Simplification et unification de l'authentification

Serge Conrad

CONSERVATOIRE NATIONAL DES ARTS ET METIERS

CENTRE REGIONAL ASSOCIE DE MIDI PYRENEES

_____

MEMOIRE

présenté en vue d'obtenir

le DIPLOME d'INGENIEUR CNAM

SPECIALITE : INFORMATIQUE

OPTION : SYSTEME RESEAUX ET MULTIMEDIA

par

CONRAD Serge

_____

« Simplification et unification de l'authentification »

Soutenu le 13 juin 2014 (sous réserve)

_____

JURY

PRESIDENT : M. Yann Pollet

MEMBRES : M. Hadj Batatia, M.Thierry Millan, M. Pascal Dayre, M. David Tsang-Hin-Sun

REMERCIEMENTS

J'adresse, tout d'abord, toute ma gratitude aux personnes qui m'ont aidé dans l'obtention et la réalisation de ce stage, notamment Claudine Morel de la formation des personnels, Michèle Chap et Robert Ricard de la Faculté des Sciences et d'Ingénierie, les directeurs de la DTSI Eric Marchadier et Stéphane Larroque, le directeur technique Abdo Malac, les directeurs de DSRT Christian Escaffre et Alexandre Gouverneur ainsi que les chargés de mission du numérique Mathieu Arlat et Jean Marc Pierson.

Je remercie, par ailleurs, le directeur du stage David Tsang-Hin-Sun pour m'avoir accordé sa confiance et les échanges constructifs que nous avons eus, tout comme je remercie mon tuteur de stage, M Pascal Dayre, pour ses remarques, et les personnes de l'équipe H3S (Céline Juan, Xavier Bonislawski et Christophe Marteau) pour leur accueil et leur ouverture d'esprit. L'authentification est par nature un sujet transverse qui intéresse de nombreuses personnes dans notre Université. Ce stage m'a, par conséquent, conduit à dialoguer avec des personnes diverses et je tiens à leur dire à quel point leur contribution me fut précieuse.

Je remercie, en outre, les personnels de l'équipe « réseau », et particulièrement Denis Mirassou, pour ses explications sur l'authentification « wifi » et « radius » ; Viviane Correge et Patrice Borel pour leurs apports sur l'authentification des messageries ; les personnels de l'équipe exploitation pour leur collaboration efficace.

Je tiens à remercier, également, les personnels du Département des Systèmes d'informations et particulièrement Jean Claude Texier et Sabine Delpech pour leur rôle de coordination, Renaud Martin Da Rocha pour l'intégration du changement de mot de passe Kerberos, et Philippe Baillion pour son apport sur la gestion des charges d'enseignement dans l'annuaire ldap.

Je remercie Jean–François Costeceque de DPROX pour les échanges concernant l'authentification des annuaires Active Directory, ainsi qu'Eric Raffaele de DTICE pour ses remarques pertinentes sur le projet annuaire unifié.

Je remercie, enfin, Michèle Menard et Michel Conrad pour la relecture du mémoire et les conseils.

GLOSSAIRE

389DS	389 Directory Server
CAS	Central Authentication Service
DES	Data Encryption Standard
EAP	Extensible Authentication Protocol
GSSAPI	Generic Security Services Application Program Interface
HOTP	HMAC-based One-time Password
HTTP	Hypertext Transfer Protocol
IPA	Idendity Policy Audit
LDAP	Lightweight Directory Access Protocol
MD5	Message Digest 5
NTLM	NT Lan Manager
NIS	Network Information Service
NSS	Name Service Switch
OATH	Open AuTHentication
OAUTH	pas de signification, différent de oath
OCRA	OATH Challenge-Response Algorithm
OTP	One-time password
PAM	Pluggable Authentication Modules
RADIUS	Remote Authentication Dial-In User Service
SAML	Security assertion markup language
SASL	Simple Authentication and Security Layer
SHA	Secure Hash Algorithm
SPNEGO	Simple and Protected GSSAPI Negotiation Mechanism
SSO	Single sign-on
TOTP	Time-based One-time Password
VPN	Virtual Private Network

Table des matières

I **Contexte**

J'ai effectué mon stage de fin d'étude Cnam à la Direction des Technologies et des Systèmes d'Information (DTSI) de l'Université Paul Sabatier, à Toulouse. L'intitulé du stage est **« Simplification et unification de l'authentification ».** L'angle d'approche pour l'étude de l'authentification a été plutôt orienté vers le système d'exploitation et enseignement. Cependant, j'ai essayé de prendre en compte le riche écosystème des universités françaises et de proposer un système qui soit généralisable et mutualisable facilement. Le mot « **Simplification »** doit être entendu au sens de « rationalisation » des procédures et le mot « **unification »** au sens de pouvoir proposer le même couple login/mot de passe pour les contextes windows et unix.

1.1 Généralités sur les Systèmes d'Informations des universités

Le système d'information des Universités, à savoir l'ensemble des ressources informatiques, peut être séparé en quatre couches :

• La couche « Infrastructure », qui comprend les systèmes d'exploitation et les bases de données.

• La couche « Interopérabilité », permet l'accès aux ressources par un référentiel commun de type annuaire. Il existe une norme écrite par le Comité Réseau des Universités, qui effectue notamment des recommandations pour cet annuaire.

• La couche « Briques Applicatives » comprend l'ensemble des logiciels nécessaires aux fonctionnements. Ces logiciels peuvent être développés localement, mais sont le plus souvent écrits et maintenus par des acteurs extérieurs.

• La « couche Externalisation » permet l'accès aux briques applicatives, généralement au travers d'un Environnement numérique de travail.

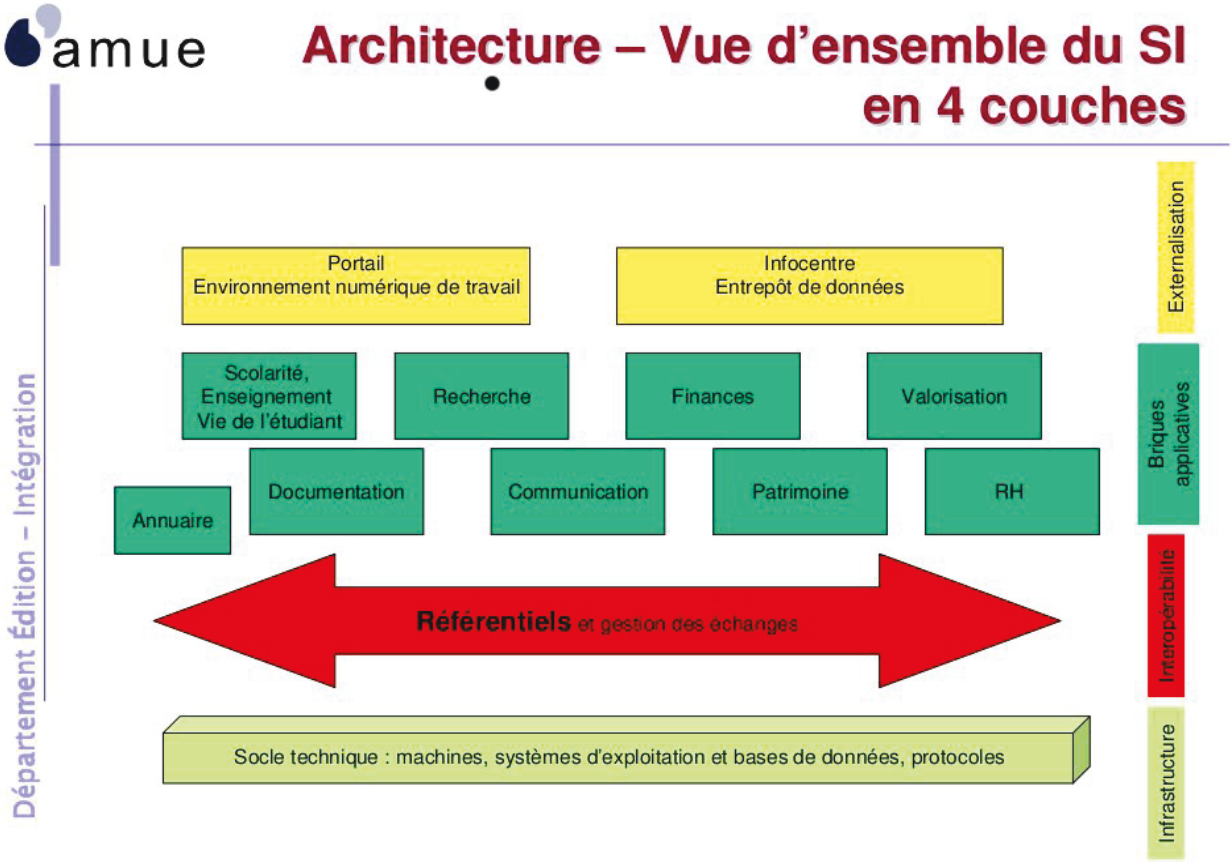


Figure 1 : Architecture des Systèmes d'Information des Universités (source : AMUE [43])

1.1.1 Des besoins applicatifs spécifiques : la couche «Briques applicatives »

Cette couche prend en compte l'ensemble des logiciels qui répondent aux besoins spécifiques des universités, parmi lesquels nous citerons :

- Le traitement de gestion de la scolarité des étudiants.
- Les logiciels de gestion des ressources humaines.
- Les logiciels de gestion budgétaire et comptable.
- Les logiciels spécifiques : Emplois du temps, gestion des heures supplémentaires, du patrimoine ...

Ces logiciels sont le plus souvent développés par des acteurs externes à l'Université, même s'ils peuvent être écrits et maintenus en local. Parmi ces acteurs externes, les plus importants sont l'Agence de Mutualisation des Universités et Établissements (AMUE) ou l'association Cocktail.

L'AMUE est un groupement d'intérêt public regroupant 80 universités et 79 établissements dont l'objectif est le développement de logiciels répondant aux besoins diversifiés de ses membres. Parmi son offre de logiciels, on trouve notamment les logiciels Apogée, pour la gestion de la scolarité, Harpege, pour la GRH et Sifac, pour la gestion budgétaire.

Un autre acteur du développement des logiciels pour les Universités est l'association Cocktail : elle développe un Progiciel de Gestion Intégré comprenant une soixantaine de modules. Une trentaine d'universités sont membres de l'association. La suite Cocktail est principalement destinée aux Universités de petites tailles et permet une intégration facile du système d'information.

1.1.2 La couche interopérabilité.

Elle permet l'accès aux ressources par un référentiel commun de type annuaire.

Cette couche peut être décomposée en deux sous-couches :

- Les mécanismes d'agrégation des données provenant de la couche « applicative », dans un référentiel.
- Les mécanismes de contrôle d'accès aux ressources informatiques de la couche « infrastructure ».

La norme « supann » définie par le comité Réseau des Universités propose un cadre de cohérence commun pour la mise en place d'un annuaire d'établissement, afin de permettre une interopérabilité inter-établissement. Cette norme préconise notamment l'utilisation d'un annuaire LDAP basé sur openLdap comme référentiel.

1.1.2.1 L'agrégation des données dans le référentiel

L'alimentation de l'annuaire d'établissement est un problème complexe du fait de la multiplicité des bases métiers et de la problématique du dédoublonnage entre les sources. Les universités ont tendance à résoudre le problème avec des solutions maison, plus à même de suivre l'état de leur système d'information.

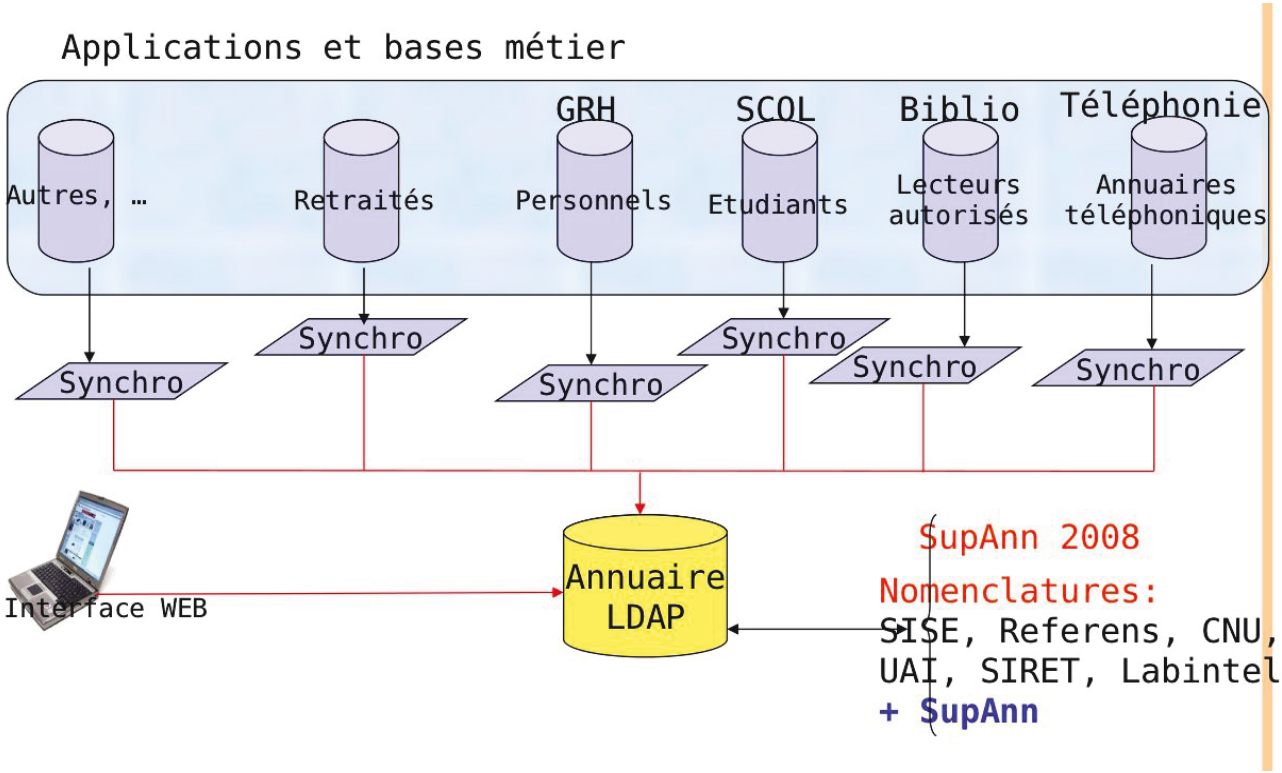


Figure 2 : Exemple d'agrégation de données dans un annuaire LDAP
(source supAnn-tech [16])

Les Universités de petite taille qui utilisent les applications métiers du consortium Cocktail bénéficient du référentiel intégré Ghrum qui automatise les problématiques d'alimentation.

A l'heure où j'écris ces lignes, l'Amue développe activement son propre mécanisme d'agrégation nommé PRISME. Il permettra la concaténation et le dédoublonnage de données RH entre plusieurs établissements. Ref (8)

Le projet Prisme possède deux composants :

• une brique logicielle de Master Data Management (MDM): qualité des données, gestion des doublons.

• une brique logicielle d'intégration des données avec Open Esb : transport des données, transcodification …

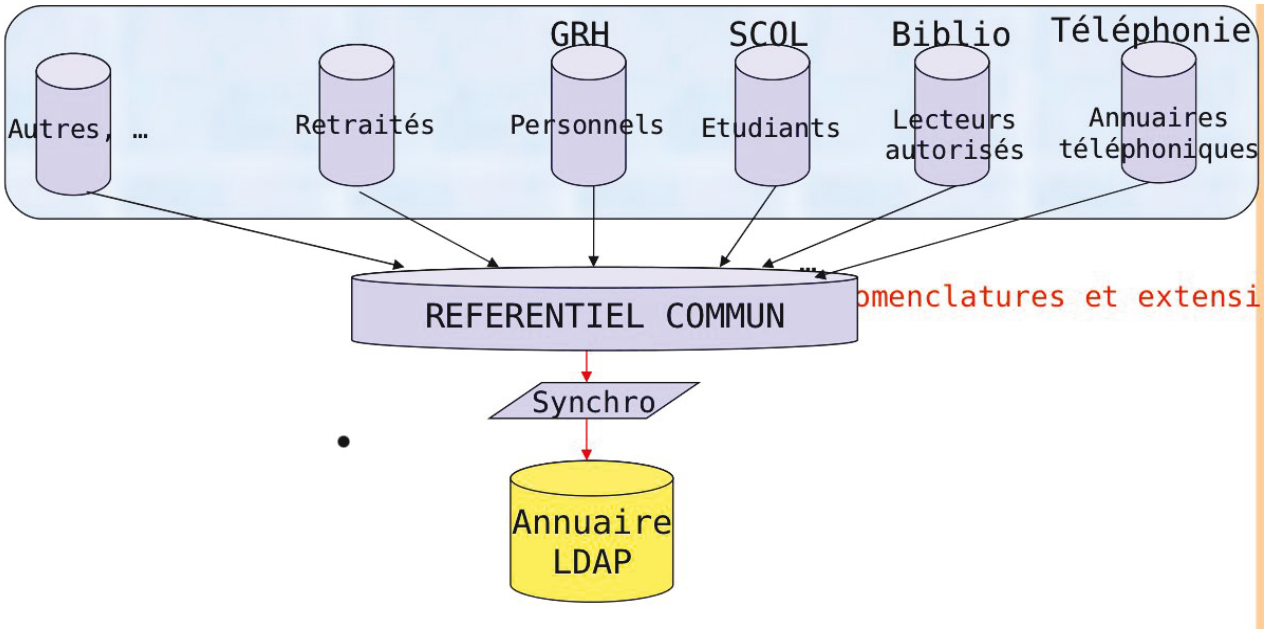


Figure 3 : Evolution future de l'agrégation des données dans un annuaire LDAP

1.1.2.2 Les mécanismes de contrôle d'accès aux ressources.

Les « consommateurs » de l'annuaire sont de plusieurs types :

• Des applications comme par exemple l'annuaire téléphonique.

• Des services d'authentification comme le serveur d'authentification réseau Radius et le service d'authentification pour les sites web CAS (Central Authentication Service).

• Des serveurs de messagerie.

• Des protocoles d'authentification systèmes pour les serveurs et postes de travail comme par exemple pam_LDAP, pgina

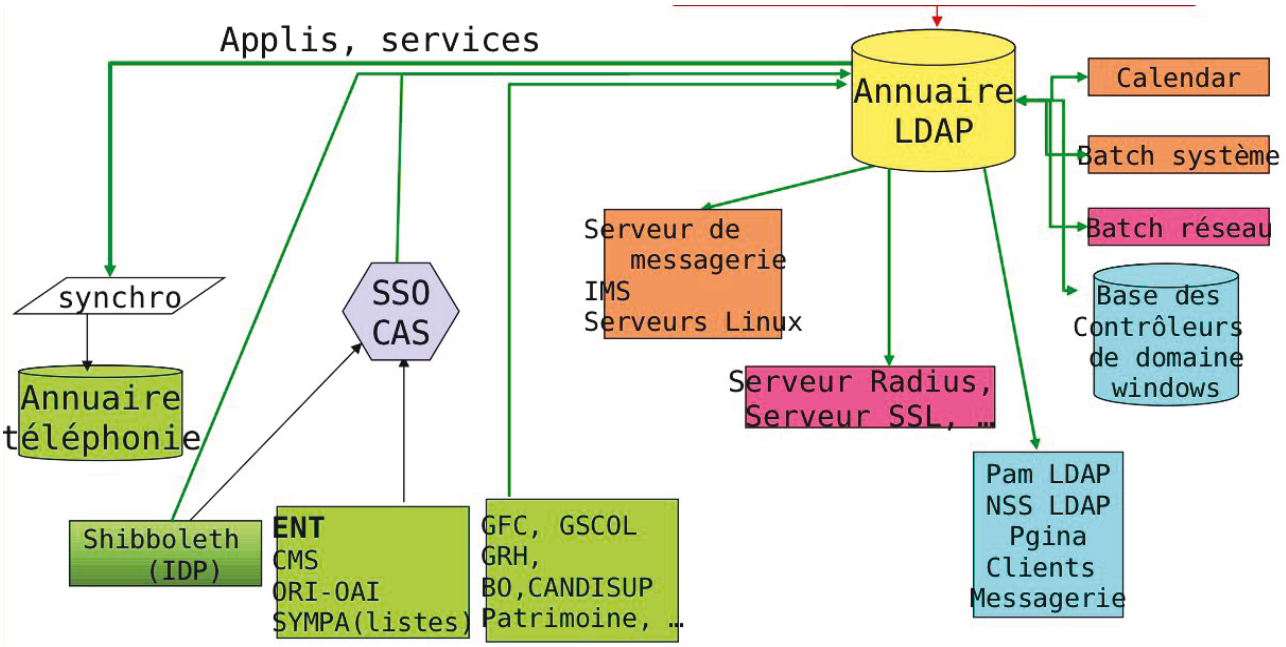


Figure 4 : Les « consommateurs » de l'annuaire LDAP

Une enquête effectuée sur les utilisations de l'annuaire dans 145 Universités et établissements français semble confirmer cette vision (enquête effectuée par le cru en 2010).

Tableau I : Enquête sur l'utilisation des annuaires dans les universités (source CRU [17])

Utilisation des annuaires	NB	Pourcentage
Authentification système	104	77.61%
Authentification mail	113	84.32%
Authentification applicative	116	86.56%
Authentification réseau (via Radius par ex.)	114	85.07%
Authentification SSO	104	77.61%
Autorisation, contrôle d accès	72	53.73%
Fédération d'identités	67	50.00%

1.1.2.3 Les recommandations du Comité Réseaux des Universités (CRU) : Les normes Supann

Pour permettre l'interopérabilité des annuaires, le CRU a émis un ensemble de recommandations sur différents sujets techniques, notamment le choix du protocole LDAP, les schémas utilisés ainsi que sur l'arborescence de l'annuaire. Ces recommandations sont connues sous le nom de norme supann. Ref [18].

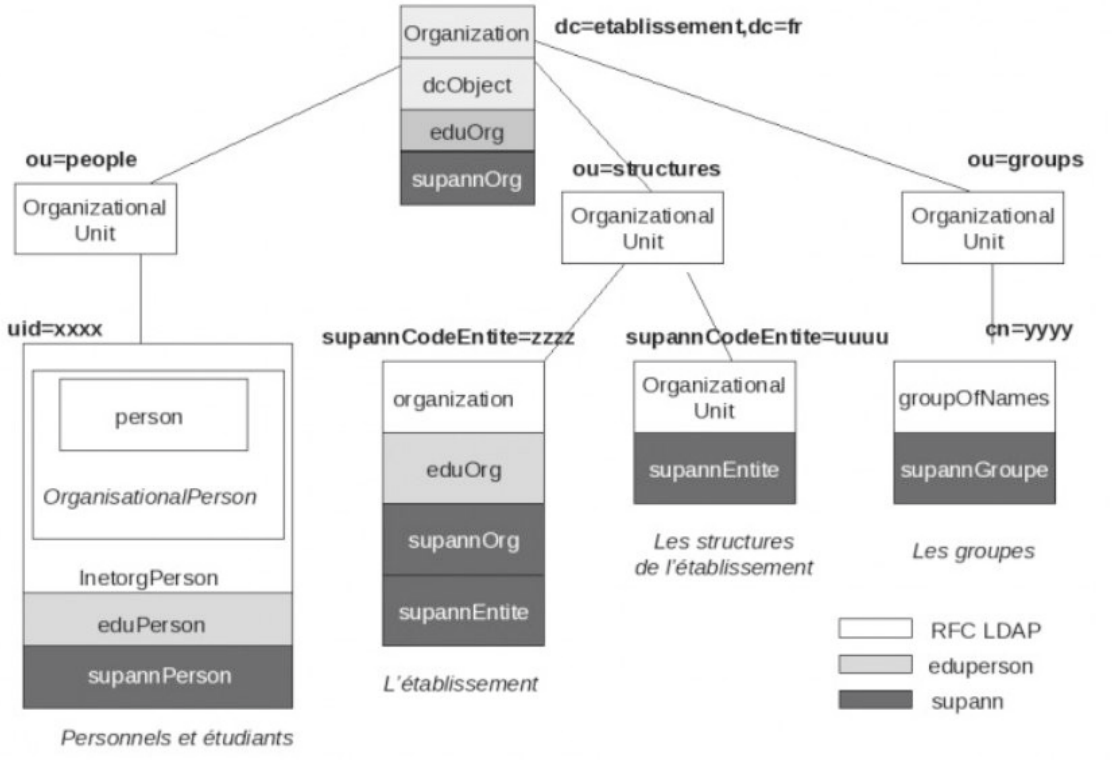


Figure 5 : La recommandation supann 2009 pour l'arborescence des informations (CRU [19])

L'établissement est également laissé libre de modifier la structure de son annuaire pour répondre à ses besoins spécifiques.

1.1.3 La couche infrastructure :

Elle comprend l'ensemble des systèmes d'exploitation et des bases de données. Cette couche n'est pas constituée d'un seul bloc, mais est généralement composée de plusieurs parcs informatiques, suivant les missions et les divisions organisationnelles de l'Université.

Dans le contexte enseignement, par exemple, chaque faculté ou institut peut posséder son propre parc informatique. Et celui-ci peut être géré soit de manière centrale par le Centre des Ressources Informatiques de l'Université, soit par une équipe autonome. Ceci implique que l'on peut trouver des procédures de gestion différentes pour le déploiement, l'authentification, le stockage...

Pour le contexte recherche, les différents laboratoires sont en général autonomes dans ces problématiques.

Les systèmes d'exploitation habituellement utilisés dans les parcs informatiques sont des postes de travail linux et windows mono-utilisateur, et des serveurs Unix et Linux multi-utilisateurs.
Les systèmes d'exploitation peuvent être installés sur des postes physiques, éventuellement en multi-boot, ou sur des postes de travail virtualisés accessibles par le réseau.
Il peut également être utilisé des bases de données dans un contexte enseignement, recherche ou administration.
On trouve par exemple fréquemment des bases Oracle, MySql ou Sql Server.

1.2 L'université Toulouse III- Paul Sabatier

L'Université a été fondée en 1969 de la fusion des Facultés de médecine, de pharmacie et des sciences. C'est également l'un des six établissements membres fondateurs du PRES Université de Toulouse.
Pour l'année universitaire 2012-2013, il y avait plus de 32000 étudiants inscrits sur l'ensemble des sites de l'université. Les enseignants et enseignants-chercheurs sont au nombre de 2609 et les personnels BIATSS au nombre de 1980.

1.2.1 L'organisation :

Conformément à la loi du 10 août 2007 « Libertés et Responsabilités des Universités », les missions principales de l'université sont :

- La formation (initiale et continue)
- La recherche scientifique et technologique
- L'orientation et l'insertion professionnelle.

A cela viennent s'ajouter d'autres missions :

- La diffusion de la culture et de la recherche scientifique.
- La participation à la construction de l'espace européen.
- La coopération internationale.

La formation est articulée autour de cinq domaines : sciences, santé, sport, ingénierie et technologie. La plupart des cursus des formations suivent le schéma LMD, dans l'objectif de la construction de l'espace européen de l'enseignement supérieur. L'université est habilitée par le Ministère de l'Enseignement Supérieur et de la Recherche pour la délivrance de 15 mentions de Licence et 110 spécialités de Master.

L' université Paul Sabatier est composée de 6 facultés et 3 Instituts dédiés à l'enseignement :

- Quatre facultés dédiées à la médecine : Les facultés de médecine de Rangueil et Purpan, la faculté des sciences pharmaceutiques et la faculté de chirurgie dentaire.
- La faculté des sciences et d'ingénierie.
- La faculté des sciences du sport et du mouvement humain.
- Deux Instituts universitaire de technologie : L'IUT « A » Paul Sabatier et l'IUT de Tarbes.
- L'observatoire Midi-Pyrénées, dont l'activité d'enseignement est dispensée au sein de la FSI et de l'IUT « A ».

La recherche est organisée autour de quatre pôles dans les thématiques suivantes:

- Sciences de la matière.
- Mathématiques, Sciences et Technologies de l'Information et de l'Ingénierie.
- Univers, Planète, Espace, Environnement.
- Sciences du Vivant

Chaque pôle est principalement composé de plusieurs unités mixtes de recherche, qui sont gérées en collaboration avec le CNRS.

Des services centraux fonctionnent en appui des structures de l'université, parmi lesquels je citerai :

- La direction du soutien aux laboratoires
- La direction des technologies et des systèmes d'information.
- La direction des services comptables

1.2.2 La gouvernance de l'université

L'université est présidée par le Président de l'université et administrée par un Conseil d'administration. La vie de l'université est régie par trois conseils.

- Le Conseil d'administration détermine la politique de l'établissement et vote le budget
- Le Conseil scientifique est consulté sur les orientations des politiques de recherche.
- Le Conseil des études et de la vie universitaire est consulté sur les orientations de formation initiale et continue.

L'université s'organise sous l'égide du directeur général des services et des directions générales adjointes (ressources humaines, pilotage et finances, patrimoine).

