité sont dans le volume Raid réseau DRBD afin d'être toujours disponibles quel que soit le nœud actif.

Notons qu'un des avantages de la solution haute disponibilité par rapport à un serveur non *heartbeaté* plus un réplica est qu'en cas de crash du serveur LDAP, on dispose toujours d'un service identique non dégradé (il a juste migré sur l'autre nœud). Dans l'autre cas, on ne dispose plus que du réplica, dans lequel on ne peut pas écrire : donc plus d'ajout d'utilisateurs, de machines, etc.

De plus cette solution ne nous empêche absolument pas, si la montée en charge l'exige, d'ajouter un réplica à notre LDAP local.

L'arborescence LDAP choisie est exposée dans la figure 1.

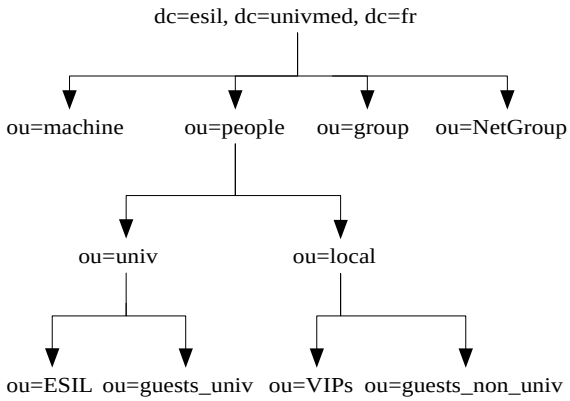

Figure 1 : *Arborescence LDAP ESIL*

Les branches *machine*, *group* et *NetGroup* gèrent respectivement les machines pour SAMBA, les groupes Unix et Windows et les groupes de machines utilisés pour les exports NFS.

Notre branche *people* est moins habituelle. Nous avons choisi de la diviser d'une part en une branche *univ* contenant les utilisateurs issus de l'annuaire central, et d'autre part en une *local* dédiée aux utilisateurs... locaux.

Dans *univ*, la branche *ESIL* contient les utilisateurs de l'UFR ESIL, la branche *guests_univ* les utilisateurs d'autres UFR mais qui doivent avoir un accès au SI ESIL (enseignants, chercheurs, etc.).

Dans *local*, la branche *guests_non_univ* a été prévue pour stocker d'éventuels utilisateurs locaux (intervenants très ponctuels, etc.). Mais à l'usage, elle s'est finalement révélée inutile, la création de comptes en central étant désormais très simple et permettant de fixer des durées aussi courtes que nécessaire. La branche spéciale *VIPs* est dédiée au service informatique. Elle contient des comptes locaux particuliers, comme par exemple les comptes spéciaux disposant de privilèges divers et associés à un service particulier (jonction au domaine Windows, utilisateur sous lequel tourne un service, etc.)

Cette arborescence nous a pour l'instant donné toute satisfaction tant en terme de souplesse que d'autonomie pour la gestion de nos utilisateurs.

Pourquoi SAMBA comme PDC plutôt qu'un Windows 2003 avec un AD ?

Encore une fois, nous privilégions les technologies libres. Nous avons un meilleur savoir-faire Linux. En outre, les fonctionnalités supplémentaires de l'AD ne nous étaient pas nécessaires et nous pouvions ainsi supprimer les 2 serveurs Windows : moins de serveurs à maintenir et moins de technologies à maîtriser...

De plus, nous avons pu ainsi consolider, puisque nous avons profité du cluster Heartbeat/DRBD/Mon hébergeant le service LDAP pour y faire également tourner SAMBA, en se reposant sur la haute disponibilité pour éviter d'avoir à créer un BDC SAMBA.

Plus de comptes non-nominatifs en dehors des comptes systèmes

Tant qu'à changer tous les *logins*, nous avons décidé d'en profiter pour éliminer tous les comptes non-nominatifs, à la source de problème de sécurité. En effet, ces comptes du style *bde*, *secretariat*, ou encore *forum* ont la particularité d'être partagés par un certain nombre (croissant) de personnes... qui doivent toutes connaître le mot de passe.

