Un monde parfait
adldap ou la synchronisation entre annuaires LDAP pour Active Directory

Laurent.Klinq@epfl.ch, EPFL-STI

Windows Active Directory forêt Intranet.epfl.ch

Le groupe WINAD *(Windows Active Directory)* élabore une méthode de gestion commune concernant les cinq domaines de faculté (STI, ENAC, SV, IC, SB) et celui des services centraux (SCX).

Un groupe de travail de WINAD, Staff, sera formé durant le mois de mai 2004 afin de créer celle-ci pour la forêt Intranet.epfl.ch.

Alain.Gremaud@epfl.ch, DIT

Préambule

Dans le cadre de l'administration d'un domaine Active Directory, il est nécessaire de définir des règles pour assurer une communication correcte entre les divers intervenants (usagers, administrateurs locaux et de domaine).

Pour l'EPFL, un groupe de travail a développé une telle normalisation (***winad.epfl.ch/core/index.asp?article=38***). Il existe cependant l'écueil de la mise en œuvre. En pratique, il est impossible à un être humain de ne pas faire preuve de créativité, particulièrement pour une tâche répétitive.

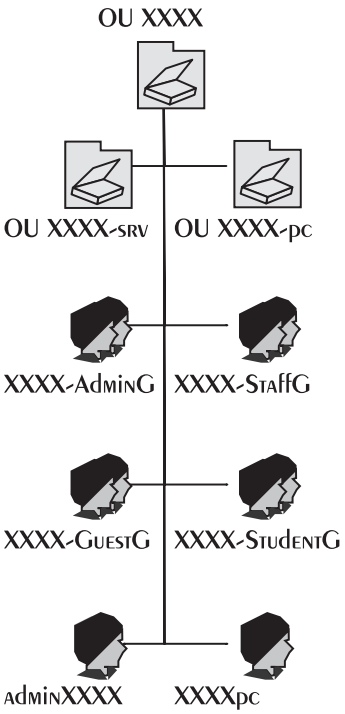
Dans le domaine de la Faculté STI que j'administre depuis sa création, je me suis efforcé de canaliser cette tendance créative. Une structure standardisée est générée pour chaque unité qui désire faire partie du domaine. Cette méthode est issue d'un travail réalisé à plus petite échelle, décrit dans mon article *Windows 2000, Active Directory et ADSI, une expérience de département, dit.epfl.ch/SA/publications/FI01/fi-8-1/8-1-page1.html.*

Une structure standardisée

La structure créée pour une unité XXXX est

XXXX = unité d'organisation contenant les éléments:

- XXXX-pc = unité d'organisation pour les PC
- XXXX-srv = unité d'organisation pour les serveurs



Quatre groupes globaux de sécurité de l'unité:

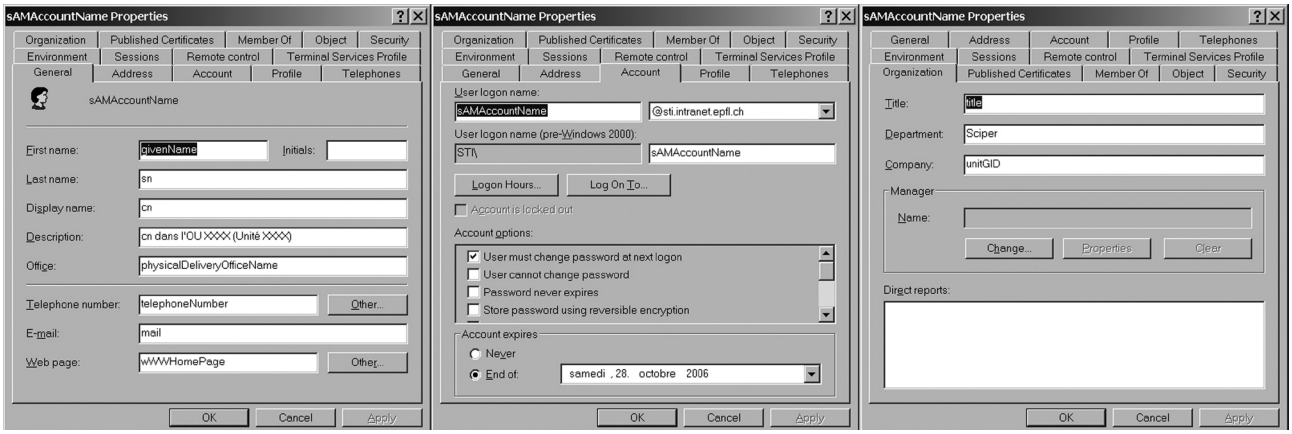
- XXXX-AdminG = comprenant les administrateurs
- XXXX-StaffG = comprenant l'ensemble des usagers
- XXXX-GuestG = comprenant les invités
- XXXX-StudentG = comprenant les étudiants

Deux comptes de gestion:

- adminXXXX = compte d'administration de l'unité
- XXXXpc = compte de service pour l'unité

Afin d'homogénéiser cette structure:

- les éléments commencent par l'acronyme officiel de l'unité;
- chaque compte de service contient l'acronyme;
- chaque suffixe désigne la fonction;
- la norme RFC 1123 s'applique pour la désignation, soit uniquement les lettres a-z, A-Z, 0-9, -.