1.2.3 Le pilotage des services numériques à l'université :

La maîtrise d'ouvrage est effectuée par **le Comité Stratégique du Numérique**. Son rôle est de valider la stratégie numérique de l'année N+1 à N+5. Il doit également valider le schéma directeur du numérique et suivre son évolution. Il est composé de 25 personnes, dont le président de l'université, les vice-présidents des conseils, les directeurs des facultés et des instituts et les chargés de missions du numérique.

Le **Comité Opérationnel Transverse** établit un lien entre la maîtrise d'ouvrage et les maîtrises d'œuvre. A noter que l'Université est dépourvue de Centre de Ressources Informatiques d'établissement, et que chaque composante dispose de son CRI périphérique, plus ou moins développé selon les cas. Le rôle du comité est de favoriser la transversalité des projets en construisant des équipes projets transverses. Il doit également aider le CSN à donner des priorités aux projets.

Le **Comité des Usagers du Numérique** évalue la qualité des services, fait remonter les demandes d'évolutions mineures au COT et les demandes d'évolutions majeures au CSN.

1.2.4 La direction des technologies et des systèmes d'informations (DTSI).

Ce service est le principal maître d'œuvre concernant la mise en place de la politique numérique décidée par le CSN. Il est composé d'environ 75 personnes et est divisé en 4 départements :

- Département système réseau télécom
- Département système d'information de gestion
- Département TICE
- Département services de proximité

Département système réseau télécom (DSRT) :

C'est le département dans lequel j'effectue mon stage. Il a une grande importance dans les problématiques d'authentification.

Les missions principales du département sont :

- Hébergement de serveurs, service de sauvegarde.
- Mise en place et exploitation de réseaux, téléphonie, services de messagerie.
- Support à l'enseignement et à la recherche.
- Support inter-universitaire.
- Services de base, infrastructure.

Parmi les services de base qui sont assurés par le DSRT :

- Protection du réseau UPS.
- Intégrité des serveurs et services hébergés.
- Mise à disposition d'applicatifs d'hébergement de sites web.
- Services de base réseau : DNS, DHCP, NEWS
- Services de base authentification : LDAP,NIS, Radius, CAS, Shibboleth

Département système d'information de gestion (DSIG) :

Les missions de Dsig sont :

• Identifier les besoins en matière de Système d'Information et formaliser le schéma directeur SI.

• Assurer la maîtrise d'oeuvre et la sécurité du Système d'Information de gestion de l'Université.

• Conseil auprès de la maîtrise d'ouvrage concernant le Système d'Information.

Département services de proximité (DPROX) :

Les missions de Dprox sont :

• Gestion du parc « administration et services communs ».

• Support visio-conférence.

• Coordination des services de proximité des composantes.

• Coordination du guichet unique, qui prend en charge toutes les questions, demandes ou incidents du domaine numérique.

Département TICE (DTICE) :

Les missions de DTICE sont :

• Étudier, proposer, mettre en œuvre et gérer les outils et services numériques nécessaires pour la communauté.

• Développer les usages au sein de l'Université, par le transfert de savoir-faire.

1.2.5 Les services informatiques des composantes :

Les composantes de l'Université Paul Sabatier, pour pallier l'absence de CRI d'établissement, possèdent généralement un service informatique. La taille et les missions de ces services informatiques sont variables, mais ils fonctionnent toujours en coordination avec la DTSI.

Les composantes de l'Université Paul Sabatier possédant un service informatique développé, dédié aux missions d'enseignement sont les IUT et la faculté des sciences et d'ingénierie.

Dans le contexte recherche, certains laboratoires, comme l'IRIT possèdent également des services informatiques.

Toutes les autres composantes possèdent généralement un ou plusieurs informaticiens de proximité.

Je détaillerai uniquement le service informatique de la FSI, où je travaille actuellement.

Le service Numérique d'Assistance et de Proximité de la Faculté des Sciences et d'Ingénierie :

Le service a les missions suivantes :

- Gestion du parc informatique de la faculté.
- Assistance aux utilisateurs.
- Support vidéoconférence.
- Exploitation de réseaux en coordination avec la DTSI

Ce service est composé de dix personnes pour une population d'environ 9000 étudiants.

1.3 L'écosystème du monde de l'éducation supérieur et de la recherche

Les organismes du monde de l'éducation et de la recherche sont reliés en réseau. Chaque réseau est géré au niveau national. En France, le réseau est géré par le Groupe d'Interêt Public Renater. Il est interconnecté avec le réseau européen Géant géré par la société à but non lucratif DANTE (Delivery of Advanced Network Technology to Europe).

Les différents opérateurs des réseaux coopèrent également pour la gestion de fédérations d'identités au travers du projet eduroam permettant d'offrir un accès sans fil à internet. Cette coopération s'effectue par l'association « Trans-European Research and Education Networking Association » (TERENA).

Le GIP Renater offre également une fédération d'identités pour les applications à travers la fédération « Education Recherche ». Renater promeut également le système Eduspot permettant d'authentifier les utilisateurs des bornes wifi par la fédération Education-Recherche. Ce système est complémentaire à eduroam et a vocation à remplacer les portails captifs des organismes.

A noter également l'existence de nombreux Consortium à but non lucratif nationaux équivalents à Renater parmi lesquels nous citerons l'américain « Internet2 », l'anglais « Janet » et le suisse « Switch ».

1.4 La problématique concernant l'authentification :

L'**authentification** est l'acte de confirmer l'identité d'une personne ou d'un objet.

Il existe trois domaines principaux où l'authentification est utilisée :

L'authentification web applicative est de nos jours couramment gérée par des serveurs d'authentification CAS ou Shibboleth. La fédération « Education Recherche » gérée par Renater permet aux utilisateurs des membres adhérents d'utiliser leur identifiant sur les applications reliées.

L'authentification sur les réseaux sans fil se fait par l'intermédiaire de serveur Radius. L'authentification s'effectue généralement par portail captif. Les universités peuvent également utiliser la fédération « eduroam » , et brancher leur portail captif sur la fédération « Education Recherche » en utilisant « Eduspot » .

L'authentification système permet d'authentifier des utilisateurs sur des systèmes informatiques banalisés ou partagés, ou sur des postes de travail virtualisés. Elle utilise généralement des annuaires informatiques comme Active Directory ou openLdap. Il n'existe pas de fédération d'identités de niveau national utilisant ce type d'annuaires. Les universités appuient généralement leur système d'authentification à l'annuaire central universitaire. Il existe cependant une volonté d'unifier les annuaires des universités notamment au niveau local.

L'authentification système a une particularité en ce qu'elle nécessite des attributs supplémentaires pour le bon fonctionnement du système d'exploitation : par exemple, le sid (Security Identifier) pour microsoft windows et l'uidNumber pour les systèmes unix. Nous nommerons ces attributs les **informations utilisateurs**.

Parmi ceux-ci, certains attributs indiquent l'emplacement des répertoires personnels, faisant du **stockage** une problématique liée à l'authentification.

L'authentification doit donc permettre à un utilisateur d'utiliser un seul couple d'identifiants (couple login /mot de passe) pour accéder à l'ensemble de ses ressources. Le mot de passe peut être remplacé par un élément physique (carte à puce) ou une caractéristique physiologique (biométrie). Elle doit idéalement fonctionner en mode **« Single Sign On »**, c'est-à-dire que l'utilisateur ne doit taper ses identifiants qu'une seule fois pour une session donnée.

Authentifier une personne ne signifie pas que celle- ci soit autorisée à accéder à une ressource informatique. Les autorisations peuvent être décentralisées ou un système complémentaire de centralisation peut être mis en place.
L'authentification par mot de passe, étant sujette à des attaques informatiques de type hameçonnage, peut également être considérée comme peu sécurisée. Certains portions du Système d'Information à forte valeur ajoutée peuvent être sécurisé avec de **l'authentification forte.**

L'authentification est une obligation légale depuis le 24 mars 2006 (Décret 2006-358), on doit pouvoir identifier toute personne utilisant des ressources électroniques.

II État de l'art des techniques d'authentification

2.1 Authentifications sur les systèmes Unix/Linux :

2.1.1 L'authentification par fichiers :

C"est historiquement le premier système d'authentification sur Unix, qui continue d'exister encore aujourd'hui. Les premières versions utilisent un fichier /etc/passwd pour stocker les informations de l'utilisateur et /etc/group pour les groupes.

Les champs du fichier passwd comprennent le login et le mot de passe nécessaire à l'authentification. Le mot de passe n'est jamais présent en clair, mais sous forme de hash. Les informations utilisateurs incluses sont l'uidNumber et le gidNumber pour la gestion des droits des fichiers, le gecos pour stocker des précisions sur l'utilisateur, le homeDirectory et le shell par défaut.

Le fichier /etc/group est principalement destiné à faire le lien entre un gidNumber et nom de groupe.

Aux alentours des années 1990, le fichier /etc/shadow a été utilisé pour stocker le mot de passe. En effet la puissance de calcul des ordinateurs augmentant, les hash de mots de passe se sont révélés sensibles aux attaques. Il a donc été nécessaire de les cacher à l'intérieur d'un fichier à accès restreint. Celui-ci n'est accessible en lecture que pour l'utilisateur root. Ce fichier sert également à gérer la durée de vie du mot de passe et du compte. [2]

Le hash d'un mot de passe est une empreinte qui permet de l'identifier , mais ne peut pas être décrypté. Une technique pour découvrir le mot de passe est de calculer le hash de toutes les combinaisons possibles et de comparer le résultat, c'est l'**attaque par force brute**. On peut plus simplement tester une quantité limitée de termes, c'est l'**attaque par dictionnaire**.

Une technique plus rapide consiste à stocker préalablement tous les hash possibles dans des tables nommées **tables arc-en-ciel** et de retrouver le résultat. Pour rendre plus compliquée l'utilisation de ces tables, on rajoute aléatoirement des caractères au mot de passe avant de passer par la fonction de hashage, c'est le **salage**. Bien entendu le sel utilisé ne doit pas être perdu et stocké à côté du hash (séparateur $).

• Exemple pour le champ 1VSCg9qa4$xkbcQknKJpzkglMHu.Bbf.
• 1 est la méthode utilisée pour le hashage (MD5)
• VSCg9qa4 est le sel.
• xkbcQknKJpzkglMHu.Bbf. est le hash du mot de passe.

Les algorithmes de hashage les plus courants :
• DES : c'est en fait une fonction de hash basée sur l'algorithme d'encryption DES.Il prend 8 caractères maximum. C'était le standard jusqu'à son obsolescence en 1999.
• MD5 : Une fonction de hashage utilisée dans les systèmes unix. Une faille a été trouvée en 1996
• SHA : C'est la fonction standard dans les systèmes actuels.

Le processus d'authentification est le suivant :
• Lorsque l'utilisateur crée un mot de passe, le système génère un sel et utilise une fonction de hashage sur la concaténation des deux éléments. Il stocke ensuite le sel et le résultat dans le fichier shadow.
• Lors d'une tentative de connexion : le système ajoute le sel au mot de passe, utilise la fonction de hashage et compare les deux résultats. S'ils sont identiques, l'utilisateur est considéré comme authentifié.

2.1.2 Gestion de la multiplicité des sources d'informations utilisateurs.

Il est apparu rapidement d'autres sources d'authentification externes au système unix (NIS, LDAP, KERBEROS ...). Pour pouvoir gérer les sources de données multiples, le système sépare l'obtention des données utilisateurs de l'authentification.
Les données utilisateurs sont gérées par le Service « **Name Service Switch** » directement implanté dans la bibliothèque C du système. Ce service est disponible à partir de la version 6 de Libc. Il permet de définir un ordre de priorité dans l'obtention des sources de noms. Son fichier de configuration s'appelle généralement /etc/nsswitch.conf.

Exemple de configuration :

```
passwd:     files                   # Indique d'utiliser le fichier /etc/passwd
shadow:     files                   # Indique d'utiliser le fichier /etc/shadow
group:      files                   # Indique d'utiliser le fichier /etc/group
```

2.1.3 Gestion de la multiplicité des sources d'authentification.

A l'origine, les programmes de login (comme /bin/login ou ssh) utilisaient les informations fournies par NSS et authentifiaient les utilisateurs. Chaque programme était compilé avec les mécanismes d'authentification, ce qui posait un problème pour la prise en charge de nouvelles sources. En 1996, sont apparus les « **Pluggable Authentication Modules** » qui déportent la problématique d'authentification.

Chaque applicatif de connexion peut déporter son authentification sur PAM. Le comportement de son authentification est alors défini dans un fichier de configuration dans le répertoire /etc/pam.d. Elle peut utiliser un ou plusieurs modules, comme par exemple le module pam_unix pour l'authentification par fichiers, pam_LDAP pour l'authentification sur LDAP ou pam_krb5 pour l'authentification sur kerberos.

Exemple de fichier de configuration simple :

```
auth      required  pam_securetty.so
auth      required  pam_unix.so shadow nullok
auth      required  pam_nologin.so
account   required  pam_unix.so
password  required  pam_cracklib.so retry=3
password  required  pam_unix.so shadow nullok use_authtok
session   required  pam_unix.so
```

Je n'aborderai pas ici la configuration de PAM, qui est très bien documentée dans son manuel.

La modularité de PAM permet d'ajouter de nouvelles fonctionnalités au processus d'authentification, comme la vérification d'un One Time Password sur un appareil mobile grâce au module PAM pam_google_authenticator.so.

A noter que PAM ne s'occupe que d'authentification et s'appuie sur NSS pour obtenir les informations utilisateurs.

PAM ne fournit pas de mécanisme de type **Single Sign On** (SSO).

Le mécanisme le plus courant d'authentification SSO pour les systèmes est kerberos. Le module kerberos pam_krb5 est dédié à l'authentification initiale et n'accepte pas les tickets

kerberos. Les interfaces **« Generic Security Services Application Program Interface »** (GSSAPI) qui permettent l'authentification par l'intermédiaire de ticket kerberos ne sont pas implémentées dans PAM. [1]

Les spécifications X/Open Single Sign-On Service (XSSO) pour les modules PAM écrites en 1997 par l'« Open Group » n'ont pas été adoptées comme standard [3] [4]

2.1.4 Les types d'authentification les plus courants:

Les authentifications Nis et LDAP permettent d'obtenir les informations utilisateurs et d'effectuer l'authentification sur leurs annuaires respectifs.

L'authentification kerberos permet de s'authentifier sur un serveur kerberos.

L'authentification radius permet de s'authentifier sur un serveur d'accès réseau radius. Ce type d'authentification est plus généralement utilisé pour les accès wifi et vpn, mais est néanmoins accessible depuis des postes unix/linux.

Les authentifications kerberos et radius doivent être couplées avec un système complémentaire pour l'obtention des informations utilisateurs (LDAP ou fichier passwd).

L'authentification samba winbind permet d'effectuer l'authentification sur un annuaire microsoft Active Directory. Les informations utilisateurs proviennent également d'Active Directory, à l'exception des identificateurs utilisateurs et groupes (uidNumber et gidNumber) qui ne sont pas présents par défaut dans Active Directory.

Tableau II : Les modes d'authentification sur Unix, reliés avec les librairies NSS et les modules PAM

Système	Librairie NSS	Module PAM	Notes
Fichiers (1)	files	pam_unix	
OpenLdap (2)	LDAP	pam_LDAP	Libnss-LDAP, nscd ?
Kerberos	Files ou LDAP	pam_krb5	
Radius	Files ou LDAP	pam_radius_auth	
Active Directory	winbind	pam_winbind	

2.1.5 Niveau applicatif : les programmes d'authentification système :

Les **programmes de connexion** aux systèmes sont également pluriels, comme par exemple le

programme de connexion en ligne de commande /bin/login, les programmes de connexion distante Secure Shell (SSH) et les managers de connections graphiques comme gdm.
Le programme ssh est particulièrement important, puisqu'il permet de se connecter à distance sur les systèmes. Il sécurise les communications grâce à l'établissement d'un tunnel crypté. Il repose sur un protocole normalisé par l'Internet Engineering Task Force (IETF).
Le programme ssh utilise PAM, mais il accepte des types d'authentification différents comme l'authentification par clé publique ou l'authentification GSSAPI. Les informations utilisateurs sont toujours fournies par NSS.
L'**authentification par clé publique** repose sur les algorithmes de cryptographie asymétrique Rivest Shamir Adleman (RSA) et sur Digital Signature Algorithm (DSA). Cette authentification impose que la clé publique soit stockée dans le répertoire utilisateur (dans le fichier ~/.ssh/authorized_keys). L'utilisateur possédant la clé privée associée peut alors se connecter sans mot de passe via ssh. La sécurité est fortement améliorée car la clé privée ne transite jamais par le réseau, et elle peut être protégée par un mot de passe. La gestion des clés est cependant contraignante.
Ssh peut utiliser directement **les API « Generic Security Services Application Program Interface »** (GSSAPI). Ssh accepte alors les Ticket Granting Ticket comme preuve d'authentification et intègre une solution SSO basée sur Kerberos. (Voir chapitre sur Kerberos)

2.1.6 La gestion des autorisations.

La gestion des autorisations est, pour des raisons historiques, complètement décentralisée.
Elle peut être effectuée à différents niveaux avec des moyens différents.[1]

Au niveau **PAM**, elle est gérée grâce au module pam_access qui peut autoriser les connexions selon différents paramètres : le nom d'utilisateur, le nom du groupe, le réseau... Le module pam_nologin permet également d'interdire l'accès à un serveur aux utilisateurs non root.
Elle est également gérée **au niveau applicatif**, et chaque programme possède ses propres règles de contrôle d'accès. Le protocole ssh peut effectuer les mêmes contrôles que pam_access, avec notamment les directives AllowHosts et AllowUsers.
Les autorisations d'accès sont également gérées entre autres par les **pare-feux** et le système **TCP Wrapper**.

2.2 Authentifications sur les systèmes Windows :

2.2.1 L'authentification locale:

Les comptes locaux windows sont stockés dans le fichier C:\WINDOWS\system32\config\SAM

Pour des raisons de sécurité, le fichier est généralement encrypté par l'utilitaire Syskey. Une protection supplémentaire est assurée par le fait qu'il est impossible de copier ce fichier pendant que windows fonctionne. D'après mes tests, il est cependant accessible en utilisant des utilitaires de type fgdump.

Sur Windows XP, il possède la structure suivante :

```
Username:RID:LMHash:NTLMHash:::
```

Le RID est l'IDentifiant Relatif de l'utilisateur par rapport au contexte. L'identifiant complet étant le SID ou IDentifiant de Sécurité, qui contient l'identificateur de l'ordinateur et le RID.

Le mot de passe est stocké suivant deux hash différents.

• Le LMHash ou Lan Manager Hash est un ancien format développé par Microsoft qui possède actuellement un très faible niveau de sécurité et est désactivé sur les systèmes récents.

• Le NTLMHash est le hash du mot de passe utilisé par le protocole New Technology Lan Manager (NTLM).

Le protocole d'authentification NTLM est utilisé lors de l'authentification interactive et de connexions réseaux sur des systèmes Microsoft Windows. Il n'est utilisé que lorsque des postes de travail ne sont pas membres d'un domaine Active Directory, pour lesquels une authentification Kerberos est préférée. Il en est, actuellement, à sa deuxième version NTLMv2, la première est considérée comme faible au niveau sécurité.

C'est un protocole de type Challenge-Response où le mot de passe ne transite jamais par le réseau. Le serveur donne un challenge à décrypter au client, et celui-ci ne peut le faire que s'il connaît le bon mot de passe. La particularité étant que le challenge n'est pas crypté avec le mot de passe, mais avec le hash de celui-ci. [7] Le corollaire étant que le hash du mot de passe devient aussi critique que le mot de passe lui-même.

Le processus d'authentification est géré par le service « Security Account Manager »(isass.exe).

2.2.2 Authentification sur Active Directory

Lorsqu'on intègre un ordinateur à l'annuaire Active Directory, les utilisateurs présents sur cet annuaire peuvent s'authentifier sur le poste de travail. Ils bénéficient alors d'informations utilisateurs étendues qui incluent un répertoire de travail réseau et un profil itinérant. (Voir le chapitre sur Active Directory).
A noter que l'ordinateur possède alors un compte sur l'annuaire. Le mot de passe de ce compte est présent sous forme cryptée dans la base de registre de l'ordinateur. Ce mot de passe est changé périodiquement et automatiquement, à l'initiative du poste de travail.
L'authentification se fait par défaut en utilisant Kerberos, bien que les systèmes d'exploitation Serveurs actuels acceptent encore l'authentification NTLMv2.

2.2.3 Autres types d'authentification

Il n'est pas prévu par Microsoft d'autre type d'authentification. Pour pouvoir se connecter avec des sources d'annuaires externes, il faut utiliser des produits tiers comme **pgina**. Ce programme modifie le processus de connexion interactive et crée un compte utilisateur local temporaire lors de la réussite de l'authentification sur une source externe. Il permet de prendre en compte des authentifications LDAP, radius, mysql et même sur un serveur de mail.[8]
Il ne permet cependant pas de connexion par le réseau, ni ne peut intégrer des informations utilisateurs étendues (comme un répertoire de travail).

2.3 Les annuaires informatiques :

Les annuaires informatiques, à la différence des bases de données, sont mis à jour de manière épisodique et doivent être plus performants en lecture qu'en écriture.

2.3.1 L'annuaire Network Information Service (NIS) :

C'est un système client/serveur développé par Sun MicroSystems en 1985 qui permet de partager un ensemble de fichiers de configuration communs. Ce système est principalement utilisé pour partager les fichiers de configuration passwd et group, mais peut également être utilisé pour les partages réseaux et les hostnames.
Il repose sur des « démons », ypserv sur le serveur et ypbind sur le client. Les deux « démons » utilisent les Remote Procedure Call (RPC), et le processus rpcbind doit tourner sur l'ensemble du parc.

Sur le client : Les informations utilisateurs sont fournies par nss, et le fichier /etc/nsswitch.conf doit être configuré. L'authentification est gérée par le module pam pam_unix.so au même titre que l'authentification par fichiers..
Concrètement, ce système ne permet de gérer des fichiers de configuration que sur un ensemble de serveurs et permet qu'ils soient répliqués dans l'ensemble d'un parc informatique. Il est cependant conçu pour tourner sur un parc de petite taille, et souffre de problème de sécurité au niveau réseau. Les hash des mots de passe sont envoyés en clair sur le réseau, et qui plus est dans un format ancien (DES).
Malgré son ancienneté, il existe encore de nombreux annuaires NIS à l'heure actuelle. La raison en est souvent qu'il faut également revoir les informations utilisateurs et l'architecture nfs lors de son abandon. [5] [6]

2.3.2 Les domaines Microsoft windows NT

Les domaines windows NT permettent de centraliser les bases de données SAM. Ils sont installables sur des serveurs Windows NT. Une réplication de type maître esclave est possible entre un Primay Domain Controller ou PDC et un Backup Domain Controller ou BDC.
Les mots de passe étaient hashés en LMHASH pour des clients Windows 95 et 98, en NTLM pour des clients Windows NT 3.5. Le hashage a évolué en NTLMv2 à partir du Service Pack 4.
A noter que les domaines windows NT sont considérés obsolètes depuis l'année 2000 et l'apparition de Windows 2000 Server.

2.3.3 La norme X500

C'est une norme pour normaliser les annuaires informatiques, écrite en 1991. Elle a été définie par l'Union Internationale des Télécommunications avec comme partenaire l'International Organization for Standardization (ISO). Cette norme incluait entre autres le Directory Access Protocol (DAP). L'objectif principal était de normaliser les services d'annuaires nécessaire à la messagerie X400.
Ces protocoles avaient pour particularité de reposer sur les couches du modèle OSI, ce qui a poussé l'émergence d'alternatives incluant LDAP reposant sur la pile réseau TCP/IP.

2.3.4 Le protocole Lightweight Directory Access Protocol (LDAP) :

Le protocole LDAP à été écrit en 1995 pour pouvoir faire fonctionner des services d'annuaires sur des réseaux TCP/IP tout en respectant au maximum les normes X500.[20]

En 1997, la version 3 du protocole LDAP est devenue une norme établie par l' Internet Engineering Task Force (rfc 3377) en intégrant notamment le framework d'authentification « Simple Authentication and Security Layer »(SASL).

Le protocole définit cinq modèles

• Le modèle d'information: Il est composé de schémas qui définissent une liste d'objets et d'attributs. Par exemple l'objet InetOrgPerson (objectclass) définit une entrée pour une personne et possède des attributs : commonName (cn) ; surname (sn)

• Le modèle de nommage décrit une organisation hiérarchique des données à l'aide d'un Directory Information Tree.

• Le modèle fonctionnel décrit comment accéder aux données. Par exemple une fonction de recherche prend en compte la base ou nœud de départ, l'étendue, le filtre et la liste des attributs à retourner.

• Le modèle de sécurité décrit les contrôles d'accès et les méthodes d'authentification. L'authentification peut être anonyme, basique (le mot de passe passe en clair sur le réseau à moins qu'un cryptage SSL ou TLS soit mis en place), ou SASL. Voir le chapitre 2.5 pour plus d'informations.

• Le modèle de répartition définit comment l'annuaire peut être réparti entre plusieurs serveurs.[22]

Il est également d'usage d'utiliser le format de fichier LDAP Data Interchange Format ou LDIF pour modifier ou afficher le contenu d'un annuaire LDAP. Ce format a été défini dans le rfc 2849.

2.3.5 Les implémentations du protocole LDAP :

La première implémentation du protocole LDAP a été faite à l'Université du Michigan en 1996. L'historique des annuaires LDAP est riche et complexe. On peut éventuellement se référer aux travaux de Bill Nelson [19] pour suivre l'évolution dans le temps des annuaires. J'intègre une copie de son historique dans l'annexe VII.

Un grand nombre d'annuaires implémente le protocole LDAP. Nous allons en étudier quelques-uns.

2.3.5.1 OpenLdap :

OpenLdap est une implémentation open-source et gratuite du protocole LDAP qui fait référence dans les annuaires LDAP. C'est une implémentation généraliste de LDAP qui permet également de faire de l'authentification système. Elle ne dispose pas d'interface graphique.

OpenLdap repose sur plusieurs types de **backend**. Le rôle du backend est de stocker et de retrouver les données lors de requête LDAP.

Les plus utilisés sont :

• Le backend bdb reposant sur la base de données berkeley db.

• Le backend hdb qui est une version optimisée du backend bdb. (optimisation de la durée d'écriture, diminution de la redondance d'informations)

Des composants logiciels, les **overlay**, peuvent permettre de modifier le comportement des back end. Par exemple :

• L'overlay unique permet d'assurer l'unicité d'un attribut.

• L'overlay contraint permet de contrôler la valeur d'un attribut à l'aide d'une expression régulière.

La configuration, dans les versions récentes est dans un backend spécial (cn=config), accessible par le protocole LDAP , ce qui permet une modification des paramètres sans redémarrage du processus.

La **réplication** est effectuée à l'aide de l'overlay syncrepl. La réplication est de type maître – esclave où c'est l'esclave qui va initier la réplication. Deux modes sont possibles

• refreshAndPersist où l'esclave récupère en continu les modifications apportées au maître.

• refreshOnly où la réplication est périodique.

Il est également possible de faire de la réplication multi-maître grâce à une configuration spéciale de syncrepl, la synchronisation du temps entre les maîtres étant alors un élément critique. [21]

Pour pouvoir utiliser l'annuaire openldap pour de l'**authentification sur système unix**, il est nécessaire d'utiliser des classes particulières pour implémenter les utilisateurs et les groupes.

Les utilisateurs doivent implémenter la classe posixAccount et éventuellement la classe shadowAccount pour une politique sécurisée du mot de passe (expiration,...)

Les groupes doivent implémenter la classe posixGroup.

Exemple : Description de la classe posixAccount telle qu'on la voit dans le schéma NIS.

objectclass (1.3.6.1.1.1.2.0 NAME 'posixAccount' DESC 'Abstraction of an account with

POSIX
attributes' SUP top AUXILIARY MUST (cn $ uid $ uidNumber $ gidNumber $ homeDirectory) MAY (userPassword $ loginShell $ gecos $ description))

L'authentification peut être déportée sur un mécanisme d'authentification externe grâce à la procédure **« SASL PassTrough Authentication »**. Techniquement, ceci nécessite que l'annuaire LDAP soit compilé pour prendre en compte ce mécanisme, la présence d'un processus système supplémentaire nommé saslauthd, et que le mot de passe de l'utilisateur commence par la chaîne « {SASL} ». Les principaux mécanismes d'authentification pris en compte sont LDAP et kerberos.