Nous avons donc remplacé tous ces comptes selon la méthode suivante, implémentée dans un script. Pour le compte *bde* par exemple :

- création d'un groupe LDAP *bde* constitué de tous les utilisateurs concernés ;
- création d'un espace disque */commun/bde* sur le serveur NFS/CIFS (accès en écriture limité au groupe *bde* et nouveaux fichiers automatiquement attribués à ce groupe) ; création au sein de cet espace d'un répertoire public_html qui sera la racine du site web associé ;
- Association d'un quota disque à ce répertoire ;
- création d'un partage CIFS *bde* sur le répertoire */commun/bde* précédemment créé, avec les mêmes limitations d'accès que pour l'espace disque ;
- création d'un alias *bde@esil.univmed.fr* qui pointe vers les adresses des utilisateurs concernés ;
- création de l'entrée DNS *bde.esil.univmed.fr* ;
- création sur le serveur web Apache d'un virtual host *bde*, dont le *DocumentRoot* pointe sur */commun/bde/public_html*.

Avec cette solution, aucun mot de passe n'est partagé. Les utilisateurs concernés reçoivent les mails adressés à bde@esil.univmed.fr, ont accès en écriture depuis toutes les machines Windows et Unix à l'espace *bde* dans lequel ils peuvent stocker leurs documents et construire leurs pages web.

Ajouter ou supprimer un utilisateur revient seulement à intervenir sur le groupe LDAP *bde*.

Le problème des *logins* étudiants illisibles

On l'a vu plus haut : adopter le LDAP central, c'était hériter de plusieurs contraintes dont le format des *logins*. Pour les étudiants en particulier, le *login* « 1 lettre plus 6 chiffres » est particulièrement peu lisible, en regard du précédent système « première lettre du prénom + nom ».

Ce changement, *a priori* léger, a eu un impact important sur l'architecture web. Les pages perso utilisaient le format du module *userdir* d'Apache, i.e. http://pages-perso.esil.univmed.fr/~login, qui devient fortement obscur avec les nouveaux *logins* numériques...

Nous sommes donc passés[7] (au prix d'un temps de recherche et de mise au point non négligeable à ajouter au coût de la migration...) à des url plus lisibles de type http://prenom.nom.perso.esil.univmed.fr pour l'ensemble des utilisateurs, par une technologie de type *mass virtual hosting* avec utilisation intensive du *mod_rewrite* d'Apache.

Synchronisation des annuaires

La synchronisation des annuaires est évidemment fondamentale dans notre nouveau fonctionnement.

Le script Perl *LDAP_sync_annus* que nous avons développé à cet effet, même s'il répond à une problématique classique, a demandé un travail important de mise au point en amont de la migration : implémentation de nombreuses options de lancement, mise au point complexe du filtre d'extraction, nécessité de très nombreuses vérifications lors des ajouts pour éviter les erreurs de saisie Apogée/Harpège...

Le script est lancé en mode synchronisation des utilisateurs présents sur les 2 annuaires en *cron* 6 fois par heure. Toute modification d'une fiche sur le LDAP central est donc répercutée à l'ESIL dans un délai raisonnable d'au plus 10 minutes. C'est le cas par exemple pour le changement de mot de passe qui se fait uniquement sur l'annuaire central via une interface web dédié.

Toutes les nuits, il est lancé en mode *check*, i.e. pas d'action mais envoi d'un mail indiquant si des ajouts ou des suppressions sont nécessaires.

Pour les modes ajout ou suppression, il doit être lancé à la main. Il y a demande de confirmation (court-circuitable par une option *yes_auto*) pour chaque ajout/suppression.