Un compte d'usager avec les rubriques LDAP

L'intérêt de cette stratégie est de fournir une gestion de parc uniforme et faciliter l'intégration des domaines existants (NT4 ou Windows 2000). L'outil existant reste complexe à utiliser et opaque. La conséquence de ce manque de lisibilité est qu'en pratique, seul l'auteur peut l'adapter. L'arrivée du contrôle d'accès pour Olympe (Distrilog), l'intégration d'un service uniforme pour chaque domaine de faculté et la mise à jour en Windows 2003 offre l'opportunité pour un développement.

Un nouvel outil

Quel serait le cahier des charges de celui-ci:

- Permettre une gestion complète des droits des individus, en particulier l'appartenance à plusieurs structures indépendantes.
- Offrir la possibilité à un administrateur de modifier le résultat obtenu sans connaissance particulière de programmation.
- Utiliser et intégrer les outils déjà existants pour développer les synergies et éviter de tomber dans le syndrome *Yet Another* ou *encore un autre*. La conséquence pratique de ce syndrome est la multiplication d'outils avec des fonctionnalités similaires, mais incompatibles entre eux.
- Éviter une prolifération de bases de données en utilisant celle déjà existantes. Il est plus simple de gérer un flux d'information que d'assurer la concordance et la synchronisation entre deux structures distinctes.
- Fournir des résultats directement interprétables. L'emploi du format textuel permet une interprétation aisée des données.
- Être capable de satisfaire, à terme, une automatisation du traitement.

Sources de données

- ▲ Le processus actuel est le suivant: extraction d'annuaires en Perl par Michel Mengis - ITOP, récupération de l'information par messagerie, mise en forme avec un tableur (Excel), exportation au format CSV.
- ▼ Le processus automatisé doit être: extraction directe de l'annuaire LDAP en format CSV.

Traitement

- ▲ Le processus actuel est le suivant: script VBS avec ADSI.
- ▼ Le processus automatisé doit être: script VBS, génération de structure LDIF.

Fréquence

- ▲ Le processus actuel est le suivant: uniquement à la création de l'unité dans le domaine AD STI.
- ▼ Le processus automatisé doit être: autant de fois que l'administrateur le désire, mais au minimum tous les jours.

Avant d'utiliser une boîte à outils comme ADSI pour réaliser ce nouveau programme, il est préférable de procéder à une lecture approfondie des fondements d'Active Directory.

Même base, résultat différent

Contrairement aux outils précédents réalisés par Microsoft, Active Directory se base sur des normes publiques. Cependant, avoir un point de départ commun ne signifie pas un résultat uniforme, voire interopérable. La mise en place d'un méta-annuaire dans l'EPFL n'est pas une découverte récente. Claude Lecommandeur a fait office de pionnier par la mise en place:

- dans une période héroïque, d'un annuaire X-500;
- puis d'un successeur possible, l'annuaire CSO;
- et enfin, de l'annuaire LDAP EPFL, source de nombreux outils de l'école.

Il serait stupide de ne pas vouloir réutiliser ce travail déjà présent de formulation et de mises à jour quotidiennes de l'information.

La principale différence entre ces deux annuaires est l'objectif à atteindre:

- dans le cas de l'EPFL, le service LDAP est orienté vers le monde du logiciel libre ou UNIX;
- pour Active Directory, il est d'abord un service fédérateur pour le monde Windows, pierre angulaire entre authentification et intégration de services.

Cette différence d'objectif ne doit pas empêcher le dialogue entre annuaires, car je le répète, les bases sont communes, et offrent naturellement le canevas de ce nouveau programme.

Cette problématique n'est pas nouvelle, de nombreuses initiatives existent, mais aucune ne présente les qualités requises, en particulier pour la simplicité. L'approche la plus prometteuse consiste à marier les techniques XML avec LDAP, malheureusement, elle n'est disponible qu'en version de test, et nécessite une infrastructure *dot Net*.

Un mariage de raison

Avec la mise en place du service Accred (outil d'accréditation), nous disposons d'une source de données fiables, car décentralisées. La mise à jour quotidienne du méta-annuaire LDAP de l'EPFL à partir d'Accred offre une information digne de confiance.

Étant donné qu'Active Directory se base sur les mêmes normes, il devrait être simple de gérer une synchronisation entre annuaires LDAP. La réalité est plus complexe.

La démarche suivie

Dans un premier temps, il faut procéder à une analyse de la demande:

- création
  - usager, tous les jours
  - structure, une fois par semaine
  - délégation, deux fois par mois
- modification
  - usager, tous les jours
  - structure, une fois par mois
- suppression
  - usager, tous les jours
  - structure, trois fois par année

De cette analyse, on peut tirer les conséquences pratiques suivantes:

- ne pas recréer des structures locales de données
  - utiliser les services existants
- respecter l'état actuel & la durée de vie
  - pas de suppression-création d'objets, mais création-modification-désactivation
- permettre la délégation

- respect des structures mises en place, communication de toutes modifications à l'administrateur concerné.
- être flexible
  - être semblable à la structure administrative de l'école
  - être capable de s'adapter aux changements de celle-ci
- pas un système fermé et propriétaire
  - intégration de standard comme LDAP et LDIF
  - proposer une boîte à outils
- assurer une communication des modifications
  - fournir un historique complet
  - intégrer un contrôle humain
- travail réutilisable
  - code source mis à disposition

Catalogue commun ?

Malheureusement, il existe plusieurs interprétations de la structure de l'annuaire. En particulier, la structure d'un individu présente deux héritages différents:

- Pour LDAP EPFL
  inetOrgPerson > organizationalPerson > person
- Pour LDAP Active Directory
  user > organizationalPerson > person

Cette différence entre les deux annuaires nécessite une phase de transformation de l'information.

