Itinéraire d'un système de gestion d'identités numériques au sein d'un EPST

Antoine Gallavardin, Christophe Monrocq, Guillaume Perréal

Itinéraire d'un système de gestion d'identités numériques au sein d'un EPST

Antoine Gallavardin
Responsable du Service Informatique du centre de Lyon-Villeurbanne
5 rue de la Doua
69100 Villeurbanne

Guillaume Perréal
Lead Developper
Pôle Informatique Scientifique
5 rue de la Doua
69100 Villeurbanne

Christophe Monrocq
Responsable Pôle Gestion Décisionnel
DSIN
1 rue Pierre-Gilles de Gennes
92761 Antony

Résumé

Fusion, migration, externalisation, changement de nom…

Autant d'étapes dans la vie d'un établissement public scientifique et technique (EPST) et donc autant d'impacts sur le système d'information.

Les systèmes de gestion des identités et des comptes sont évidemment concernés, car ils pilotent toutes les informations des utilisateurs, internes et externes, afin de leur assurer un service efficace (messagerie, accès aux applications).

En 10 ans, Irstea a changé de nom, intégré la fédération RENATER, migré de ActiveDirectory 2003 à ActiveDirectory 2012, externalisé sa messagerie sur Partage, mis en place un système Single Sign On et intégré le système SINAPS. Et en cette fin d'année, Irstea s'apprête à fusionner avec l'INRA pour donner naissance à l'INRAE.

Après une présentation du contexte d'Irstea, nous reprendrons les grandes étapes de cette évolution, avec pour chacune d'elles un retour d'expérience technique allant de l'abandon de l'une ou l'autre des solutions, à l'adaptation de briques existantes voire au développement en interne ou externe.

Nous continuerons sur un retour d'expérience méthodologique et stratégique regroupé en 4 axes :

- *l'interopérabilité entre les différents composants du système d'information ;*
- *l'usage important des ressources proposées par la communauté ESR (Partage pour la messagerie, SINAPS pour le pilotage des identités, SupAnn pour la structuration des données) ;*

– *la sollicitation des réseaux de prestataires, des réseaux métiers et communautaires ;*

– *le principe de la cathédrale et du bazar.*

Mots-clefs

Partage, SINAPS, ORCID, ActiveDirectory, FusionDirectory, identité, annuaire, provisioning, cycle de vie, messagerie, SupAnn

1 Introduction

Le système de gestion des identités est non seulement le premier composant utilisé lors de l'arrivée d'un nouveau collaborateur, mais c'est aussi le premier impacté lors d'un changement d'organisation. C'est, de fait, une brique essentielle du système d'information.

Le système de gestion des identités de l'Irstea est né, a grandi et vit en en fonction des évolutions imposées, souhaitées et planifiées dans le cadre de la modernisation du système d'information actuel et futur.

Cet article est la transcription de la genèse d'un système de gestion des identités, partant d'un besoin local à une nécessité institutionnelle, avec des retours d'expérience sur la gestion à long terme et les solutions techniques à des problématiques précises.

Ceci n'est en aucun cas un guide pas à pas ou un guide de bonnes pratiques, mais plutôt un recueil de retours d'expérience destinés à ceux qui ont un projet de gestion des identités et qui sont tentés par l'approche « cathédrale » ou « bazar » décrite par Eric S. Raymond dans son ouvrage « La cathédrale et le bazar » [1].

La plupart des étapes sont accompagnées de « règles » qui émanent de son ouvrage et qui se sont vérifiées à maintes reprises.

Après avoir ainsi décrit la genèse d'un annuaire technique d'établissement, l'article continuera sur sa jonction avec les systèmes d'information RH avant de conclure.

2 Le contexte

2.1 Présentation de l'institut

Irstea est un établissement à caractère scientifique et technique (EPST) qui, jusqu'en 2012, s'appelait Cemagref.

Ses thèmes de recherche sont regroupés en 3 départements scientifiques : Territoires, Écotechnologie, Eau.

L'institut est composé de 700 chercheurs, 250 doctorants, 290 chercheurs associés et est réparti sur 8 sites distincts en France métropolitaine.

La Direction des Systèmes d'Information est divisée en 3 pôles :

– le pôle Gestion Décisionnelle en charges des systèmes de gestion financière, ressources humaine et immobilière,

– le pôle Informatique Scientifique en charge du développement d'applications scientifiques,

– le pôle Informatique, Réseaux et Technologies de l'Information en charge des infrastructures informatiques.

Une équipe informatique de centre sous la responsabilité fonctionnelle de la DSI est présente sur chaque site avec leur infrastructure de stockage et de virtualisation.

Le 1 janvier 2020, l'Irstea et l'Inra (Institut National de la Recherche Agronomique [2]) fusionneront pour donner naissance à l'Inrae.

2.2 Un SI fragmenté et isolé

2.2.1 Un système d'information fragmenté

En 2007, et du fait de la limitation de certaines liaisons réseaux interrégionales, chaque site administrait son propre système d'information, composé notamment d'un service d'annuaire et de messagerie.

La majorité des sites Irstea disposait d'un domaine ActiveDirectory local et d'une messagerie Exchange, sauf le site de Lyon qui avait le quatuor NIS / Samba / OpenLdap / Dovecot.

Cette disparité technique rendait difficile la gestion quotidienne des comptes informatiques et des droits et des boîtes de messageries. Il n'y avait en outre que très peu d'échange de données et de dialogue entre les différents pôles de la DSI et les services informatiques régionaux.

2.2.2 Un institut non interconnecté

L'Irstea était, à l'époque, connecté aux systèmes d'information de l'Enseignement Supérieur et de la Recherche uniquement par les liaisons réseaux fournies par RENATER et utilisait quelques listes de diffusion opérées par le Comité Réseaux des Universités.

La notion de fédération d'identité, d'EduRoam était connue, mais leurs implémentations étaient délicates en raison de l'absence d'un annuaire technique d'établissement correctement implémenté et renseigné.

3 La mise en place d'un annuaire d'établissement

3.1 Mise en place de deux annuaires sur le site de Lyon

Règle n°1 : « Tout bon logiciel commence par gratter un développeur là où ça le démange » [1]

3.1.1 Un annuaire technique local

Sur le site de Lyon, 2 sources de données liées aux identités coexistaient :

– une base NIS pour les comptes informatiques [3],

– une application Web avec une base de données pour l'annuaire téléphonique de Lyon,

Cette disparité était contraignante au quotidien et nécessitait des mises à jour régulières sur ces deux systèmes différents et par des acteurs différents.