7 Tous les détails techniques de cette mise en place à : http://la.firme.perso.esil.univmed.fr/website/article.php3?id_article=82

Pour pallier aux erreurs de saisie Harpège/Apogée en attendant leur correction, on a la possibilité d'ignorer certains utilisateurs en définissant une variable de configuration. Ceci permet, entre autres, de ne pas rapatrier des utilisateurs affectés à tort dans l'UFR.

Utilisateur locaux

Nous avons développé un autre script Perl *LDAP_add_local_user* qui automatise la création d'un utilisateur local dans la branche *local -> guests_non_univ*.

Gestion des groupes

LDAP propose un mécanisme de gestion de groupes. Chaque utilisateur dans la branche people dispose d'un *gidNumber*. Dans la branche group, les groupes sont référencés avec, entre autres, le *gidNumber*, leur nom (*cn*) et une liste d'utilisateurs dans l'attribut *memberUid*.

Nous nous servons beaucoup des groupes, en particulier, classiquement, pour les accès aux ressources partagées. Par exemple nous devons pouvoir donner l'accès à certaines imprimantes au groupe *EtudiantsInfo* mais à certaines autres uniquement au groupe *EtudiantsInfo1ereAnnee*.

Nous ne pouvions donc nous satisfaire d'un système où nous devions déposer les utilisateurs à la main dans un groupe ou un autre, en particulier dans un contexte étudiant où les groupes changent chaque année...

Nous avons donc développé le script Perl *LDAP_rebuild_groups* qui met à jour les groupes dans notre serveur LDAP local à partir d'un fichier texte. Ce dernier obéit à une syntaxe simple permettant de définir les groupes soit en intension à partir d'un filtre LDAP quelconque, soit en extension en listant les *logins*.

Ce fonctionnement nous permet une grande souplesse. Les modifications, ajouts ou suppression de groupe se font sans intervention manuelle dans l'annuaire : il suffit de modifier le fichier texte et de lancer le script.

3.5 Les problèmes non techniques... et non prévus...

Lorsque nous avons migré, nous n'avions peut-être pas anticipé tous les problèmes techniques, mais nous n'en étions pas loin. Quelques surprises nous attendaient la première semaine, mais rien d'insurmontable.

En revanche, et c'est surtout là que nous avons puissamment subi l'aspect *pilote* de notre démarche, nous étions bien naïfs par rapport aux flux d'information inter-services dans l'université, voire inter-universités, et nous avions largement sous-estimé à quel point nous en dépendions...

Voici donc, accompagnés des solutions que nous avons pu leur apporter, les principaux problèmes de type système d'information, finalement bien plus épineux que tous les aspects techniques...

Les délais d'inscription des étudiants à la rentrée

Désormais, un étudiant ne peut disposer d'un compte informatique à l'ESIL avant qu'il ne soit dûment inscrit à l'université, puisque c'est cette inscription qui insère l'étudiant dans Apogée et donc dans l'annuaire.

Or, les enseignements nécessitant l'utilisation des ressources informatiques commencent à l'ESIL immédiatement après la rentrée.

Il y a donc eu une grosse levée de boucliers de la part des enseignants contre le nouveau système, car il n'était pas question de commencer les TP le 21 Septembre si la rentrée était le 15...

Donc, première leçon : faire le forcing pour négocier auprès de la scolarité des créneaux d'inscription aussi proches que possible de la rentrée. Ça n'est pas forcément évident, et nécessite de s'y prendre bien en avance, de préférence en bonne intelligence avec les autres UFR concernées. Un bon relationnel et des partenaires consciencieux et motivés côté scolarité s'imposent...

Cet aspect est loin d'être un détail car le risque n'est rien moins que de devoir créer tout ou partie des comptes étudiants en local pour une semaine, perdant ainsi un des gros bénéfices de la migration...

Ceci constitue sans doute, après réflexion, la principale justification à l'existence d'une branche *local* dans le serveur LDAP d'UFR.

Il est donc bon de prévoir une procédure d'ajout rapide d'utilisateur local... tout en restant intransigeant afin que ce type d'ajout reste exceptionnel, sous peine de se voir infliger un double travail systématique...

