Provisionnement d'un annuaire SUPANN avec DYNA

Pierre-Olivier Terrisse
Université de Nantes / DSI / IRTS

tutoJRES 11
Annuaires : mise en œuvre de SupAnn 2008
1er avril 2009

Historique

- Dyna est le gestionnaire d'identité de l'Université de Nantes
- Il date de début 2002 pour générer l'annuaire LDAP de l'Université de Nantes.
- Il a été totalement refondu et sa nouvelle version a été déployée au cours de l'été 2008.
- Il supporte environ 7000 comptes du personnel (membres de l'Université ou travaillant dans le giron de l'Université) et 40000 comptes d'étudiants, avec un flux d'environ 13000 étudiants entrant et sortant par an.
- Il synchronise en continu plus de 20 bases de données : annuaires LDAP mais aussi services web, exécution de scripts…

SUPANN à l'Université de Nantes

Nous disposons de multiples annuaires LDAP : pour la messagerie, pour le WiFi, pour les accès nomades…

SUPANN est utilisé par :

- le fournisseur d'identité Shibboleth (fédération d'identité de Renater)
- E-Charlemagne (suivi des anciens étudiants de Polytech'Nantes)
- l'application de gestion du C2I.

Ces applications n'utilisent que des attributs liés aux utilisateurs : pas les structures ni les groupes.

Notre implémentation de SUPANN 2008 contient les structures, comme cela est prévu par sa spécification.

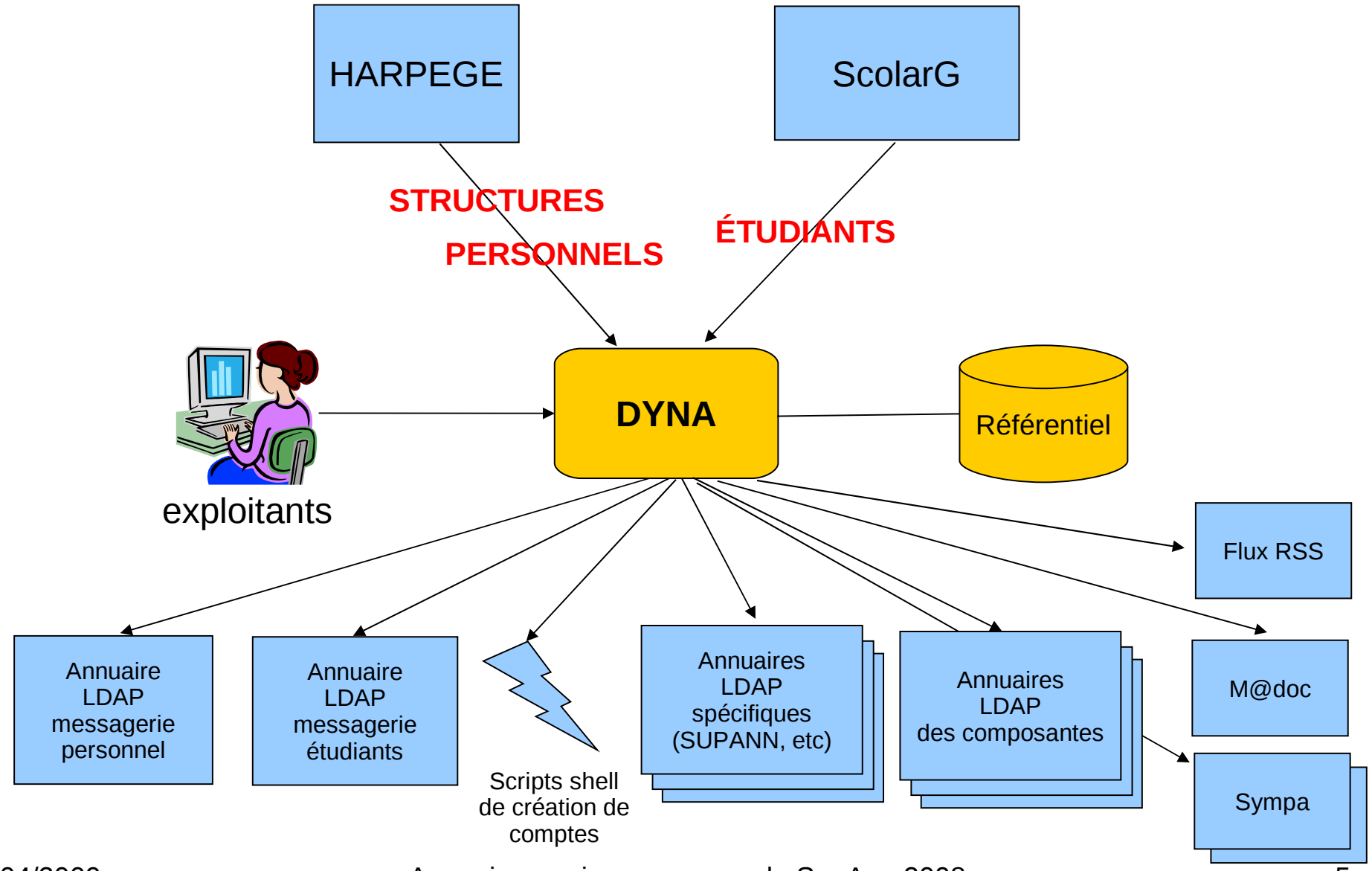
Elle ne contient pas de groupes, mais ceux-ci pourraient facilement être ajoutés en cas de nécessité.