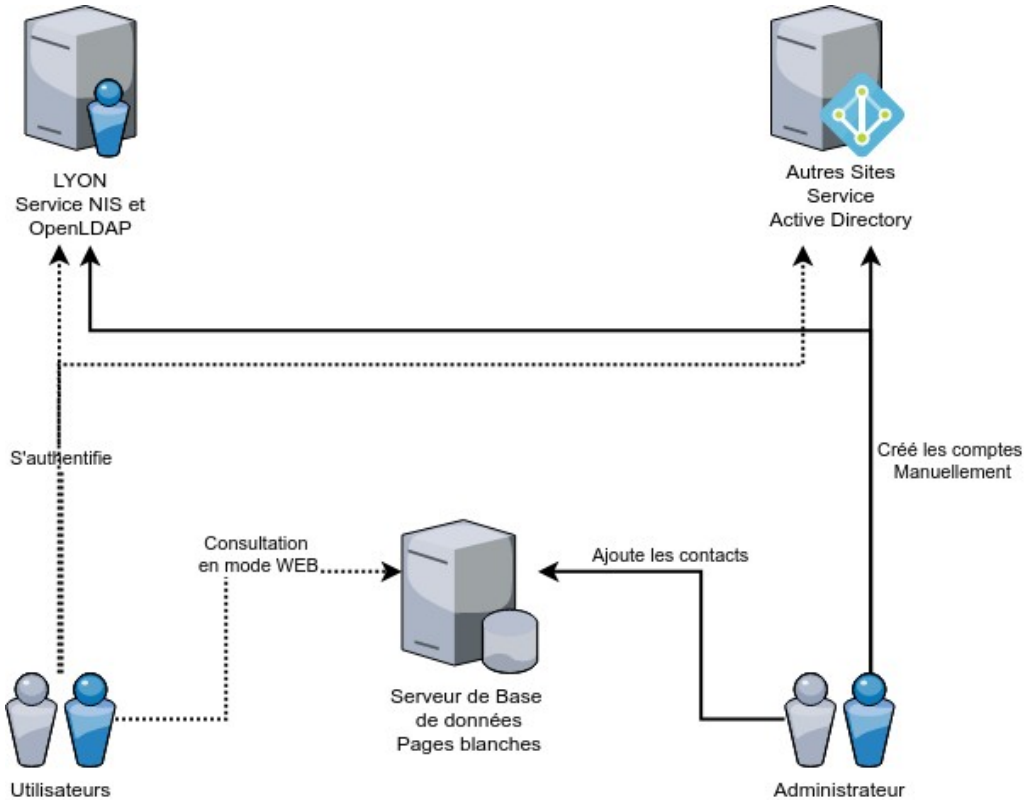

Figure 1 : Disparité des annuaires techniques et fonctionnels

Afin de répondre à la problématique du référentiel de compte et d'annuaire téléphonique local, l'équipe informatique de Lyon a mis en place la pile applicative suivante :

- stockage des données : OpenLDAP [4] ;
- console de gestion : Gosa2 [5] ;
- scripts de bascule : « migrations tools » [6].

L'injection des identités et des groupes a été faite par l'équipe de Lyon, mais le lien avec le contrôleur de domaine NT4 en Samba 3 [7] a été assuré par la société Opensides (lien avec les comptes et groupes utilisateurs et les comptes machines).

3.1.2 Un annuaire pages blanches local avec les données nationales

Règle n°2 : « Les bons programmeurs savent quoi écrire. Les grands programmeurs savent quoi réécrire (et réutiliser). » [1]

En 2008, un autre besoin local est apparu : disposer d'un annuaire de type « pages blanches », regroupant les informations des agents de tous les centres et alimenté de manière automatisée.

Cet annuaire devait être :

- accessible en mode web,
- interrogeable par des clients de messagerie,
- exportable sous un format lisible comme un fichier CSV afin de le consulter hors ligne.

Le protocole commun entre les annuaires ActiveDirectory et OpenLdap étant le protocole LDAPv3, le service informatique de Lyon a développé un script en Perl chargé de recopier les identités de l'annuaire OpenLDAP de Lyon et de l'Active Directory des autres centres pour les déverser dans un autre annuaire OpenLDAP centralisé. Ce script générait également un fichier CSV à la volée.

Une première version d'un annuaire établissement a ainsi vu le jour de manière automatique avec un minimum d'information.

Cette étape a été réalisée en un temps très court, car tous les composants étaient facilement disponibles :

- Perl pour le script de copie d'annuaire [8],
- une interface web de consultation : Contagged [9].

Le retour sur investissement a été immédiat au vu du temps consacré à la mise en œuvre de cet annuaire d'établissement.