Les diplômes co-habilités

À l'ESIL comme dans de nombreuses autres structures, certains diplômes sont co-habilités par différentes universités.

Certains des étudiants de ces diplômes sont donc normalement inscrits dans une autre université (appelons-là Ux), et figure donc dans un autre Apogée...

Comment dès lors faire en sorte qu'ils apparaissent dans l'annuaire central, exclusivement nourri du point de vue des étudiants, par l'Apogée de l'université de la Méditerranée (appelons-là Um) ?

Ce problème là s'avère *particulièrement* pénible. Il faut savoir que les Apogée d'établissement communiquent des informations au ministère (remontées SISE) indiquant entre autres le nombre d'étudiants et par là-même... le montant de la subvention attribuée à l'établissement...

On comprendra donc que dans ces conditions, toute discussion évoquant l'idée que certains étudiants d'une université soient comptés dans l'Apogée d'une autre se déroule dans un climat hautement passionnel...

De plus un étudiant, à cause de ces remontées SISE, ne peut normalement figurer que dans un seul Apogée.

En fait, une fois consultés longuement les services de scolarité et autres instances ad-hoc, il s'est avéré qu'il existait un statut particulier (droits fixés à 0€) permettant d'inscrire un étudiant dans un autre Apogée que celui de son université « administrative » sans qu'il ne soit pris en compte une deuxième fois dans les remontées SISE.

Une fois la solution technique trouvée, il faut prévoir un temps proportionnel à la bonne volonté de Ux pour obtenir une réunion entre les décideurs de niveau adéquat des deux universités qui puisse acter que Ux accepte que les étudiants de tel diplôme figure dans l'Apogée de Um (avec toutes les clauses restrictives nécessaires...).

Et, dernier écueil, il faudra réaliser l'inscription à Um des étudiants de Ux, à partir de l'extraction Apogée que Ux

doit désormais fournir. Il est certaines rumeurs qui prétendent, comme un informaticien pourrait le penser, que les Apogée savent communiquer entre eux et donc régler ce type de problèmes en quelques minutes.

Mais dans notre cas, rien de tel ne s'est produit. Ux nous a fourni une extraction sous forme de fichier Excel, que la scolarité de Um a dû ressaisir à la main dans Apogée...

On comprendra donc aisément la nécessité d'aborder ces problèmes inter-universitaires *très* en avance... et malgré tout se préparer à fonctionner avec des comptes locaux un gros début d'année pour ces étudiants co-habilités...

Erreurs de saisie Harpège et Apogée et lien avec les services centraux

Apogée et Harpège nourrissent l'annuaire central et donc désormais notre base d'utilisateurs. Nous utilisons les codes diplômes/étapes Apogée, les affectations d'UFR (*supannAffectation*) et code laboratoire d'Harpège pour définir les groupes des utilisateurs (via des filtres LDAP dans notre fichier texte dédié), leur attribuer un certain quota disque, les inscrire à tel ensemble de listes de diffusion, leur donner accès à telle ou telle ressource partagée, les faire apparaître dans le bon laboratoire, département ou diplôme dans l'annuaire d'UFR, etc. Bref, un système éminemment séduisant pour un informaticien.

Oui, sauf que tout repose sur des données sur lesquelles nous n'avons pas directement la main, et que nous avions, encore une fois, sous-estimé ce *détail*...

Les données Harpege en particulier sont souvent incorrectes.

Le cas le plus classique : le code laboratoire Harpège est erroné car la DRH ne sait pas exactement que tel personnel est dans telle équipe de tel laboratoire. Souvent, par défaut, les personnels sont donc affublés d'un code laboratoire « générique » (il en existe un par UFR).