La position d'un objet est déterminée par son chemin. À la différence de LDAP, Active Directory (AD) référence chaque objet avec une identification unique, un nombre codé sur 128 bits. Cette identité est indépendante du nom, de la position et de l'état de l'objet. Un numéro de version avec les dates de modification et de création est également conservé. Ainsi, les droits de sécurité sont liés à cette identification unique et pas à son nom. Cette méthode permet de renommer ou déplacer un objet en conservant ses droits propres et d'hériter de ceux dont il sont issus d'après leur position dans l'annuaire. En conséquence, chaque objet est unique durant la durée de vie du domaine.

Un individu unique

Par exemple, la représentation du même usager dans son laboratoire d'origine dans les deux annuaires:

- LDAP EPFL
  cn=Francois Avellan, ou=LMH, ou=ISE, ou=STI, o=epfl, c=ch
- LDAP AD STI
  cn=favellan, ou=LMH, ou=ISE, dc=STI, dc=intranet, dc=epfl,dc=ch

La hiérarchie reflète les deux origines de chaque annuaire:

- LDAP EPFL, une origine X-500.
- LDAP Active Directory STI, un couplage entre DNS et LDAP.

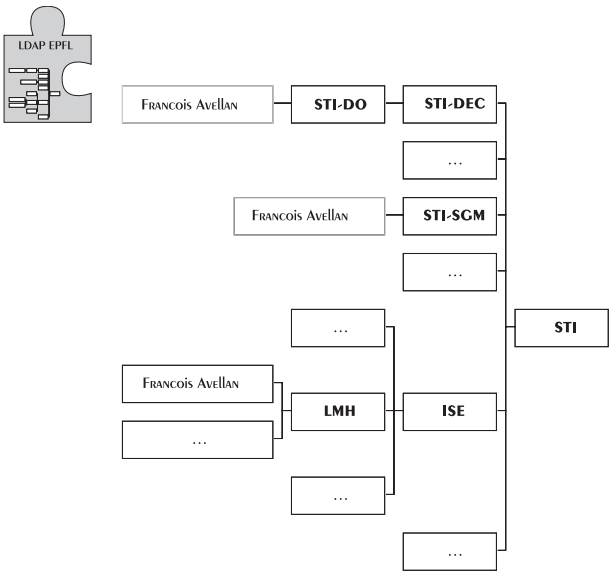
La différence entre les noms de référence est issue de l'application pour le domaine de la faculté STI des règles de désignation définies par le groupe WinAD. On peut également remarquer que par souci de compatibilité, les caractères accentués ne sont pas représentés. Pour un laboratoire, il est aisé de réaliser une relation univoque entre un usager dans l'annuaire LDAP EPFL avec celui d'Active Directory. Si on désire réaliser cette correspondance au niveau d'un institut, ou d'une Faculté, le problème devient plus complexe par les différentes fonctions que possède un individu (qui malgré les tentatives de clonage, est heureusement encore unique).

Pour l'usager ci-dessus, le professeur François Avellan possède trois rôles dans notre faculté

- Directeur du Laboratoire de Machine Hydraulique.
- Professeur dans la Section de Génie Mécanique.
- Vice-Doyen de la Faculté Sciences et Techniques de l'Ingénieur.

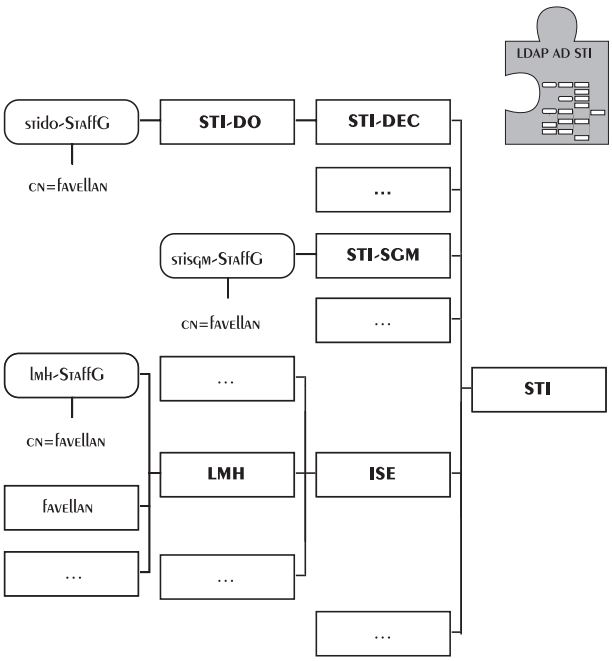
Comment sont représentés ses rattachements dans les deux annuaires:

LDAP EPFL



Dans l'annuaire LDAP, il est représenté par autant d'usagers que de fonctions, en l'occurrence, trois.

LDAP Active Directory, domaine STI

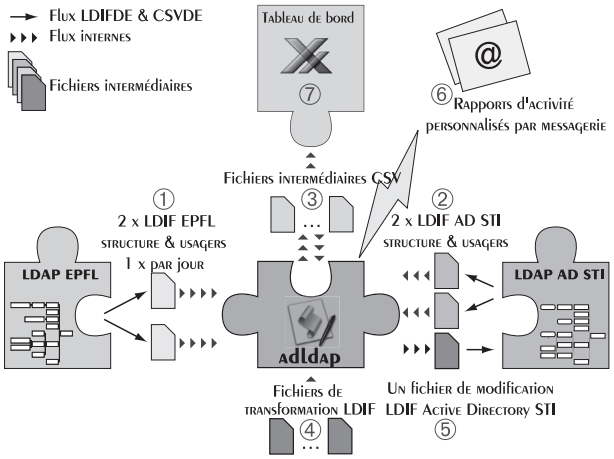


Un des principes de fonctionnement d'Active Directory est qu'un utilisateur est unique, et les différents rôles sont rendus possibles par l'appartenance de celui-ci à chacun des groupes de sécurité concernés.