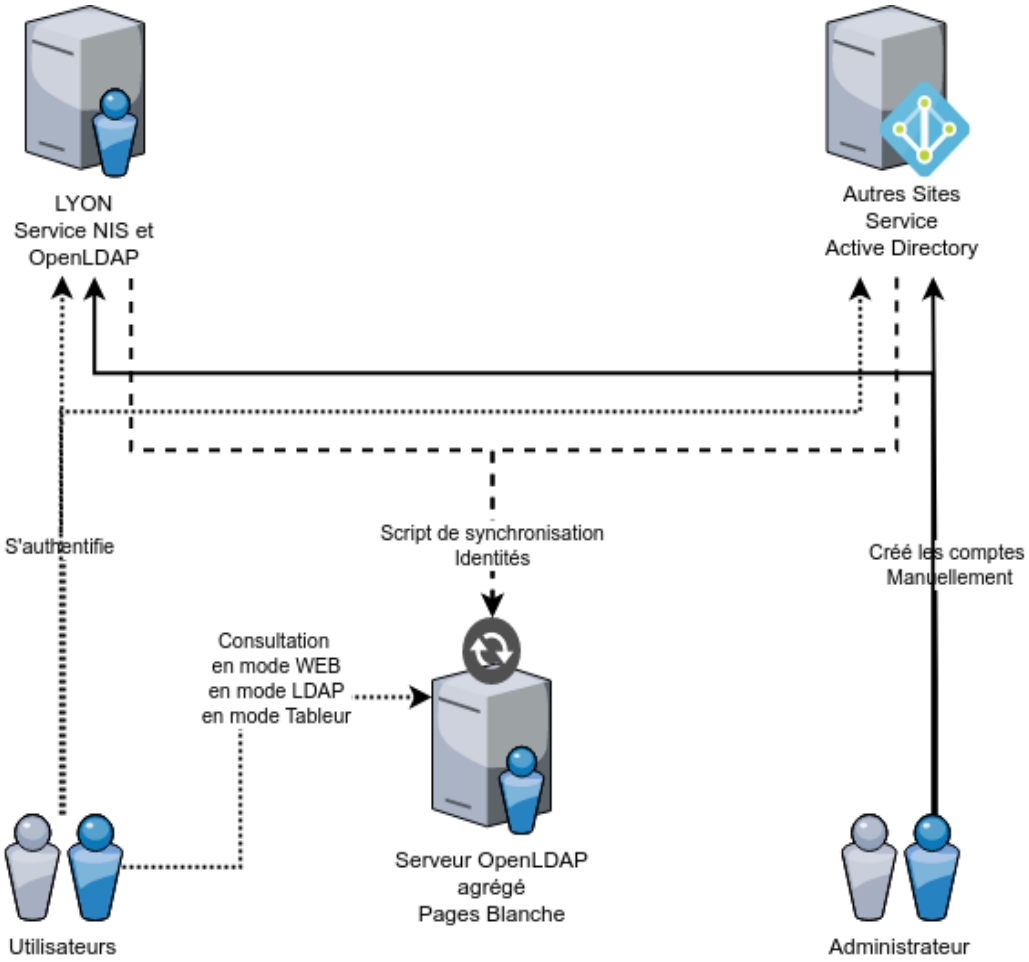

Figure 2 : Agrégation des annuaires techniques pour construire un annuaire fonctionnel

3.2 De l'intérêt de la règle du « Keep It Simple » et de la communauté

3.2.1 Analyse d'un échec

Règle n°3 : « Prévoyez d'en jeter un, car de toute manière, vous le ferez. » [1]

En 2008, le service informatique de la Direction Générale (intégré ensuite à la DSI, lors d'une réorganisation en 2010) a lancé un projet pour mettre en place un méta annuaire (indépendamment de l'annuaire pages blanches cité plus haut).

Celui-ci avait pour objectif de :

- fournir un socle d'échange d'identités entre divers systèmes sans remettre en cause l'autonomie de gestion de ces systèmes (OpenLDAP et AD dans notre cas et éventuellement avec SAP, logiciel utilisé pour notre gestion des Ressources Humaine et des finances),
- structurer les données de cet annuaire par la mise en place d'une organisation de l'annuaire et d'un schéma spécifique.

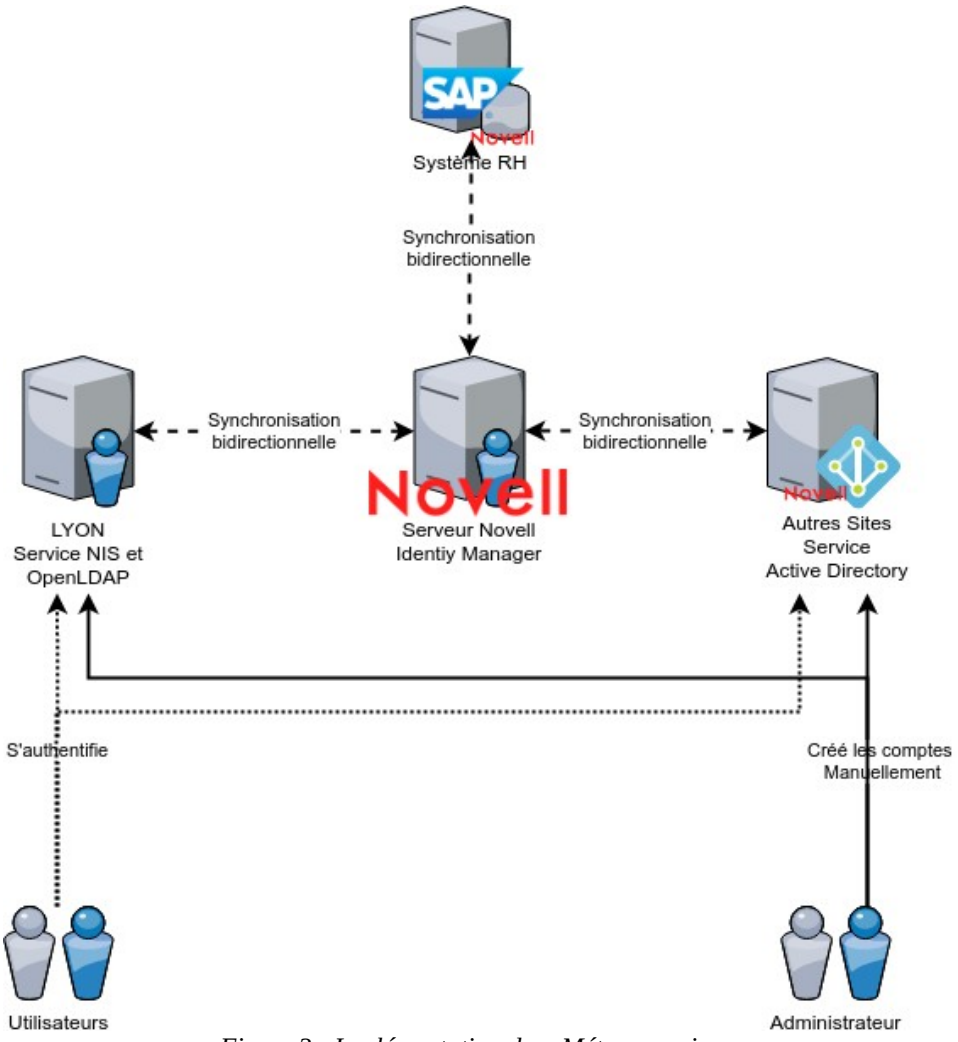

Figure 3 : Implémentation du « Méta annuaire »

Ce projet s'est arrêté pour plusieurs raisons :

- mode de licensing non adapté : coût à l'objet synchronisé ;
- intégration complexe : installation de client de synchronisation sur les contrôleurs de domaine, introduction de nouveaux éléments techniques peu maîtrisés (Novell eDirectory et Novell Identity Manager) ;
- problématique technique sur les mots de passe (mise à jour impossible vers et depuis un OpenLDAP) ;
- périmètre ambitieux, car il nécessitait de fédérer 8 annuaires (7 Active Directory, 1 OpenLDAP), unifier les contenus, structurer les données, sans avoir les ressources humaines en adéquation ;
- résistance au changement de certains acteurs.