2.3.5.2 Active Directory :

Active Directory (AD) est un annuaire commercial de Microsoft orienté système qui permet de recenser des utilisateurs et des ordinateurs d'un réseau. Il intègre diverses technologies telles qu'un annuaire LDAP, un serveur kerberos et un serveur DNS.
C'est un annuaire d'une grande extensibilité qui permet de gérer les besoins d'un réseau local à ceux d'une entreprise multinationale. Le serveur LDAP utilise un protocole propriétaire qui ne respecte que partiellement le protocole LDAP.
Il s'appuie sur une structure logique particulière : Un annuaire AD est assimilé à une forêt et peut être composé d'arbres, de domaines, de sites et d'unités d'organisations.
Une **forêt** est une frontière de sécurité, tous les domaines qui sont à l'intérieur établissent par défaut des relations de confiance (d'approbation dans la terminologie Microsoft).
Dans une forêt, il existe au moins un catalogue global qui contient une copie des attributs les plus utilisés de tous les objets AD de la forêt.
Une forêt peut être composée de plusieurs **arborescences de domaines (arbres)** qui posséderont des noms différents : Par exemple un arbre cnam.fr et un arbre ipst.fr.
Un arbre peut être composé d'un ou plusieurs domaines. Il aura alors un domaine racine et éventuellement des domaines enfants. Par exemple toulouse.cnam.fr.
Un **domaine** est une frontière administrative pour les objets présents. Les objets d'un domaine seront répliqués entre les différents contrôleurs de domaine qui l'administrent. La réplication est de type multi-maître, bien qu'un des contrôleurs de domaine possède certains privilèges, comme celui de contrôler la distribution des Rid des objets aux autres contrôleurs.

Un domaine peut être séparé en plusieurs **sites**, qui représentent des entités géographiques qui peuvent être reliées entre elles par des liens réseaux de moins bonne qualité. Pour faciliter la recherche sur les objets de la forêt, il peut être alors intéressant de mettre un catalogue global sur le site distant.
Il est également possible d'établir des **relations d'approbations** entre des forêts différentes, pour que les utilisateurs d'une forêt A puissent utiliser les ressources de la forêt B. La relation peut être monodirectionnelle ou bidirectionnelle, transitive ou non transitive. [9]
Une relation d'approbation peut, aussi, être faite avec un royaume Kerberos implémenté sur version Mit ou Heimdal. Cette solution est notamment utilisée pour unifier le mot de passe entre le monde Windows Active Directory et les annuaires openLdap. [12], [13], [14].
Le compte utilisateur dans AD doit posséder un attribut supplémentaire nommé altSecuritiesIdentities. Il sera de la forme{Kerberos} principalKerberos@RoyaumeKerberos et fait le lien avec le principal du royaume Kerberos.

Il faut faire attention à l'encryptage du ticket kerberos qui doit être compris par l'ensemble des acteurs de l'authentification (serveur kerberos, serveur ad, postes de travail).Les types d' encryptions ne posent cependant plus de problèmes avec des systèmes windows « modernes » : windows 7, Windows 2008,..

Il est également possible d'effectuer des délégations de contrôle dans le but de décentraliser l'administration de l'annuaire.
C'est aussi un annuaire qui intègre des outils de gestion de parc informatique, comme le déploiement de stratégies de sécurité et l'installation de logiciels. Il s'interface également avec d'autres logiciels Microsoft comme Windows Deployment Services ou Microsoft Exchange.
L'authentification des utilisateurs s'effectue par défaut par le serveur Kerberos, bien qu'il soit encore possible d'utiliser l'authentification NTLMv2. L'utilisation de Kerberos fournit une solution d'authentification Single Sign On entre les différents ordinateurs, serveurs de fichier et bases de données qui composent l'Active Directory.
Active Directory permet également de gérer les autorisations de connexion par la mise en place de stratégie de groupes.
La Procédure de changement de mot de passe nécessite un mot de passe en clair. Il est impossible de synchroniser le mot de passe avec le hash d'un mot de passe provenant d'un

autre annuaire.[34]

2.3.5.3 389 Directory Server:

Historiquement, 389 Directory Server (anciennement nommé Fedora Directory Server) est le successeur de Netscape Directory Server, l'un des premiers successeurs de l'annuaire original de l'université du Michigan.

Il possède beaucoup de points communs avec openLdap.

Les différences notables sont :

- Un modèle de réplication multi-maître.
- Une interface graphique
- Effectue la synchronisation des comptes et des mots de passe avec Microsoft Active Directory.

L'annuaire 389 Directory Server est un logiciel open-source et gratuit développé par le projet Fedora. Le projet Fedora est notamment l'auteur de la distribution linux Fedora et est soutenu par la société Red Hat. Il est installable sur l'ensemble des distributions linux. A noter que la société Red Hat vend une version commerciale du produit nommé « Red Hat Directory Server » qui comprend une assistance technique.

Figure 6 : Synchronisation des mots de passe entre Active Directory et 389 DS (source [23])

Fonctionnement de la synchronisation des mots de passe :
.AD vers LDAP : Installer un programme client PassSync.msi dans Active directory ... Le programme récupère le mot de passe lors du changement dans l'AD par ctrl alt suppr et le synchronise avec celui de 389 DS.
LDAP vers AD : La commande ldappasswd peut modifier le mot de passe dans l'AD. Car l'utilisateur tape le mot de passe en clair à ce moment.
UserPassword est crypté dans l'annuaire LDAP(pour des raisons de sécurité). Modifier directement cet attribut ne modifiera pas le mot de passe dans l'AD. (AD n'accepte pas de mot de passe crypté)

2.3.5.4 Free Ipa

C'est une solution de management d'identités qui repose sur l'intégration de différents composants open-source. Elle intègre un annuaire 389 directory server, le serveur Mit Kerberos, le serveur dns bind, un service de certificats ainsi que le composant winbind de samba 4. Il existe de la même manière que 389 directory server, une version gratuite provenant du projet Fedora et une version payante avec support de red hat.
Le point fort de free ipa est sa facilité d'installation et son intégration des différents composants.
Il permet également, en utilisant winbind et une relation d'approbation avec active directory, d'offrir aux utilisateurs windows de pouvoir se connecter aux postes et serveurs linux clients de freeipa. Cette facilité repose sur une génération d'un uidNumber et gidNumber pour les comptes windows.
La réciproque n'est pas vraie, c'est à dire les utilisateurs linux ne peuvent pas se connecter sur les postes windows, et les postes windows ne peuvent pas s'authentifier directement sur le serveur freeipa.

FreeIpa intègre également un système de contrôle d'accès aux systèmes.
FreeIpa est un annuaire dédié authentification système et il impose une certaine architecture à l'annuaire ainsi qu'aux objets de celui-ci : L'annuaire est plat et ne comporte pas d'unité d'organisation, les objets utilisateurs doivent implémenter un certain nombre de classes dont la classe ipaobject. [24]

2.4 L'interopérabilité avec Windows pour Linux et Unix

2.4.1 Samba 3

Samba est un ensemble de logiciels pour Linux et Unix qui permettent différentes actions :

- La transformation d'un poste linux en serveur de fichiers pour des postes Windows en implémentant le protocole SMB/CIFS
- L'émulation d'un domaine Windows NT, le serveur Samba joue alors le rôle de PDC.
- L'intégration dans Active Directory en tant que serveur membre.
- L'authentification du poste linux sur Active Directory en utilisant le « démon » winbind.

Lorsqu'il est configuré comme **contrôleur de domaine**, Samba 3 peut stocker sa base de données soit dans des fichiers, soit dans un annuaire OpenLdap.
Samba 3 n'intègre pas de mécanisme de réplication, mais peut profiter du mécanisme de LDAP pour offrir un système maître-esclave [27]
L'intégration de Samba dans LDAP est intéressante car elle peut permettre de fournir un serveur d'authentification pour des postes windows et linux. Il faut que les utilisateurs présents dans l'annuaire soient créés en implémentant les classes posixAccount et sambaSamAccount. Les postes windows authentifiés pourront également accéder à un espace de stockage fourni par le protocole SMB. Cependant l'authentification se fera par NTLMv2 uniquement, et les postes ne profiteront pas de l'apport des stratégies de groupes pour la gestion des systèmes.

Le service **winbind** est implémenté grâce à un « démon ». Celui-ci fournit les informations utilisateurs à NSS et effectue l'authentification par l'intermédiaire d'un module PAM. Winbind peut être configuré de plusieurs manière pour l'obtention des valeurs uidNumber et gidNumber.

- Génération à la demande et stockage dans un fichier local.
- Calcul à partir du Rid de l'utilisateur windows, permettant d'avoir des valeurs déterministes.
- Utilisation des valeurs présentes dans l'Active Directory. A partir de windows 2008, les annuaires Microsoft intégrent par défaut les attributs nécessaires.(RFC 2307)

L'authentification par défaut utilise le mécanisme Simple and Protected GSSAPI Negotiation Mechanism (SPNEGO). Ce mécanisme teste l'authentification ntlmv2 puis l'authentification

kerberos. Il est évidemment préférable d'utiliser l'authentification kerberos en désactivant ntlmv2 sur les serveurs Windows. [26]

2.4.2 Samba 4

La version 4 de samba a pour objectif une interopérabilité complète avec les annuaires Active Directory. Elle intègre donc un serveur Kerberos, un annuaire de type LDAP et un serveur DNS.

L'annuaire utilise un moteur LDB qui, identiquement à Active Directory, n'est pas complètement conforme au protocole LDAP. Il n'est donc plus possible d'utiliser le même serveur pour utiliser une solution d'authentification native Linux et Windows comme c'était le cas avec Samba 3.

Le but de Samba 4 est de fournir une solution open-source de contrôleur de domaine pouvant s'intégrer avec un domaine Active Directory. A l'heure où j'écris ces lignes, il manque encore cependant quelques fonctionnalités par rapport à la solution Microsoft : Un serveur samba ne peut approuver un domaine extérieur, le développement de l'interface graphique a été abandonnée, et la réplication des partitions Sysvol (contenant les stratégies de groupes et divers scripts) ne peut être émulée qu'avec la commande rsync. La version 4.1 apporte la compatibilité avec windows Server 2012, et notamment son protocole de fichier SMB3. [28]

2.4.3 System Security Services Daemon (sssd) :

Ce projet était à l'origine intégré à FreeIpa, mais est devenu autonome. C'est un démon pour machines linux qui permet d'accéder à des sources d'identités et d'authentification externes.

Il est composé d'un module NSS et d'un module PAM qui agissent uniquement en communiquant avec le « démon ». C'est ce dernier qui effectue tous les contrôles.

Il permet de relier les machines avec différents back ends, dont openldap, kerberos, active directory et IPA et se présente donc comme un système de management d'identités côté client.

Il utilise un système de cache persistant, qui permet de faire de l'authentification hors ligne.

Il supporte également les approbations Kerberos « cross-realm ».

Pour l'authentification sur Active Directory, il peut utiliser deux méthodes d'authentification pour obtenir les identités de l'annuaire :

• Par SASL/GSSAPI, ce qui implique que l'ordinateur soit membre du domaine pour pouvoir s'identifier. Cette méthode repose donc sur samba winbind et est préférable.
• Par authentification classique en fournissant un login et un mot de passe d'un compte autorisé à lire dans l'annuaire.
A défaut de présence des attributs nécessaires dans Active Directory, ssd peut également faire du mapping d'uidNumber et gidNumber d'une manière proche de winbind.[35]

2.5 Les serveurs d'authentification :

2.5.1 Kerberos

Kerberos est un système d'authentification dont l'origine provient du projet Athena du Massachusetts Institute of Technology (MIT) en 1980. C'est une référence en terme d'authentification et il est implémenté dans l'ensemble des systèmes d'exploitation actuels. Il permet un mécanisme d'authentification Single Sign On entre des ressources informatiques d'une même entité. Le mot de passe ne transitant pas par le réseau, il est d'une grande sûreté même dans des environnements réseaux hostiles. Il permet également d'assurer que les ressources sur lesquelles on cherche à se connecter sont bien les bonnes par un mécanisme d'authentification mutuelle. A noter que Kerberos ne s'occupe que d'authentification, et ne fournit aucune des informations utilisateurs nécessaires à la connexion sur un système d'exploitation. Il doit donc être couplé dans ce cas là avec une source externe d'information, comme un annuaire LDAP. Le serveur Kerberos peut également être utilisé comme source d'authentification par les serveurs réseau (Radius) ou web (CAS, Shibboleth)

L'authentification repose sur la notion de Royaume, frontière administrative où le serveur fait autorité pour authentifier les ordinateurs hôtes, les services et les utilisateurs. Il est également possible d'établir des relations d'approbations entre différents Royaumes, entre entités se faisant confiance. Les entrées dans la base de données d'authentification sont nommées des principaux Kerberos. Elles sont de la forme Name[/Instance]@REALM pour les utilisateurs, et Service/Hostname@REALM pour les services. Par exemples : util1@REALM pour un utilisateur standard, admin1/admin pour un administrateur et host/serveur1.domain.fr@REALM pour un service.

L'authentification Kerberos se passe entre trois composants : le Key Distribution Center (Kdc), le client et le serveur d'application. Dans le but d'assurer la sécurité du système, les opérations d'authentification sont relativement complexes, nous allons simplement aborder le processus : [15]

Figure 7 : Les opérations d'authentification kerberos (source [13])

La requête initiale AS_REQ est non encryptée, elle comprend essentiellement le principal du client.
La réponse AS_REP comprend une partie cryptée par la clé secrète du client (notée KUser) et donc décryptable par lui, et une partie cryptée par la clé secrète du Ticket Granting Server (KTGS) : Le Ticket Granting Ticket (TGT)
AS_REP = { PrincipalService , Timestamp , Lifetime , SKTGS }KUser { TGT }KTGS
Les deux composants contiennent une clé de session (notée SKTGS) qui est une suite de caractères aléatoires.
Si l'authentification réussit, le client décrypte sa partie,stocke la clé de session et le TGT.

Le client désire accéder à un service, il ne possède pas encore le ticket nécessaire. Il s'adresse alors au TGS par l'intermédiaire d'une demande TGS_REQ

Cette demande contient un champ Authenticator qui est le principal du client et un timeStamp, le tout crypté par la clé de session, ainsi que le TGT
TGS_REQ = (PrincipalService , Lifetime , Authenticator) { TGT }KTG
Le TGS décrypte le TGT et en extrait la clé de session. Il s'en sert pour décrypter l'Authenticator et vérifie que le timeStamp est dans la fourchette du temps autorisé.
Il fournit alors une réponse TGS_REP qui contient une partie cryptée par la clé de session et une partie cryptée par la clé secrète du service demandé : Le Service Ticket. Les deux composants contiennent également une suite de caractères aléatoires qui servira à la communication entre le client et le service : la clé de service
TGS_REP = { PrincipalService , Timestamp , Lifetime , SKService }SKTGS { TService } KService

Le client envoie alors une requête au serveur d'application qui contient, de la même manière que le TGS_REQ , un Authenticator crypté par la clé de service, ainsi que le ticket de service
AP_REQ = Authenticator { TService }KService

Il existe plusieurs implémentations du protocole dont les plus connus sont MIT Kerberos, Heimdal Kerberos et Active Directory. L'implémentation Heimdal a débuté en Suède en réponse à une loi américaine restreignant l'exportation de logiciels cryptographiques. La loi américaine (Export Administration Regulations Title 15 chapter VII, subchapter C) a été depuis considérablement adoucie, même s'il existe encore quelques restrictions.

Le contenu peut être stocké dans une base de données locale, ou dans un annuaire LDAP. La réplication de la base de données entre des serveurs kerberos multiples est de type maître-esclave. Lors de l'utilisation d'un annuaire LDAP, le mécanisme de réplication est celui de l'annuaire, et peut donc être paramétré en mode maître-esclave, ou en mode multi-maître. A noter que la surface d'exposition des serveurs LDAP et des serveurs Kerberos peut être différente, et que la réflexion sur politique de sécurité doit suivre. [13]

2.5.2 Les mécanismes d'utilisation de Kerberos :

Il existe différentes implémentations de Kerberos dont les API n'ont pas été standardisés. Pour résoudre ces difficultés, il existe les api **« Generic Security Services Application Program**

Interface » ou GSSAPI, interfaçant les applications avec les mécanismes de sécurité. Dans la pratique GSSAPI est presque exclusivement utilisé pour interfacer les serveurs Kerberos. Cette interface accepte les TGT de Kerberos et est implémentée par exemple dans le « démon » ssh. GSSAPI est un standard de l'IETF référencé dans le RFC2743.

Le framework d'authentification **Simple Authentication and Security Layer** (SASL) apporte une interface structurée entre des protocoles et des mécanismes. Comme défini dans le rfc 4422, l'objectif de SASL est de permettre à de nouveaux protocoles d'utiliser des mécanismes existants et de permettre à des protocoles existants d'utiliser de nouveaux mécanismes, sans redéfinir le protocole.

Figure 8 : Le framework SASL (source rfc 4422)

Il permet d'interfacer les API GSSAPI et est notoirement implémenté dans le protocole LDAP.

Une autre approche dans l'utilisation de GSSAPI est par le biais de l'utilisation du mécanisme « **Simple and Protected GSSAPI Negotiation** » plus connu sous son abréviation SPNEGO.
Le mécanisme est un standard de l'IEF référencé dans la rfc 4178. Il permet de déterminer quels mécanismes GSSAPI sont disponibles, et de les tester, les uns après les autres.
Les principaux utilisateurs de SPNEGO sont les systèmes Microsoft et permettent d'effectuer une négociation entre les protocoles NTLM et Kerberos, lors de l'authentification système sur Active Directory. Le mécanisme Spnego de Microsoft utilise des extensions et est documenté sur le site de l'éditeur.[10]

L'authentification Spnego est également utilisée lors de l'authentification HTTP par l'intermédiaire de navigateur internet. Elle est documentée dans la RFC 4178. [40] Le premier navigateur utilisant le mécanisme Spnego est Internet Explorer de Microsoft, mais les navigateurs les plus courants implémentent actuellement ce mécanisme (Firefox, Chrome...). Ceci permet notamment d'utiliser un ticket Kerberos lors d'une procédure d'authentification web.

Figure 9 : utilisation de spnego lors d'une authentification HTTP (source [11])

2.5.3 L'authentification réseau avec radius :

Radius (Remote Authentication Dial-In User Service) est un protocole d'authentification client serveur répondant principalement aux besoins d'authentification d'éléments réseaux comme des commutateurs, des points d'accès réseau sans fil ou des serveurs d'accès distant. Ces clients Radius peuvent également être appelés Network Access Server (NAS) ou Authenticator dans la terminologie 802.1x ou EAP et permettent d'accéder au réseau de l'entreprise.

La dernière version normalisée par l'IETF du protocole RADIUS date de 2000 (RFC 2865 et 2866).

Le protocole Extended Authentication Protocol EAP est un framework d'authentification qui est déployé sur les points d'accès au réseau. Il s'occupe de la négociation avec le demandeur (supplicant) et peut résoudre les requêtes d'authentification qu'il comprend. Il peut également s'appuyer sur un serveur d'authentification Radius pour les traiter.

Les serveurs Radius récents supportent le protocole EAP. [41]

La norme 802.1x de l'IEEE définit l'encapsulation du protocole EAP dans un réseau local.

Figure 10 : Authentification wifi utilisant les protocoles 802.1x, EAP et Radius (source [25])

Le protocole Radius implémente le protocole AAA signifiant Authentication, Authorization et Accounting. Les concepts d'authentification et d'autorisation sont similaires à ceux de l'authentification système.

L'Accounting permettant la traçabilité de la consommation des ressources réseaux pouvant donc conduire à une facturation. Le serveur Radius peut authentifier les utilisateurs lui même ou s'appuyer sur un autre système d'authentification comme LDAP, Active Directory,

Kerberos ou un autre serveur Radius. A noter que dans le cas d'une authentification Kerberos, le Ticket Granting Ticket obtenu n'est pas transmis au Supplicant. Ce cas de figure n'est pas prévu par le protocole Radius, et interdit de fait une authentification SSO.

Il existe de nombreuses implémentations du protocole dont les plus connues sont la version open source FreeRadius et Steel-Belted Radius Enterprise Series de la société Juniper. Le système d'exploitation Windows Server intègre également un rôle Radius. Le protocole connaît un successeur qui a comme nom Diameter (le diamètre est le double d'un rayon écrit radius en anglais). Celui – ci n'est pas encore adopté car n'est pas implémenté dans les matériels les plus anciens.

2.5.4 L'authentification web :

L'authentification web classique repose sur le protocole HTTP. Le type d'authentification est paramétrée sur le serveur web. Les types les plus courants sont

- basic : le mot de passe transite en clair à moins que la communication ne soit encryptée par SSL.
- Digest : Utilise des fonctions de hashage md5
- Spnego : Negociation entre une authentification NTLM et Kerberos
- Par certificats

Les serveurs web peuvent également déléguer l'authentification à des serveurs externes (Bases de données ou annuaires LDAP) et procéder à des filtres d'autorisations.

Figure 11 : Authentification Basique au travers du protocole HTTP

L'authentification web SSO est une problématique assez ancienne qui permet à l'utilisateur de ne s'authentifier qu'une seule fois pour un ensemble de sites web utilisant le même référentiel.
La première approche de SSO s'est effectuée par l'intermédiaire des cookies, informations naviguant dans les entêtes des pages HTTP. Le logiciel emblématique de ce type d'authentification est Central Authentication Service (CAS).
Le protocole Security assertion markup language (SAML) a permis par la suite de fédérer des identités provenant de multiples fournisseurs, ainsi que d'échanger des attributs entre les applications et les fournisseurs. Le logiciel shibboleth en est une référence dans le monde universitaire.
Les applications grand public se sont tournées dans un premier temps vers les protocoles OpenId pour l'authentification et Oauth pour les autorisations. Les applications les plus populaires (Facebook, Twitter ,Google+...) implémentent actuellement le protocole Oauth V2

2.5.4.1 Authentification web sso avec CAS :

Le projet Central Authentication Server (CAS) est un système d'authentification originellement développé par l'Université de Yale (Etats-Unis). Il est maintenu depuis 2004 par le consortium à but non lucratif JASIG. CAS est gratuit et open-source.
CAS est dédié à l'authentification d'applications web dans un contexte SSO. Un utilisateur peut utiliser plusieurs applications web, en ayant besoin de s'authentifier une fois, uniquement.

Il existe également un module pam nommé pam_cas qui peut trouver son utilité pour l'authentification sur des serveurs SFTP accessibles via des navigateurs web.
CAS est écrit en Java et nécessite de s'exécuter dans une machine virtuelle Java par l'intermédiaire d'un conteneur de Servlet. (par exemple Tomcat)
Dans l'authentification CAS, les crédentials d'authentification sont gérés par le serveur CAS et les applications n'ont jamais accès à ces informations.

L'authentification se passe en quatre phases :

- Le client demande à se connecter à l'application.
- L'application génère une url pour l'authentification sur le serveur CAS.

  http(s)://cas_server/cas/login?service=http(s)://appli_server/application1

Si l'utilisateur ne possède pas de session SSO active sur ce serveur, le serveur demande un login et un mot de passe.

• Le serveur cas redirige une url vers le serveur d'application en indiquant un numéro de ticket de service

http(s)://appli_server/application1?ticket=ST-8670-123buTvFFjo980

• Le serveur d'application demande une validation du ticket au serveur CAS.

https://cas_server/cas/serviceValidate?service=http://other_server/application1&ticket=ST-8670-123buTvFFjo980

Le serveur CAS retourne un message XML contenant l'identifiant de l'utilisateur.

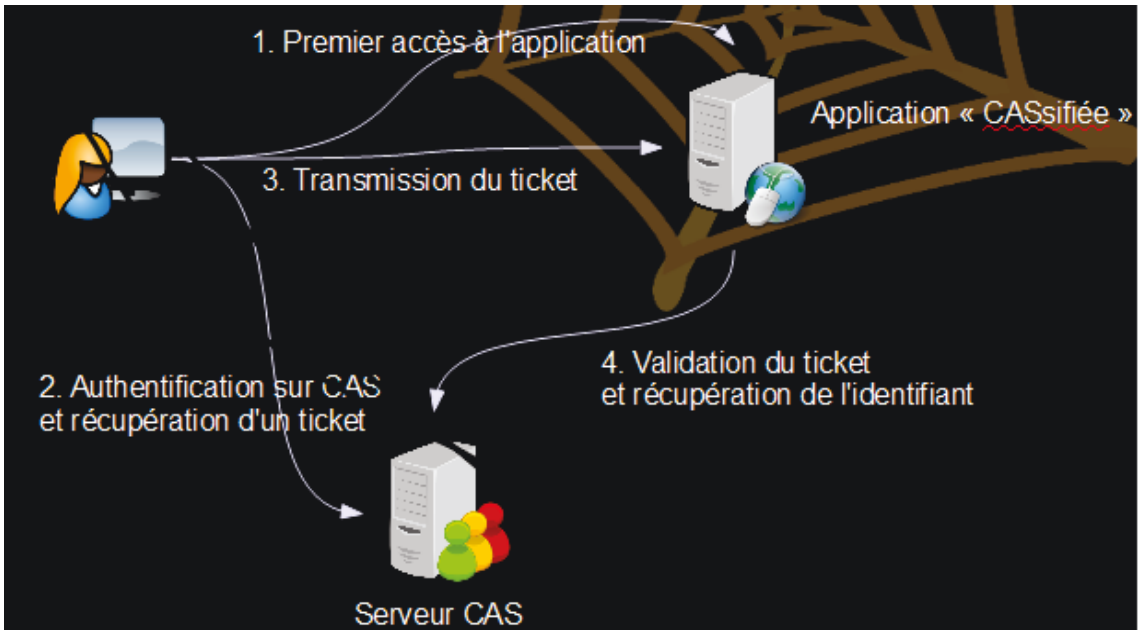


Figure 12 : Cinématique d'authentification sur un serveur CAS (source [29])

Concernant le référentiel d'authentification des utilisateurs, il peut être stocké dans une base de données sur le serveur CAS, ou déporté sur un autre système d'authentification comme LDAP ou Radius.

Le serveur CAS peut également utiliser le mécanisme SPNEGO pour authentifier les utilisateurs par l'intermédiaire de leur ticket TGT. Il doit intégrer le royaume Kerberos et posséder un principal de service ayant la forme HTTP/casserver@ROYAUME. Le navigateur web doit être également configuré pour fournir le TGT lors de la demande d'authentification.

La version 3 de CAS permet également, de manière identique à Shibboleth, de partager des attributs utilisateurs avec les applications par l'intermédiaire du protocole SAML.

2.5.4.2 Le protocole SAML

Security assertion markup language (SAML) est un standard informatique reposant sur XML. Il définit un cadre sécurisé pour l'échange d'informations entre sites partenaires. SAML est un standard du consortium OASIS dont la dernière version date de 2005 (SAML v2).

La première utilisation de SAML v2 est le single sign on web, mais permet également d'autres cas d'utilisations comme des requêtes sur des attributs, la transmission de la demande à un autre fournisseur d'identités dans le cadre d'une fédération ou la mise en place du single sign off. SAML contient plusieurs composants imbriqués permettant de répondre aux différents besoins.

Les **assertions** contiennent des informations de sécurité qui peuvent être de trois types : Authentification, Attributs ou décision d'autorisation. Une assertion est entourée de balises XML <saml:Assertion …>... </saml:Assertion>
Les messages SAML sont échangés dans un **protocole** qui définit une requête et une réponse. Une requête commence par la balise <samlp:Request>
La couche **bindings** permet d'interagir avec les protocoles de communication existant comme par exemple HTTP ou SOAP.

Les **Profiles** définissent les combinaisons d'assertions, protocole et binding à utiliser pour un cas d'utilisation particulier.

Figure 13 : Imbrication des composants du protocole SAML

Le protocole SAML définit deux acteurs dans l'échange de messages :

« Identity Provider » ou fournisseur d'identités est le responsable du management d'identité. Il est le producteur des assertions SAML.

« Service Provider » ou fournisseur de service contrôle l'accès aux services et aux ressources.

Figure 14 : Fonctionnement de SAML2 dans un profil web sso avec échange d'attributs (source [30])

2.5.4.3 Shibboleth

Shibboleth est un logiciel open-source qui permet faire de l'authentification SSO pour des organisations hétérogènes. Shibboleth est gérée par un consortium dont les membres fondateurs sont Internet2, Janet et SWITCH. Ces entités sont également des consortiums regroupant des universités américaines, suisses et anglaises. Il est développé en Java et fonctionne grâce à un conteneur web de type Tomcat.
Il implémente le protocole SAML qui lui permet de partager des attributs et d'effectuer de la fédération d'identités.

La fédération d'identités permet à plusieurs organismes de mettre en commun leur fournisseurs d'identités pour l'authentification. Elle implique la mise en mise en place d'un nouveau service permettant à l'utilisateur d'indiquer son fournisseur d'identité d'origine. Ce service est nommé « Discovery Service » ou également WAYF (Where Are You From?) dans la version 1 de Shibboleth.

Figure 15 :Cinématique de l'authentification Shibboleth

Le Discovery Service peut être centralisé au niveau d'une fédération et fournir un sélecteur de fournisseur d'identités aux fournisseurs de services. La fonctionnalité « Centralized Discovery Service » de Shibboleth répond à ce besoin. Dans le domaine universitaire, le groupe d'intérêt public Renater fournit un Discovery Service centralisé aux Universités.