Au contraire de l'annuaire LDAP EPFL, où trois usagers avec le même identificateur existent, pour l'annuaire LDAP Active Directory STI, un seul utilisateur appartient à trois groupes de sécurité.

Il est nécessaire d'identifier dans quelle structure doit être créé la personne. Ce choix est facilité par la présence dans l'annuaire LDAP EPFL d'une propriété commune entre l'individu et l'unité.

Quatre clés pour un programme



Le puzzle…

LDIF

Pour décrire et manipuler les données contenues dans un serveur LDAP dans un format textuel, il existe le format LDIF (LDAP Data Interchange Format). Il est généralement utilisé pour modifier le schéma ou assurer une entrée en masse d'éléments, il est la clé de voûte de cette démarche.

Dans un souci de compatibilité, le format utilisé dans LDIF est uniquement de l'ASCII 7 bits ! Pour intégrer les caractères accentués, ils sont d'abord convertis en UTF-8 (deux octets 8 bits), puis convertis en Base64, ce qui revient à de l'ASCII 7 bits... Pour différencier cette représentation intitulée, *binaire*, des autres valeurs; elle est séparée de la rubrique par "**::**" dans LDIF au lieu de "**:**".

Avant de coder le programme pour obtenir le résultat désiré. Il est préférable de définir quatre éléments qui seront l'ossature de celui-ci:

Un translateur pour LDIF

L'utilisation de la solution précédente a fait émerger que la maintenance d'un logiciel où les fonctionnalités sont entièrement réalisées dans celui-ci n'est possible que par l'auteur! Ce constat est le point de départ de cette démarche, dans une version initiale, il consistait à élaborer un méta langage textuel de manipulation d'objet Active Directory.

Après une brève étude sur Internet, il est vite apparu que ce langage existait, c'est LDIF. L'idée de départ s'est modifiée dans un translateur de LDIF. Il est plus rapide de modifier un fichier texte pour obtenir la fonctionnalité désirée que de coder celle-ci dans un langage de programmation.

Fichier de transformation pour un usager

```
'Template to generate a standard User in STI
Domain
' Version 1.0 , 4 fevrier 2004
' First, generate the user
dn:CN=##sAMAccountName##,##BaseDN##
changetype: add
accountExpires: 128066328000000000
cn: ##sAMAccountName##
company: ##employeeID##
department: ##gid##
description: ##cn## dans l'OU ##UnitName##
(##Unit_Description##)
displayName: ##cn##
division: ##UnitName##
employeeID: ##employeeID##
givenName: ##givenName##
homePhone: ##telephoneNumber##
info: ##info##
l: ##l##
postalCode: ##postalCode##
mail: ##mail##
name: ##sAMAccountName##
objectClass: user
physicalDeliveryOfficeName: ##physicalDelive-
ryOfficeName##
sAMAccountName: ##sAMAccountName##
sn: ##sn##
telephoneNumber: ##telephoneNumber##
title: ##title##
userPrincipalName: ##sAMAccountName##@sti.intr
anet.epfl.ch
st: ##gid##
wWWHomePage: ##wWWHomePage##
```

Résultat obtenu

```
dn:CN=marmotta,ou=lmm,ou=imx,dc=sti,dc=intranet
,dc=epfl,dc=ch
changetype: add
accountExpires: 128066328000000000
cn: marmotta
company: 163743
department: 10825
description: Ariane Marmottant dans l'OU lmm
(Laboratoire de métallurgie mécanique)
displayName: Ariane Marmottant
division: lmm
employeeID: 163743
givenName: Ariane
info: Ariane Marmottant
l: Lausanne
postalCode: 1015
name: marmotta
objectClass: user
sAMAccountName: marmotta
sn: Marmottant
title: Assistant-e
userPrincipalName: marmotta@sti.intranet.epfl.ch
st: 10825
```

En pratique, chaque fonctionnalité du processus de synchronisation est incarnée par un fichier de référence représentant l'ensemble des opérations dans un format LDIF. Il est aisé pour un non-spécialiste de modifier celui-ci pour atteindre le but recherché.

Pour découpler le processus de création du fichier LDIF de la phase d'analyse, un fichier intermédiaire est généré en format CSV (valeurs séparées par virgule, *Comma Separated Values*). L'ensemble de ces fichiers est le point de départ du tableau de bord.

Un tableau de bord

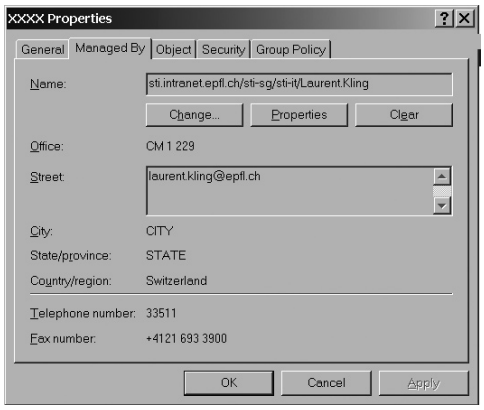
Quoique l'ensemble du processus soit représenté par des fichiers texte, il est utile de disposer à chaque moment du processus d'un tableau de bord propre à l'état actuel de la structure. On pourrait trouver du plaisir à réaliser un tel outil, mais comme le temps dont je dispose est restreint, il me paraît

plus simple et avantageux de simplement utiliser un tableur pour cette fonction. Un petit fichier de référence (26 Ko), vide au départ, contient la macro qui permet d'importer tous les fichiers texte des résultats intermédiaires. On dispose ainsi d'un outil pour visualiser, trier, modifier, comparer les résultats obtenus par rapport à un état défini de la structure.