La première tentative d'avoir un annuaire global authentifiant s'est donc terminée par un échec, mais elle a été riche d'enseignements, car elle a mis en lumière l'importance des pré-requis suivants :

- utilisation des briques logicielles maîtrisées,
- démonstration de l'utilité d'un tel système au quotidien pour les informaticiens et les utilisateurs,
- anticipation des évolutions, en phase avec les besoins de l'institut,
- définition d'un périmètre réalisable**.**

3.2.2 De l'utilité des rencontres métiers

Règle n°8 : **« *Étant donné un ensemble de bêta-testeurs et de co-développeurs suffisamment grand, chaque problème sera rapidement isolé, et sa solution semblera évidente à quelqu'un. » [1]***

L'annuaire, mis en place par l'équipe de Lyon, répondait à la problématique de la centralisation des identités, mais pas à celle de la centralisation de l'authentification.

Nous étions devant une double problématique :

- trouver une méthode simple adossée à un OpenLDAP,
- faire en sorte que cette méthode soit non intrusive auprès de l'utilisateur et des techniciens informatiques.

Cette dernière a été résolue rapidement au FOSDEM [10], en discutant avec un administrateur d'annuaire, qui a traduit le problème autrement :

« Le problème n'est pas de récupérer les mots de passe, mais de fournir une possibilité d'authentification pour chaque utilisateur »

La différence de socle technique (OpenLDAP et ActiveDirectory) n'était finalement pas une contrainte en soi. Il s'agissait de récupérer pour chaque personne sa méthode d'authentification et de la stocker dans le champ « userPassword » de l'annuaire consolidé.

- Pour OpenLDAP : le mot de passe est simplement synchronisé, car c'est un champ comme un autre.
- Pour ActiveDirectory : le mot de passe est remplacé par une instruction de délégation SASL vers un serveur mandataire [11].

Une expérimentation a été faite rapidement et a été concluante.

3.3 Consolider, structurer et corriger

Les aspects « identification » et « authentification » pouvant être assurés par un seul composant et de manière pérenne, il ne restait qu'à le mettre en place avec des données valables.

Ce nouveau composant, « l'annuaire Maître » a été mis en œuvre en 3 phases :

- mise en place d'une infrastructure répartie du service d'annuaire,

– récupération et structuration des informations,

– utilisation des données et traitement des incohérences.

3.3.1 Mise en place de l'infrastructure

L'infrastructure mise en place est un ensemble de 4 serveurs OpenLDAP (1 « maître » et 3 « esclaves ») sous Debian [12] en utilisant les schémas standards inetOrgPerson et supann2009.

Ce service est accessible en interne uniquement via les protocoles LDAP et LDAPS en connexion anonyme pour les informations de type « pages blanches » et en mode authentifié pour le reste.

3.3.2 Récupération et structuration des informations

Règle n°6 : ***« Traiter vos utilisateurs en tant que co-développeurs est le chemin le moins semé d'embûches vers une amélioration rapide du code et un débogage efficace. »*** **[1]**

Règle n°15 : ***« Quand vous écrivez un logiciel jouant le rôle d'une passerelle quelconque, prenez soin de perturber le moins possible le flot de données - et ne perdez *jamais* d'éléments d'information, à moins que la machine destinataire vous y oblige ! » [1]***

Cette phase a été la plus complexe, car il a été nécessaire de faire dialoguer les composants du système information des ressources humaines et ceux du système d'infrastructure.

Cela a donné naissance à un programme appelé « Agrégateur » qui a permis de :

– collecter les données depuis les annuaires techniques via le protocole LDAP,

– compiler, trier les identités par le biais de règles métiers,

– collecter les données depuis les outils RH via des fichiers CSV,

– enrichir les identités depuis les informations RH en utilisant le format Supann2009 utilisé dans le cadre de la fédération RENATER [13],

– mettre en place un système de références croisées permettant de connaître l'identifiant de la personne sur les divers outils du SI via le champ « supannRefId » [14],

– injecter les données dans l'annuaire principal.

Les règles métiers et l'enrichissement des identités ont donné lieu à de nombreux d'échanges, car beaucoup de cas particuliers existent (agents titulaires, chercheurs hébergés, prestataires internes et externes, éméritats, startups, etc...).

Il a fallu déterminer pour chaque type de personne un formalisme particulier, car la différenciation des personnes se faisait désormais par la valeur des attributs et non par la position de la fiche utilisateur dans l'annuaire comme auparavant (formalisme imposé par Supann2009).

3.3.3 Utilisation des données

Une mise en qualité des données a été nécessaire, car de nombreuses incohérences existaient tant sur les annuaires techniques que dans la base RH. Afin de révéler ces incohérences, une nouvelle version de l'outil « Pages Blanches » a été développée pour afficher et mettre en avant les données des personnes et leurs affectations.

Une communication a été faite auprès des agents afin qu'ils vérifient leurs propres informations et qu'ils demandent leur correction, si nécessaire, via un formulaire dédié.

Le pôle de développement travaillait sur une application de gestion d'ordres de mission et de déplacement. Cette application a été la première à être connectée à cet annuaire pour utiliser le système d'affectation et de responsabilité pour le flux des autorisations de mission.

3.3.4 Traitement des incohérences

Pour corriger les incohérences remontées, un groupe de support « annuaire » a été mis en place comprenant une personne a minima de chaque pôle de la DSI et du service des ressources humaines.

Cette diversité a été nécessaire, car des opérations des mises à jour ont dû être menées de manière conjointe entre les différents membres du groupe de support annuaire.

Une interface de consultation des journaux de l'agrégateur a été mise en place pour ces acteurs afin de cibler plus facilement les actions correctrices à mener. Il a fallu près de 9 mois pour arriver à un résultat satisfaisant.

