Réalisation d'un webservice Supann

Martial Lebec
Direction du système d'information
Université Paris-Dauphine
Place du Maréchal De Lattre De Tassigny
75016 Paris

Vincent Bruhier
Direction du système d'information
Université Paris-Dauphine
Place du Maréchal De Lattre De Tassigny
75016 Paris

Lionel Lenoble
Direction du système d'information
Université Paris-Dauphine
Place du Maréchal De Lattre De Tassigny
75016 Paris

Résumé

L'université Paris-Dauphine a construit son référentiel Supann à partir des bases de données métier de la scolarité (Apogee) et des ressources humaines (Harpege). Seulement, toutes les personnes qui doivent accéder au SI de l'université ne sont pas éligibles à ces bases ou y sont intégrées en retard. Bien sûr l'approche organisationnelle est à privilégier pour faire disparaître ces exceptions. Toutefois il restera toujours une désorganisation résiduelle et nous avons décidé de la traiter de manière méthodique. Ainsi nous avons développé un webservice Supann permettant aux applications déjà existantes dans l'université de créer et modifier des utilisateurs dans l'annuaire LDAP, de manière simple et totalement contrôlée.

Le webservice est écrit en Java et implémente un modèle à 3 couches : interface SOAP, contrôleur transactionnel et classes métier. Il utilise le projet verifSupann [4] de l'université de Nantes pour assurer la conformité à la spécification Supann2009. Il propose un contrôle d'accès par authentification LDAP ou ticket CAS.

Le webservice Supann est conçu pour s'intégrer facilement dans les processus de gestion d'identités externes à la DSI: bibliothèque universitaire, département d'éducation permanente, laboratoires de recherche, etc. Son déploiement à la bibliothèque a permis de capter plus d'un millier d'identités qui échappaient au système central d'authentification. Jusqu'alors ces personnes étaient saisies comme comptes locaux dans plusieurs applications profitant déjà de l'annuaire (ressources documentaires, cours en ligne, WiFi, etc.).

Mots clefs

Supann, webservice, SOAP, Java, gestion des identités.

1 Introduction

Durant les années 2000 les établissements d'enseignement supérieur et de recherche ont créé leurs annuaires électroniques centraux. La construction de ces référentiels aura probablement vu autant de façons de faire que d'établissements, sans qu'un logiciel ou une méthode se soit imposée. En revanche, la structure et la sémantique des informations contenues dans un annuaire d'établissement d'enseignement supérieur a pu être normalisée : c'est la spécification Supann du Comité Réseau des Universités [1] [2].

L'université Paris-Dauphine a mis en production son annuaire Supann en septembre 2009. Il a été implémenté sous OpenLDAP 2.4 et il a remplacé plusieurs annuaires autonomes. L'annuaire Supann est l'unique référentiel des identités et, à ce titre, il est la source du système central d'authentification (CAS). Il est alimenté quotidiennement par les bases de données métier de la scolarité (Apogee) et des ressources humaines (Harpege). Seulement toutes les personnes qui doivent accéder au Système d'Information (SI) de l'université ne sont pas éligibles à ces bases ou y sont intégrées en retard. De ce fait l'authentification CAS n'a pas encore pu s'imposer comme l'unique moyen d'authentifier une personne dans le SI. Bien sûr l'approche organisationnelle est à privilégier pour faire disparaître ces exceptions. Toutefois il restera toujours une désorganisation résiduelle et nous avons décidé de la traiter de manière méthodique. Ainsi nous avons développé un webservice Supann permettant aux applications déjà existantes dans l'université de créer et modifier des utilisateurs dans l'annuaire LDAP, de manière simple et totalement contrôlée.

Ce développement s'inscrit dans le projet de « gestions des identités » de l'université Paris-Dauphine.

2 Fonctions du webservice

Le webservice Supann a pour objectif de réaliser des actions élémentaires sur les objets Supann, directement dans l'annuaire Ldap. On entend par « objet Supann » les personnes, structures et groupes dont la spécification Supann 2009 définit le modèle (cf. [1], chapitres 4,5 et 6). Dans sa version actuelle, le webservice Supann ne manipule que les objets représentant des personnes, c'est-à-dire les objets de la branche « ou=people ».