Une deuxième possibilité d'erreur réside dans l'affectation à l'UFR. Si un personnel est hébergé exclusivement dans l'UFR1, (par exemple un thésard car son directeur de thèse lui fournit un bureau, ou un enseignant qui fait sa recherche au sein d'un labo de l'UFR1) mais dépend administrativement d'une autre UFR2, l'UFR1 n'a pas la main sur sa fiche, donc ne peut pas, par exemple, réinitialiser son mot de passe... Il faudrait pour cela que le personnel passe par l'informaticien de l'UFR2, qu'il ne connaît pas et avec qui il n'a jamais été en rapport. La bonne solution est de faire modifier son entrée Harpège afin qu'il soit bi-affecté à UFR1 et à UFR2.

Un autre cas, plus sournois, et potentiellement plus grave est lié à la double affectation Harpège. Ce logiciel peut gérer pour les enseignants-chercheurs deux affectations, l'une dite *principale* (c'est l'affectation administrative, celle de l'enseignement, là ou est l'emploi) et l'autre dite *recherche* qui n'a aucune incidence sur la première. L'affectation principale est celle qui sert, par exemple, à générer les listes électorales. Imaginons maintenant qu'un enseignant-chercheur, disons par exemple le directeur comme c'est arrivé à l'ESIL, soit affecté *à tort* à l'ESIL comme affectation principale et à son UFR administrative comme affectation recherche. Imaginons que, ne le voyant pas apparaître sur les listes électorales, son UFR administrative s'en émeuve *sérieusement* auprès de la DRH. Cette dernière corrige bien vite son erreur en se préoccupant uniquement de mettre la bonne UFR en affectation principale et, parce qu'elle ne perçoit pas que cette information peut être utilisée en aval, supprime tout bonnement l'affectation ESIL... Le lendemain, un mail issu du script de synchronisation informe le service informatique ESIL qu'il doit supprimer de son UFR... le directeur. Heureusement, notre choix de disposer d'un vrai serveur LDAP local avec des procédures de destruction non automatiques, va nous permettre de continuer de faire exister le directeur en attendant que sa situation revienne à la normale.

Le problème qui se pose donc est le suivant : comment faire corriger ses petites erreurs à la DRH ? Voici la procédure officielle qui nous a été communiquée lors de notre première demande :

- lister les erreurs sur un courrier ;
- faire valider ce courrier par la DRH de l'UFR ;
- cette dernière communique le courrier au secrétaire général ;
- le SG statue, puis fait parvenir le courrier aux responsables techniques Harpege ;
- Ces derniers font finalement la modification demandée.

Évidemment, si la DRH centrale n'est pas immédiatement d'accord ou le message transmis pas assez clair, il s'ensuit d'autres allers-retours de courrier...

On voit bien ici le cœur du problème, qui est typiquement un problème de système d'information : la souplesse et la réactivité nécessaire pour la gestion des utilisateurs au quotidien est en décalage par rapport aux procédures de communication inter-services. Une vraie réflexion au plus haut niveau à l'université est nécessaire afin de mieux identifier les flux d'information qui relient certains services et les faciliter. Il faut également sensibiliser les services centraux au fait que les données des bases métier font partie d'un système d'information de plus en plus global et donc que leur modification a désormais un impact qui sort largement de leurs bureaux.

Dans notre cas, une montée au créneau (et sa dépense d'énergie associée) a finalement permis que soit acceptée, par la DRH et le CRI, une désynchronisation de certaines données entre LDAP et Harpège, en particulier le code laboratoire. Il a été obtenu que ce dernier puisse être modifié dans l'annuaire par les responsables d'UFR, et que cette modification génère un mail à la DRH.

Pour toutes les autres corrections d'erreur, la procédure « courrier » reste l'unique solution...

On l'aura compris, ces aspects de communication d'information doivent être pris en compte et réglés *avant* de se lancer dans la migration...

4 Aspects humains : que reste-t-il à l'informaticien d'UFR ?

Nous sommes actuellement à une croisée de chemins. L'adoption quasi inévitable du système d'information central dépossède l'informaticien d'UFR de l'exploitation de services, historiquement considérés à la fois comme « prestigieux » et constituant son cœur de métier : mail,

DNS, etc.