Des rapports d'activité personnalisés par messagerie

Le courrier électronique est une méthode efficace pour transmettre l'état d'un système aux personnes concernées.

Pour déterminer l'administrateur d'une unité, j'utilise les données présentes dans l'unité d'organisation (OU):



À la fin du processus journalier, deux types de messages en format CSV sont envoyés:

- un message pour l'administrateur du domaine sur le déroulement du processus;
- un message contenant, le cas échéant, les modifications pour l'administrateur de l'unité concerné. Le message contient également la liste des comptes non identifiés.

Un archivage automatique

Dans l'outil précédent, la documentation était réalisée par l'incorporation de la date et de l'heure de l'exécution du processus dans les fichiers créés. Avec la méthode utilisée par ce nouvel outil, le nombre de fichiers intermédiaires générés est important, souvent supérieur à 16, et ce mode de classement devient vite ingérable. La solution qui vient immédiatement à l'esprit est l'utilisation de la structure de fichier de n'importe quel ordinateur en dossier et sous-dossier.

En pratique, à la première exécution du programme un dossier est créé. Son nom est simplement le jour en question. Comme le processus pour obtenir le résultat est itératif, le même principe est appliqué avec les heures des exécutions successives.

Ainsi, chaque étape du processus d'analyse et de modification est conservée, permettant une traçabilité élevée des modifications.

Unicode, UTF-8

La représentation de l'information qui suit des chemins tortueux a permis de quitter les rivages anglo-saxons (EBCDIC, ASCII 7 bits) pour s'arrêter dans les îlots propriétaires (PC, Windows, Macintosh,…) ou nationaux, et enfin atteindre la terre promise, la représentation Unicode (deux octets). Comme en informatique, il est impossible de faire fi des héritages antérieurs, la représentation utilisée dans les méta-annuaires est UFT-8 (UCS Transformation Format). Sous ce vocable mystérieux se cache un encodage qui permet de convertir un caractère Unicode (16 bits) en son équivalent ASCII 8 bits.

En pratique, si le caractère est de l'ASCII 7 bits, sa représentation UTF-8 est identique. Pour les autres caractères, ils sont codés sur plusieurs octets (de deux à six). Les caractères accentués sont représentés sur deux octets en UTF-8.

Actuellement les systèmes d'exploitation (Windows 2000, XP, 2003, Unix, Mac OS X) supportent une représentation Unicode.

Base64

Une autre méthode pour incorporer des caractères accentués (codage 8 bits) dans un format uniquement 7 bits est d'utiliser la transformation Base64. Comme son nom l'indique, l'idée sous-jacente de Base64 est de n'utiliser que 6 bits comme valeur utile ($2^6 = 64$). En conséquence, trois caractères 8 bits (24 bits) sont équivalents à quatre caractères 6 bits (encore 24 bits). Les 64 caractères utilisés en base64 sont: "ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz0123456789+/". Comme se pose le problème de la longueur de la chaîne de caractère initiale (qui n'est que rarement un multiple de trois), les caractères manquants sont remplacés par "=".

LDIFDE

Cet outil est l'implémentation de Microsoft de LDIF sous la forme d'une ligne de commande:

```
LDIF Directory Exchange
General Parameters
==================
-i  Turn on Import Mode (The default is Export)
-f filename Input or Output filename
-s servername The server to bind to (Default to DC of logged
                                                    in Domain)
-c FromDN ToDN Replace occurences of FromDN to ToDN
-v  Turn on Verbose Mode
-j  Log File Location
-t  Port Number (default = 389)
-u  Use Unicode format
-?  Help
Export Specific
==============
-d RootDN The root of the LDAP search (Default to Naming
                                                      Context)
-r Filter LDAP search filter (Default to "(objectClass=*)")
-p SearchScope Search Scope (Base/OneLevel/Subtree)
-l list List of attributes (comma separated) to look for
                                                in an LDAP search
-o list List of attributes (comma separated) to omit
                                                    from input.
-g  Disable Paged Search.
-m  Enable the SAM logic on export.
-n  Do not export binary values
Import
======
-k  The import will go on ignoring 'Constraint Vio-
                    lation' and 'Object Already Exists' errors
-y  The import will use lazy commit for better per-
                                                      formance

Credentials Establishment
=========================
Note that if no credentials is specified, LDIFDE will bind as
the currently logged on user, using SSPI.
-a UserDN [Password | *]  Simple authentication
-b UserName Domain [Password | *] SSPI bind method
```

Le format LDIF offre la possibilité de manipulation du contenu: **création**, **modification** et **suppression**. Contrairement à LDAP, une entité Active Directory ne peut être recréée, chaque objet est unique. En conséquence, un processus de suppression-création en masse n'est pas possible. En pratique, on ne détruit pas un objet Active Directory, on le désactive et on l'isole.