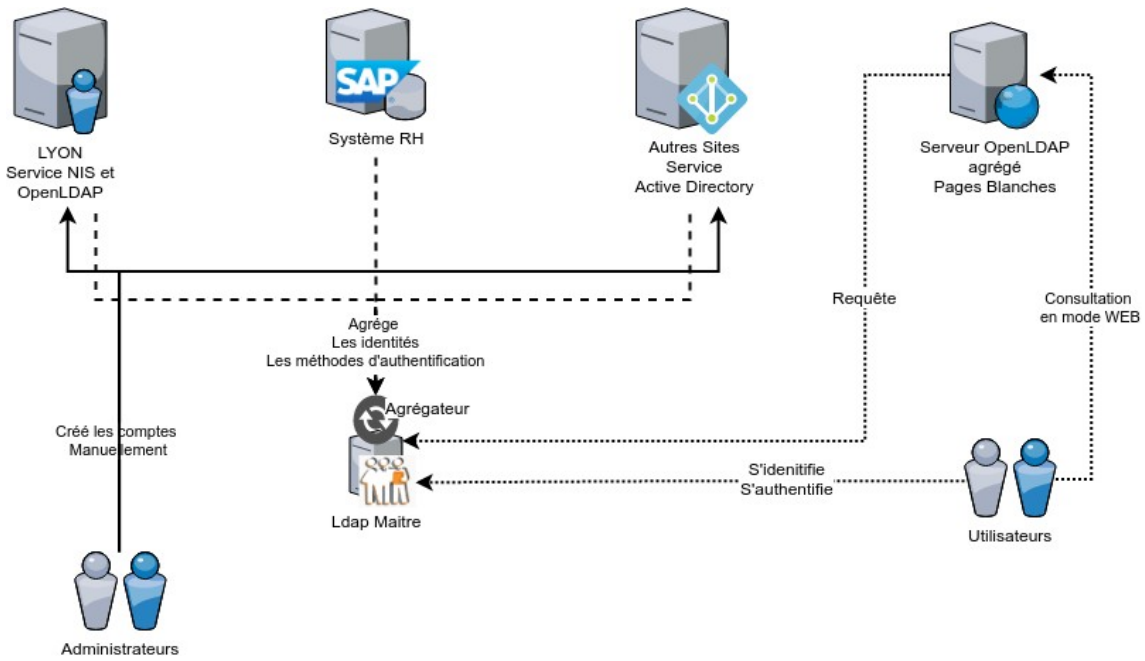

Figure 4 : Mise en place d'un annuaire centralisé avec des informations Supann provenant de la base RH

3.4 Retour d'expérience

La mise en place d'un annuaire n'est pas un défi technique, mais surtout un défi organisationnel, de communication et de dialogue entre tous les acteurs. En effet, la mise en place technique est aisée à partir du moment où une solution a été trouvée et validée.

Le plus important est la qualité de la donnée stockée et manipulée qui fait la réputation d'un annuaire et c'est cette mise en qualité des données qui a pris le plus de temps.

Durant ce long projet (plusieurs années), les facteurs de réussite ont été :

- l'agilité : mettre en place un annuaire fonctionnel par itération et vérifier les informations stockées et diffusées au fil de l'eau ;
- la communication : une communication ciblée afin d'accompagner chacun des membres permet de bien faire comprendre la démarche ;
- la visibilité du service rendu pour les utilisateurs, nécessaire pour bien communiquer :
  - L'application web page blanches est un composant psychologiquement important, car il permet de donner une réalité au projet pour ses acteurs et est une plus-value immédiate pour l'utilisateur.
  - L'unicité de l'authentification : un seul annuaire d'authentification pour toutes les applications évite une multiplicité de compte et de mot de passe.

4 Évolutivité et accessibilité

4.1 Une série d'évolutions en perspective

- En 2012, Renater récupère la gestion du système de visioconférence RMS (Remote Meeting System) mis à disposition par l'IN2P3 [15], l'intègre à la Fédération et désactive les comptes locaux. Irstea doit alors se doter d'un Fournisseur d'identité et donc supporter le formalisme Supann.
- Fin 2014, Irstea intègre le projet de l'AMUE [16] : SINAPS [17], un outil de gestion des référentiels de personnes et de structures.
- En 2015, Irstea prend part à la phase pilote de « Partage » [18], l'offre de messagerie de RENATER. Une diffusion des identités doit être mis en place en direction de cette messagerie externalisée.
- En 2015 également, afin de moderniser l'infrastructure Active Directory (unification, simplification, mise en adéquation du nom de l'institut), Irstea entame une migration d'une forêt multi-domaine ActiveDirectory 2003 (7 domaines <site>.cemagref.fr) vers une forêt mono-domaine ActiveDirectory 2012 (1 domaine irstea.priv).

Toutes ces évolutions ont induit des modifications régulières de l'outil d'authentification et de gestion des identités.

A posteriori, les évolutions peuvent être regroupées en 2 phases distinctes :

– Mise en place des flux de diffusion des données d'authentification sur les systèmes clients (Partage, Annuaire LDAP), en cours de migration ou non (Active Directory 2003 ou Active Directory 2012) afin d'asservir le SI à partir d'un composant central appelé « Passport », que nous détaillons plus loin.

– Mise en place des flux de diffusion des comptes depuis le Référentiel RH en utilisant le progiciel SINAPS et le composant mis en place durant l'étape précédente, et diffusion des données d'authentification.

4.1.1 Explications

Les données d'authentification devaient être diffusées vers plusieurs consommateurs comme suit :

Backend	localisation	Protocole	Usage	Diffusion
Active Directory 2012	Interne	LDAPS	Contrôleur de domaine, authentification de comptes pour le nouveau domaine Irstea.priv	Mot de passe format AD
Active Directory 2003	Interne	LDAPS	Contrôleur de domaine, authentification de comptes pour l'ancien domaine cemagref.fr	Mot de passe format AD
OpenLDAP Lyon	Interne	LDAPS	Annuaire d'authentification du site de Lyon	Mot de passe format SSHA / SAMBA
OpenLDAP national	Interne	LDAPS	Annuaire d'authentification (SSO / fédération / Radius)	Mot de passe format SSHA / SAMBA
Partage	Externe	HTTPS api REST BSS	Plateforme collaborative	Mot de passe (format SSHA) et informations page blanches

– La diffusion du mot de passe vers les 2 instances d'ActiveDirectory et l'instance OpenLDAP de Lyon est nécessaire afin de garder une cohérence lors de la migration de AD2003 vers AD2012 et de OpenLDAP vers AD2012. La synchronisation des comptes a été assurée par le prestataire dans le cadre de la migration.

– La diffusion du mot de passe vers « l'annuaire maître » est nécessaire pour que chaque personne puisse accéder aux ressources RENATER, web et EduRoam. La synchronisation des comptes est assurée par l'agrégateur.

– L'encodage des mots de passe en format SAMBA est nécessaire pour assurer l'authentification sur le contrôleur de domaine SAMBA NT4 pour Lyon le temps de la migration et aussi pour faciliter l'intégration avec EduRoam via FreeRadius [19].