Le Discovery Service peut également être installé au côté du fournisseur de service. Ceci permet de le mettre en conformité avec la charte graphique et de ne présenter que les fournisseurs d'identités acceptés. Il existe plusieurs possibilités d'implémentation comme la fonctionnalité « Embedded Discovery Service » de Shibboleth ou le Wayf du consortium suisse Switch.
Il est également possible d'installer Shibboleth dans une configuration bilatérale entre un fournisseur d'identité et un fournisseur de service, sans inscription dans une fédération. Ceci peut permettre des coopérations inter-fédérations.

Le fournisseur d'identité peut déléguer l'authentification à des serveurs externes, par exemple un serveur LDAP ou un serveur CAS. De manière similaire au serveur CAS, il peut également accepter les TGT Kerberos obtenus lors de la phase d'authentification système. A l'heure actuelle, il faut compiler un plugin développé par le consortium Switch nommé « Kerberos-login-handler ».

Pour pouvoir profiter de l'authentification Sso et notamment des attributs fournis par le protocole SAML, les applications doivent être compatibles Shibboleth. Cette démarche est connue sous le terme de « Shibboliser » une application. [31]

2.5.4.4 L'authentification web grand – public :

Le premier essai pour faire de l'authentification web à grande échelle en utilisant des crédentiels internet a été effectué par Microsoft en 1999 avec son service Passport.

2.5.4.4.1 Le protocole openId :

En 2005, le protocole OpenId est apparu. Il permet de mettre en place un service de d'authentification décentralisé permettant de faire de l'authentification unique. Le modèle se pose sur des liens de confiance entre les fournisseurs d'identités openId et les fournisseurs de service.
Il est utilisé par des sites comme Google, Yahoo qui sont fournisseurs OpenId. Il existe également des fournisseurs d'identités OpenId externes qui n'offrent pas de contenu comme le site verysignlabs de Symantec. Il peut être couplé avec le protocole d'autorisation oauth version 1.

Figure 16 :Cinématique d'authentification avec un compte openId du fournisseur Google

2.5.4.4.2 Le protocole oauth 2:

En 2012 les spécifications du protocole d'autorisation Oauth v2 ont publiées comme standard par l'IETF dans la rfc 6749. Ce protocole permet à des propriétaires de ressources de déléguer l'autorisation d'accès à des fournisseurs d'identités tiers. Il utilise un mécanisme de pseudo authentification : Si l'utilisateur est autorisé d'accès, il est considéré comme authentifié de fait par le fournisseur. [32]

Figure 17 :Cinématique d'autorisation oauth 2 avec un compte Google

Le protocole possède beaucoup de composants optionnels, et il est peu probable que deux implémentations de oauth2 soient compatibles entre elles. Il est actuellement implémenté par Facebook,Twitter et Google. Ce dernier, bien qu'utilisant encore openId, préconise l'utilisation d'oauth2 aux développeurs d'applications.

Oauth 2 permet de mettre en place des mécanismes d'autorisation en applications, et par exemple de permettre à une application web d'émettre des tweets à la place de l'utilisateur.

Le protocole « OpenId Connect » est différent de openId. Il permet d'utiliser une surcouche au dessus de oauth2 permettant d'assurer l'authentification.

2.5.4.4.3 De l'utilité des réseaux sociaux pour les Universités.

Certaines Universités réfléchissent à la mise en place de passerelles entre l'authentification universitaire et celle en provenance des réseaux sociaux. [33] Les cas d'utilisation sont des applications web fournissant des services à des personnes externes à l'Université et nécessitant une authentification. Un groupe de travail du consortium Internet2 essaye notamment de mettre en place un fournisseur d'identité Shibboleth servant de passerelle avec les réseaux sociaux. Cette passerelle est actuellement un pilote.

Le groupe de travail est accessible sur le site https://spaces.internet2.edu/display/socialid/

Figure 18 :Vue d'ensemble de la passerelle « Social to Saml » (source Cirrus Identity)

2.6 Gestion des groupes avec Grouper

C'est un outil de gestion de groupes développé par le consortium internet2 qui permet de centraliser la gestion de groupes dans une base de données. Le développement de cet outil vient du constat que la hiérarchie de la gestion des groupes augmente au fur et à mesure que les services numériques augmentent. Il est de plus nécessaire de pouvoir déléguer la gestion de ces groupes, sans multiplier les accès en écriture sur un annuaire LDAP. Les utilisateurs pourront administrer leurs groupes dans grouper, mais c'est grouper qui aura la charge de mettre à jour les groupes dans l'annuaire LDAP. Ces groupes vont permettre de participer à la mise en place de mécanismes d'autorisation centralisés. [36]

Figure 19 :Les composants de Grouper

2.7 L'authentification forte :

L'utilisation d'un système Sso simplifie la vie des utilisateurs en leur permettant de ne retenir qu'un login et un seul mot de passe. Elle augmente cependant la problématique de sécurité lors d'un détournement du mot de passe par une action malveillante (phishing par exemple). La mise au point d'une authentification forte peut améliorer la sécurité.

Il n'existe pas de définition stricte de l'authentification forte. On peut cependant parler de niveau d'assurance (Level of Assurance) pour être sur que l'utilisateur est bien celui qu'il prétend être.

Le National Institute of Standards and Technology (NIST), une agence fédérale américaine, propose 4 niveaux d'assurances, permettant de calculer les risques lors d'une usurpation d'identités. Chaque niveau d'assurance peut proposer un mode d'authentification différent, avec notamment la mise en place d'une authentification multifacteurs.

Comme communément vu dans la littérature, les facteurs d'authentification utilisés appartiennent à trois types :
Ce que l'on sait: Mot de passe ,code Personal Identification Number (PIN), ...
Ce que l'on possède : Une carte à puce, un périphérique générant des One Time Password (OTP),...
Ce que l'on montre : empreinte biométrique.

Une authentification multi-facteurs peut donc regrouper différents modes d'authentification. Parmi les solutions courantes, nous avons l'exemple de la carte à puce protégée par un code pin, qui peut contenir également plusieurs facteurs comme des empreintes biométriques, un certificat X509... Les cartes d'identités de certains pays (par exemple la Belgique) contiennent des certificats X509 et peuvent être utilisées pour l'authentification sur certains sites gouvernementaux.
De nombreux sites webs (Google, Dropbox) proposent également une authentification multi-facteurs basée sur un mot de passe et un OTP.

Les OTP sont des mots de passe qui ne peuvent être utilisés qu'une seule fois. Il en existe plusieurs sortes dont ceux basés sur les messages SMS qui peuvent présenter des problèmes de sécurité en cas de présence de Trojan sur les téléphones portables.[39]
Le groupe « initiative for Open AuTHentication » ou OATH (formés par plusieurs compagnies dont Verisign et Symantec) a participé a l'élaboration de plusieurs RFC soumis à l'IETF concernant les OTP. [38] Voici les protocoles standardisés :

- HMAC-Based One-Time Password (HOTP), rfc 4226 :

Le mot de passe est généré à partir d'un compteur ainsi que d'une clé secrète partagé entre le serveur et le dispositif générateur d'OTP (token otp, application sur un smartphone,...)

- Time-Based One-Time Password (TOTP), rfc 6238 :

Le mot de passe est généré à partir d'une clé secrète partagée et est valide pour une courte durée. (30 secondes). Ceci implique que le serveur et le dispositif générateur d'OTP soient synchronisés.

- OATH Challenge-Response Algorithm (OCRA), rfc 6287 :

Le serveur présente un code qui doit être traité par un dispositif OTP qui générera la réponse.

Le dispositif OTP doit être programmé pour connaître le secret partagé avant de générer des OTP. Ceci peut se faire à la main, ou bien en scannant un code QR (Quick Response) dans le cas d'un smartphone. Des logiciels générateurs d'OTP implémentant les protocoles existent sur les smartphones, comme par exemple Google Authenticator ou Authy. Il existe également des systèmes sous formes portatives , ou de clés usb qui génèrent un otp lorsqu'on appuie sur un bouton. (Yubikey ou securId de RSA Security).

Le système d'authentification forte doit pouvoir s'intégrer dans l'existant, que ce soit au niveau pam, des applicatifs, mais aussi au niveau du serveur SSO Cas et Shibboleth. Google authenticator fournit, par exemple, un module pam. Le serveur Cas accepte un mécanisme OTP

Surfnet a également travaillé à intégrer le protocole SAML2 avec un système d'authentification OTP :

Figure 20 : Intégration d'authentification à deux facteurs avec le protocole SAML2 (source Surfnet)

2.8 Le management d'identités

Le management d'identités est l'ensemble des processus permettant d'allouer un identifiant aux utilisateurs membres du système d'information, de gérer le cycle de vie de cet identifiant, et fournir des services d'authentification associés.

Le management d'identités dans les Universités se fait, généralement, en agrégeant des données de sources multiples (base de données du personnel, des étudiants,...) dans un annuaire LDAP. Cette procédure est généralement effectuée par des programmes développés par les Universités.

Des nouveaux besoins sont pressentis par certaines Universités comme la possibilité de déléguer les procédures d'administration, la prise en compte de fournisseurs d'identités externes. Pour pouvoir y répondre, le cœur du système d'information est réorienté vers une base de données intermédiaire nommée « référentiel ». L'annuaire LDAP devenant un annuaire d'authentification comme un autre.[42]

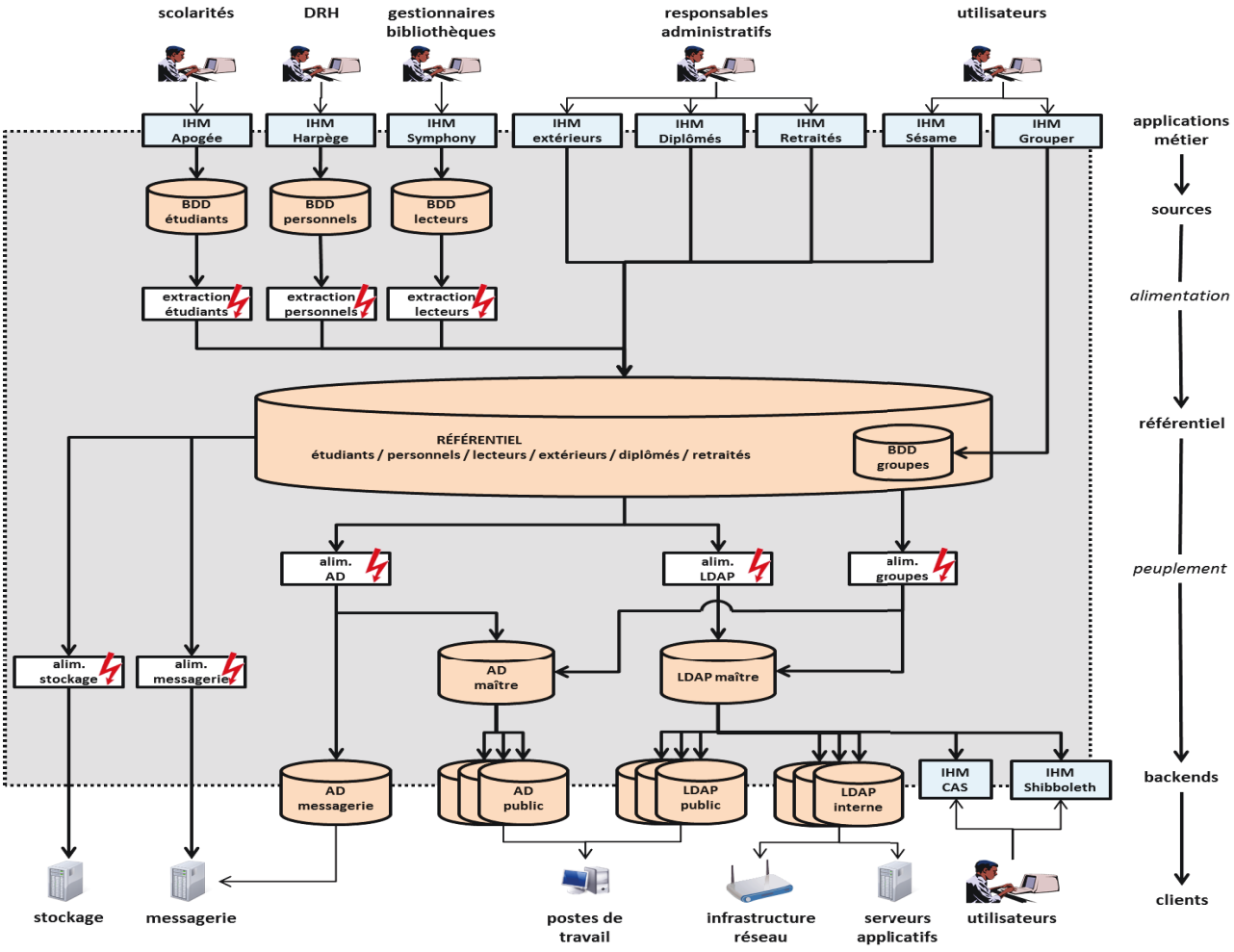


Figure 21 Architecture du futur système Sésame 2 de l'université de Rennes (source [42])

Les processus d'approvisionnement du référentiel peuvent être gérés par des logiciels spécialisés comme Talend Open Studio ou le framework de développement Java spécialisé

dans la gestion d'identités open IDM. La future solution de l'AMUE nommée prisme est également à ranger dans cette catégorie.

Les processus de gestion d'identités doivent également intégrer des solutions d'authentifications, parmi lesquelles nous pouvons citer :

- un mécanisme d'unification des logins et mots de passe, entre les postes de travail unix et windows.
- un mécanisme sso, destiné aux applications web reposant sur CAS, ou shibboleth.
- un mécanisme de fédération d'identités pour certaines applications web.
- un mécanisme de sso pour la connexion sur les serveurs unix, nécessitant l'utilisation des api GSSAPI sur les « démons » ssh, ainsi que la généralisation de kerberos.
- Un mécanisme de « true sso » permettant de ne s'identifier qu'une fois à la connexion sur un système et de ne plus s'authentifier à la connexion sur une ressource web. Ceci nécessite l'utilisation de kerberos au niveau des serveurs sso web (cas, ou shibboleth) ainsi qu'une configuration des navigateurs web.
- La mise en place de l'authentification forte

2.9 Authentification des éléments de stockage

Les baies de stockages fonctionnant en mode fichier, connues également sous le nom de Network Attached Storage (NAS), incorporent un système d'exploitation. Elles utilisent les fonctionnalités de celui-ci pour s'authentifier sur des serveurs externes. Le NAS exporte généralement les protocoles CIFS et NFS utilisés respectivement par les systèmes windows et linux. Les NAS peuvent unifier les données et les exporter à la fois en CIFS et NFS. Le constructeur Netapp est un précurseur de cette méthode. La première solution proposée est de mapper les identités des utilisateurs Active Directory dans les attributs de LDAP [44]. La deuxième solution est de se reposer sur Active Directory pour authentifier les utilisateurs sur les systèmes windows et linux. Les attributs des utilisateurs devront également comprendre les éléments nécessaires à la connexion sur les systèmes Linux. [45]

III Étude de l'existant

3.1 Les applications au cœur du Système d'Information

L'Université Paul Sabatier utilise les applications Harpege et Apogee, pour la gestion de ses personnels, ainsi que des étudiants de six facultés. Ce sont les deux bases principales qui alimentent le référentiel des utilisateurs. Il existe également une base de données « Invités » permettant d'intégrer les personnels extérieurs au Système d'Information de manière temporaire. Les informations provenant de ces bases sont agrégées dans un annuaire LDAP par une procédure logicielle appelée « sablage ». Elle insère les nouveaux comptes et supprime les anciens par l'intermédiaire de commandes unitaires de type « ldapadd ». A cette occasion, un identifiant unique est généré par un algorithme prenant en entrée le nom et le prénom de l'utilisateur.

3.2 L'annuaire LDAP de l'Université :

L'architecture LDAP repose sur 3 machines virtuelles :un annuaire maître et deux replicats. L'ensemble repose sur une infrastructure Xen utilisant la réplication DRBD.

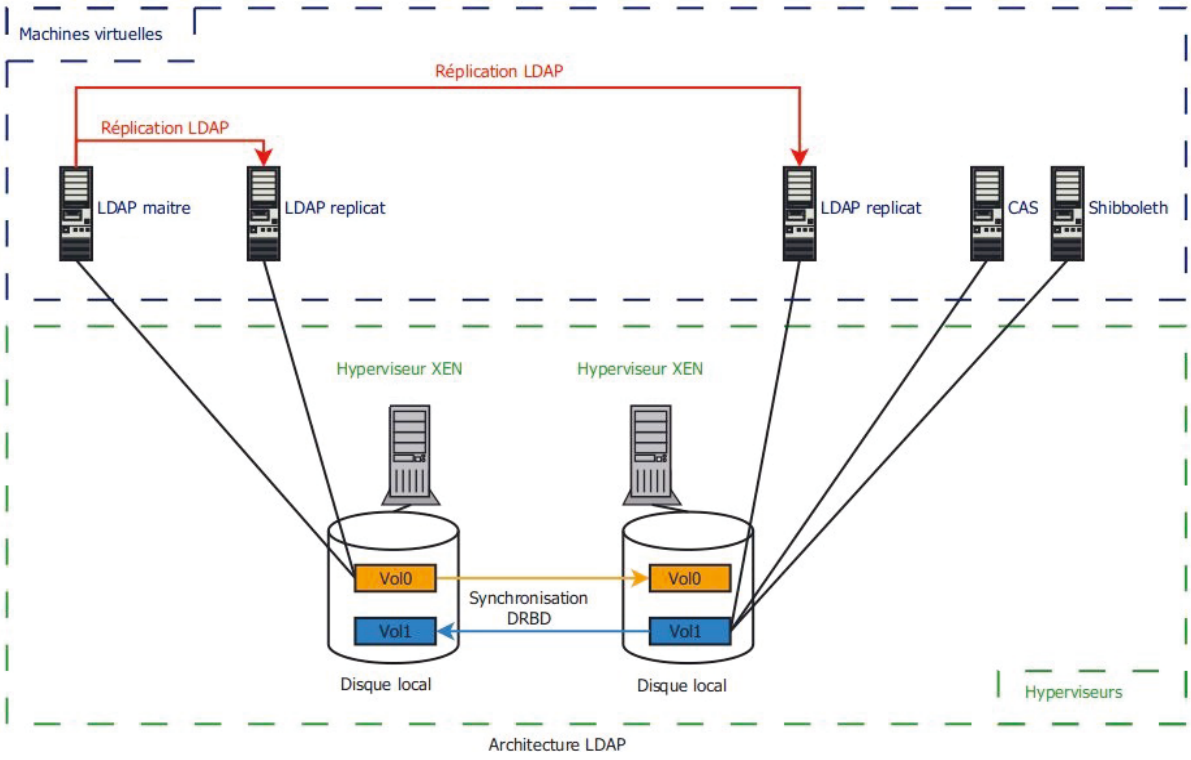


Figure 22 : architecture physique de l'annuaire LDAP de l'université

L'arborescence des informations (DIT) :

Elle est répartie dans trois unités d'organisations nommées people, group, appli.

Par rapport aux recommandations supann effectuées par renater, l'Université n'implémente pas l'unité « structures » permettant de représenter la structure de l'établissement. L'unité « appli » permet de stocker des comptes applicatifs implémentant uniquement les classes applicationProcess et simpleSecurityObject.

Les entrées de l'unité « people » implémentent les cinq classes préconisées par Renater (person, OrganisationalPerson, InetorgPerson, eduPerson et supannPerson) et une classe supplémentaire nommée mipPerson. Cette classe fait partie du schéma mip, défini par le défunt groupe MIP annuaires inter-universitaire pour pallier les déficiences des anciennes versions du schéma supann. Elle permet de représenter des attributs du profil étudiants et est largement rendue obsolète par les dernières versions supann.

Les attributs utilisés :

La discrimination entre Etudiants et Personnels est faite grâce à l'attribut multivalué eduPersonAffiliation.

Il est valué avec la valeur « Employee » pour les personnels et la valeur « Student » pour étudiants.

A noter que certaines personnes sont, à la fois, « Employee » et « Student ». L'attribut eduPersonPrimaryAffiliation permet, alors ,de préciser l'affiliation principale.

La faculté ou l'institut sont représentés pour les étudiants par l'attribut mipLibCmp.

Un étudiant inscrit à l'Université prépare un diplôme principal qui est précisé par les attributs mipCodDiplome et mipLicDiplome. Ce diplôme est l'objectif de sa formation et il peut attendre plusieurs années avant de l’acquérir.

Chaque année est représentée par une étape et est valuée par les attributs mipCodEtape et mipLicEtp. Un étudiant peut parfois préparer plusieurs étapes durant une même année universitaire, il y a cependant une étape principale qui est représentée par l'attribut mipCodEtape1.

Exemple de valuation de ces attributs :
mipCodDiplome: SDMDF111
mipLicDiplome: SDMDF111$DEUST METIERS DE LA FORME
mipLibCmp: APS$F2SMH
mipCodEtape1: SDMDF2111
mipCodEtape: SDMDF2111
mipLicEtp: SDMDF2111$DEUST METIERS FORME 2A

Le numéro d'étudiant est représenté par l'attribut supannEtuId. Le cycle de vie des étudiants dans l'annuaire est géré grâce à l'attribut mipStatut. Celui-ci peut avoir comme valeur « En Attente » ou « Actif ». (Voir chapitre 3.4)

Les employés possèdent un numéro d'employé supannEmpId et une affectation supannAffectation qui est le laboratoire, ou le département pour lequel ils travaillent.

3.3 Les clients de l'annuaire :

Les applications clientes de l'annuaire sont habituelles dans les Universités : un annuaire téléphonique, un serveur d'authentification SSO pour les applications web (CAS), un serveur Shibboleth permettant de faire de la fédération d'identités grâce à la fédération Renater, et un concentrateur Virtual Private Network (VPN) permettant de se connecter au réseau local de l'Université, depuis l'internet. L'annuaire LDAP permet également la connexion d'appareils portables sur des réseaux wifi. Ces derniers sont aux nombres de deux.
Le réseau « ups » est géré par un portail captif et un serveur central radius relié à l'annuaire LDAP universitaire. Il permet également l'accès du réseau aux partenaires du service mobilité mip wifi par l'intermédiaire des serveurs remip. (Réseau régional de la recherche en Midi Pyrénées)
Le réseau « eduroam » utilise le standard 802.1x et permet l'accès au réseau aux partenaires internationaux du service mobilité eduroam. Il repose sur le serveur central radius mais aussi sur les serveurs de la fédération.

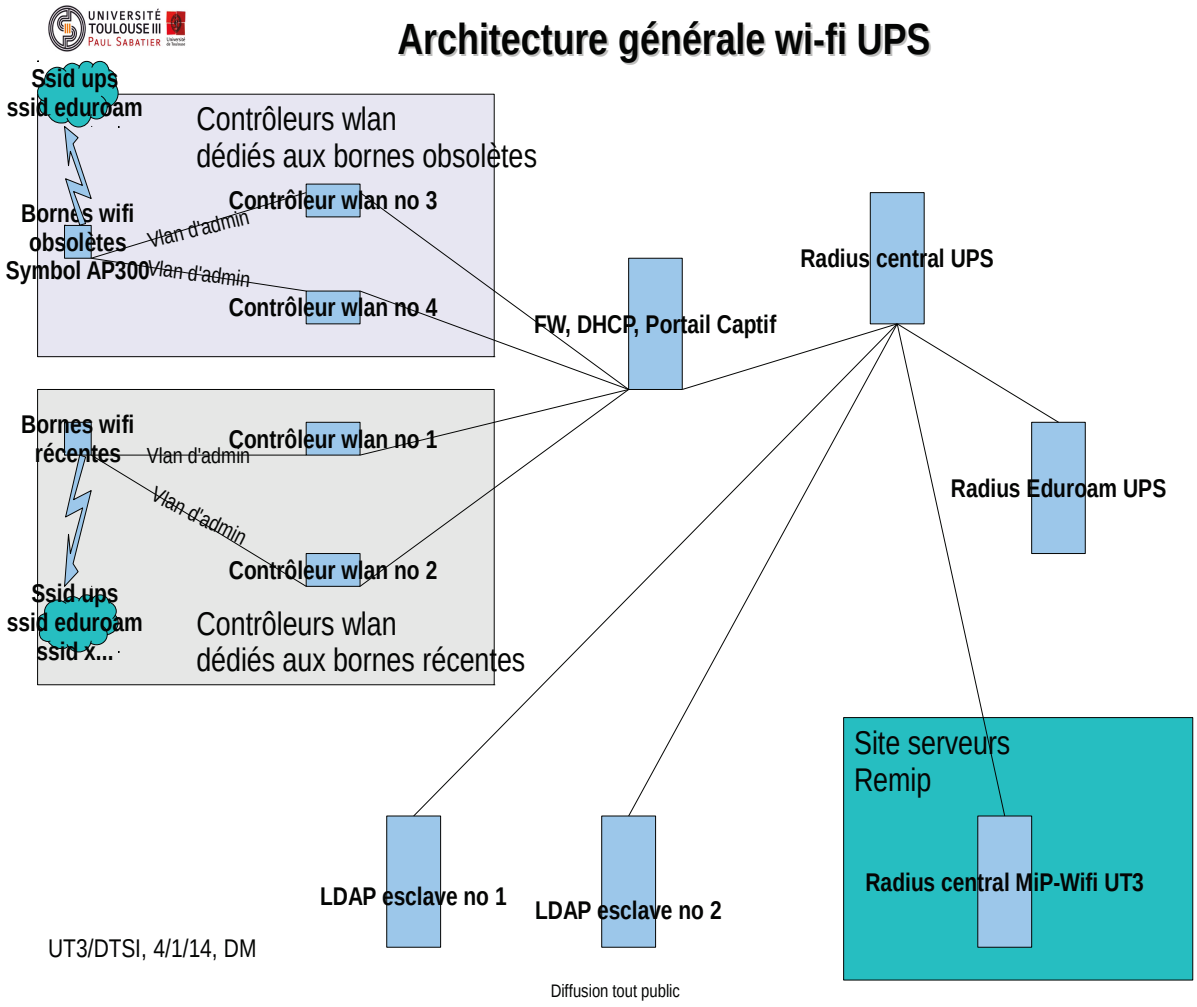


Figure 23 : Architecture générale wifi UPS

3.4 Le cycle de vie des utilisateurs dans l'annuaire

La présence des personnels dans l'annuaire LDAP de l'université est conditionnée par son statut dans l'application harpege. Dès qu'un personnel n'est plus directement payé par l'Université (fin cdd, retraite, mutation …) , il disparaît de l'annuaire de l'Université.

Le cycle de vie des étudiants est géré par le rythme des années universitaires et de son statut à l'Université (attribut mipStatut à l'Université). A une date spécifique (fin d'année universitaire), tous les étudiants ayant un statut actif passent à au statut « En Attente » et tous les étudiants ayant un statut « En attente » disparaissent de l'annuaire de l'Université. Les

étudiants ayant terminé leurs études restent donc un an supplémentaire dans l'annuaire de l'Université.

3.5 Les autres annuaires d'authentification de l'Université :

Etant donné la grande diversité de l'Université, il est impossible d'avoir une vision exhaustive des annuaires d'authentifications utilisés. Voici cependant une liste des principaux annuaires utilisés par la DTSI et la FSI pour des problématiques d'authentification système. Chaque annuaire représenté est indépendant des autres.