Les fonctions du webservice sont les suivantes :

- implémenter le modèle de données des personnes ;
- contrôler ou fournir les identifiants des personnes ;
- fournir un mécanisme transactionnel pour des traitements complexes ;
- fournir une interface SOAP authentifiée.

Le modèle des personnes est parfaitement décrit dans la spécification Supann 2009. Il repose sur 2 notions : le profil et la catégorie. Le profil est défini au chapitre 5 de la spécification. D'abord on définit un profil « commun » qui intègre tous les attributs Ldap d'un objet « personne Supann ». Puis on le décline en deux autres profils : « étudiant » et « personnel ». La catégorie est définie à l'annexe 2. Elle repose sur l'attribut eduPersonAffiliation du profil commun. Le webservice est assure que les données injectées ou modifiées dans l'annuaire Ldap respectent le modèle décrit ci-dessus.

L'identifiant des personnes n'est pas imposé mais encadré par la spécification Supann 2009 (cf. § 5.5 [1]). Chaque établissement choisit donc son modèle d'identifiant. Par ailleurs, l'identifiant peut répondre à des règles différentes suivant les catégories de personnes. Par exemple, nos

identificateurs uniques (uid) d'étudiants et de personnels sont respectivement les numéros Apogee et Harpège et sont générés par ces bases. Alors que ceux des lecteurs extérieurs de la bibliothèque sont générés par le webservice et maintenus dans l'annuaire. Le webservice fournit une primitive pour obtenir un identifiant.

Dans le cas général de l'alimentation de l'annuaire à partir des bases de données des étudiants et des personnels, le traitement est suffisamment simple pour ne pas avoir besoin d'implémenter de transactions. Par contre dès que le traitement implique plusieurs écritures, a fortiori dans plusieurs bases, un moteur transactionnel est nécessaire. Le webservice fournit un moteur transactionnel permettant d'intégrer des opérations portant sur l'annuaire Supann et sur d'autres éléments du système d'information.

L'interface de programmation de l'application annuaire Supann est l'interface générique d'Openldap, à savoir les commandes ldapsearch, ldapmodify, etc. ou les librairies Ldap JNDI, PhpLdap, etc. Le webservice implémente un code « métier Supann » extensible et fournit une interface SOAP. L'interface SOAP propose deux modes d'authentification : ticket CAS ou compte LDAP.

3 Usages du webservice à l'Université Paris Dauphine

Le webservice propose des méthodes génériques que nous utilisons pour consolider nos logiciels de gestion des identités. Ainsi nous avons implémenté les interfaces pour créer des personnes en fonction de leur profil (étudiant, personnel ou autre) et de leur catégorie. Nous avons connecté ces interfaces à un formulaire destinés aux administrateurs fonctionnels de l'annuaire. Par ailleurs nous avons étendu les primitives de création de personnes à la création de personnes « test » pour nos différents usages : démonstrations de l'ENT, tests d'applications, etc.

Enfin, le webservice permet également d'enchaîner plusieurs primitives ou de faire appel à des sources de données autres que l'annuaire Supann. Une première application du webservice dans ce sens a été faite pour l'inscription des lecteurs extérieurs de la bibliothèque universitaire (registered-readers) dans l'annuaire Supann.