4.1.2 Réalisation

L'objectif est d'avoir une interface de gestion de compte informatique unifié, quels que soit les backends internes (Annuaire Active Directory ou OpenLDAP) ou externes (PARTAGE).

L'outil « Passport » joue ce rôle en se présentant comme un «frontal » de gestion via une interface web pour les administrateurs et via une API en cas de besoin.

« Passport » a été construit en interne et subdivisé en 4 parties :

- un annuaire OpenLDAP [4] interne pour stocker les données des comptes répliqués depuis « l'annuaire maître » ;
- une console de gestion, FusionDirectory [20], pour afficher les informations et soumettre les modifications de mot de passe auprès des différents systèmes d'authentifications ;
- un outil de synchronisation d'identité, Ldap Synchronisation Connector (LSC) [21], pour synchroniser l'annuaire « Passport » depuis « l'annuaire maître » ;
- des scripts « maison » pour la diffusion des mots de passe.

Afin de savoir vers quel système propager le mot de passe, chaque compte dispose de sa référence croisée sur les différents systèmes avec les différentes méthodes (LDAP, API...).

Ces informations sont maintenues par la tâche de synchronisation LSC et stockées dans le champ « supannRefId » comme suit :

```
{LDAPMASTER}uid=gaston.lagaffe, ou=people, dc=irstea, dc=fr
{PARTAGE}gaston.lagaffe@irstea.fr
{AD2012}cn=Lagaffe Gaston, ou=utilisateurs, ou=lyon, dc=irstea, dc=priv
{LDAPLYONSEARCH}gaston.lagaffe@irstea.fr
```

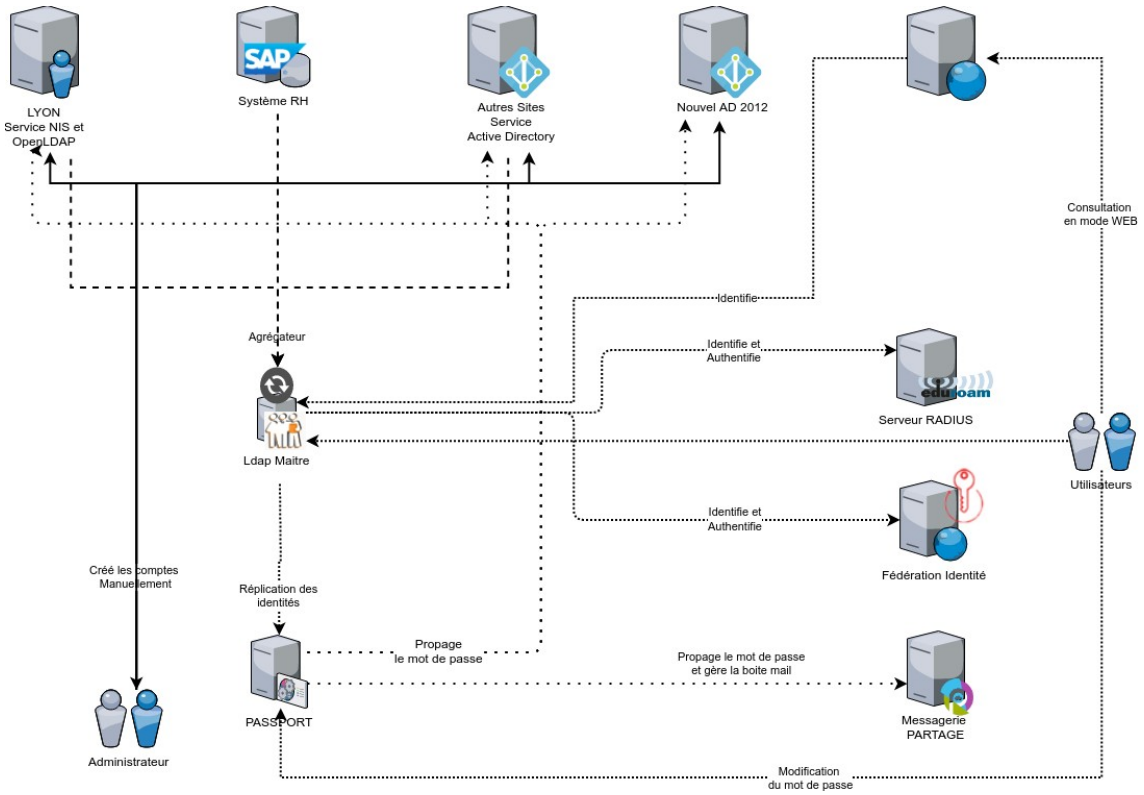

Figure 5 : Annuaire technique et réplication des identités dans un contexte de migration

La mise en production de ce service a été assez aisée, car il s'agissait de mettre en place un nouvel outil et non de remplacer un existant.

Une communication a été faite aux utilisateurs afin de leur demander de changer leur mot de passe. Cette opération a été d'autant plus facile que l'accent a été mis sur les plus-values liées au changement, telles que l'unicité du mot de passe, l'accès à « EduRoam » et à « Partage » et non sur les motivations techniques inintéressantes pour l'utilisateur final.

4.2 Diffusion des identités depuis le référentiel RH

4.2.1 Explications

Un compte apparaît dans l'annuaire maître après avoir été créé dans les annuaires techniques et complété par les données RH via l'agrégateur.

La création des comptes est assurée par les informaticiens et non par les gestionnaires des ressources humaines.

Un décalage entre l'accès aux outils et la signature du contrat de travail est donc possible ainsi que des erreurs de saisies, pénalisantes pour l'utilisateur.

En 2014, l'Amue [16] lance SINAPS [17] pour faciliter l'échange des données entre les composants de l'AMUE tels que APOGEE [22], HARPEGE [23] ou d'autres outils via des échanges de fichiers XML.

Même si l'Irstea n'utilise pas les produits de l'AMUE , l'institut s'est inscrit comme site pilote de SINAPS , car c'est une opportunité de connecter le système d'information RH et la gestion des comptes en formalisant les échanges.

SINAPS est alors l'occasion idéale pour piloter les comptes depuis le système RH, mais en raison des retards pris de part et d'autre, cette étape a été la dernière à être mis en œuvre.

« Passport » a introduit un point de passage obligatoire pour le changement de mot de passe. C'est ce point de passage qui sera utilisé par SINAPS pour transformer une identité numérique en compte informatique. SINAPS est un progiciel basé sur Ebx [24] pour la gestion des changements et Iway [25] pour la diffusion / réception de changement d'identité et de structure via un espace FTP ou un service web.