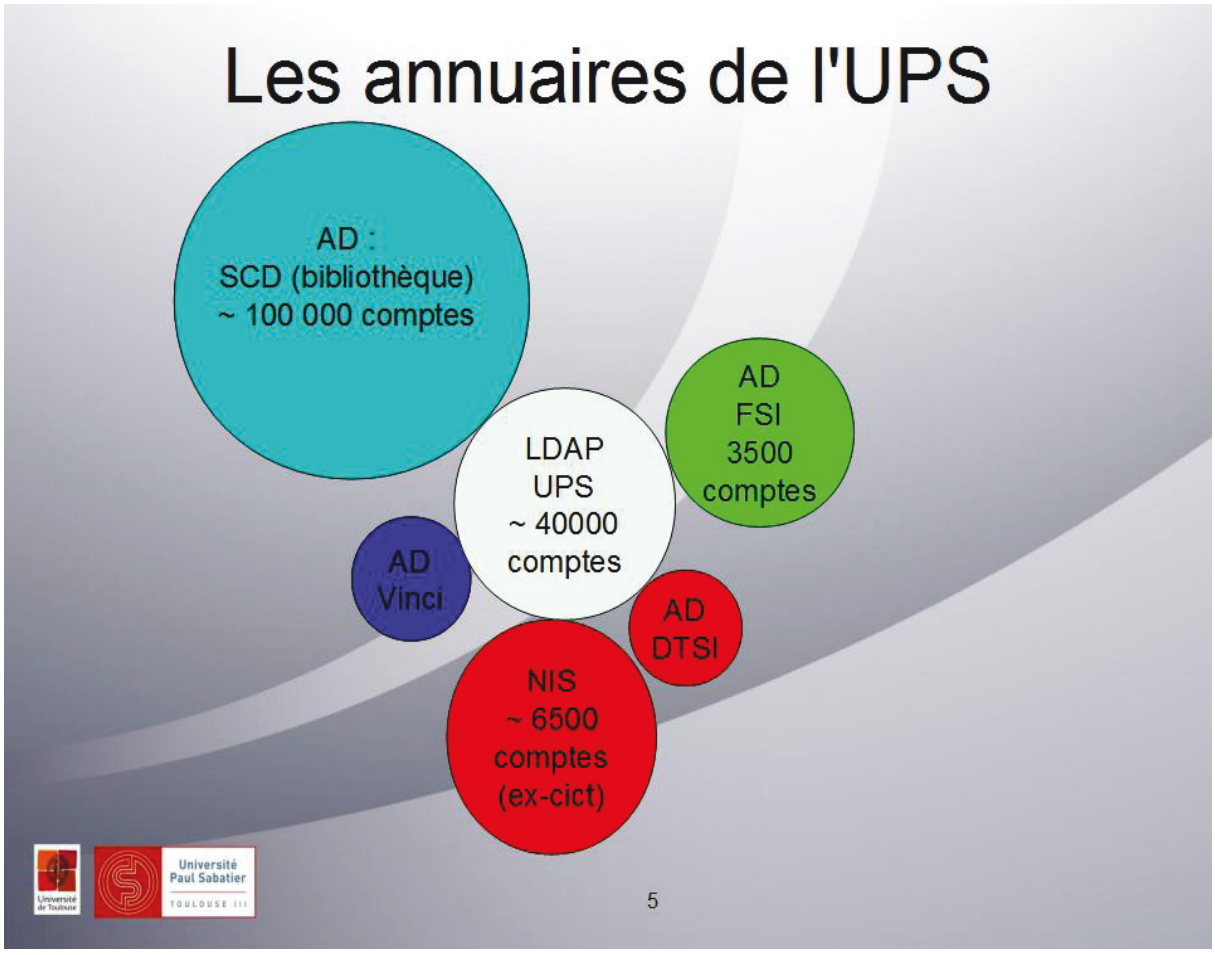


Figure 24 : Les annuaires de l'université Paul Sabatier

3.5.1 L'annuaire NIS ex-cict

Le serveur NIS d'authentification est historiquement antérieur à l'annuaire LDAP de l'université. Il était le serveur d'authentification principale du défunt Centre Interuniversitaire de Calcul de Toulouse (CICT). Les services clients de cet annuaire ont une messagerie cict.fr qui est en phase d'extinction, l'authentification des sites web hébergés par dsrt, ainsi que l'accès des serveurs Unix d'enseignement.

La gestion des comptes, historiquement stockés dans le fichier /etc/passwd, a subi une amélioration.

La base des comptes est stockée dans une base de données qui contient le login , et le mot de passe... il existe une interface graphique qui permet d'intervenir sur la base de données, de créer des comptes et les modifier...Une procédure extrait la base de données et écrase le fichier /etc/passwd sur le serveur maître NIS deux fois par heure. Le mot de passe des utilisateurs peut être modifié par une application web en mode libre service.

La plate-forme d'hébergement web et son projet d'évolution :

Le DSRT gère deux serveurs d'hébergements de site web qui contiennent actuellement 200 sites web actifs. Les serveurs sont des serveurs linux qui utilisent apache et mysql.

L'authentification pour la connexion des administrateurs des sites web se fait par des comptes NIS L'authentification pour la base mysql se fait par un compte mysql et un mot de passe distinct.

Une migration de la plate-forme d'hébergement est prévue vers un système plus sécurisé, et qui séparerait chaque site web dans une machine virtuelle. Une étude préliminaire a eu lieu pour savoir quels site web veulent migrer et lesquels ne souhaitent pas continuer. Les résultats de cette enquête sont disponibles dans une base mysql.

Les serveurs d'enseignements :

Le DSRT gère plusieurs serveurs d'enseignement de la FSI. Ceux ci comprennent deux serveurs Sun Os pour l'enseignement, ainsi que deux serveurs Oracle. Les deux serveurs d'enseignement Sun sont branchés sur l'annuaire NIS tandis que les bases oracle utilisent des comptes locaux.

Sur cet annuaire repose les services suivant : une messagerie avec le nom de domaine cict.fr, l'authentification des sites web hébergés par dsrt, ainsi que l'accès des serveurs Unix d'enseignement.

L'espace de stockage des utilisateurs :

Un espace de stockage est mis à la disposition des utilisateurs. Pour des questions quantitatives, il est réparti entre une ancienne baie de stockage Net app et des montages NFS sur des serveurs multiples.

3.5.2 Les annuaires Active Directory gérés par la DTSI

Il existe au moins trois annuaires Active Directory distincts.

Le premier nommé DSTI est géré par DSRT Il sert à l'administration d'une plate-forme de virtualisation VMWare et à l'authentification d'un serveur de fichier accessible aux personnels de la DTSI. Il est composé de trois serveurs Windows 2008 R2 dont deux sont virtuels et un physique. Le serveur physique est nécessaire pour pouvoir redémarrer les composants de l'infrastructure virtuelle.

Les utilisateurs peuvent changer leur mot de passe par un site web via le module pour IIS nommé IISADMPWD.

L'annuaire Vinci géré par DPROX sert à alimenter un serveur de fichier utilisé par l'administration centrale de l'université.

L'annuaire SCD permet l'authentification d'utilisateurs, provenant des trois universités de Toulouse, à des postes en libre service dans la bibliothèque de l'université.

Les trois annuaires sont indépendants et possèdent leur propre base de données login/mot de passe.

3.5.3 Les annuaires d'authentification des composantes.

La situation est complexe car chaque composante possède généralement son propre service informatique, son parc informatique avec ses procédures de gestion et d'authentification.

Parmi les divers instituts, facultés et laboratoires de l'université, nous allons étudier l'authentification de la Faculté des Sciences et d'Ingénierie. Celle-ci possède un service

informatique nommé Service Numérique d'Assistance et de Proximité (SNAP) séparé en deux branches : une partie dédiée à la gestion du parc administration et une partie dédiée à la gestion du parc enseignement. A noter que la création du SNAP est récente (2011). Avant cette date, la FSI était séparée en plusieurs UFR et chacun possédait son propre service informatique. Pour cette raison les procédures de gestion ne sont pas généralisées sur l'ensemble du parc et il existe souvent des îlots ayant leur propre procédure.

Le parc enseignement possède plus de mille machines avec les systèmes d'exploitation windows ou linux. Une grande majorité de ces machines est reliée à des serveurs d'authentification servant également de serveurs de fichiers. Il existe un domaine principal Active Directory regroupant l'authentification d'une vingtaine de salles pour des postes de travail windows et linux (avec la technologie winbind pour l'authentification sur linux ainsi qu'un montage d'un répertoire réseau cifs). Un autre domaine Active Directory indépendant permet l'authentification d'une dizaine de salles du département de Biologie. Il existe également plusieurs annuaires Samba/LDAP permettant l'authentification de deux ou trois salles sur des systèmes Windows et Linux.

3.6 Présentation d'une solution idéale

Selon les recommandations supann, la mise en œuvre des processus d'authentification passe par la mise en place d'un annuaire ldap implémenté le plus couramment dans la version openldap. Cet annuaire doit représenter la population de l'université. Cependant les besoins en authentification de l'université dépassent la limite de son annuaire. La solution d'authentification peut donc être adossée à des fédérations d'utilisateurs comme la fédération « Education Recherche » pour l'authentification web pilotée par Renater et accessible à partir de serveurs Shibboleth, ou la fédération « eduroam » pour l'authentification sans fil et accessible à partir de serveurs Radius.
La solution doit également intégrer une solution de « single sign on » pour les applications web mais peut également prendre en compte un mécanisme permettant de lier l'authentification système avec l'authentification web. La généralisation de kerberos sur les

serveurs d'authentification web comme sur le poste client avec le paramétrage adéquat des navigateurs web permet ce type de SSO.

Un mécanisme de centralisation de la gestion des groupes comme Grouper peut être mis en place. Il permet de déléguer la gestion des groupes à des utilisateurs privilégiés.

Les applicatifs à forte valeur ajoutée peuvent également être protégés par un système d'authentification forte comme une authentification à double facteur.

Les systèmes partagés comme les postes de travail dans les salles d'enseignement, les serveurs multi - utilisateurs ou les postes de travail virtualisés ont également besoin d'une solution d'authentification. Classiquement, les postes de travail Linux sont authentifiés sur un annuaire ldap et les postes windows sur Active Directory. Il est cependant tout à fait possible d'utiliser Active Directory pour authentifier les postes linux en ajoutant par exemple les attributs posix aux attributs des utilisateurs AD et en s'appuyant sur des solutions comme samba winbind ou sssd. Cette solution permet également de fédérer diverses entités en créant une arborescence de domaine. Au niveau Toulousain, on peut imaginer un domaine racine ne contenant pas d'utilisateurs et géré par la COMUE, des domaines enfants gérés par les services centraux des universités et contenant les mêmes utilisateurs que l'annuaire ldap, ainsi que des sous-domaines gérés par les composantes permettant de répondre à leurs besoins d'administration. Cette solution reposant sur la transitivité et des relations bilatérales des approbations permettrait de créer une fédération pour l'authentification système.

Pour obtenir une authentification SSO avec les applications web universitaires, l'implémentation Microsoft du protocole Kerberos étant propriétaire, il est préférable de se reposer sur une implémentation open source du protocole kerberos (comme MIT kerberos).

Les serveurs d'authentification web (CAS, Shibboleth) seront paramétrés pour accepter l'authentification par ticket kerberos. Les utilisateurs Active Directory seront créés avec un attribut « AltSecurityIdentities » indiquant leur identité sur le royaume Kerberos. L'authentification sur linux devra utiliser le module pam pam_krb5 sur le royaume Kerberos tout en obtenant les informations utilisateurs depuis Active Directory (via samba winbind par exemple)

Il existe plusieurs solutions pour le stockage des données utilisateurs : comme par exemple la cohabitation de deux serveurs de fichiers (un serveur nfs tournant sous linux et intégré au domaine windows et un serveur de fichiers cifs) jusqu'à l'utilisation d'une baie de stockage netapp exportant ses données en utilisant à la fois le protocole cifs et le protocole nfs.

L'avantage de cette solution est qu'elle permet la création d'une fédération d'utilisateurs pour l'authentification système, avec une intégration réaliste dans le système d'information des universités. Ce type d'authentification peut être amené à être de plus en plus important dans l'avenir étant donné le possible avènement de la virtualisation du poste de travail ou de la délocalisation des datacenters.

L'inconvénient est d'une part qu'il repose sur trois systèmes d'authentification (openldap, kerberos, active directory, qui devront être gérés par des processus centraux) dont deux sont open source et un propriétaire, et d'autre part qu'il n'a jamais été testé à ma connaissance sur une grande échelle.

IV Travaux effectués

4.1 Choix du périmètre initial :

Le choix du périmètre initial est clairement orienté enseignement puisqu'il comprend la rénovation de l'annuaire NIS de la DSRT ainsi que l'intégration des annuaires windows de la FSI. Ce choix est dicté par le fait que la population touchée est la plus grande et souvent la même, les enseignants et les étudiants ayant souvent besoin d'accès aux serveurs unix et aux salles PC. C'est également une demande importante de la part de la communauté enseignante, soumise à forte contribution en début d'année pour faire fonctionner le système (distribution des logins et mots de passe, communication avec les différents acteurs du système)

Nous devons proposer une solution qui puisse être globalisée rapidement à d'autres problématiques de l'université et ainsi qu'à d'éventuels nouveaux besoins (cloud computing, virtualisation du poste de travail)

Parmi les trois domaines relevés de l'authentification, nous nous occuperons de l'authentification système tel qu'elle est gérée par le Département Système Réseaux et Telecom et la Faculté des Sciences et d'Ingénierie, en cherchant à unifier les procédures avec les autres cas d'utilisation.

Figure 25 : Diagramme des cas d'utilisation de l'authentification dans le périmètre initial

4.2 Objectifs et Cahier des Charges :

L'objectif principal est de rénover l'annuaire NIS du dsrt. L'annuaire NIS repose sur des serveurs Sun qui ne sont plus maintenus. Cette migration est également associée à des problématiques annexes :

- La nécessité de transférer les espaces de stockage associé à l'ancienne plateforme d'authentification sur la nouvelle.
- Simplifier les procédures de création de comptes notamment pour les besoins d'enseignements
- Unifier les identifiants (login/mot de passe) avec ceux utilisés sur l'intranet de l'université.

L'objectif secondaire est de proposer une solution pouvant être utilisée par l'ensemble des composantes de l'université. La solution doit notamment prendre en compte l'intégration du monde windows généralement administré grâce à Active Directory.

- Solution d'unification des identifiants Active Directory avec l'intranet de l'université.
- Simplifier les procédures de création de comptes sur Active Directory

Enfin la solution doit permettre la mise en place d'un système d'authentification unique de type « Single Sign On » permettant à l'utilisateur de s'authentifier une seule fois, que ce soit sur des ressources informatiques physique (serveurs) ou internet (application web)

Voici un diagramme présentant les différents cas d'utilisation concernant la demande de création des comptes systèmes :

Figure 26 : Diagramme des cas d'utilisation pour la création des comptes systèmes

4.3 Étude de l'état de l'art et choix d'une solution

L'objectif du stage est de simplifier et d'unifier l'authentification système dans un périmètre défini, mais pouvant également être étendu à l'ensemble de l'Université. Nous devons tenir compte de l'écosystème dans lequel l'Université évolue et suivre les recommandations des normes éditées par les groupes de travail. (Cru, normes supann).

Un autre impératif est d'être conscient des divisions organisationnelles et du morcellement des équipes d'administration système pour pouvoir proposer une solution utilisable sur le terrain sans modification des contraintes organisationnelles.

Étude des solutions possibles :

- Utilisation de l'annuaire LDAP existant comme annuaire d'authentification système unix.

avantage : solution préconisée par les normes Supann

inconvénients : ajout de nouvelles classes dans cet annuaire. Difficultés à valuer certains attributs : uid,gid, home directory sans connaître les besoins de certaines populations. Difficultés à allouer des ressources à une population de 40000 personnes (home directory).Grande division organisationnelle à l'Université, beaucoup de composantes ont déjà leurs solutions d'authentification et ne désirent pas les modifier.

- Active Directory d'Etablissement comme cœur du système d'informations.

N'est pas adapté à l'existant. Peu conforme avec les normes Supann.

- Active Directory avec modification du mot de passe piloté par l'intranet de l'Université.

Trop d'annuaires Active Directory à l'Université, et des divisions organisationnelles importantes.

- Active Directory avec modification du mot passe piloté par un script.

Inconvénient : le mot de passe ne peut être modifié qu'en clair, et doit donc être stocké sous cette forme dans l'annuaire de l'Université

- Samba 4

avantage : permet contrairement à Active Directory, d'injecter un mot de passe sous forme de hash par un script de synchronisation.

Inconvénient : A cause de la séparation traditionnelle du monde windows et du monde unix, peu de personnels ont des compétences dans les deux environnements. Les domaines Active Directory sont généralement gérés par des personnels utilisant peu linux.

- 389 Directory Server

Permet de synchroniser les mots de passe de manière bidirectionnelle entre Ad et linux.

Les mêmes inconvénients que pour Samba 4.

- Pgina :

inconvénient : perte de fonctionnalités due à la disparition d'Active Directory

- Kerberos :

avantages : permet d'unifier les mots de passe linux et windows

permet de centraliser uniquement l'authentification et non les problématiques annexes (informations utilisateurs, autorisations …) et correspond bien à l'organisation de notre Université.

permet également d'évoluer vers une solution Single Sign On

La solution définie est donc

Un serveur kerberos stockant l'UID et le mot de passe de l'Université.

Un serveur d'authentification LDAP tampon contenant uniquement une sous-population de l'annuaire LDAP universitaire. Ce serveur ne stockera pas de mot de passe.

Le serveur LDAP permettra également la gestion des utilisateurs extérieurs au système d'information.

Le serveur LDAP tampon interrogera directement le serveur kerberos pour valider l'authentification, via un mécanisme SASL

Aucune modification sur l'annuaire LDAP universitaire

Les serveurs windows bénéficieront de l'unification du mot de passe par le mécanisme des approbations de domaines.

Il va de soi que cette solution peut également être considérée comme une étape vers plus d'intégration des annuaires, sous réserve également qu'une réflexion politique et organisationnelle soit menée de pair. Une réflexion pourrait être engagée pour l'intégration de l'annuaire LDAP tampon avec l'annuaire LDAP universitaire, ainsi que pour la généralisation du mot de passe dans le serveur kerberos.

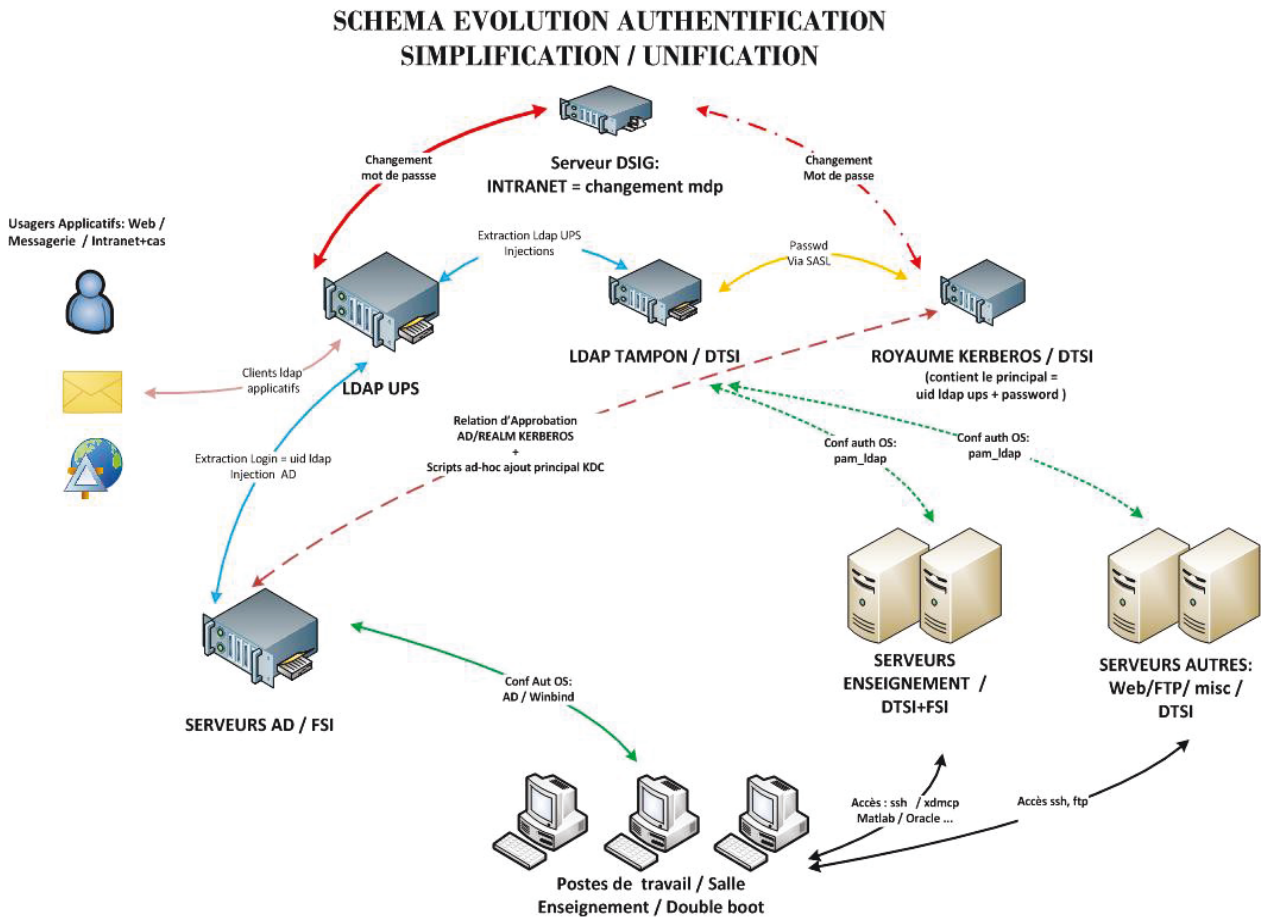


Figure 27 : Simplification et unification de l'authentification à l'université Paul Sabatier

4.4 Étude des risques

4.4.1 Inscription administrative des étudiants

L'apparition des étudiants dans l'annuaire est tributaire de la procédure d'alimentation, ainsi que de l'inscription administrative des étudiants. (CF III 1.2)

Bien que pour des raisons légales, il est obligatoire que l'étudiant soit inscrit administrativement pour pouvoir suivre des cours, certains étudiants ont une inscription tardive qui a lieu après le début des cours.

Il est également d'usage de créer des comptes pour ces étudiants, les obligations pédagogiques dans notre environnement sont pour une majorité d'acteurs plus importantes que les obligations légales.

Notre système doit donc accepter une certaine souplesse et permettre à des entités de demander la création de comptes temporaires, le temps de régler ces problèmes d'inscriptions.

J'ai effectué une étude quantitative en septembre 2013 mettant en correspondance les demandes par les secrétariats de créations de comptes, comparés à la présence du bon Code Etape Apogee dans l'annuaire universitaire (signe d'une inscription administrative finalisée)

La liste fournie par le secrétariat n'est également qu'une représentation de la réalité, et certains étudiants présents sur cette liste ne suivront peut-être aucun cours.

En comparant avec la présence dans l'annuaire universitaire sans autre critère, on s'aperçoit que le pourcentage de présence de comptes est plus élevé.

Rappel : Les étudiants restent un an supplémentaire dans l'annuaire universitaire après leurs études avec l'attribut mipStatut = En Attente.

L'idée est donc de garder également les comptes actifs dans l'annuaire LDAP tampon, les étudiants présents l'année précédente pourront se connecter dés leur premier cours.

Il reste également certains types de comptes, qui par nature, ne sont pas dans l'annuaire universitaire. (intervenants extérieurs, …)

Pour pouvoir les gérer ainsi que les comptes étudiants temporaires, nous allons étudier un outil de création de compte et de réinitialisation du mot de passe : LDAP Account Manager

4.4.2 Disponibilité d'une ressource centrale pour l'authentification

Le serveur Kerberos devenant une ressource centrale, il faudra s'assurer de sa disponibilité. Ce serveur sera déployé sur l'infrastructure de virtualisation du DSRT.

La sauvegarde et le monitoring seront effectués par les moyens classiques du DSRT. (Monitoring des services par nagios, sauvegardes effectuées sur des baies de sauvegarde).

Le serveur kerberos est divisé en deux « démons « : Le serveur kadmind qui est chargé de la création des principaux et de la modification des mots de passe associés, et le serveur kdc chargé de la distribution des tickets d'authentification.

Des tests de charge ont montré que le serveur kadmind était consommateur de ressources processeur, notamment pour le changement du mot de passe. (Le hashage du mot de passe met un certain temps à s'accomplir, notamment pour être moins vulnérable aux attaques par force brute). Ce serveur est également mono thread et ne tire parti que d'un seul processeur. Il faut donc prévoir que le changement du mot de passe par l'utilisateur peut échouer, et traiter cette possibilité.

Le serveur kdc sera lui redondé sur un deuxième serveur par réplication. Un mécanisme de timeout permet alors aux clients de l'interroger lorsque le premier ne répond plus.

Pour assurer une disponibilité maximum du serveur principal (intégrant kadmind et kdc), nous mettrons également en place VMWare Fault Tolerance. Ce serveur sera donc résistant aux pannes matérielles des serveurs hôtes.

4.4.3 Une période de transition nécessaire :

Le mot de passe doit être présent dans Kerberos avant la première connexion, la communication doit atteindre sa cible

Le mot de passe des utilisateurs est présent dans l'annuaire universitaire sous forme de hash. Pour intégrer un mot de passe dans un serveur kerberos, celui-ci doit être « en clair », sous forme non cryptée. Comme il est impossible de décrypter le hash d'un mot de passe, il est nécessaire de passer par une phase de transition où les utilisateurs devront changer leur mot de passe avant de d'effectuer leur première connexion.

Comme les salles informatiques dédiées à l'enseignement sont réparties dans un grand nombre de bâtiments, il est nécessaire d'effectuer une communication concernant la mise à jour du mot de passe. Il semble également opportun de mettre quelques matériels dédiés à cette tâche dans des endroits stratégiques de l'Université. (Postes en libre accès sans authentification et ne permettant que de se connecter sur le site internet de l'Université)

4.4.4 Les difficultés organisationnelles

Le nouveau système d'authentification tel qu'il est défini ici est transverse à plusieurs départements.

Le Département DSIG s'occupe des créations des comptes dans le LDAP universitaire et des procédures de changement de mot de passe par l'intermédiaire d'un site internet. Cette procédure devra à la fois changer le mot de passe dans l'annuaire LDAP universitaire et le mot de passe dans le serveur kerberos.

Le département DSRT s'occupe de la maintenance des serveurs LDAP et kerberos, de la synchronisation des comptes entre le LDAP universitaire et le LDAP tampon, ainsi que de la création des principaux kerberos. Il devra donc également se charger du stockage des répertoires personnels pour les serveurs unix.

Pour l'authentification windows, ce sont les composantes qui administrent les serveurs Active Directory qui s'occuperont de la création des comptes, ainsi que de la mise en place de la relation d'approbation avec le royaume kerberos universitaire. Cette relation devra être étudiée avec le Département Réseaux Systèmes et Télécommunication.

4.5 Simplification de l'authentification à DSRT

Je viens de présenter succinctement l'objectif du nouveau système d'authentification. Il faut cependant partir de l'existant et considérer que tous les annuaires sont en production. Il est donc important de chercher à simplifier cet existant.

4.5.1 Étude de l'existant pour le stockage

Il n'existe pas de point de montage unique pour les données utilisateurs. Les points de montage NFS ont été créés dans le temps sur les différents serveurs clients du domaine NIS, ainsi que sur une baie de stockage dédiée NetApp.

Le stockage est une problématique annexe à l'authentification. Il est donc opportun de profiter d'une simplification de l'authentification pour simplifier le stockage. On va dans un premier temps se contenter de connaître quelle est la taille des données utilisateurs réparties sur le parc des serveurs.

4.5.1.1 Étude du fonctionnement du montage des partitions

L'ensemble des points de stockage est partagé par l'intermédiaire d'une map Nis qui s'appelle auto.users. Cette map est utilisée par le service autofs des serveurs, et est configurée par l'intermédiaire du fichier /etc/auto.master pour les serveurs de type linux.

Voici la ligne concernant la configuration du montage des home directory dans le fichier auto.master:

```
/users          yp:auto.users   tcp
```

Voici quelques lignes de la map auto.users

```
fog -rw,hard,intr nfs1.cict.fr:/vol/nfs11/nfs110/fog
maitmeca -rw,hard,intr nfs1.cict.fr:/vol/nfs11/nfs110/fog/maitmeca
```

Le montage du point est effectué à la demande en fonction du groupe de l'utilisateur :
Le montage de nfs1.cict.fr:/vol/nfs11/nfs110/fog se fera sur /users/fog lorsqu'un utilisateur du groupe fog se connecte.

4.5.1.2 Étude des différents points de montage

Les points de montage sont centralisés sur la map nis auto.users. Cette map contient 344 lignes, faisant une bijection entre les groupes unix et les espaces de stockage.

L'obtention de la liste des points de montage se fait en deux étapes à partir de ce fichier :

- Obtention du point grâce aux commandes unix cut et sed

La commande cut -d' ' -f3| sed 's/\(.*\)\/\(.*\)/\1/' transforme par exemple la ligne *fog -rw,hard,intr nfs1.cict.fr:/vol/nfs11/nfs110/fog* en *nfs1.cict.fr:/vol/nfs11/nfs110/*

- Suppression des doublons avec les commandes unix sort et uniq.

On obtient alors la liste des points de montage qui contient 44 entrées réparties sur six serveurs.

```
aurore.cict.fr:/aurore1
bahia.cict.fr:/bahia1
bahia.cict.fr:/bahia2
nautile.cict.fr:/nautile1
nfs1.cict.fr:/vol/nfs11/nfs11
...
```

Il suffit de transformer ce fichier en un script shell ayant cette forme.

```
ssh aurore.cict.fr df -k aurore1
...
```

Et de l'exécuter depuis le serveur d'administration qui possède des autorisations de connexion sans mot de passe sur l'ensemble du parc.
Ceci a permis d'estimer la taille des données utilisateurs pour une migration du stockage sur une nouvelle baie
Baie Net app nfs1 : 1100 Go
Ensemble des serveurs : 328 Go

4.5.2 Etude de l'existant annuaire Nis

L'annuaire NIS effectue des opérations d'authentification pour **les types de comptes** suivants :

• Les comptes de la messagerie de l'ancien domaine cict.fr. La grande majorité des comptes a été migrée sur le nouveau domaine universitaire univ-tlse3.fr , mais le domaine est toujours actif et permet notamment d'offrir une messagerie web à certains types de personnels n'étant pas recensés dans l'annuaire LDAP.