Un sentiment couramment éprouvé dans cette situation est celui de la perte de son savoir-faire, d'une diminution du niveau de qualification du poste.

Or nous pensons au contraire que cette mutation du métier, *a priori* difficilement évitable, peut au contraire s'avérer profitable sur de nombreux points, sous réserve d'une organisation centrale ouverte et bien pensée.

Pour commencer la centralisation amène quelques avantages directs :

- moins de gestion « critique » à assumer dans l'UFR avec des moyens humains inadaptés, et donc moins de stress ; les services « 24h/24 » et les moyens nécessaires sont logiquement centralisés et mutualisés ;
- moins d'exploitation quotidienne ;
- finalement du temps gagné, sans doute ce dont les services informatiques d'UFR si mal dotés en ressources humaines ont le plus besoin...

Au lieu de se morfondre dans la nostalgie d'un métier que le nouveau paysage informatique rend de plus en plus irréaliste, pourquoi ne pas plutôt profiter de la nouvelle situation pour tenter de donner plus d'intérêt à notre travail.

Tout d'abord, au niveau UFR, on peut profiter du temps gagné pour se lancer dans des initiatives locales personnelles. N'est-ce pas le moment de se documenter enfin à fond sur cette technologie que l'on a repérée il y a un moment sans jamais avoir eu le temps de s'y pencher vraiment ? Ou de mettre en place ce service de dépôt de documents sécurisés de grande capacité que vous demande depuis si longtemps cette équipe de recherche ? Il y a peut-être moyen d'optimiser l'assistance utilisateur en mettant en œuvre des moyens de communication innovants qui feront gagner encore un peu de temps ? Et pourquoi ne pas se (re)mettre à développer un peu, il y a sûrement quelques tâches récurrentes à automatiser ? Les projets ne manquent pas si on a du temps...

Au niveau université, c'est le moment de se rapprocher de la communauté des informaticiens et/ou du CRI pour mutualiser temps et compétences en mettant en place des solutions identiques élaborées ensemble.

Un fonctionnement intéressant, mis en place à l'université de la Méditerranée, est le suivant : le CRI crée des groupes de travail ouverts aux informaticiens d'UFR pour élaborer des solutions destinées à être ensuite déployées dans l'ensemble de l'université. L'informaticien d'UFR est ainsi partie prenante dans la partie la plus motivante des projets, à savoir la réflexion en amont et la mise en place, tandis qu'exploitation et maintenance sont logiquement prises en charge par le CRI qui dispose des moyens et de la structure nécessaires. De plus les solutions sont standards au sein de l'université, ce qui améliore la mobilité des utilisateurs et assure un savoir-faire partagé chez les informaticiens, toujours appréciable dans une communauté...

Et si l'on n'a pas la chance de disposer d'un tel fonctionnement (parce que l'informatique centrale est externalisée par exemple), il est toujours possible de participer à son niveau à un projet libre régional ou national, qui profite à l'ensemble de la communauté.

Le lecteur nous trouvera sans doute dans cette dernière partie bien plus optimiste qu'en 2001 dans [2]. Mais nous disions déjà à l'époque que le problème majeur de l'informaticien d'UFR était le surbooking. Or l'évolution actuelle, via la mutualisation, propose une solution à ce problème toujours bien réel dans bien des sites. Et l'autre voie possible, à savoir une embauche massive, semble moins que jamais politiquement prioritaire (ce qui ne doit pas nous empêcher de continuer de lutter pour...).

Profitons donc, lorsque c'est possible, de la situation présente pour améliorer notre qualité de travail et se confectionner un poste aussi proche que possible de nos aspirations.

Évidemment, le risque est là que la centralisation au niveau des universités se poursuive logiquement au niveau de sociétés internationales spécialisées et que les politiques gouvernementales aillent vers la suppression des postes en UFR (voire plus tard des CRI...).