4.2.2 Réalisation

La mise en place de SINAPS a nécessité de :

- définir quelles applications sont maîtres de quelles données (qui a autorité sur la donnée en cours ?) ;
- définir les équivalences de champs entre SINAPS et les applications consommatrices - le schéma Supann a alors été très utile, car il couvrait une grande partie des données, les autres étant assurées par les schémas FusionDirectory ;
- Développer les interconnexions entre les applications [20] ;
- Repenser les flux de créations de comptes.

Le dernier point est un point important.

En effet, une identité existe suite à son apparition dans SINAPS, pour les internes, et dans Passport, pour les externes. Active Directory n'est donc plus la source.

Ce changement de flux a induit :

- une information auprès des demandeurs de poste : le compte ne peut être créé que si le dossier RH est complet ;
- une formation des gestionnaires de compte informatique : la source des comptes n'est plus Active Directory ;
- un rapprochement des identités entre le SI RH, les identités dans « Passport » et les comptes sur les backends (Partage, OpenLDAP, ActiveDirectory).

Ces opérations ont été faites sites par sites.

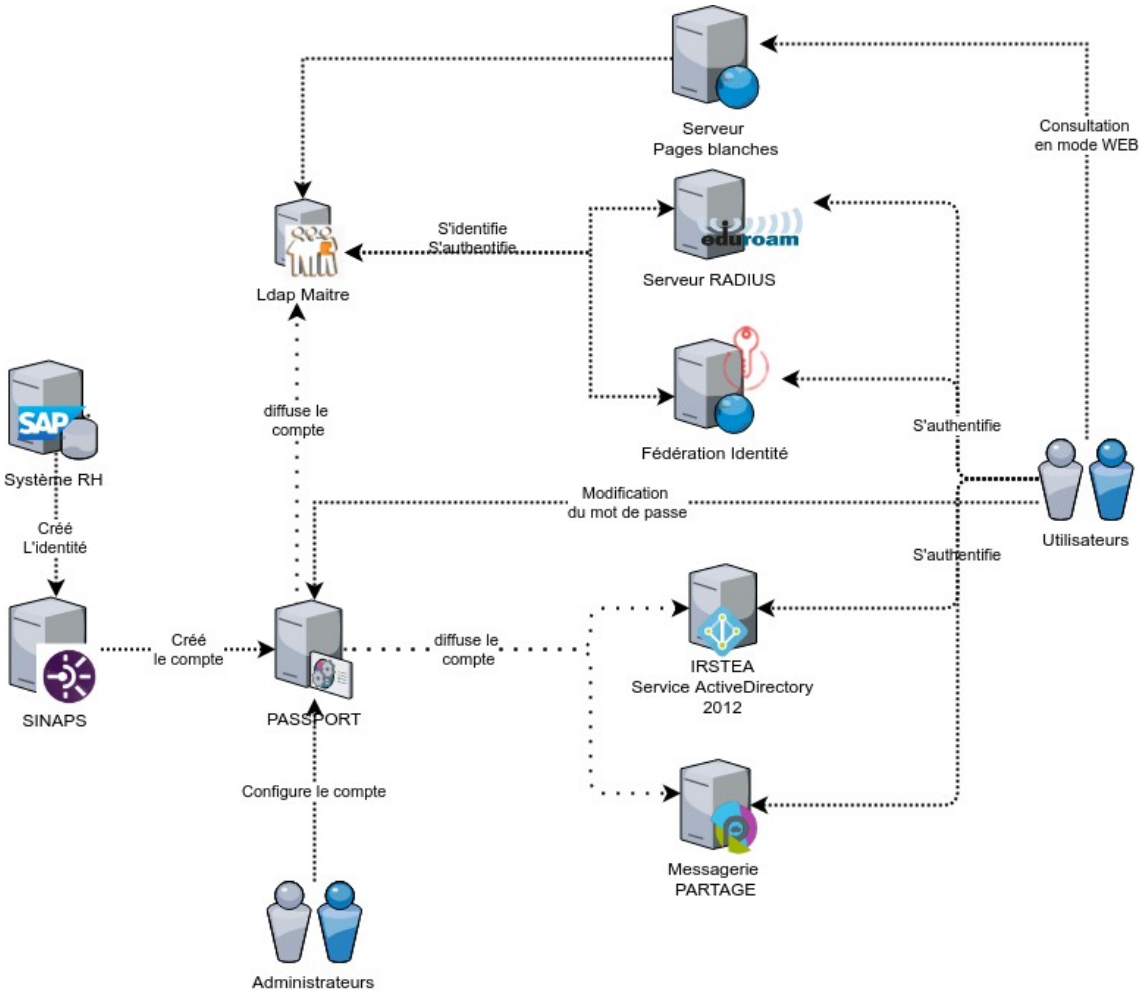

Figure 6 : Provisioning de compte, et leurs usages internes et externes avec la solution SINAPS

4.3 Retour d'expérience et projection

Encore une fois, la communication a été un élément important, car ces différents projets ont été complexes à appréhender, non pas par les acteurs du changement, mais par ceux qui le subissent.

En effet, même si les évolutions suivent un fil directeur : « Mise en place d'un annuaire d'identité technique complet dépendant de la base RH », les impacts sur la gestion courante sont nombreux :

- support à assurer dans un contexte changeant avec de nombreux cas particuliers,
- modification, au fil de l'eau, des flux de synchronisation nécessitant des vérifications régulières des informations diffusées,
- dialogue à assurer entre plusieurs acteurs ayant une vision différente de la problématique.

La phase de diffusion des identités depuis le Système d'Information RH a été celle qui a accusé le plus de retard, car cette phase a nécessité l'intervention de plusieurs prestataires pour le développement des interconnexions entre SAP, SINAPS et FusionDirectory.

La disponibilité des prestataires et de la maîtrise d'œuvre a pu être un frein dans sa mise en place. Ce retard aurait pu être plus important, car Irstea a été le premier à utiliser SINAPS en dehors du socle applicatif « AMUE » (pas d'applications telles que HARPEGE ou APOGEE...), et le webservice fournit par Iway.

Tout était donc à découvrir. L'expertise technique de chacune des parties a été facilitatrice dans cette mise en place. La maîtrise des outils a été donc primordiale.