CSVDE

Si on désire travailler avec un format compatible avec un tableur, CSVDE génère les mêmes informations que LDIFDE sous la forme d'une liste de valeurs séparées par une virgule *(CSV ou Comma Separated Values)*. Les valeurs pouvant prêter à confusion sont incluses entre guillemets. Heureusement, les paramètres sont identiques à ceux de LDIFDE. Ce format est plus simple à lire par un programme de post-traitement. En mode d'importation, au contraire de LDIFDE, CSVDE permet uniquement la création ou la destruction d'objets.

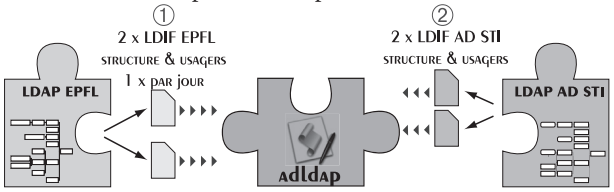
Un piège commun à ces outils est que les valeurs d'un attribut ne sont générées que si celui-ci n'est pas vide. En conséquence, en fonction des données présentes, le nombre d'attributs peut varier, même avec le format CSV.

Encodage utilisé par LDIFDE & CSVDE

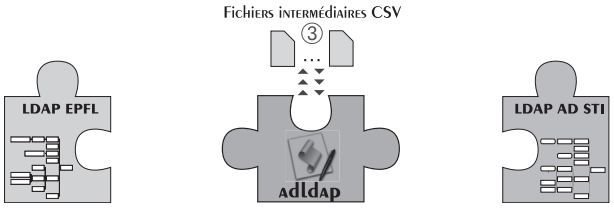
Par souci de *simplicité*, Microsoft a décidé de rajouter deux variantes à ces encodages, une représentation hexadécimale pour CSVDE en lieu et place de Base64. Le texte qui en résulte est quand même encodé en UTF-8. Et l'utilisation du codage propre à Windows pour l'importation avec LDIFDE, évitant le double transcodage en UTF-8 puis Base64. Cette fonctionnalité présente avec les derniers *Service Packs* n'est évidemment pas documentée (peut-être que Microsoft veut encourager la curiosité intellectuelle des programmeurs avec ce genre de pratique).

Tendre vers un état idéal

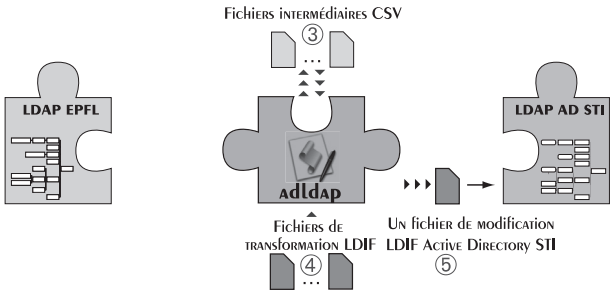
Il est exclu que d'un coup de baguette magique, on puisse passer de l'état antérieur, avec des structures manipulées par des êtres humains, à une structure automatisée. Le processus est récursif, il comporte les étapes suivantes:



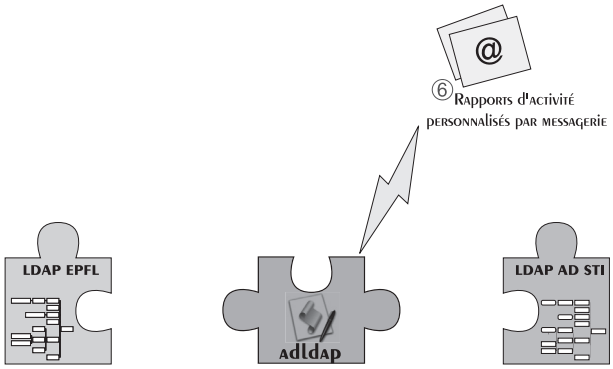
① génération de la structure idéale à partir de l'annuaire LDAP EPFL, pour le jour courant
② génération de structure actuelle avec LDAP du domaine Active Directory STI



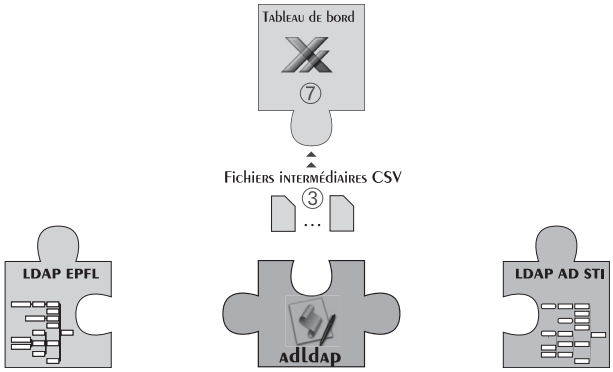
③ comparaison et génération des fichiers intermédiaires



④ génération des modifications pour un stade déterminé avec le translateur LDIF
⑤ modification avec LDIF de l'annuaire LDAP Active Directory

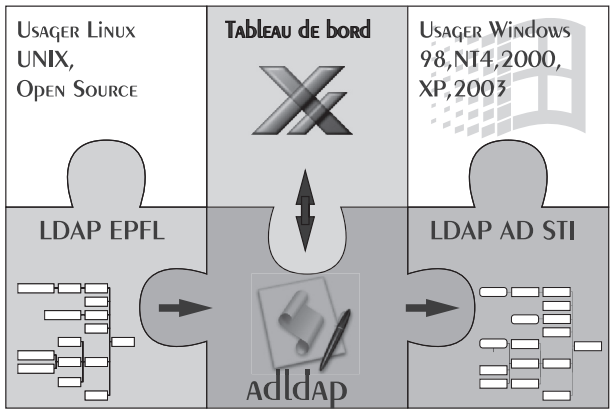


⑥ émission des rapports d'activité personnalisés aux administrateurs concernés.