Mais nous pensons que notre meilleure arme contre cette voie d'externalisation maximum et la fuite de nos emplois est de montrer, car nous en sommes persuadés, que la qualité de service fournie par une personne motivée et présente physiquement est incomparable avec celle d'une société extérieure, forcément moins réactive et moins disponible. Ceci sera d'autant plus vrai si nous parvenons à profiter des bénéfices de la centralisation pour prendre du recul par rapport aux tâches quotidiennes et nous montrer indispensables auprès des utilisateurs d'une part en participant à la mise en place de solutions centralisées pérennes et d'autre part en proposant des services locaux simples, innovants et efficaces.

Conclusion

Migrer vers le SI central depuis son SI autonome n'est pas, on l'a vu, une opération triviale, surtout en tant que pionnier... Il s'agit d'un travail important, qui demande beaucoup d'énergie, une abondante communication vers les utilisateurs et une sérieuse réflexion en amont, bien sûr du point de vue de l'architecture à adopter mais surtout au niveau des flux d'information entre les différentes composantes dépositaires des données sur lesquelles on va désormais reposer.

Nous espérons que notre expérience, exposée ici avec les divers écueils à surmonter, vous sensibilisera à ces problèmes et vous permettra, si vous décidez de vous lancer vous aussi, d'argumenter plus facilement lors des réunions préparatoires à provoquer impérativement avec tous les services concernés (CRI, mais surtout DRH et scolarité) et les instances décisionnelles. Pour éviter nos déboires, il faudra y exhiber et faire valider, *avant* de se lancer dans la migration, les inévitables adaptations du SI central permettant aux bonnes informations de circuler sans entraves. Pensez en particulier à optimiser les délais d'inscription des étudiants, à obtenir une procédure simple et rapide de demande de modification des fiches Harpège à la DRH, à mettre au point une communication aussi automatisée que possible entre les Apogée en cas de diplômes co-habilités...

À l'université de la Méditerranée, notre action pilote a permis de mettre à jour de nombreux blocages au niveau du SI central. Certains ont pu être levés, d'autres aménagés

au mieux. Les discussions initiées entre les différents services contribuent à éliminer peu à peu les derniers problèmes. Le terrain défriché va permettre de faciliter le travail des autres UFR désireuses de migrer. Elles pourront s'appuyer directement sur nos développements, prévus pour être aussi portables que possibles et destinés à être mutualisés. Elles agiront à leur tour sur le SI central, poursuivant l'amélioration des échanges d'informations.

Au niveau national, nous espérons que nous ferons aussi gagner du temps à quelques-unes des nombreuses UFR ou entités similaires confrontées à une même problématique de migration, qui devient difficilement contournable dans le contexte actuel à base d'ENT et de services centralisés.

En termes de bilan, il faut retenir que la migration amène de nombreux avantages, tant techniques que logistiques. En particulier, elle peut conduire à un gain de temps pour l'informaticien d'UFR en diminuant le nombre de services à maintenir et en simplifiant l'environnement technique. C'est pourquoi nous osons envisager la mutation du métier impliquée par la centralisation des services sous un angle optimiste : elle peut peut-être permettre de sortir légèrement de l'urgence quotidienne pour se réorienter vers des projets motivants, aussi bien en local qu'en central. Et si cet article, en facilitant le processus de migration, peut contribuer finalement à l'amélioration de la qualité de travail de quelques informaticiens, alors nous n'aurons vraiment pas perdu notre temps...

Bibliographie

[1] Nicolas Schmitz, Solution haute disponibilité pour Linux : un cluster avec Heartbeat et DRBD. Dans Actes de la conférence JRES2005, Marseille, Décembre 2005.

[2] Gérard Milhaud, Olivier Pagé, Petit manuel anti-dépression à l'usage des administrateurs systèmes et réseaux, Dans Actes de la conférence JRES 2001, Décembre 2001.