La mise en place du lien entre le SIRH et Passport a permis de :

- mettre en évidence les écarts d'information sur les identités (changement du nom matrimonial, différence entre le nom officiel et le nom d'usage),
- définir des règles de gestion des comptes et encadrer les « entorses » telles que la prolongation d'un compte mail en cas de fin de publication pour un doctorant,
- faciliter la saisie des comptes (diminution des inversion prénom/nom, orthographe des chercheurs étrangers),
- corriger à la source les problèmes d'affectation,
- valider « Passport » comme outils de distribution d'identité interopérable.

Comme évoqué en introduction, le système de gestion des identités est le premier composé impacté en cas de modification d'organisation. Ce sera encore le cas en 2020, car l'Irstea et l'Inra fusionnerons pour constituer l'Inrae.

La mise en place de « Passport » comme système de diffusion d'identité à l'Irstea est un atout important dans le processus de fusion, car il permet de garder le même point de distribution de comptes de l'infrastructure de l'ex Irstea dans le futur institut Inrae avec le formalisme Supann.

Cela donnera une base de départ intéressante dans le cadre d'une refonte totale du système de gestion des identités et des habilitations à l'Inrae prévue en 2022, d'autant plus que SINAPS a été retenu comme solution de gestion de référentiel d'identité et de structures.

5 Conclusion

Cette analyse a été faite de manière rétrospective et a permis d'extraire une approche peu orthodoxe mais fonctionnelle. La mise en place de ces annuaires et des divers composants a pris énormément de temps du fait du peu de ressources allouées et du contexte très changeant de l'époque.

Cependant, dans un contexte « Enseignement Supérieur et Recherche » où les besoins apparaissent chaque jour, les personnes en charge de ce projet ont pu retenir que les points suivants étaient primordiaux :

- l'interopérabilité des systèmes, afin de ne pas dépendre d'une technologie pouvant être opaque - des protocoles standards de dialogue (API REST ou SOAP / LDAP) et d'authentification (LDAP / HTTP-AUTH / CAS / SAML) pouvant s'interfacer entre eux ont été privilégiés ;
- la mise en œuvre progressive par petites étapes et l'affichage du résultat actuel et de l'étape suivante ;
- l'écoute des besoins futurs afin de pouvoir y répondre le temps venu (intégration d'ORCID [26], interface de gestion des extérieurs et de parrainage) ;
- le maintien d'une veille sur les réseaux métiers et sur les travaux en cours des partenaires (groupe fédération, groupe SupAnn) et éditeurs des solutions utilisées (Partage, Ldap Synchonisation Connector [21], LemonLDAP:: NG [27], Fusiondirectory [28]) ;
- une attitude participative avec les communautés ou prestataire en étant « consom'acteur » des logiciels utilisés, par la soumissions de bugs bugs, l'expressions de besoins et de souhait d'évolutions, voire en suggérant des orientations ;
- le maintien d'un lien régulier entre les différents acteurs de la chaîne des identités (acteurs métiers et techniques).

La gestion des identités est un projet important afin de bien identifier chaque acteur du système d'information, qu'il soit interne, externe, et leur assurer un service de qualité tout en respectant les contraintes légales comme le Règlement Général de la Protection des Données.

Pour cela, la gestion des identités demande une attention, une maîtrise et une souplesse de la part de l'entité qui la pilote, car c'est le premier composant impacté en cas d'évolution (changement de nom, fusion...) et que les aspects techniques liés à ces problématiques sont souvent sous-estimés.

Bibliographie

[1] Eric S. Raymond, La cathédrale et le Bazar, 1998, http://www.linux-france.org/article/these/cathedrale-bazar/cathedrale-bazar-2.html

[2] INRA, Institut national de la recherche agronomique, http://www.inra.fr/

[3] NIS, Network Information Service, https://fr.wikipedia.org/wiki/Network_Information_Service

[4] OpenLDAP Project, Site officiel OpenLDAP, http://www.openldap.org/

[5] Cajus Pollmeier, The Gosa Project, https://github.com/gosa-project/gosa-core

[6] PADL Software Ltd, Migrations Tools,
https://www.padl.com/OSS/MigrationTools.html

[7] The Samba Group, Samba and LDAP,
https://wiki.samba.org/index.php/Samba_&_LDAP

[8] Jérôme Fenal, Utilisation deNet::LDAP, 2005,
http://articles.mongueurs.net/magazines/linuxmag68.html

[9] Cosmocode, https://github.com/cosmocode/contagged

[10] Fosdem Organization, Free Open Source Software Developer's European Meeting,
https://fosdem.org/

[11] Clément Oudot, Pass-Trough authentication with SASL,
https://ltb-project.org/documentation/general/sasl_delegation

[12] The Debian Project, The Debian Project, https://www.debian.org/

[13] Renater - groupe SupAnn, Norme SupAnn 2009,
https://services.RENATER.fr/documentation/supann/2009/index

[14] Groupe Supann, Attribut supannRefId, 2009,
https://services.renater.fr/documentation/supann/2009/listeattributs#supannrefid

[15] Institut national de physique nucléaire et de physique des particules,
https://in2p3.cnrs.fr/

[16] AMUE, Agence de mutualisation des universités et des établissements,
http://www.amue.fr/

[17] AMUE, Logiciel SINAPS,
http://www.amue.fr/pilotage/logiciels/sinaps/presentation/

[18] RENATER, PARTAGE par RENATER, https://partage.renater.fr/

[19] Alan T. DeKok, Protocol and Password Compatibility, http://deployingradius.com/documents/protocols/compatibility.html

[20] Opensides, Fusiondirectory - SINAPS, https://www.fusiondirectory.org/sinaps-amue/

[21] LSC authors, LDAP Synchronization Connector, https://lsc-project.org/doku.php

[22] AMUE, Gestion de la scolarité, des enseignements et des étudiants,
http://www.amue.fr/formation-vie-de-letudiant/logiciels/apogee/

[23] AMUE, Gestion des RH dans l'enseignement supérieur,
http://www.amue.fr/ressources-humaines/logiciels/harpege/

[24] TIBCO, TIBCO Orchestra Network, https://www.orchestranetworks.com/product

[25] Information builder, Iway Service Manager,
https://www.informationbuilders.com/fr/home

[26] ORCID consortiem, Connecting research and researchers, https://orcid.org/

[27] LL::NG authors, LemonLDAP::NG, https://lemonldap-ng.org/welcome/

[28] FusionDirectory Authors, FusionDirectory, https://www.fusiondirectory.org/

Index des figures