⑦ observation de l'état actuel par l'intermédiaire du tableau de bord.

Le processus doit être répété jusqu'à l'obtention de la structure idéale.



Le puzzle réussi

Pour réaliser la transition de la structure antérieure vers la structure à jour, il faut passer par les stades suivants:

A adaptation de la structure AD (Active Directory STI) pour les unités existantes (noms identiques avec EPFL)
B création des nouvelles structures AD, à partir d'EPFL
C création des nouveaux usagers AD, à partir d'EPFL
D déplacement des usagers AD existants dans les unités
E suppression des anciens usagers AD (ceux qui n'existent plus dans EPFL)
F mise à jour des groupes de sécurité pour les usages possédant plusieurs fonctions
G identification des comptes de services

Le détail de ces étapes

Phase A et B: adaptation et création de la structure Active Directory

Ces phases sont primordiales. La position d'un objet dans LDAP est représentée par son nom et son chemin (DN, Distingual Name) décrit sous forme textuelle. Comme indiqué précédemment, Active Directory identifie un objet par son identificateur unique codé sur 128 bits. Ainsi, la position ou le nom d'un objet LDAP ne garantit pas sa concordance avec son homologue Active Directory. Il est nécessaire d'établir cette relation d'unicité avec une clé présente dans chaque objet et dans chaque annuaire. Il n'existe pas dans l'EPFL une identification unique pour chaque objet. On utilise deux attributs disponibles dans l'annuaire LDAP de l'EPFL:

- pour les unités d'organisation (OU, *Organizational Unit*), le GID;
- pour les usagers, l'identification IMAP qui est unique dans l'école.

Malheureusement, un usager ne possède pas forcément d'attribut GID dans le domaine STI. L'usager hérite de sa position dans la hiérarchie et le GID de l'unité d'organisation (OU). Pour simplifier cette opération, le programme vérifie uniquement la concordance entre les deux annuaires LDAP pour leurs structures communes. En conséquence, l'organisation interne d'une unité n'est pas affectée.

C'est une condition impérative dans une structure possédant des délégations de gestion.

Phase C: création des nouveaux usagers.

Avec la condition que les deux phases précédentes soient réalisées, il est possible de vérifier la concordance entre les usagers de l'annuaire EPFL (EPFL) avec ceux du domaine Active Directory (AD). En pratique, les comptes utilisateur se classent dans une des catégories suivantes:

- usager EPFL: usager actuel dans AD qui se trouve dans la même structure AD & EPFL;
- usager EPFL à créer: usager n'existant pas dans AD;
- usager EPFL à déplacer: usager existant dans AD, mais dont la structure n'est pas correcte (structure AD <> structure EPFL);
- usager EPFL hors faculté: usager dont la Faculté d'origine n'est pas STI;
- usager EPFL ancien: usager identifié comme tel, mais qui ne fait plus partie de la Faculté;
- usager AD de gestion: compte de gestion, identifié comme tel;
- usager AD de service: tout autre compte, probablement un compte de service, mais le rôle reste à identifier.

Une fois cette classification établie, il est facile de créer les nouveaux usagers à partir des données de l'annuaire LDAP EPFL

Phase D: déplacement des usagers

Il est probable qu'un usager, lors de la durée de sa vie dans la faculté STI, puisse passer par différentes fonctions et rattachements. À chaque nouveau rattachement, l'usager est déplacé dans l'unité de laquelle il est rattaché et fait partie de son groupe de sécurité *Staff*. Les informations le concernant sont automatiquement mises à jour (comme le bureau ou le numéro de téléphone). Pour éviter une interruption immédiate de l'accès à son ancienne unité (il n'a pas déjà déménagé par exemple), il reste dans le groupe de sécurité d'origine. Ce dernier principe peut être modifié dès la phase de migration terminée.

Phase E: suppression des anciens usagers

Si un usager n'est plus référencé dans l'annuaire de l'école, il ne travaille plus pour la Faculté, et de ce fait, son compte n'a pas lieu d'être présent. Comme dans le cas précédent, le compte d'un usager est équivalent à un accès à ses ressources, il est probable que la modification de l'annuaire ne soit pas synchrone avec la fin réelle de l'activité. Pour éviter un trou de sécurité, l'usager est automatiquement déplacé (et pas supprimé) dans une zone réservée du domaine. Il est également supprimé du groupe de sécurité *Staff* de sa dernière unité de rattachement (il perd automatiquement l'accès au serveur de fichier par exemple).

Si l'administrateur local désire néanmoins réintégrer un usager dans son unité (car par exemple, l'usager ne fait plus partie de l'école, mais continue une relation de travail), il est possible de le remettre dans son unité. Il sera catalogué comme un compte de service qui, par définition, est sous la responsabilité de l'administrateur local.

Phase F: mise à jour des groupes de sécurité pour les usages possédant plusieurs fonctions

Cette nouvelle fonctionnalité est un des aspects les plus intéressants de ce programme. En effet, il n'est pas rare qu'un usager possède plusieurs rattachements, par exemple, pour un enseignant, faire partie d'un laboratoire, d'une section pour l'enseignement et peut-être d'une fonction de gestion.