• Les comptes d'administration des sites web hébergés par DSRT. Les deux serveurs web du dsrt sont des clients du domaine NIS. Les applications hébergées sont des applications des universités de Toulouse car ce service est une rémanence des missions inter-universitaires du Cict.

• Les comptes destinés aux étudiants pour des missions d'enseignement. Plusieurs serveurs destinés à l'enseignement sont donc clients du domaine Nis.
• Les comptes des personnels de l'université, principalement des enseignants et des personnels techniques.
• Les comptes liés à des problématiques diversifiées, pour lesquels les besoins exprimés se sont plus ou moins dilués avec le temps.

J'ai étudié les comptes de cet annuaire avec les **objectifs** suivants :
• Mieux connaître les diverses populations du point de vue quantitatif.
• Essayer de faire un lien avec l'annuaire LDAP de l'université pour savoir quel pourcentage de comptes NIS pouvaient être identifiés sur celui-ci.

Les sources de données utilisées pour effectuer cette étude :

• Les map Nis passwd et group. Elles ont été utilisées pour fournir les informations suivantes : login, gecos qui contient généralement le nom et le prénom, et le nom du groupe. Le lien entre les fichiers passwd et group est effectué grâce au gidNumber.
• L'annuaire LDAP universitaire, utilisé principalement pour calculer un taux de présence des comptes NIS dans celui-ci. La difficulté principale a été de résoudre les éventuelles fautes de frappe présentes dans l'annuaire NIS en utilisant l'algorithme de Levenshtein.
• Pour les sites web, la base de donnée mysql qui contient les résultats de l'enquête concernant les désirs de migration des utilisateurs sur une future plate-forme. Les administrateurs des sites ayant répondu favorablement migreront, tandis que les autres verront leurs sites fermés. Cette base de donnée contient l'URL du site, ainsi que les identités des administrateurs.
• Les fichiers de configuration des serveurs Apache, qui contiennent les sites web actuellement actifs sur la plate-forme.

La méthode utilisée :

La méthode utilisée pour étudier l'annuaire NIS a été axée sur le recoupement de diverses sources de données ainsi que sur l'utilisation d'expressions régulières pour pouvoir discriminer les types de comptes en fonction de leurs formes.

L'outil utilisé est le logiciel d'intégration de données Talend Open Studio. Le choix s'est porté sur ce produit pour sa facilité à croiser diverses sources de données ainsi que pour la possibilité d'intégration de code java.
Un autre objectif était également l'étude du produit en lui-même avec comme vision son utilisation pour une synchronisation entre l'annuaire LDAP universitaire et le futur annuaire LDAP tampon. Cet objectif a été abandonné par la suite, car l'équipe système qui s'occupe de la maintenance des plate-formes d'authentification a une culture plus orientée commandes systèmes et ne possède pas matériellement le temps de maîtriser ce type de logiciel. (Voir Annexe 1 pour l'utilisation de Talend Open Studio.)

Les conditions de recherche utilisées pour discriminer les types de population :

- Les comptes messagerie

Ce sont les comptes dont le type de shell est égal à « /bin/mesonly »

- Les comptes des personnels de l'université :

Ce sont les comptes répondent aux critères suivants :

1. Le login ne contient pas de chiffre
2. Le login moins le premier caractère est présent dans le gecos. Par exemple le compte avec le login sconrad avec un gecos « Serge Conrad »
3. Le nom et prénom, tel qu'ils sont présents dans le gecos, sont identifiables dans le LDAP universitaire par le nom et le prénom, et avec un statut personnel (eduPersonAffiliation = Employee). Cette recherche est faite en autorisant deux caractères différents, en calculant la distance de Levenshtein entre le gecos et le nom et le prénom du LDAP universitaire.

- Les comptes web actifs :

Les comptes web actifs sont présents dans les fichiers de configuration d'Apache des serveurs web.
J'ai écrit un script perl créant un fichier contenant les sites web actifs. Il contient le login NIS d'administration ainsi que l'URL du site. Il utilise les directives ServerName et DocumentRoot des VirtualHost. Lorsque les sites sont paramétrés avec la directive

VirtualDocumentRoot, ce qui est la majorité des cas, j'ai également utilisé le contenu des dossiers concernés.

Exemple de configuration des fichiers httpd.conf

```
<VirtualHost 195.220.59.66>
ServerName www.reseau-amerique-latine.fr
DocumentRoot /users/resamela/resamela/web/docs
...
<VirtualHost 195.220.59.65>
        VirtualScriptAlias /etc/httpd/vhosts-utm/%2/web/cgi-bin
        VirtualDocumentRoot /etc/httpd/vhosts-utm/%2/web/docs
...
</VirtualHost>
```

Le répertoire /etc/httpd/vhosts-utm contient alors une liste de liens symboliques contenant une partie de l'URL du site et le login NIS (présent le home de l'utilisateur)

```
lrwxrwxrwx  1 root root  18 Sep 14  2007 japonais -> /users/wwwutm/wjap
```

- Les comptes web non actifs :

Ce sont les comptes qui ne sont pas des comptes web actifs (règle précédente) et dont le login commence par la lettre w et le home directory contient www ou web.

- Les comptes des étudiants :

Les comptes étudiants ont été discriminés suivant la forme du login NIS. L'étude des populations a permis d'établir cinq catégories répondant à cinq expressions régulières différentes.

1. Le login a la forme d'un numéro étudiant : l'expression régulière est ^[0-9]{8}
2. Le login a la forme Premiere lettre prénom + Nom + Année universitaire : l'expression régulière est ^[a-z]{3,7}(12|13)
3. Le login a la forme d'un UID LDAP: l'expression régulière est ^[a-z]{3}[0-9]{4}[a-z]
4. Le login a la forme M suivi de chiffres : l'expression régulière est ^M[0-9]+
5. Le login a la forme d'un compte générique commençant par un radical suivi de chiffres : l'expression régulière a la forme ^(radical1|radical2|...)[0-9]+

4. 5.2.1 Les comptes de l'ex messagerie cict.fr :

Ces comptes ont été discriminés par le type de shell égal à « /bin/mesonly »

Les comptes messageries entités sont ceux ne répondant pas au critère « compte personnel de l'université ».

Type de compte		Présent dans NIS	Présent dans LDAP
Comptes messageries	Personnel	312	90
	Entités	54	

4.5.2.2 Les comptes administrations des sites web :

Ces comptes ont été discriminés par les règles numéro 3 et 4. Les comptes web non actifs peuvent déjà être considérés comme obsolètes et désactivés.

Type de compte		Présent dans NIS	Présent dans LDAP
Comptes Web	Actifs	210	
	Non actifs	164	

4.5.2.3 Les comptes étudiants :

Voici les résultats pour les comptes des étudiants. On remarquera qu'en enlevant les comptes génériques, plus de 90 % des comptes d'étudiants sont présents dans l'annuaire LDAP de l'Université.

Type de compte		Présent dans Nis	Présent dans LDAP
Enseignement	Générique	1150	91
	NomAnnée	680	494
	Numéro Étudiant	2399	2310

	Uid LDAP	511	508
	M suivi de chiffres	32	29
TOTAL		4772	3432

4.5.2.4 Les comptes personnels :

Ce sont les comptes qui ne sont pas de type « messagerie » (voir règle 1) et sont du type « personnel » (voir règle 2).

Le répertoire /etc/httpd/vhosts-utm contient alors une liste de liens symboliques contenant une partie de l'URL du site et le login NIS (présent le home de l'utilisateur)

->

> Le répertoire /etc/httpd/vhosts-utm contient alors une liste de liens symboliques contenant une partie de l'URL du site et le login NIS (ce dernier étant présent dans le home de l'utilisateur)

Type de compte		Présent dans NIS	Présent dans LDAP
Personnels		419	196
> Type de compte		> Présent dans NIS	> Présent dans LDAP
> Comptes Web	> Actifs	> 210	0
	> Non actifs	> 164	0

4.5.2.5 Les fichiers de sortie de l'analyse

L'analyse a permis d'obtenir des listes des personnes identifiées sur l'annuaire LDAP. Nous avons donc des fichiers en sortie qui contiennent les informations suivantes :

Pour les étudiants :

login nis;groupe nis;uidNumber;gidNumber;home directory;uid LDAP;code Etape Apogee

20906923;pcp1l2;23468;1168;/users/pcp1l2/20906923;smg9880a;DDPCI171
21104635;fog;26983;561;/users/fog/fog/21104635;frl0751a;EDINF1111
21202075;fog;27432;561;/users/fog/fog/21202075;frl0751a;EDINF1111

Pour les personnels :

login nis;groupe nis;uidNumber;gidNumber;home directory;uid LDAP;affectation supann
conrad;fog;1503;561;/users/fog/fog/conrad;cns3060a;Service numérique d'assistance de proximité

4.5.3 Choix de groupes de la population devant migrer sur LDAP tampon :

Après cette analyse quantitative qui a permis de déterminer quels sont les types de groupe présents dans l'annuaire LDAP, nous allons étudier plus finement les populations.

Cette analyse reprendra l'ensemble des personnes possédant un compte NIS et ayant été identifiés sur l'annuaire LDAP de l'Université. L'objectif de l'étude est de déterminer les formations (de par leur attributs mipCodEtape et mipLicEtp) et les entités (de par leur attribut supannAffectation) qui utilisent majoritairement les ressources informatiques.

Pour les étudiants, les données en entrées sont :

une liste de toutes les formations répertoriées dans l'annuaire nis sous forme d'attribut mipLicEtp

la liste de tous les étudiants répertoriés dans l'annuaire nis croisés à leur formation.

Un script écrit en perl, permet de définir quelles formations sont des gros consommateurs des ressources informatiques, et celles qui le sont moins…

Nb utilisateurs NIS	Nb utilisateurs LDAP	Formations
85	100	EDMAT1111$L2 MATHEMATIQUES
4	51	EDPCH1111$L2 SCI. PHYS. CHIMIQUES

Cette étude m'a permis de proposer que les comptes de certaines formations soient automatiquement créés sur l'annuaire LDAP tampon, et non plus à la demande comme c'est le cas depuis le début. Dans l'exemple précédent, seule la formation L2 MATHEMATIQUES

bénéficiera d'une création automatique. Les autres pourront bénéficier d'une synchronisation unitaire basé sur l'uid

Les autres types de comptes (web, messageries et systèmes) ne bénéficieront pas dans un premier temps de la migration sur l'annuaire LDAP.

4.5.4 Mise en place serveur LDAP Tampon

L'infrastructure openldap tampon est composée d'un serveur maître et d'un serveur esclave. La version d'openldap est 2.4 issue du système de packaging Debian. La réplication utilise l'overlay SyncRepl .

4.5.4.1 Définition du Directory Information Tree

Différents types d'utilisateurs :

Notre annuaire LDAP tampon doit pouvoir gérer deux types d'utilisateurs :

• Ceux synchronisés avec l'annuaire LDAP. Le mot de passe est stocké sur le serveur Kerberos. La gestion des comptes (synchronisation et suppression) se fait par l'intermédiaire de scripts.

• Ceux non synchronisés (car non présents dans celui ci). Le mot de passe est stocké dans le serveur LDAP. La gestion des comptes se fait par l'intermédiaire du logiciel LDAP Account Manager.

Parmi les comptes synchronisés, nous avons 4 cas de figure …

Les formations synchronisées

Les étudiants synchronisés au niveau individuel

Les personnels synchronisés de par leur affectation.

Les personnels synchronisés au niveau individuel

Des attributs multivalués :

De plus, de nombreux étudiants sont inscrits dans plusieurs formations et des personnes comme les thésards ont à la fois le statut étudiant et personnel .

Parmi les prérequis à prendre en compte pour la conception du DIT, il faut également parler de la forme de l'arborescence des répertoires des utilisateurs (home directory).

A l'heure actuelle les répertoires des utilisateurs sont montés dans une arborescence de type /users/groupe. Le pole H3S de Dsrt souhaite conserver cette arborescence sur le nouveau système. Ceci permettrait également de créer un répertoire partage dédié à un groupe :

/users/groupe/partage et permettant aux enseignants de déposer des données qui leur sont destinées.

Ceci complique un peu le processus de synchronisation. En effet, dans l'annuaire LDAP un étudiant est souvent inscrit à plusieurs formations. Il est inscrit à un diplôme principal et peut préparer des diplômes complémentaires. Ceci est traduit par la valuation des attributs suivants :

mipcodetape1 = code de l'étape principale

mipcodetape attribut multivalué qui contient tous les codes des étapes auxquelles l'étudiant est inscrit.

Présentation du DIT :

Pour les raisons exposées plus haut, nous avons opté pour l'arborescence LDAP suivante :

Tableau III: L'arborescence des informations dans l'annuaire LDAP tampon

Unités d'organisation	Unités d'organisation	Objectif
Group	etudiant	stocker les étudiants qui bénéficieront de la synchronisation intégrale et automatique par le code Apogee de leur formation
	exceptionetu	Synchronisation d'étudiants sur une base unitaire par uid
	personnel	stocker les personnels qui bénéficieront de la synchronisation intégrale et automatique par le code supannAffectation de leur affectation
	exceptionpers	Synchronisation de personnels sur une base unitaire par uid
	manuel	stocker des groupes locaux au LDAP tampon, non présents sur le LDAP universitaire.
	Transverse	stocker des groupes transverses (transverses à plusieurs formations sans jamais être une étape principale)
People	ups	Tous les utilisateurs synchronisés de l'annuaire LDAP universitaire
	manuel	stocker les utilisateurs locaux au LDAP tampon
	archive	stocker les utilisateurs qui ont disparu de l'annuaire LDAP universitaire, avant suppression

4.5.4.2 Définition des classes et des attributs :

Les classes et les attributs utilisés sont volontairement les plus simples possibles, et uniquement dédiés à l'authentification.

Les groupes sont créés uniquement avec la classe posixGroup

Tableau IV : Les classes et attributs utilisés pour les groupes dans l'annuaire openldap

Attribut	Classe	Obligatoire ?	Notes
cn	posixGroup	OUI	Nom du groupe
description	posixGroup	NON	MipLicEtape ou supannAffectation
gidNumber	posixGroup	OUI	
memberUid	posixGroup	NON	Membres secondaires

L'attribut cn sera également le nom du répertoire unix des homes directory des utilisateurs associés. Le nom doit être simple et sera généré lors de la synchronisation.

L'attribut description représentera l'attribut mipLicEtape du groupe LDAP universitaire pour des étudiants, ou supannAffectation pour les personnels.

L'attribut memberUid est attribut multivalué contenant les membres secondaires du groupe. Son utilité est de fournir l'accès au répertoire partage de la formation secondaire grâce au mécanisme de sécurité nfs.

Les utilisateurs sont créés avec les classes inetOrgPerson, posixAccount et shadowAccount:

Tableau V : Les classes et attributs utilisés pour les utilisateurs dans l'annuaire openldap

Attribut	Classe de provenance	Obligatoire ?	Notes
uid	posixAccount	OUI	Identifiant rdn
cn	inetOrgPerson	OUI	Nom commun
sn	inetOrgPerson	OUI	Nom de famille
givenName	inetOrgPerson	NON	Prénom
mail	inetOrgPerson	NON	
gidNumber	posixAccount	OUI	Groupe primaire
uidNumber	posixAccount	OUI	
homeDirectory	posixAccount	OUI	
loginShell	posixAccount	NON	
userPassword	posixAccount	NON	{SASL}uid@Royaume

La classe shadowAccount est intégrée par défaut pour pouvoir par la suite provoquer des expirations de comptes.
Le mot de passe ne sera pas stocké sur le LDAP tampon, mais sur un royaume kerberos en profitant de la technique Pass Through Authentification de SASL.
L'attribut gidNumber contient le groupe principal de l'utilisateur. Dans le cas d'un étudiant, il doit être équivalent à l'étape principale du LDAP universitaire (attribut mipcodetape1).
Le homeDirectory d'un utilisateur doit être équivalent à /users/nomgroupe/uid
Le nom de groupe est le cn de la classe posixGroup correspond au gidNumber de l'utilisateur.
Il faut cependant noter que les groupes principaux et secondaires changent sur une base régulière (à priori une fois par an) tout au long de la scolarité de l'étudiant.
Il faut donc que ces valeurs soient resynchronisées à intervalles réguliers et déplacer le home directory de l'utilisateur dans le répertoire de la nouvelle étape principale lorsque celle-ci change.

4.5.4.3 Plan d'attribution des uidNumber et gidNumber :

Les uidNumber et gidNumber sont des nombres. Ce sont les véritables identifiants utilisés par le système de fichiers lors de l'attribution des droits de sécurité.

Comme il existe deux modes de création de comptes dans l'annuaire NIS, il faut également qu'il existe trois étendues d'attribution des **uidNumber** :

1. Les comptes locaux à l'annuaire LDAP tampon seront créés à la main. Leur plan d'attribution sera de 30000 à 34999.
2. Les comptes synchronisés avec l'annuaire LDAP universitaire seront créés par un script en perl. Leur uid sera auto généré avec la première valeur libre sur la plage 40000 – 60000.

Pour le **gidNumber** :

1. Les groupes locaux auront comme plage d'adresse possible de 20001 à 39999
2. Les groupes destinés à la synchronisation avec le LDAP universitaire des valeurs comprises entre 40000 et 60000.

Les nombres pris en compte sont supérieurs à 30000 pour un impératif technique. Lors du transfert des données des homes de l'annuaire NIS vers l'annuaire LDAP, il va exister à un moment donné des répertoires provenant de l'annuaire NIS (identifié donc par le uidNumber et gidNumber) et des répertoires provenant de l'annuaire LDAP tampon sur le périphérique de stockage. Il faut donc qu'il n'y ait pas de chevauchement entre ces identifiants.

Il existe différentes procédures de création de compte. Par mesure de sécurité, nous avons installé un overlay assurant l'unicité des uidNumber et gidNumber : l'overlay « unique ». Voir l'annexe II pour la procédure.

4.5.5 Processus de créations des groupes et utilisateurs :

4.5.5.1 Synchronisation avec l'annuaire LDAP universitaire :

Les **groupes pour les étudiants** correspondent aux étapes dans l'annuaire universitaire. Pour les **personnels**, ils correspondent aux affectations.

Le **nom du groupe unix** est un nom simple défini manuellement par rapport au libellé de l'étape (attribut mipLicEtp) ou de l'affectation pour un personnel. Il sera présent dans un fichier en entrée dans le script de synchronisation.

Par exemple pour les étudiants ERIIT1111$M2R INFORMAT. ET TELECOMS ;m2rinfotel

Le **groupe primaire**:

Dans l'annuaire LDAP tampon, il est défini par l'attribut monovalué gidNumber de l'utilisateur.

Pour un étudiant, c'est généralement le groupe unix correspondant à l'attribut mipCodEtape1 dans l'annuaire LDAP universitaire.

Pour un personnel, c'est le groupe unix correspondant à l'attribut supannAffectation dans l'annuaire LDAP universitaire.

Le **groupe secondaire** :

Dans l'annuaire LDAP tampon, il est défini par l'attribut multivalué uidMember du groupe.

Un étudiant sera membre secondaire des groupes unix auxquels il est inscrit (attribut mipLicEtp valué) et dont il n'est pas membre primaire.

Un enseignant sera membre secondaire des groupes unix dans lesquels il enseigne

Exemple pour un étudiant :
uid=abc1234a
mipLicEtp: EMIAR1111$M1 IARF
mipLicEtp: ERIIT1111$M2R INFORMAT. ET TELECOMS
mipCodEtape1: ERIIT1111
mipCodEtape: ERIIT1111
mipCodEtape : EMIAR1111

Son groupe primaire sera m2rinfotel, et son groupe secondaire m1iarf.

Pour les enseignants, le groupe secondaire n'est pas inscrit dans l'annuaire LDAP universitaire puisqu'ils ne sont membres que du groupe correspondant à leur affectation. Nous avons dû faire remonter le besoin au département DSIG pour qu'il fasse apparaître l'attribut mipCodEtape donnant les étapes enseignées dans l'annuaire LDAP.

Processus de synchronisation des étudiants

La création des étudiants, lorsqu'elle est faite par groupe, se base sur l'attribut mipCodEtape1. Dans l'exemple précédent, l'utilisateur abc1234a sera créé lors du parcours du groupe (mipLicEtp= ERIIT1111$M2R INFORMAT. ET TELECOMS) uniquement.
Si on demande uniquement la synchronisation de (mipLicEtp=EMIAR1111$M1 IARF), l'étudiant abc1234a ne sera pas créé.
En cas de besoin l'étudiant devra être créé manuellement, ou le script devra être modifié pour utiliser l'attribut mipLicEtp et créer les groupes d'utilisateurs à la demande et non au début comme c'est le cas actuellement. Nous pressentons cependant que le risque de rencontrer ce cas de figure est faible.

Création des personnels :

La création se base sur l'attribut supannAffectation. Lorsqu'un utilisateur est à la fois étudiant et personnel, le statut personnel prime et l'utilisateur a comme groupe primaire le groupe lié à son affectation.

Groupes Transverses :

Ce sont des groupes issus de formations complémentaires, tel que les certificats informatique C2I. Ces formations ne sont jamais des étapes principales d'étudiants et donc des groupes principaux dans le LDAP tampon.

Cependant, pour prendre en compte la grande transversalité de ce type de formation, j'ai utilisé une procédure spéciale de création de comptes :

- Création d'un groupe dans l'unité d'organisation transverse.
- Parcours du LDAP universitaire en prenant en compte l'attribut mipLicEtp et non plus mipCodEtape1.
- Si le groupe correspondant à l'étape principale est présent dans le LDAP tampon, ce groupe est le groupe primaire de l'utilisateur.
- Sinon le groupe primaire est le groupe transverse.

Exemple avec un étudiant :

mipCodEtape1: HLSAN2111
mipCodDiplome: ALSAN114
mipCodDiplome: CUC2I121
mipLicDiplome: ALSAN114$DFGS PHARMACIE 2E AN
mipLicDiplome: CUC2I121$C2I
mipCodEtape: CUC2I2121
mipCodEtape: HLSAN2111
mipLicEtp: CUC2I2121$C2I
mipLicEtp: HLSAN2111$DFGSM 2E ANNEE PHARMACIE

Cet étudiant aura comme groupe primaire le groupe dfgsm2an s'il est présent, sinon le groupe C2i.

Création par utilisateur :

Le processus de synchronisation créera les comptes sur la base du groupe (et donc sur les notions d'affectations et d'étapes).

Cependant pour pouvoir créer des utilisateurs sans créer l'ensemble des membres du groupe, une option permettra de synchroniser des utilisateurs avec l'annuaire LDAP sur la base de l'uid d'un utilisateur.

Création manuelle :

Il est possible de créer des utilisateurs de façon manuelle dans les cas de figure suivants :

- Un utilisateur autorisé à se connecter sur les ressources n'est pas présent dans l'annuaire LDAP universitaire.
- Un étudiant a besoin de se connecter à des ressources informatiques, sans que l'inscription administrative n'ait été totalement terminée. Il peut être alors nécessaire de créer un compte temporaire pour pallier le retard.

Un script permet alors de créer des utilisateurs par l'intermédiaire de fichier dans l'ou manuel du LDAP tampon, et une interface web fournie par le programme LDAP Account Manager permet de créer des utilisateurs de façon interactive.

Il est également possible de déléguer l'accès à cette interface à des services comme l'exploitation ou le guichet unique du numérique de la DTSI pour faciliter la création de comptes.

Comptes Web :

Ces comptes actuellement sur l'annuaire NIS pourront être créés dans l'annuaire LDAP tampon par une procédure spéciale. La procédure est développée avec le logiciel Talend Open Studio et créera un compte dans l'ou web dédié avec comme UID le login NIS et injectera le mot de passe.

Après le processus de création initiale, la création de nouveaux comptes pourra se passer à travers l'interface web fournie par LDAP Account Manager.

Outils utilisés :

Les outils utilisés pour le management des comptes seront les suivants :

- Pour la synchronisation entre l'annuaire LDAP tampon et l'annuaire LDAP universitaire :

Un script perl synchroLdapUniv.pl pour la création des comptes et un script archiveUsers.pl pour l'archivage.

• Pour la création de comptes manuels : Un script perl addManuel.pl et l'interface web fourni par lam.
• Pour les comptes web : Un processus créé avec Talend open Studio pour la synchronisation initiale, puis les comptes seront gérés par l'interface web.

Stockage et changement du mot de passe :

Le mot de passe des comptes synchronisés sera stocké sur un serveur Kerberos. L'authentification fonctionnera sur le LDAP tampon grâce à une procédure de « Pass Through Authentication », dédiant celle-ci aux serveurs kerberos. Le changement du mot de passe dans le royaume Kerberos devra s'effectuer au travers du site intranet de l'Université. Le mot de passe des comptes manuels sera stocké sur le serveur LDAP tampon. Il ne sera pas possible de changer ce mot de passe depuis les serveurs d'enseignement. Les commandes passwd et slappasswd seront désactivées car il est impossible de faire la distinction à ce niveau entre les comptes synchronisés et les comptes manuels. Pour rendre possible le changement de mot de passe, nous utiliserons l'interface web self-service fournie avec le logiciel LDAP Account Manager version pro.

Voici un tableau résumant le processus de création de comptes avec les notions vues précédemment :

Tableau VI: Les différents types de synchronisation sur l'annuaire LDAP tampon

Type de groupes	Spécificité	Provenance	Attribut ou données utilisés	Nom du fichier entrée	Emplacement groupe destination LDAP tampon	Outil utilisé pour la création	Changement mot de passe
Etudiants	Par groupe primaire	LDAP	mipCodEtape1	l_mipLicEtp	ou=etudiant	synchroLdapUniv.pl	Intranet
	Par groupe transverse	LDAP	mipCodEtape	l_mipLicEtpTransverse	ou=transverse	synchroLdapUniv.pl	Intranet
	Unitaire	LDAP	uid	l_etudiantsups	ou=exceptionetu	synchroLdapUniv.pl	Intranet
Personnels	Par affectation	LDAP	supannAffectation	l_supannAffectation l_sgce	ou=personnel	synchroLdapUniv.pl	Intranet
	Unitaire	LDAP	uid	l_personnelsups l_sgce	ou=exceptionpers	synchroLdapUniv.pl	Intranet
Manuel	Par groupe	Fichier local	Prenom et nom	Fichiers dans le rep autorisationsManuel	ou=manuel	addManuel.pl	LDAP account manager
	Par utilisateur	Interface web	Interface web	Interface web lam	ou=manuel	LDAP Account Manager	LDAP account manager
Web	Sites actifs	nis	login	/etc/passwd et httpd.conf	cn=WEB	Talend Open Studio	LDAP account manager

Exemple de Fichier l_mipLicEtp :

ERIIT1111$M2R INFORMAT. ET TELECOMS;m2rinfotel

EMIAR1111$M1 IARF;m1iarf

Algorithme du script de synchronisation des comptes :

Voici les différentes actions menées par le script synchroLdap.pl.

Comme vu auparavant, ce script synchronise les utilisateurs pour les groupes d'étudiants, les groupes de personnels, les groupes transverses étudiants, ainsi que les utilisateurs par unité.

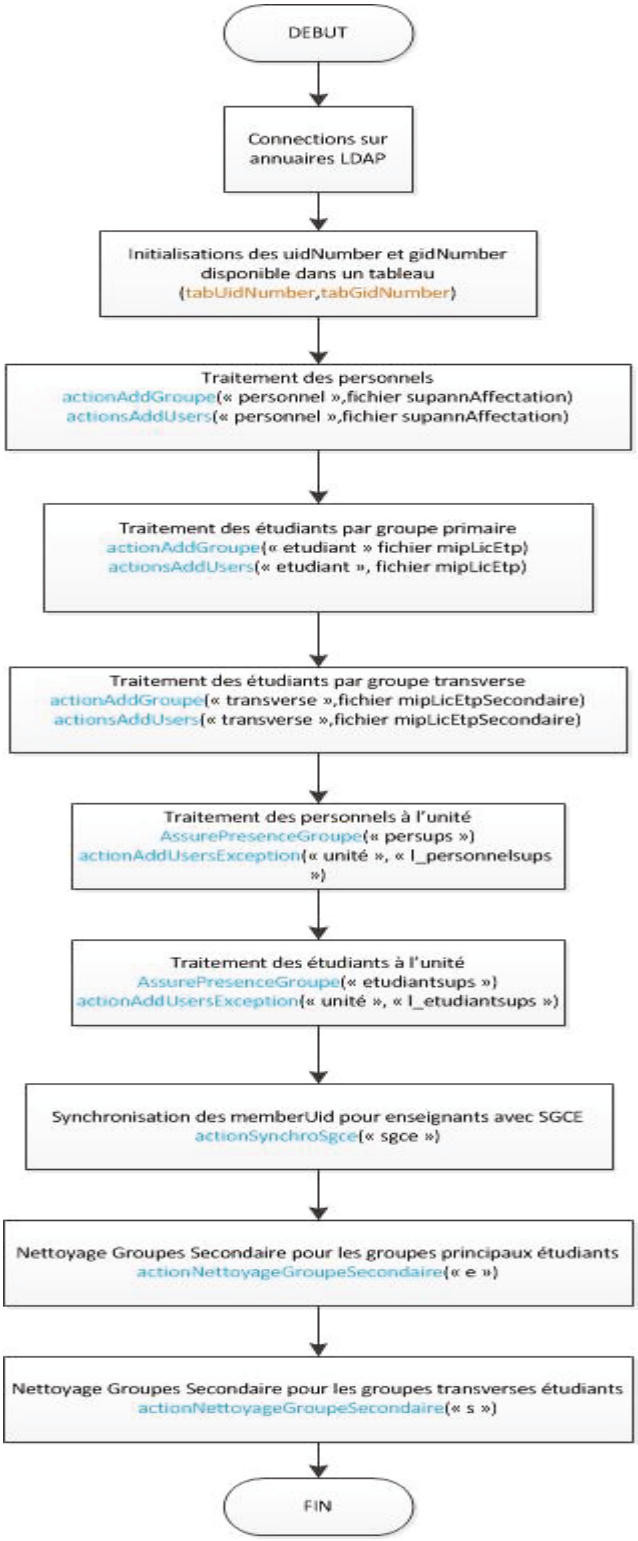


Figure 28 : Algorithme du script de synchronisation avec l'annuaire LDAP universitaire

A noter que le processus de synchronisation des membres des groupes secondaires se passe en deux étapes :
Ajout des nouveaux attributs memberUid lors de l'exécution de la fonction actionAddUsers, même si l'utilisateur est déjà présent dans le LDAP tampon.
Suppression des attributs memberUid qui ne sont plus d'actualité lors de l'exécution de la fonction
actionNettoyageGroupeSecondaire.