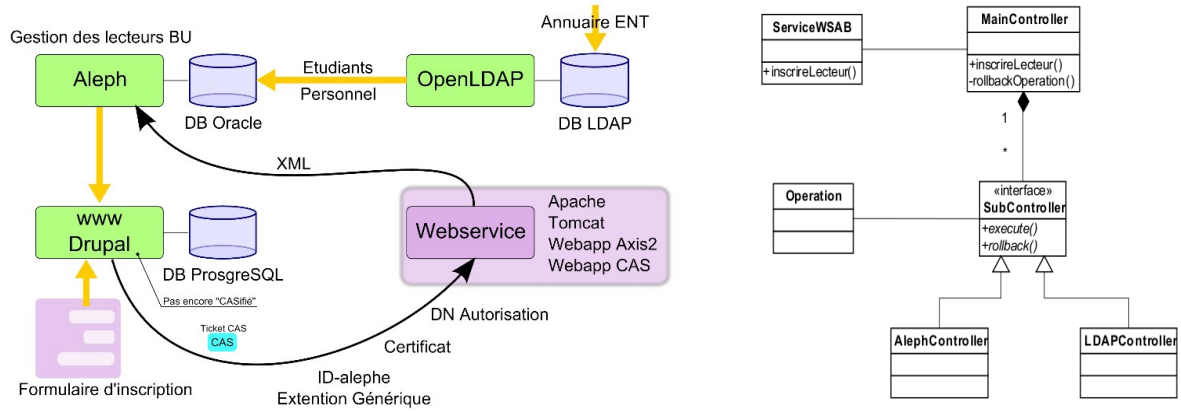

Figure 1 : Scénario d'usage et diagramme de classe pour la création des « lecteurs extérieurs »

Dans ce cas d'usage (Figure 1, à gauche), une application Drupal cassifiée présente un formulaire d'inscription. La validation d'une inscription déclenche une transaction qui consiste à rechercher une personne dans une base de donnée externe (Aleph), à créer une entrée dans l'annuaire Supann pour cette personne et à mettre à jour la base externe avec l'identificateur unique fourni par l'annuaire et le webservice.

4 Architecture du webservice

Le webservice est un logiciel Java qui implémente trois couches:

- la couche service, point d'entrée du webservice ;
- la couche métier, en charge du traitement des données ;
- la couche contrôleur, interface entre les couches service et métier.

Par ailleurs, le webservice est structuré en deux librairies Java :

- la librairie générique qui implémente le « métier » Supann et la mécanique du webservice ;
- la librairie spécifique qui doit être modifié par chaque établissement pour implémenter ses traitements particuliers.

4.1 Couche service

Le webservice Supann est une collection de fonctions mises à disposition des applications clientes au travers des interfaces SOAP et GET. Ces interfaces sont implémentées dans la couche service et exposées par le moteur de webservices Apache Axis 2. Concrètement elles consistent en une classe Java dans laquelle chaque fonction du webservice est une méthode de classe.

Le webservice est conçu pour exécuter des actions élémentaires : ajouter une personne dans l'annuaire, ajouter ou retirer un attribut (couple clé/valeur), etc. La logique est de proposer un ensemble d'actions élémentaires, des « primitives Supann », permettant de construire des traitements métiers sûrs. Les principales primitives sont les suivantes :

- ajouterSupannPersonne(categorie, nom, prenom)
- ajouterSupannEtudiant(categorie, nom, prenom,INE,etablissement,supannRefID)
- ajouterSupannEmploye(categorie, nom, prenom,supannRefID)
- ajouterAttribut(rdn,attribut,valeur)
- retirerAttribut(rdn,attribut,valeur)
- chercherSupannPersonne(chaine)
- verifierSupannPersonne(rdn)

Chaque profil de personnes (commun, étudiant, personnel) dispose d'une primitive spécifique pour ajouter une personne. Le premier argument de ces primitives est la catégorie (au sens de l'annexe 2 de la spécification Supann). Elle sert à ventiler la demande sur les objets adéquats dans la couche métier. Pour toutes ses primitives, la couche service réalise une vérification syntaxique des arguments.

4.2 Couche métier

La couche métier implémente les classes d'objets Supann et les traitements menés sur les sources de données. Chaque traitement se matérialise par l'implémentation d'un sous-contrôleur qui est déclenché par le contrôleur principal (en couche contrôleur). Afin de garantir la réversibilité des traitements, chaque sous-contrôleur dispose d'une méthode d'exécution *execute* et d'une méthode de réversion *rollback*.

4.2.1 Contrôleur de données Supann

Ce sous-contrôleur métier est assure la vérification des données transmises par la couche service et des écritures dans l'annuaire LDAP. En pratique, il instancie un objet Supann qui construit une entrée LDAP qui est elle-même transmises, pour vérification, à la librairie verfiSupann [4]. Si l'entrée est conforme, elle est écrite dans l'annuaire.