Dans le cas de Faculté STI, ces appartenances multiples concernent près de la moitié des structures (54 sur 114) et concernent 249 affiliations supplémentaires.

Phase G: identification des comptes de services

Après la mise en œuvre de cette méthode, les comptes non identifiés se retrouvent dans la catégorie des comptes de services. En fait, la majorité sont des comptes de test, des usagers créés ne respectant pas les règles de l'école. La séparation entre les bons grains et l'ivraie est du ressort de chaque administrateur local.

En pratique

Une simulation 1:1 du domaine réel

L'observation des méthodes de travail des étudiants en génie mécanique, où la part de simulation est très impor-

tante, et ma formation d'architecte, où les maquettes numériques et en carton m'ont enseigné la formidable capacité des méthodes de simulation. Il serait illusoire de développer ce genre d'outil sans simulation.

Pour mon travail d'intégration d'installation pour l'expérience Laptop (voir article dansle FI 5/03, ***dit.epfl.ch/publications-spip/article.php3?id_article=126***) j'avais déjà créé un domaine Active Directory virtuel possédant les mêmes propriétés que le réel. La réutilisation du fichier de la machine virtuelle VmWare m'a permis de disposer d'un domaine fonctionnel, mais ne possédant pas des objets identiques à ceux du domaine réel.

Active Directory Faculté STI			
Avant		Après	
9 février 2004		*10 février 2004*	
53	structures d'unités	114	structures d'unités
30	délégations de gestion	30	délégations de gestion
648	comptes d'usagers: 463 corrects 100 à déplacer	1135	comptes d'usagers – 249 affiliations supplémentaires dans 54 structures
	85 anciens	85	comptes anciens
102	comptes de service	225	comptes de service
131	comptes à identifier	130	comptes à identifier

Comment extraire l'ensemble des objets désirés du domaine réel pour les transcrire dans ce mode de simulation? La solution est très simple, en utilisant LDIF !

En pratique, avant de procéder aux manipulations sur l'objet réel, j'ai appliqué les mêmes opérations au domaine virtuel.

Cette méthode m'a permis de débusquer un certain nombre d'erreurs, souvent corrigées par des tests de validité supplémentaires.

Il est improbable qu'un être humain respecte l'ensemble des normes définies dans l'école pour la création d'un objet utilisateur sans apporter sa touche personnelle. Ceci entraîne parfois une erreur dans un traitement automatique des informations.

Je plaide naturellement coupable pour les rares objets que je n'avais pas créés par script.

Une boîte à outils

Un des objectifs secondaires est de disposer d'une boîte à outils. Le domaine de la gestion système présente le paradoxe que malgré le fait que nous manipulons quotidiennement des ordinateurs, ne nous fassions pas plus appel aux méthodes standardisées de gestion.

Contrairement au travail précédent réalisé sur mesure, je me suis efforcé dans celui-ci d'utiliser au maximum les outils existants. Par exemple LDIF, pour éviter de réécrire des parties importantes de création, modification et suppression des objets dans Active Directory.

Le principal avantage de cette démarche est qu'on passe plus de temps à comprendre les outils, et à tirer parti de ceux-ci, qu'à coder une application. C'est également le même principe qui m'a poussé à utiliser un tableur comme outil de présentation des résultats.

Le principe du translateur permet de l'utiliser comme source de fonctions annexes

Par exemple, il est nécessaire de disposer régulièrement de comptes liés à un usage spécifique des salles de PC en libre-service de notre Faculté.

Pour éviter de mettre en œuvre un compte générique unique, un compte par usager est créé. La simple modification et combinaison de fichiers de transformation (celui d'une structure et celui d'un usager) m'a permis de réaliser rapidement cette nouvelle fonctionnalité. Elle permet en partant d'un fichier Excel contenant les informations spécifiques pour trois cours (trois lignes de 9 valeurs) et de générer trois structures indépendantes avec 40 usagers chacune.

Les résultats sur un domaine en production

Pour ceux qui sont arrivés à la fin de cet article, voici les résultats de l'application de cette boîte à outils AD-LDAP sur un domaine réel, celui de la Faculté STI.

Après ce changement massif de l'état du domaine, on pourrait s'attendre à de nombreuses rectifications. En fait, il n'en est rien, car uniquement 6 usagers (sur plus de 1100) posaient problème, en particulier pour des comptes où l'identificateur de l'usager avait été modifié pour suivre des pratiques antérieures. Le seul effet inattendu est l'utilisation accrue de l'outil d'accréditation pour assurer la concordance entre la structure réelle et celle de l'annuaire.

Dans les 3 semaines suivant la mise en service, 17 usagers sont arrivés dans la faculté, 19 usagers ont quitté celle-ci et 10 ont changé d'affectation.

La génération automatique des rapports d'activité personnalisés permet un meilleur contrôle des comptes de gestion et évite les éléments surnuméraires.

Cet outil est évidemment à disposition de mes collègues qui gèrent comme moi, un domaine de Faculté.

Conclusion

Ce travail propose un schéma collaboratif entre deux univers que chaque partisan présente comme unique, alors qu'en fait, chacun retire le bénéfice de l'emploi de l'autre:

- pour le monde *Open Source*, c'est la satisfaction que la qualité propre d'Active Directory soit issue de l'utilisation pertinente de travaux réalisés dans le cadre de réflexion publique, les RFC;
- pour les aficionados de Microsoft, c'est qu'il est vain de considérer une position dominante à un instant donné sans prendre en considération les fondements théoriques des technologies employées.■