Le script d'archivage des comptes :

Le script d'archivage est chargé de la suppression des comptes et de l'archivage des données utilisateurs. La politique de suppression est la même que celle de l'annuaire LDAP universitaire, à savoir l'utilisateur conserve son compte tant qu'il est présent dans le LDAP universitaire, même avec le statut « En attente »(attribut mipStatut). Ceci a également l'avantage de simplifier les problèmes de connexion en début d'année universitaire, si la procédure d'inscription administrative a du retard.
La durée de l'archivage des données doit être définie au niveau politique et la suppression automatique peut être enclenchée au bout de la période.

Le script repose sur les mêmes fichiers d'entrée que le script de synchronisation.
Ils contiennent l'identifiant du groupe sur le LDAP universitaire ainsi que le nom du groupe unix.
Exemple : EMIAR1111$M1 IARF;m1iarf

L'algorithme est le suivant :

Pour tous les groupes autorisés à se connecter (parcourir les fichiers)

Créer un filtre pour le LDAP universitaire selon le type du groupe

Etudiants : forme mipCodetape1 pour l'étape principale.

Groupe transverse : forme mipCodEtape pour l'étape transverse.

Personnels : forme supannAffectation pour l'affectation

Affecter la liste des UID dans un tableau

Sur le LDAP tampon, récupérer le gidNumber à partir du nom du groupe

Parcourir tous les utilisateurs du LDAP tampon ayant ce groupe comme groupe principal.

Si l'UID n'est pas présent dans le tableau, l'utilisateur est à archiver.

Fpour

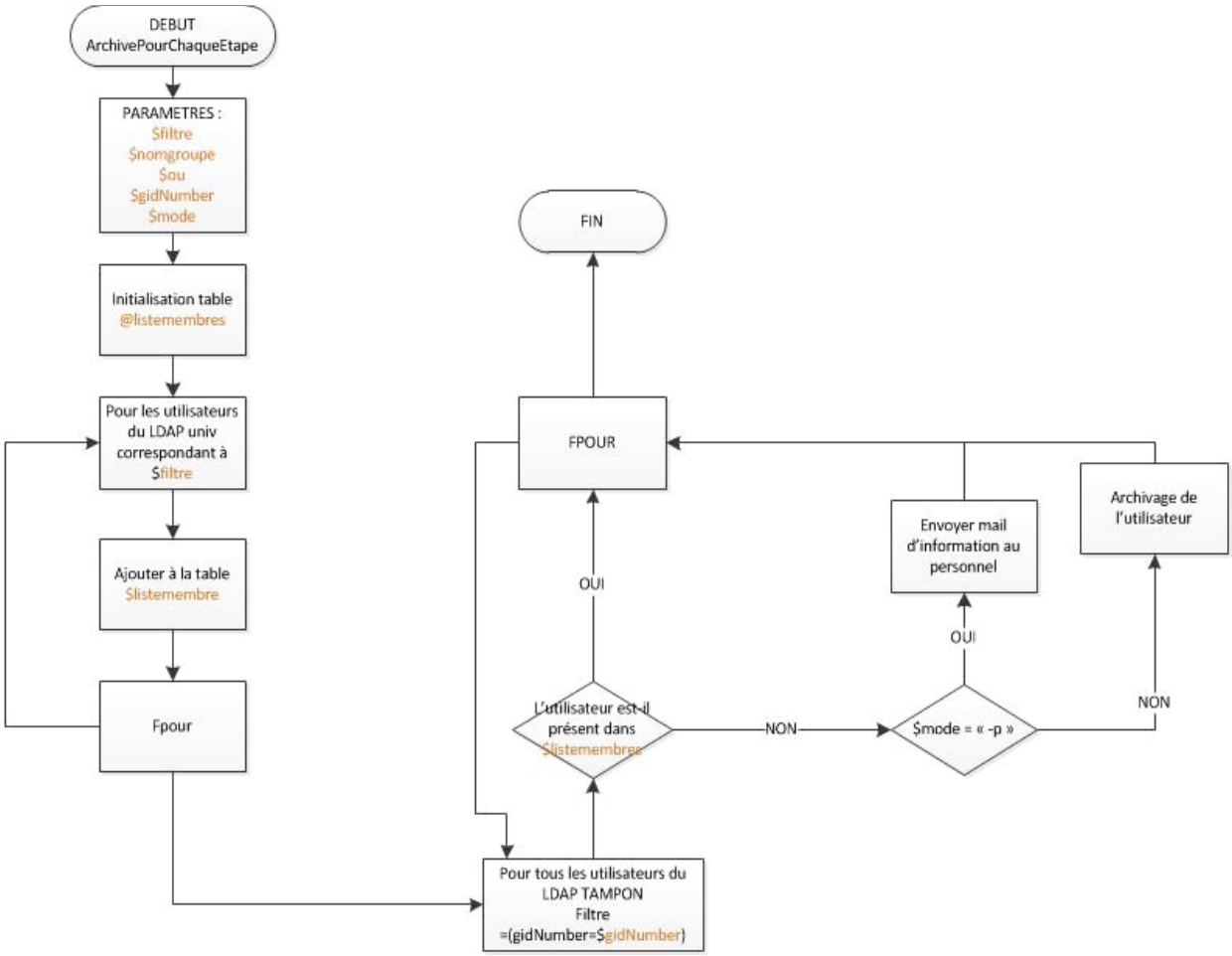


Figure 29 : Algorithme du script d'archivage avec l'annuaire LDAP universitaire

4.5.5.2 La création manuelle des comptes :

Cette procédure a été mise en place pour pallier certains manques du système d'informations de l'université. Ces comptes seront stockés dans l'unité d'organisation ou=manuel,ou=people pour les utilisateurs et dans l'unité ou=manuel,ou=groupe pour les groupes. Ces comptes sont indépendants de l'annuaire LDAP universitaire. Leur durée de vie doit être gérée et doit être négociée avec l'ensemble des acteurs. Pour gérer la durée de vie, la classe shadowAccount est intégrée dans les comptes. L'attribut shadowExpire permet de définir une date d'expiration.

Le mot de passe, à l'inverse des comptes synchronisés, est stocké dans l'annuaire LDAP tampon avec l'attribut userPassword. Pour changer ce mot de passe, l'utilisateur se connectera sur le site de changement de mot de passe self-service utilisant le programme LDAP Account Manager version pro.

Deux procédures de création de compte sont mises en place :

- Création des comptes version batch :

J'ai écrit un script en perl permettant de créer des comptes manuels en prenant en entrée des fichiers de type csv.

Chaque fichier présent dans un répertoire sera converti dans un groupe dans l'unité d'organisation ou=manuel,ou=group. Un répertoire éponyme sera également créé sur le serveur de fichier.

- Création des comptes avec l'interface Web de LDAP Account Manager :

Le logiciel LDAP Account Manager est installé sur un serveur web nommé lam-admin permettant de gérer les bases de données LDAP tampon. Elle est sur le même réseau que les machines LDAP. L'interface est celle fournie par l'interface Ldap Account Manager.

L'administration de la base LDAP via lam se fait par des utilisateurs LDAP qui auront des droits en écriture sur la branche ou=manuel, ou=people. Il est donc nécessaire de définir les listes de contrôle d'accès de ces utilisateurs(ACL).

Le processus prend également en charge la création du répertoire home directory de l'utilisateur. Cette opération s'effectue par le plugin lamdaemon de lam et implique les prérequis suivants :

- La machine sur lequel s'exécute le script doit pouvoir monter la baie de stockage Netapp en root (avec l'équivalent de l'option nfs no_root_squash)
- Elle doit être cliente du domaine LDAP tampon grâce à la configuration de pam_LDAP
- Elle doit autoriser les connexions en ssh, uniquement pour les comptes d'administration de lam.

Le serveur web apache doit être sécurisé et la communication avec le serveur openldap doit être cryptée en utilisant le protocole LDAP.

Figure 30 : Présentation de l'interface web LDAP Account Manager lors de la création d'un compte

Changement de mot de passe :

Le changement de mot de passe est bloqué depuis les machines clientes de l'annuaire. La raison principale est l'utilisation de « Pass Through Authentication » des comptes

synchronisés avec l'annuaire LDAP.(userpassword de la forme {SASL}uid@royaume).Le changement est bloqué au niveau des modules PAM.

Pour pouvoir proposer ce service aux utilisateurs, nous utilisons le mécanisme « connexion self-service » intégré à Lam Pro. Ce service permet de créer une page web de changement de mot de passe, uniquement accessible aux utilisateurs présents dans l'unité d'organisation manuelle.

Ce service permettra également aux utilisateurs d'initialiser leur mot de passe avant la première connexion. Ils devront se connecter sur un serveur web dédié et indiquer leur adresse email pour initier la procédure.

Techniquement, le service sera installé sur un serveur web séparé. Il sera associé avec un compte LDAP possédant des droits acl sur le mot de passe des utilisateurs. Ce compte ne gérant pas les home directory, il n'implémentera pas la classe posixAccount mais uniquement la classe simpleSecurityObject.

4.5.5.3 Import des comptes web depuis l'annuaire NIS

Les comptes web de la plate-forme d'hébergement ex-cict, actuellement gérés par l'annuaire NIS, pourront être intégrés dans l'annuaire LDAP tampon. Les serveurs web devront être reconfigurés d'une authentification NIS vers une authentification LDAP. Ceci devra sans doute être intégré dans un projet plus global de refonte du service de plate-forme d'hébergement.

J'ai mis au point une procédure d'intégration des comptes web (login et mot de passe) dans l'annuaire LDAP en utilisant un job talend. Il prend en entrée le fichier /etc/passwd pour le login NIS, le fichier /etc/shadow pour le mot de passe, la base de données services web pour les coordonnées des administrateurs, et un fichier contenant une correspondance entre le login NIS et l'URL du site web. Ce dernier fichier provient d'un script préliminaire étudiant les fichiers de correspondances d'Apache.

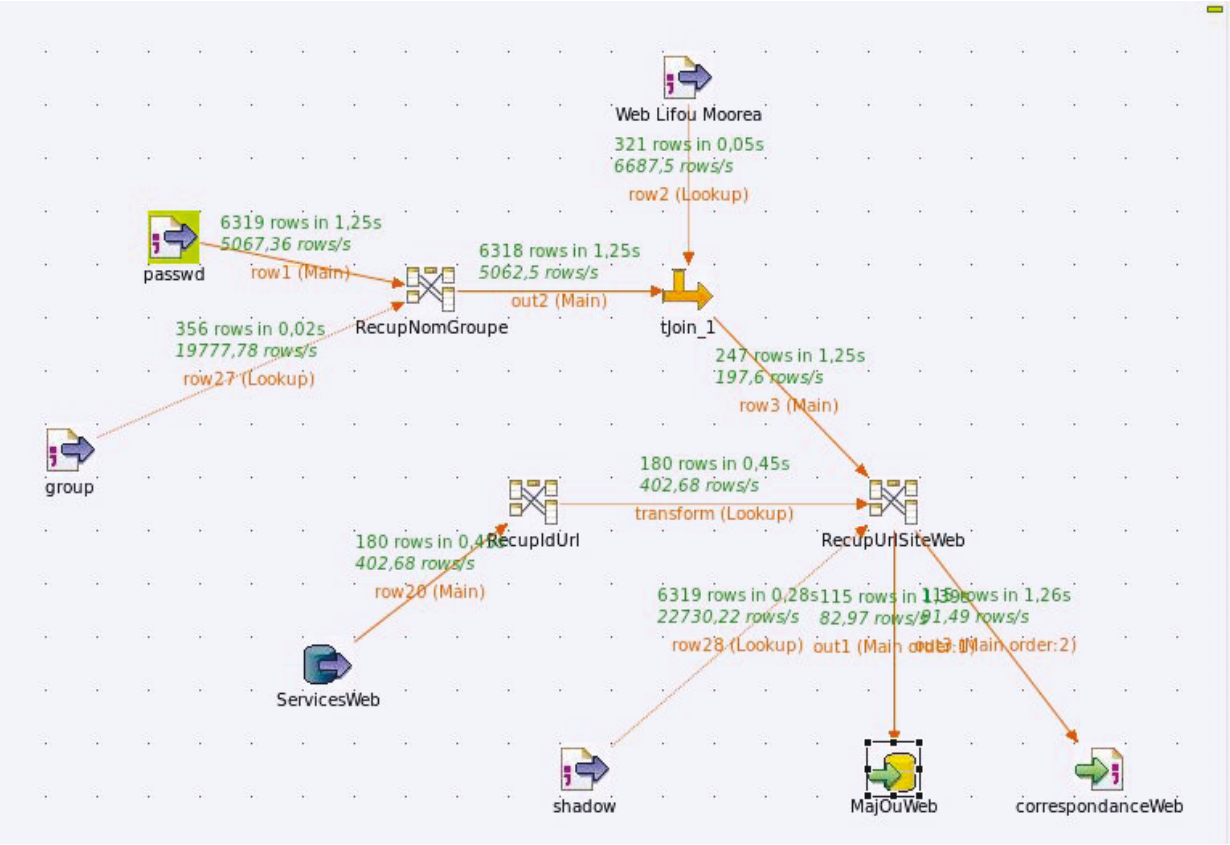


Figure 31 : Job Talend effectuant l'intégration les comptes web NIS dans l'annuaire LDAP

4.5.5.4 Processus de transfert des données depuis l'ancienne infrastructure de stockage :

Comme vu précédemment, les répertoires home directory des utilisateurs NIS sont stockés sur une baie de stockage net app hors garantie et différents serveurs. L'objectif est de profiter de la migration vers l'annuaire LDAP pour migrer toutes les données sur une nouvelle baie de stockage Net App.

Deux cas de figures existent :

• Les comptes NIS dont on a trouvé une correspondance dans l'annuaire LDAP universitaire. Un compte identique sera alors crée sur l'annuaire LDAP tampon, le compte NIS supprimé, les données de l'utilisateur affectées au compte de l'annuaire LDAP tampon,puis transférées sur la nouvelle baie de stockage. Le home directory sera également modifié (sous la forme /users/$group/$user).

• Les autres comptes continueront d'exister dans l'annuaire NIS. Les données seront également sur la nouvelle baie de stockage, mais en gardant l'ancien chemin.

A cause de cette double utilisation de la ressource de stockage, il est nécessaire que les plages des uidNumber des utilisateurs NIS et des utilisateurs LDAP ne se chevauchent pas.

Prérequis :

• Les utilisateurs du LDAP universitaire doivent être déjà synchronisés sur le LDAP tampon, et donc posséder un uidNumber et un gidNumber.

• Le nouveau serveur de stockage NetApp 2240 doit être configuré et accessible en root depuis le serveur qui effectuera la synchronisation des données.

• Les répertoires de destination doivent exister sur le serveur de stockage.

• Les fichiers de correspondance « anciens, nouveaux » doivent exister. Ceux-ci contiennent des informations par utilisateur dont : l'ancien home directory, le nouveau home directory, l'uidNumber et le gidNumber provenant de l'annuaire LDAP tampon

Obtention des fichiers de correspondance :

Le fichier de correspondance est un fichier csv ayant la structure suivante :

« nisUserHomePath;nisUserGroupName;nisUserName;ldapUserGroupName;ldapUserName;ldapUserGroupIdName;ldapUserIdName;ldapUserHomePath »

Tableau VII : Les champs du fichier de correspondance pour la synchronisation des données NIS - LDAP

Champ	Signification
nisUserHomePath	Le home directory du NIS
nisUserGroupName	Le nom de groupe du NIS
nisUserName	Le login du NIS
ldapUserGroupName	Le nom de groupe du LDAP tampon
ldapUserName	L'UID du LDAP tampon
ldapUserGroupIdName	groupe principal (gidNumber) du LDAP tampon
ldapUserIdName	l'uidNumber du LDAP
ldapUserHomePath	Le home directory du LDAP tampon

Exemple :

/users/pcp1l2/21104911;pcp1l2;21104911; prepacing2;hrc0702a;40030;45306;
/users/prepacing2/hrc0702a

Ce fichier sera obtenu grâce à un job Talend qui va croiser les fichiers d'études du NIS avec les utilisateurs créés sur l'annuaire LDAP tampon. Il est croisé avec le LDAP tampon grâce à un composant tMap pour obtenir les uidNumber et gidNumber des utilisateurs.

Figure 32: Job Talend effectuant la correspondance entre les utilisateurs NIS et la base LDAP tampon

La synchronisation des home directory :

La synchronisation est effectuée par un script développé par un ingénieur de l'équipe H3S, Christophe Marteau. Ce script effectue un rsync qui synchronise les anciens homes directory NIS répartis sur plusieurs serveurs de stockage sur la nouvelle infrastructure de stockage NetApp, en modifiant le propriétaire du répertoire de destination avec l'uidNumber et gidNumber du LDAP tampon.

4.6 Simplification de l'authentification à la FSI

Nous allons étudier les annuaires Active Directory de la FSI pour obtenir la liste des populations utilisatrices. Le but de cette étude est d'obtenir la liste des Codes Apogée et des Affectations des utilisateurs dans le but d'automatiser les procédures de création de comptes.
Nous aurons de fait une unification des identifiants de connexion, première étape vers l'unification de l'authentification.

4.6.1 Étude des annuaires Active Directory :

4.6.1.1 Unités d'organisation

Le « Directory Information Tree » est simple. Tous les utilisateurs et les groupes sont présents dans une unité d'organisation people. Les comptes ordinateurs sont quant à eux répartis dans une arborescence d'unités d'organisations nommése « ordinateurs », représentant les salles informatiques.

4.6.1.2 Groupes

Chaque utilisateur possède comme groupe principal « Utilisateurs du Domaine ». Il est également dans membre d'un groupe représentant généralement son étape principale. Le cas des étudiants préparant plusieurs diplômes ou étant en enjambement sur deux années n'est pas traité. Ils ne sont membres que d'un groupe.
Le nom du groupe est structuré de manière à avoir certaines informations : diplôme préparé, année en cours (étape au sens apogée) et année universitaire :
Exemple le groupe « M1-INFO-1314 » pour les étudiants préparant l'étape Maîtrise informatique 1ère année lors de l'année universitaire 2013 2014.
Les enseignants et personnels sont quant à eux tous membres du groupe spécial « Profs ».

4.6.1.3 Points de stockage

Le profil des utilisateurs est de type itinérant et est stocké sur un des contrôleurs de domaine. Ceci est nécessaire car certains logiciels réclament un enregistrement de licence par utilisateur, et le fichier licence est stocké sur le profil.

Les utilisateurs possèdent un dossier de base sur le réseau qui leur permet de stocker des données. Ce dossier est stocké sur un serveur de fichier windows. Il est accessible aux postes windows et linux grâce au protocole cifs.
Les utilisateurs disposent également de répertoires partagés sur le serveur de fichier windows. Un répertoire « partage » possédant des droits d'accès en écriture pour tous les utilisateurs authentifiés, ainsi qu'un répertoire « partage restreint » dans lequel seuls les membres du groupe « profs » ont le droit d'écriture.

4.6.1.4 Étude des populations

Les populations sont de trois types :
Les personnels techniques qui sont membre du Service Numérique d'Assistance et de Proximité.

Les enseignants qui possèdent des comptes dans l'annuaire ont trois profils différents.
• Une majorité proviennent des départements d'enseignement classiques. « Département informatique » pour l'annuaire dédié à l'enseignement de l'informatique, «Département Biologie et Géosciences » pour l'enseignement de la biologie.
• Une autre partie vient d'entités de recherche de l'université. L'Institut de Recherche en Informatique de Toulouse est très bien représenté dans l'annuaire « informatique ». Nous avons cependant de nombreux enseignants qui proviennent de laboratoires très divers de l'université.
• Une dernière partie est composée d'enseignants extérieurs et intervenants provenant d'entreprises. Cette population n'est à priori pas présente dans l'annuaire LDAP universitaire. (à moins d'être dans la base invité, mais sans affectation)

Les groupes étudiants sont généralement une retranscription des étapes Apogée de l'annuaire universitaire. Par exemple les étudiants membres du groupe de l'active directory L3-INFO-1314 sont tous inscrits à l'étape apogée ELINF1111$L3 INFORMATIQUE.
Voici des tableaux résumant les comptes trouvés dans l'Active Directory.

Tableau VIII : Étude des populations des annuaires Active Directory de la FSI

ENTITES	DESCRIPTIONS	QTE
Départements d'enseignement	DEPARTEMENT INFORMATIQUE	46
	Département Biologie et Géosciences	29
	Département Electronique-Electrotechnique-Automatique	5
	DEPARTEMENT DE MATHEMATIQUES	3
	Département de Mécanique	2
	DEPARTEMENT DE CHIMIE	1
	Département de Physique	1
Service informatique	Service numérique d'assistance de proximité	13
Laboratoires	Inst. Recherche en Informatique Toulouse UMR 5505	23
	UMR 5277 Inst. de Rech.en Astrophysique et Planétologie IRAP	3
	UMR 5566 Lab Etudes Géophysique Océanographique LEGO	2
	Lab. Physique Homme Appliquée à Environnement EA	1
	Lab.Matériaux Durabilité des Constructions Tlse EA 3027	1
	UMR 5505 I.R.I.T.	1
	Laboratoire Evolution et Diversité Biologique UMR 5174	1
ETAPE APOGEE	EDDST1111$L1 STS	746
	ELBCP1111$L3 BIO. PARCOURS BCP	214
	EMBEC1111$M1 ECOLOGIE	189
	EMBBT1111$M1 BBT	180
	EMINF1131$M1 INFORMATIQUE	179
	EMBMA1111$M1 MABBS	146
	EDINF1111$L2 INFORMATIQUE	133
	EMBST1111$M1 BIOSANTE	119
	ELINF1111$L3 INFORMATIQUE	111
	...	

4.6.2 Amélioration du processus de création des utilisateurs :

De la même manière que pour l'annuaire openldap tampon, la gestion des identités des utilisateurs se fait en deux parties. L'arborescence des utilisateurs doit être également divisée :

• Une unité d'organisation ups où les comptes seront créés et supprimés par des scripts en fonction de leur cycle de vie sur l'annuaire LDAP universitaire. Le mot de passe utilisé sera déporté sur le royaume kerberos de l'Université, à l'aide d'une relation d'approbation entre le domaine Active Directory et le royaume Kerberos.

• Une unité d'organisation locale, où les comptes pourront être créés à la main, ou à l'aide des anciens scripts qui seront toujours fonctionnels. Les mots de passe seront locaux

Je vais présenter un script permettant l'automatisation de la création des comptes, avec un login basé sur celui de l'annuaire universitaire, et se basant sur la notion d'étape apogée. Ce script prend en entrée deux fichiers

Un fichier csv autorisationAffectations

« affectation ; nom local ad »

• L'affectation est égale à celui de l'attribut supannAffectation de l'annuaire LDAP

• Le Nom local sera le nom du groupe de sécurité Active Directory.

Exemple :

Service Numérique d'assistance à la proximité;snap

Un fichier csv autorisationsEtapes :

« Libelle Etape Apogee ; Nom Local AD »

• Le libelle Apogée est égal à celui de l'attribut mipLicEtp de l'annuaire LDAP

• Le Nom local sera le nom du groupe de sécurité Active Directory.

Exemple :

ELBCP1111$L3 BIO. PARCOURS BCP;L3BCP

Les utilisateurs créés seront affectés au groupe principal « utilisateurs du domaine ».Pour les groupes secondaires, ils seront affectés dans tous les groupes dans lesquels ils sont inscrits dans le LDAP universitaire, et qui sont présents dans le fichier autorisationsEtapes.
Les scripts sont écrits en powershell et exécutés de manière régulière par le planificateur de tâches.
Les algorithmes sont présentés dans les annexes.

4.7 Unification de l'authentification :

L'unification des identifiants des utilisateurs est obtenue en synchronisant les comptes avec ceux de l'annuaire universitaire. Cette synchronisation est faite pour les comptes de l'annuaire LDAP tampon et pour les annuaires Active directory.
L'unification de l'authentification est obtenue en utilisant le mot de passe des principaux du royaume Kerberos. Le lien de l'annuaire openldap avec le royaume kerberos vient de la procédure « PassThrough Authentication », en attribuant à l'attribut userPassword la valeur « {SASL}uid@ROYAUME ».
Le lien des annuaires active directory avec le royaume kerberos provient d'une relation d'approbation monodirectionnelle. Les domaines Active Directory doivent approuver le royaume kerberos. Un attribut supplémentaire doit être ajouté pour chaque utilisateur de l'AD : l'attribut altSecuritesIdenties avec comme valeur « Kerberos:uid@ROYAUME »

Le mot de passe de Kerberos doit être positionné lorsque l'utilisateur modifie son mot de passe sur l'intranet de l'Université. La procédure de changement de mot de passe est maintenue par le service DSIG. Nous avons donc exprimé les besoins et demandé que cette nouvelle opération soit intégrée dans la procédure.

4.7.1 L'installation des serveurs Kerberos :

Le service Kerberos est installé sur deux machines virtuelles.
Le premier serveur comporte le service kadmind pour la création des principaux et le changement de mot de passe et le kdc pour la distribution de ticket.
La disponibilité est assurée par le mécanisme Fault Tolerance de Vm Ware. Ce mécanisme permet qu'une machine de backup prenne immédiatement la succession si le serveur a un problème. La principale limitation de Fault Tolerance est qu'il ne peut être mis en place que

sur des machines monoprocesseurs. Cependant le service kadmind, qui est le plus gourmand en ressource processeur, est monothread et donc ne tire parti que des ressources d'un processeur.
Le deuxième serveur ne possède que le service kdc, et répond à l'authentification uniquement si le premier serveur ne répond pas dans le temps imparti. Le mécanisme de synchronisation est à l'initiative du serveur maître et est effectué toutes les quinze minutes.
Le backend utilisé est File. Les serveurs sont sauvegardés par les systèmes de sauvegarde du service H3S. Le monitoring est fait par nagios. Il effectue des statistiques sur le nombre de tickets délivrés, ainsi que sur le temps de réponse des différents services. Ceci permet d'être informé en temps réel sur les dysfonctionnements des services, car une personne est toujours d'astreinte pour surveiller le monitoring nagios.

Il faut également que l'ensemble des serveurs impliqués dans le processus d'authentification soient synchronisés au niveau de l'heure car l'authentification Kerberos n'autorise pas par défaut un décalage de plus de 5 minutes. Le protocole NTP doit donc être configuré.

4.7.2 Création des principaux

La création des principaux est effectuée par le script de synchronisation de l'annuaire LDAP tampon. C'est celui ci qui doit ajouter un principal lorsqu'il crée un utilisateur.
Techniquement un utilisateur spécial nommé dsrtadm est créé sur le serveur kadmind, pour pouvoir se connecter par l'intermédiaire du système de clef ssh. Cet utilisateur est relié à un principal kerberos nommé dsrtadm/admin dont la keytab (fichier qui contient le hash du mot de passe) est stocké dans son répertoire. Le fichier de droit de kerberos krb5.acl donne les droits d'administration à tous les utilisateurs se terminant par /admin.
Il est également envisageable de dédier la création et la suppression des principaux kerberos à DSIG dans le cadre d'une généralisation de l'utilisation de kerberos à l'ensemble de l'Université.

La création des principaux est effectuée en utilisant les API Kerberos de perl. Si la création du principal échoue, on ajoute un avertissement dans les logs et on prévient l'équipe système par email.

Le script de synchronisation Active Directory teste également la présence des principaux kerberos, et envoie des avertissements aux équipes en cas d'absence.