4.2.2 Primitive de génération des identifiants

Le webservice implémente une classe permettant de générer les identifiants des personnes. Cette classe est prévue pour être surchargée afin d'implémenter le traitement spécifique à chaque catégorie de personne, dans chaque établissement. Pour des raisons évidente, cette classe est une ressource critique.

4.3 Couche contrôleur

La couche contrôleur assure la liaison entre la couche service et la couche métier. Elle implémente le contrôleur principal qui ordonnance les sous-contrôleurs. Elle est responsable de l'exécution transactionnelle des traitements ainsi que de la gestion d'exception à remonter au client. Le contrôleur principal appelle les sous-contrôleurs de la couche métier et les sous-contrôleurs de sécurité définit dans la couche contrôleur .

Les sous-contrôleurs de sécurité sont au nombre de trois :

- DnsController, pour filtrer l'application appelante par adresse IP, nom d'hôte ou nom de domaine ;
- CASController, pour filtrer l'utilisateur de l'application appelante par ticket CAS ;
- AuthorizationController, pour calculer les autorisations du duplet (application,utilisateur) vis-à-vis de la méthode appelée.

Notre objectif est de permettre à une application web d'appeler le webservice en propageant l'authentification CAS de son utilisateur/navigateur client au webservice. Nous sommes dans le cas classique d'un proxyCAS+webservice [4].

Le webservice reçoit deux informations : l'application qui appelle le webservice et l'uid de la personne qui utilise l'application. Le sous-contrôleur *AuthorizationController* exploite ces deux données pour déduire son comportement vis-à-vis de l'annuaire LDAP : soit il opère sous l'identité de la personne (compte personnel) et les autorisations sont celles des ACLs LDAP de la personne ; soit il opère en utilisant une identité d'application (compte système LDAP) et les autorisations sont celles des ACLs LDAP de ce compte.

5 Particularité des attributs composites Supann

Les attributs composites et leurs attributs multivalués associés disposent de primitives spéciales auxquelles sont associés des méthodes de la classe d'objet sous-jacente.

Les primitives spéciales sont les suivantes :

- ajouterSupannEtudInscription(dn,supannEtablissement, supannEtuAnneeInscription, supannEtuRegimeInscription, supannEtuSecteurDisciplinaire, supannEtuTypeDiplome, supannEtuCursusAnnee, supannEntiteAffectation, supannEtuDiplome, supannEtuEtape, supannEtuElementPedagogique)
- retirerSupannEtudInscription(dn,supannEtablissement, supannEtuAnneeInscription, supannEtuRegimeInscription, supannEtuSecteurDisciplinaire, supannEtuTypeDiplome,

supannEtuCursusAnnee, supannEntiteAffectation, supannEtuDiplome, supannEtuEtape, supannEtuElementPedagogique)

- ajouterSupannRoleEntite(dn,supannRoleGenerique, supannTypeEntiteAffectation, supannEntiteAffectation)
- retirerSupannRoleEntite(dn,supannRoleGenerique, supannTypeEntiteAffectation, supannEntiteAffectation)

6 Conclusion

Le développement de ce webservice Supann a été motivé par des besoins spécifiques de l'université Paris Dauphine. La généralisation du code s'est imposée au fur et à mesure du développement, parce qu'elle permettait de consolider nos autres programmes de gestion des indentités. Une version générique du code source de ce webservice sera prochainement mise en ligne. Cette version permettra a minima d'interroger un annuaire LDAP au travers d'un appel SOAP ou GET. Il suffira alors aux établissements qui le souhaite de spécialiser et compiler les fonctions qui leurs sont nécessaires, suivant les consignes de programmations qu'il nous reste à rédiger.

7 Bibliographie

[1] CRU, recommandations Supann 2009
http://www.cru.fr/documentation/supann/index

[2] TutoJRES n°11, Mise en oeuvre de Supann 2008
http://www.jres.org/tuto/tuto11/index

[3] Université de Nantes, verifSupann - Valideur SUPANN
https://sourcesup.cru.fr/projects/verifsupann

[4] Vincent Mathieu, Présentation de CAS
http://www.esup-portail.org/consortium/espace/SSO_1B/cas