4.7.3 Procédure de changement de mot de passe

La procédure de changement de mot de passe est intégrée dans le processus de changement de mot de passe de l'intranet géré par le service DSIG. Ce processus est consommateur de temps processeur car le démon kadmind utilise des opérations string-to-key délibérément intensives pour préserver de certains types d'attaques. Si trop de changements de mot de passe sont initiés en même temps, le serveur kadmind peut ne plus répondre aux sollicitations pour une courte période de temps. D'après mes tests, une vingtaine de changements de mot de passe simultanés mettent le serveurs à la limite de ses possibilités. Il est donc préférable que le processus client teste le résultat d'un changement de mot de passe et informe l'utilisateur de la réussite ou de l'échec de celui-ci.
La première version de la procédure de dsig n'implémente pas de test de la réussite de ce changement et sera modifiée dans un futur proche.

4.7.4 Authentification depuis l'annuaire LDAP Tampon

L'authentification sur l'annuaire LDAP tampon est déportée sur le serveur Kerberos par le mécanisme de « Pass Through Authentication ».
Ce mécanisme permet de déléguer le mécanisme de vérification du mot de passe à un processus séparé. Le mécanisme est sélectif et il n'affecte que les utilisateurs dont l'attribut userPassword possède le marqueur « {SASL} ».
Le processus externe utilisé est le processus saslauthd. Celui peut être configuré de différentes manières et peut dédier l'authentification à des fichiers, un autre serveur LDAP, un serveur Kerberos ou tout autre système supportant le mécanisme pam.[44]

Pour les comptes synchronisés avec l'annuaire LDAP tampon, nous mettrons comme valeur « {SASL}uid@UNIV-TLSE3.FR » pour l'attribut userPassword.
L'UID de l'utilisateur et le principal kerberos correspondant seront donc identiques.

Il faut que le serveur exécutant saslauthd soit autorisé à interroger le serveur Kerberos :
Il doit exister un principal host/hostname.univ-tlse3.fr dans la base de données kerberos.

La keytab (fichier contenant le hash du mot de passe) doit être présente sur le serveur exécutant saslauthd dans la keytab par défaut. La keytab par défaut est celle définie par la directive default_keytab_name dans /etc/krb5.conf.

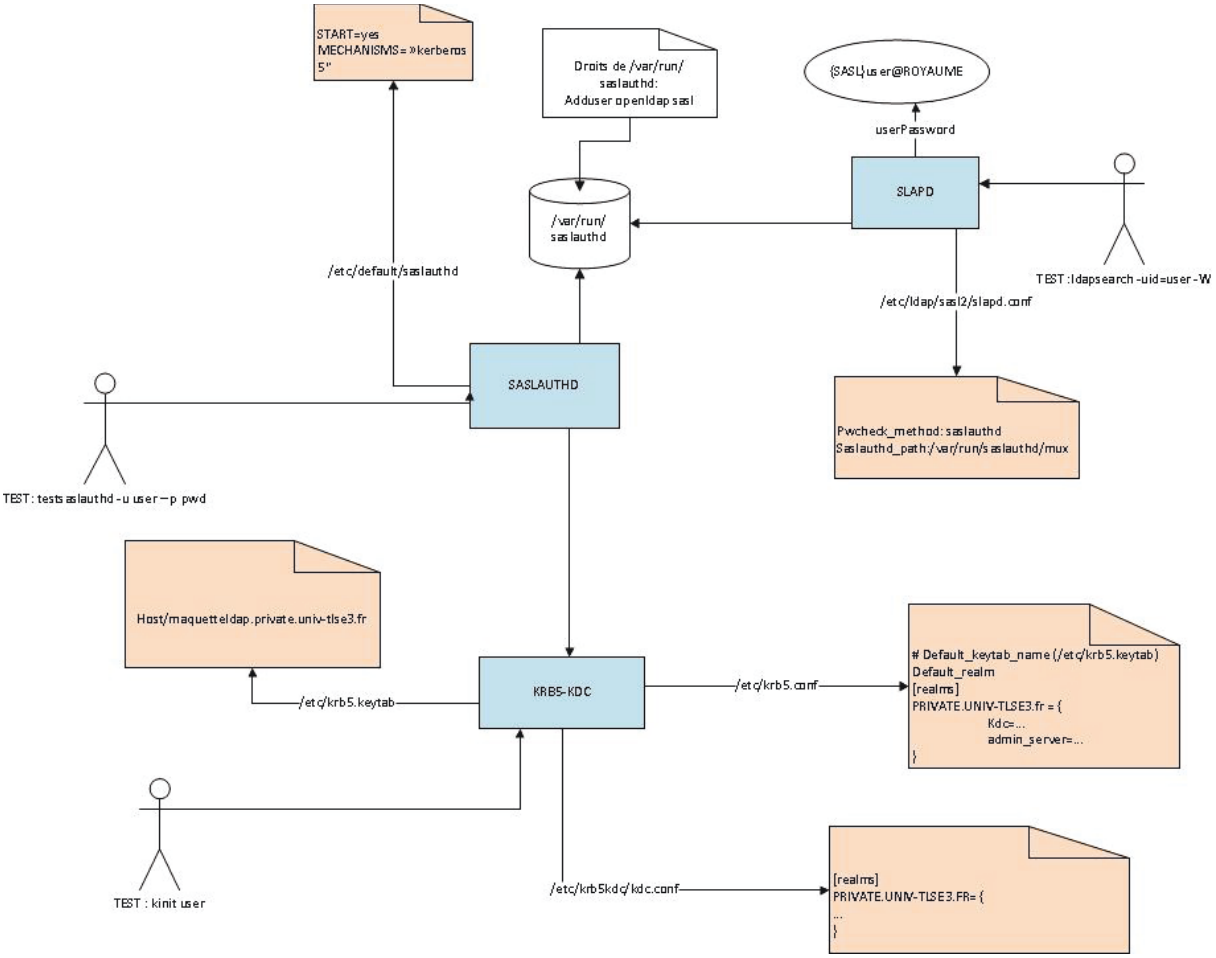


Figure 33: Description de la procédure de « PassThrough Authentication » entre LDAP et kerberos

4.7.5 Authentification depuis l'annuaire Active Directory :

Pour profiter du serveur Kerberos depuis Active Directory, il faut définir une relation d'approbation entre les deux entités.

Une relation d'approbation permet généralement aux utilisateurs d'un domaine windows d'accéder aux ressources d'un autre domaine windows. Elle peut être mono ou bi-directionnelle. Par exemple, les utilisateurs d'un domaine B peuvent accéder aux ressources

d'un domaine A si le domaine A approuve le domaine B. Elle peut être transitive ou non, c'est à dire que les utilisateurs d'un domaine C peuvent accéder aux ressources du domaine A si le domaine B approuve le domaine C et que le domaine A approuve le domaine B avec une relation transitive.
Dans notre cas, nous créerons une relation d'approbation monodirectionnelle et non transitive entre le domaine windows et le royaume Kerberos.

La relation d'approbation peut être créée par interface graphique ou ligne de commande. Voici la commande permettant d'approuver le royaume Kerberos UNIV-TLSE3.FR depuis un domaine windows de test TEST.SNAP.FSI :
netdom trust TEST.SNAP.FSI /Domain:PRIVATE.UNIV-TLSE3.FR /add /realm /passwordT:toto

Parallèlement, il faut créer sur le serveur Kerberos un principal nommé krbtgt/TEST.SNAP.FSI@UNIV-TLSE3.FR. La forme du principal commençant par krbtgt indique que ce principal peut créer des tickets Ticket Granting Ticket (TGT).
Le mot de passe associé au principal doit être le même que celui fourni à la relation d'approbation Windows.

Implication dans le nommage des domaines windows :
Le cœur d'un domaine Active Directory est composé d'un annuaire LDAP et d'un royaume Kerberos. Pour cette raison et pour pouvoir différencier les royaumes Kerberos, il faut faire attention de ne pas nommer de la même façon les domaines Windows et le royaume Kerberos. Le fait que nous avons créé un royaume kerberos nommé UNIV-TLSE3.FR implique qu'on ne peut pas créer de domaine windows UNIV-TLSE3.FR

Effectuer le lien entre les utilisateurs du domaine windows et les principaux kerberos :
Dans le processus de connexion des utilisateurs dans le domaine windows, les informations utilisateurs (nom, prénom, cn, login, sid) proviendront de l'Active Directory. Seule l'authentification est déportée sur le royaume kerberos.

Pour ce faire, il faut que chaque utilisateur possède un attribut nommé altSecurityIdentities qui indique l'identité du principal correspondant au compte. L'attribut altSecurityIdentities doit être de la forme Kerberos:login@UNIV-TLSE3.FR ou login est l'uid de l'utilisateur.

Les utilisateurs windows possèdent également un mot de passe Active Directory et ils peuvent se logguer de deux manières sur les postes de travail:

- login uid@TEST.SNAP.FSI avec le mot de passe Active Directory
- login uid@UNIV-TLSE3.FR avec le mot de passe kerberos.

Pour ne pas ajouter de la confusion, il convient de ne pas distribuer le mot de passe Active Directory aux utilisateurs. Il est également préférable de régler le domaine par défaut de l'ensemble du parc sur le royaume Kerberos. Les utilisateurs alors pourront se logger en tapant uniquement leur UID associé au mot de passe kerberos. Ce réglage se fait simplement en utilisant les stratégies de groupe Active directory.

Un dernier réglage consiste à ajouter la localisation du serveur kdc aux postes de travail . En effet, l'authentification initiale et la demande KRB_AS_REQ a lieu entre le poste de travail client et le serveur Kerberos. Le poste de travail connaît le nom du royaume par l'intermédiaire du champ altSecurityIdentities, il lui manque la connaissance du ou des serveurs kdc de celui-ci.
On peut par exemple l'ajouter sur chaque poste par une ligne de commande :
ksetup /addkdc UNIV-TLSE3.FR kdc.private.univ-tlse3.fr

Authentification depuis des postes linux :

Bien que les postes linux puissent s'authentifier nativement sur l'annuaire LDAP tampon, ils sont actuellement configurés avec de l'authentification winbind sur les Annuaires Active Directory.
De plus l'espace de stockage est géré par le protocole cifs sur un serveur de fichier Windows et permet d'unifier l'espace de stockage des utilisateurs d'Active Directory.

L'authentification depuis les postes linux peut être configurée en utilisant winbind pour obtenir les informations utilisateurs et le module pam pam_krb5 pour la vérification du mot de passe.
L'utilisateur obtient alors un tgt fourni par le serveur kerberos. Comme le serveur de fichier est membre du domaine qui approuve le royaume kerberos, il accepte le tgt de l'utilisateur pour que celui-ci accède à son répertoire réseau cifs.
Le montage cifs peut se faire en utilisant autofs avec comme configuration :
* -fstype=cifs, sec=krb5i, user=&, uid=$UID, cruid=$UID, file_mode=0700, dir_mode=0700, noserverino ://DC1/data/&

4.7.6 Monitoring de Kerberos :

Le serveur kerberos étant un service critique pour l'authentification, nous avons installé des plugins nagios pour le monitorer. Ces plugins sont exécutés depuis un serveurs nagios avec une connexion en ssh sans mot de passe.

Les plugins nagios effectuent un ou une série de test et retournent une valeur de sortie indiquant le résultat ainsi qu'une phrase d'explication. Pour générer des graphiques, centreon est intégré a nagios et utilise les résultats des plugins. Pour ce faire le retour des plugins a été modifié avec l'ajout des valeurs à monitorer par nagios.

Vérifier le fonctionnement du serveur kadmind :

Le plug-in check_kadmin.pl est un script perl se connectant simplement au serveur kadmind. Il mesure la durée de connexion et renvoie un état warning ou critical si un certain seuil est dépassé.
Nous considérons que le seuil warning est à 10 secondes et le seuil critique à 20 secondes.

Exemple d'utilisation :

```
./check_kadmin.pl  -w 10 -c 20 -u nagios -k /var/spool/nagios/nagios.keytab -r UNIV-TLSE3.FR
OK: Connected to kadmin daemon in 0.0274930000305176 seconds | kadmin-time=0.0274930000305176s;;;;
```

Vérifier le fonctionnement du serveur kdc :

Le plugin check_kdc effectue simplement un kinit pour récupérer un ticket depuis le serveur kdc.

Le résultat est donc binaire, on peut avoir STATE_OK ou STATE_CRITICAL.

Exemple d'utilisation :

check_kdc -H kdc.private.univ-tlse3.fr -p nagios@UNIV-TLSE3.FR -k /var/spool/nagios/nagios.keytab -P 88

- OK : kinit response time : 0.015 | kdc-time=0.015s;;;;
- CRITICAL Getting Kerberos ticket: kinit: Cannot contact any KDC for realm 'UNIV-TLSE3.FR' while getting initial credentials

V Conclusion

La mise en place de l'authentification unifiée sur les systèmes unix a eu lieu en mars 2014. Le livrable comprend six machines virtuelles : deux serveurs kerberos redondés, deux serveurs openldap, un serveur web dédié à l'administration manuelle des comptes et un serveur web dédié au changement des mots de passe locaux à l'openldap. La gestion des identités repose sur la modification de trois procédures : la synchronisation des comptes sur l'annuaire LDAP tampon et l'archivage des comptes obsolètes qui sont développés en perl, la modification du mot de passe du principal kerberos depuis l'intranet de l'université.

La phase la plus délicate a été la mise en place de la communication nécessaire, les utilisateurs devant changer leur mot de passe avant la première connexion. Une bonne proportion des utilisateurs s'est équipée de smartphone et a pu les utiliser pour effectuer cette opération.

Une évolution souhaitable de l'authentification est la mise en place d'un mécanisme d'un SSO de type système. Il faut pour ce faire utiliser les modules pam pam_krb5 et autoriser l'authentification GSSAPI sur les « démons » SSH des serveurs unix. Ceci permettrait aux utilisateurs de naviguer d'un serveur à l'autre sans avoir à retaper de mot de passe.

La prochaine étape prévue est la mise en place de l'authentification unifiée sur les postes de travail des salles d'enseignement de la Faculté des Sciences et d'Ingénierie par l'intermédiaire

des contrôleurs de domaine Active Directory. Les différents composants sont actuellement en test et la migration profitera du retour d'expérience acquise à DSRT.

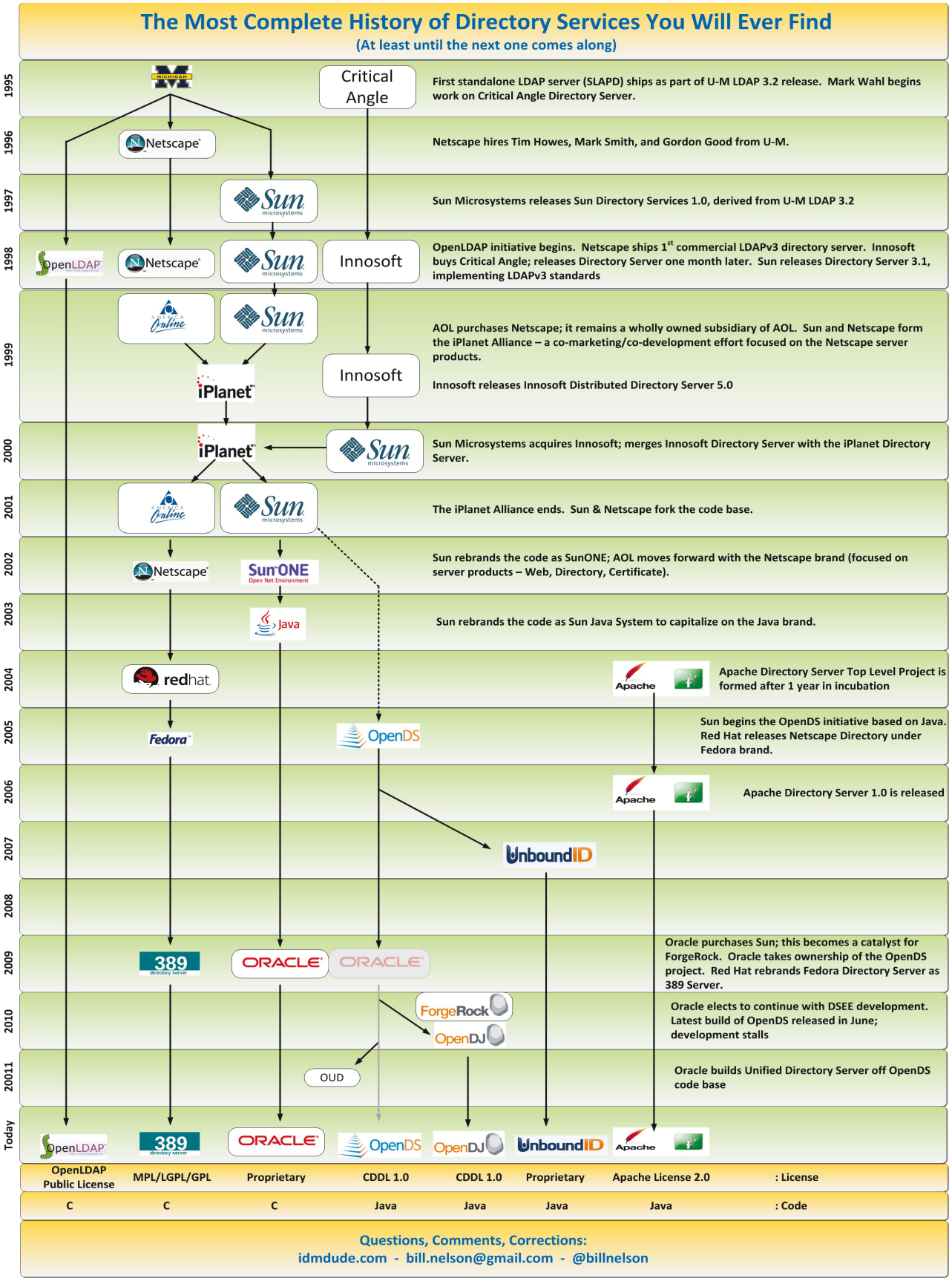
Une autre évolution possible concerne les bases de données Oracle dont on peut faire évoluer l'authentification vers une authentification LDAP ou kerberos.

Il est également souhaitable de généraliser l'utilisation de kerberos aux serveurs d'authentification CAS et Shibboleth. Ceci permet d'effectuer des opérations SSO entre l'authentification système et l'authentification web. L'utilisateur se connectant sur un poste de travail ou un serveur verra son identité connue s'il se connecte sur une liste de sites prédéfinis, au prix d'une configuration préalable du navigateur internet.

La problématique associée du stockage doit être réfléchie, en unifiant par exemple les données des utilisateurs sur des éléments de stockage utilisant à la fois le protocole Cifs pour le monde windows et le protocole Nfs pour le monde linux. Cette opération, comme vu dans le chapitre 2.9, a pour préalable un rapprochement entre les annuaires LDAP et Active Directory.

Enfin, il peut être intéressant d'étendre la portée d'utilisation du système à l'ensemble de l'Université et d'en faire profiter ses diverses composantes. Pour ce faire, il faudrait penser à une architecture Active Directory globale reliant les annuaires des différentes composantes au moyen de relations d'approbations. Ouvrir une discussion avec la communauté d’universités et d’établissements (Comue) permettrait d'établir les bases d'une fédération « authentification système ».

ANNEXES Historique des annuaires LDAP [19]



BIBLIOGRAPHIE

AUTHENTIFICATION

[1] Challenges in identity management and authentication.Dag-Erling Smørgrav 2012 EuroBSDCon
http://blog.des.no/2013/09/challenges-in-identity-management-and-authentication/

AUTHENTIFICATION UNIX

[2] Unix password encrytion considered insecure. Philip Leong. Chris Tham. USENIX 1991
http://www.cse.cuhk.edu.hk/~phwl/mt/public/archives/papers/crypt_usenix91.pdf

[3] Pluggable Authentication Modules. Dag-Erling Smørgrav. 2003
http://www.freebsd.org/doc/fr/articles/pam/article.html

[4] X/Open Single Sign-On Service (XSSO) Pluggable Authentication Modules.The Open Group.1997
http://pubs.opengroup.org/onlinepubs/008329799/toc.pdf

[5]Why Sun's nis will never die. Paul Venezia. Info world.
http://www.infoworld.com/d/data-center/why-suns-nis-will-never-die-219683

[6] S Taruna, Jyoti Chauhan . " Centralized Authentication Using Network Information System (NIS) ", Vol.2 - Issue 3 (March - 2013), International Journal of Engineering Research & Technology (IJERT) , ISSN: 2278-0181 , www.ijert.org
http://www.ijert.org/browse/volume-2-2013/march-2013-edition?download=2860%3Acentralized-authentication-using-network-information-system-nis&start=300

AUTHENTIFICATION WINDOWS

[7] Microsoft NTLM. Site officiel de Microsoft.
http://msdn.microsoft.com/en-us/library/windows/desktop/aa378749%28v=vs.85%29.aspx

[8] pgina site officiel. Question fréquemment posée.
http://pgina.org/faq.html

[9] What are domains and forests. Microsoft
http://technet.microsoft.com/en-us/library/cc759073(v=ws.10).aspx

[10] Simple and Protected GSS-API Negotiation Mechanism (SPNEGO) Extension
http://download.microsoft.com/download/9/5/E/95EF66AF-9026-4BB0-A41D-A4F81802D92C/[MS-SPNG].pdf

[11] HTTP-Based Cross-Platform Authentication by Using the Negotiate Protocol
http://msdn.microsoft.com/en-us/library/ms995329.aspx

KERBEROS

[12] Emmanuel Blindauer. "Référentiel d'authentification interopérable et ouvert: Kerberos". conférence Journées Réseaux 2009.
https://2009.jres.org/planning_files/article/pdf/132.pdf

[13] Nicolas Greneche. "(Securely) Kerberize my University". conférence Journées Réseaux 2011.
https://2011.jres.org/archives/4/index.htm

[14] Guillaume Rousse. "Retour d'expérience sur l'utilisation de Kerberos à l'INRIA.". conférence Journées Réseaux 2011.
https://2011.jres.org/archives/75/index.htm

[15] Kerberos Protocol Tutorial. Fulvio Ricciardi.
http://www.kerberos.org/software/tutorial.html

ANNUAIRES

[16] JM Antoine. "Enjeux d'un annuaire SupAnn, contexte et perspectives".
https://www.jres.org/tuto/tuto11/index

[17] "Etat des lieux des annuaires d'établissements en 2010". Enquête
https://www.cru.fr/documentation/supann/enquete2010

[18] "Recommandations SupAnn 2009". Site officiel
https://www.cru.fr/documentation/supann/2009/index

[19] Bill Nelson. "The Most Complete History of Directory Services You Will Ever Find".
http://idmdude.com/2012/04/13/the-most-complete-history-of-directory-services-you-will-ever-find/

[20] The Lightweight Directory Access Protocol. 1995. Thimoty Howes.
http://www.citi.umich.edu/techreports/reports/citi-tr-95-8.pdf

[21] Le logiciel openldap. Clément Oudot.Raphaël Ouazana.Sébastien Bahloul. Formation Linagora
http://linagora.org/contrib/annuaires/formations/openldap

[22] Understanding LDAP. Heinz Johner, Larry Brown, Franz-Stefan Hinner, Wolfgang Reis, Johan Westman. IBM. SG24-4986-00
http://physik.uibk.ac.at/hephy/grid/project/LDAP_ibm.pdf

[23] Jean-Noël Chardron. "Synchronisation d'annuaire Active Directory et de base LDAP 389DS".
http://opal.resinfo.org/ojs/index.php/opal/article/view/44/22

[24] FreeIpa. Tuto Jres. Jérôme Fenal.
https://www.jres.org/_media/tuto/tuto13/tutojres-13-jeromefenal.pdf

[44] OpenLDAP Software 2.4 Administrator's Guide
http://www.openldap.org/doc/admin24/

RADIUS

[25] eduroam - a technical overview
https://www.eduroam.us/technical_overview

SAMBA

[26] smb.conf — The configuration file for the Samba suite. Manuel d'utilisation
http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html

[27] The Official Samba 3.5.x HOWTO and Reference Guide
http://www.samba.org/samba/docs/man/Samba-HOWTO-Collection/

[28] Samba 4. wiki officiel
https://wiki.samba.org/index.php/Samba

SSO pour les applications web

[29] CAS, OpenID, Shibboleth, SAML : concepts, différences et exemples. Clément Oudot. RMLL 2011
http://fr.slideshare.net/coudot/rmll-2011-websso

[30] Security Assertion Markup Language A Brief Introduction to SAML.Tom Scavo.NCSA
http://grid.ncsa.illinois.edu/presentations/saml-intro-dec05.ppt

[31] Installation d'un SP Shibboleth et Shibbolisation d'application. Renater.
https://services.renater.fr/federation/docs/installation/sp_decembre2012#installation_d_un_sp_shibboleth_et_shibbolisation_d_application

AUTHENTIFICATION GRAND PUBLIC

[32] OpenId Connect. The MITRE Corporation.
civics.com/wp-content/uploads/2012/04/OpenID-Connect-Lecture-for-MIT.pptx

[33] Can Social Identities Make Your Life Easier?John Krienke. David Langenberg. Dedra Chamberlin. CAMP 2013
https://spaces.internet2.edu/download/attachments/37650846/ID+Week+Social+Identities+Preso+%281%29.pdf?version=1&modificationDate=1385051215240

DIVERS

[34] Synchronizing to/from Active Directory. LDAP Synchronisation Connector
http://lsc-project.org/wiki/documentation/2.1/howtos/activedirectory

[35] SSSD. Client Side Identity Management. Linux Days 2012
https://fedorahosted.org/sssd/raw-attachment/wiki/Documentation/linuxdays-2012-sssd.pdf

[36] Mise en oeuvre de la gestion des groupes via Grouper dans une université au sein du consortium ESUP-Portail en France
http://schedule2012.rmll.info/IMG/pdf/RMLL2012-Grouper.pdf

AUTHENTIFICATION FORTE

[37] Step-up Authentication-as-a-Service . Surfnet. 2012
http://www.surf.nl/binaries/content/assets/surf/en/knowledgebase/2012/rapport_step-up_authentication-as-a-service_architecture_and_procedures_final.pdf

[38] OATH Reference Architecture, Release 2.0 .Initiative for Open AuTHentication (OATH)
http://www.openauthentication.org/files/download/oathPdf/ReferenceArchitectureVersion2.pdf

[39] SMS-Based One-Time Passwords: Attacks and Defense. Collin Mulline, Ravishankar Borgaonkar, Patrick Stewin, and Jean-Pierre Seifert. 2013
http://www.mulliner.org/collin/academic/publications/mulliner_dimva2013.pdf

Request For Comment de l'IETF

[40] SPNEGO-based Kerberos and NTLM HTTP Authentication in Microsoft Windows rfc4559
http://tools.ietf.org/html/rfc4559

[41] Radius support for EAP. RFC 3579
http://www.ietf.org/rfc/rfc3579.txt

MANAGEMENT D'IDENTITES

[42] Sésame 2 : vers une gestion d’identités moderne.Pascal Aubry, Henri Jacob, Saâd Aït Omar
https://conf-ng.jres.org/2013/document_revision_1476.html?download

[43] "AMUE : PRISME - Référentiel des données partagées".
https://2009.jres.org/planning_files/slideshow/pdf/130.pdf

STOCKAGE

[44] Integration of a Netapp Storage System with a unix based LDAP Server. Network Appliance. TR-3464. 2Avril 006
http://www.netapp.com/us/system/pdf-reader.aspx?pdfuri=tcm:10-61150-16&m=tr-3464.pdf

[45] Unified Windows and UNIX Authorization Using Microsoft Active Directory LDAP as a Directory Store. Ellie Berriman, Reena Gupta, Srinivas Addanki, NetApp
March 2010. TR-3458
http://www.netapp.com/us/media/tr-3458.pdf

LISTE DES FIGURES

LISTE DES TABLEAUX

RESUME

Etude de la simplification et de l'unification de l'authentification, pour l'accès à un réseau informatique, dans le contexte des Universités. Le problème est scindé, alors, en trois niveaux différents : celui de l'authentification réseau, de l'authentification applicative et de l'authentification système.

Une solution est proposée, ensuite, intégrant l'unification de l'authentification, dans un contexte qui tienne compte, à la fois, de la fédération d'identités et de l'authentification unique.

Le remplacement d'un annuaire NIS, en production, par un annuaire LDAP, incluant le transfert des données des utilisateurs, est, alors, envisagé.

Enfin, est examiné comment s'intégreront les annuaires d'authentification OpenLDAP et Active Directory, grâce à un royaume Kerberos.

Mots clés : OpenLDAP, Active Directory, Kerberos, SSO

SUMMARY

Study of the simplification and unification of authentication to a computer network, in a University setting. The problem is then split between three levels: network authentication, software authentication and system authentication.

A solution is suggested, encompassing the unification of authentication, in a context that takes both identity merging and SSO into account.

The replacement of a NIS directory, currently in use, with an LDAP directory, including transfer of user data, is then considered.

Finally, the integration of openLDAP and Active Directory authentication, thanks to a Kerberos realm, is analysed.

Keywords : OpenLDAP, Active Directory, Kerberos, SSO.