Migration vers SUPANN 2008

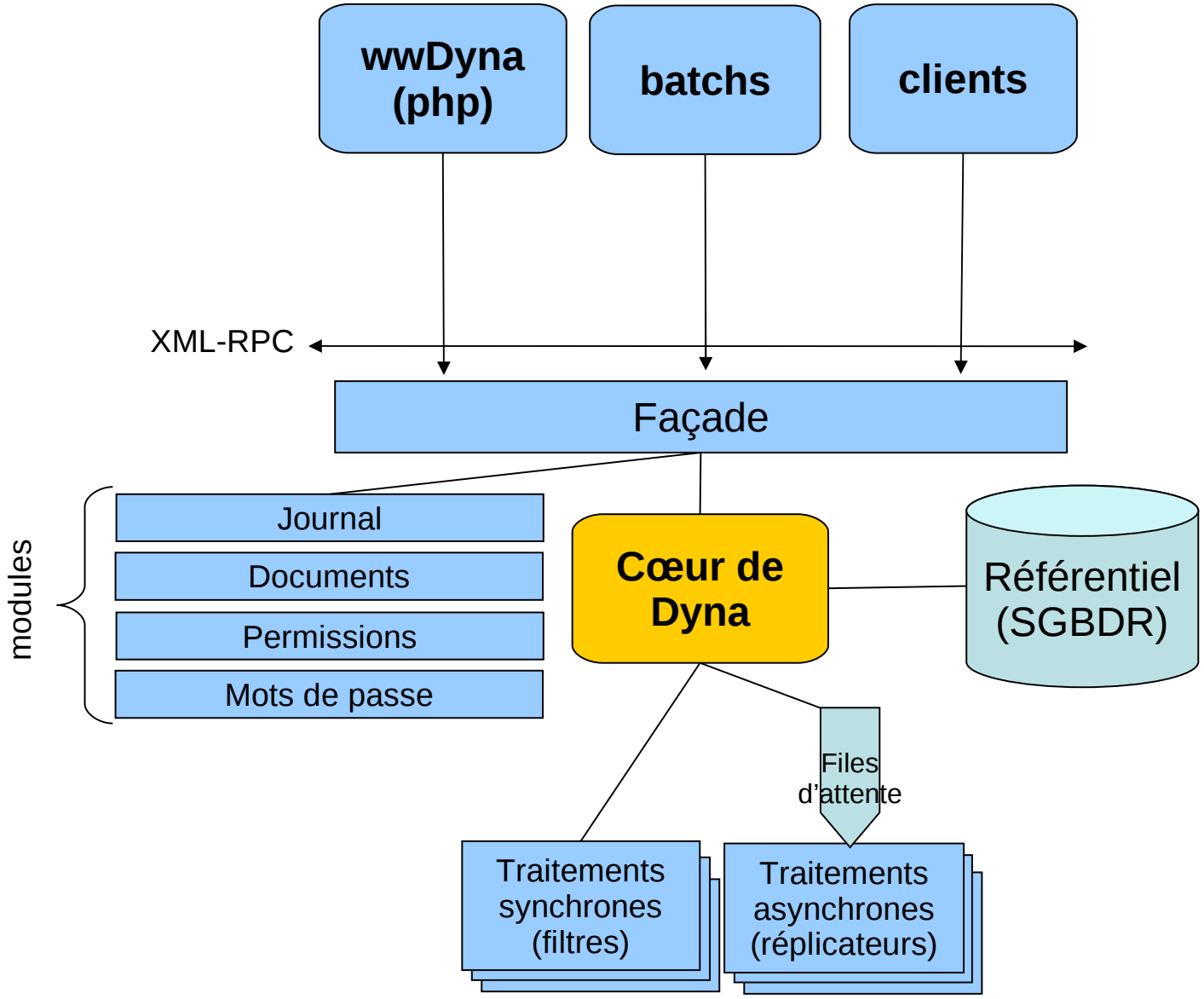
- Procédure de migration de SUPANN 2003 vers SUPANN 2008 :
- écriture d'un réplicateur Dyna pour SUPANN 2008
- génération de l'annuaire LDAP SUPANN 2008 de test
- validation de cet annuaire par rapport aux spécifications
- test sur les applications clientes
- génération de SUPANN 2008 sur le serveur de production

Durée totale : 3 mois

Les flux autour de Dyna



Architecture de Dyna 2.1



Le client Dyna

- La façade de Dyna, écrite en Java, offre une API sous forme d'un service web XML-RPC : créer, modifier ou supprimer un compte, un groupe, un rôle, etc.

- Le client permet d'exprimer en XML les modifications que l'on souhaite soumettre à Dyna. La transformation des objets Java en XML et réciproquement est assurée par JAX-B (Java API for XML Binding) qui permet de s'affranchir des détails de bas niveau.

- Reprise sur erreur : en cas d'indisponibilité du serveur Dyna, le client peut stocker temporairement les fichiers XML à soumettre.

Les filtres

Les entrées envoyées à Dyna sont ensuite soumises à un ensemble de filtres qui permettent de mettre en œuvre les règles de gestion des comptes.
Il existe trois sortes de filtres :

- en **initialisation** : pour les entrées nouvelles ;

- en **vérification** : avant l'insertion dans le référentiel : à ce stade, l'entrée soumise peut être refusée ;

- en **envoi** : après l'insertion dans le référentiel mais avant l'envoi dans les queues de réplication.

Les filtres s'exécutent d'une manière synchrone dans des processus distincts et communiquent avec le cœur par XML-RPC.
Il est possible d'attacher autant de filtres que l'on veut à un ensemble d'entrées.

Les réplicateurs

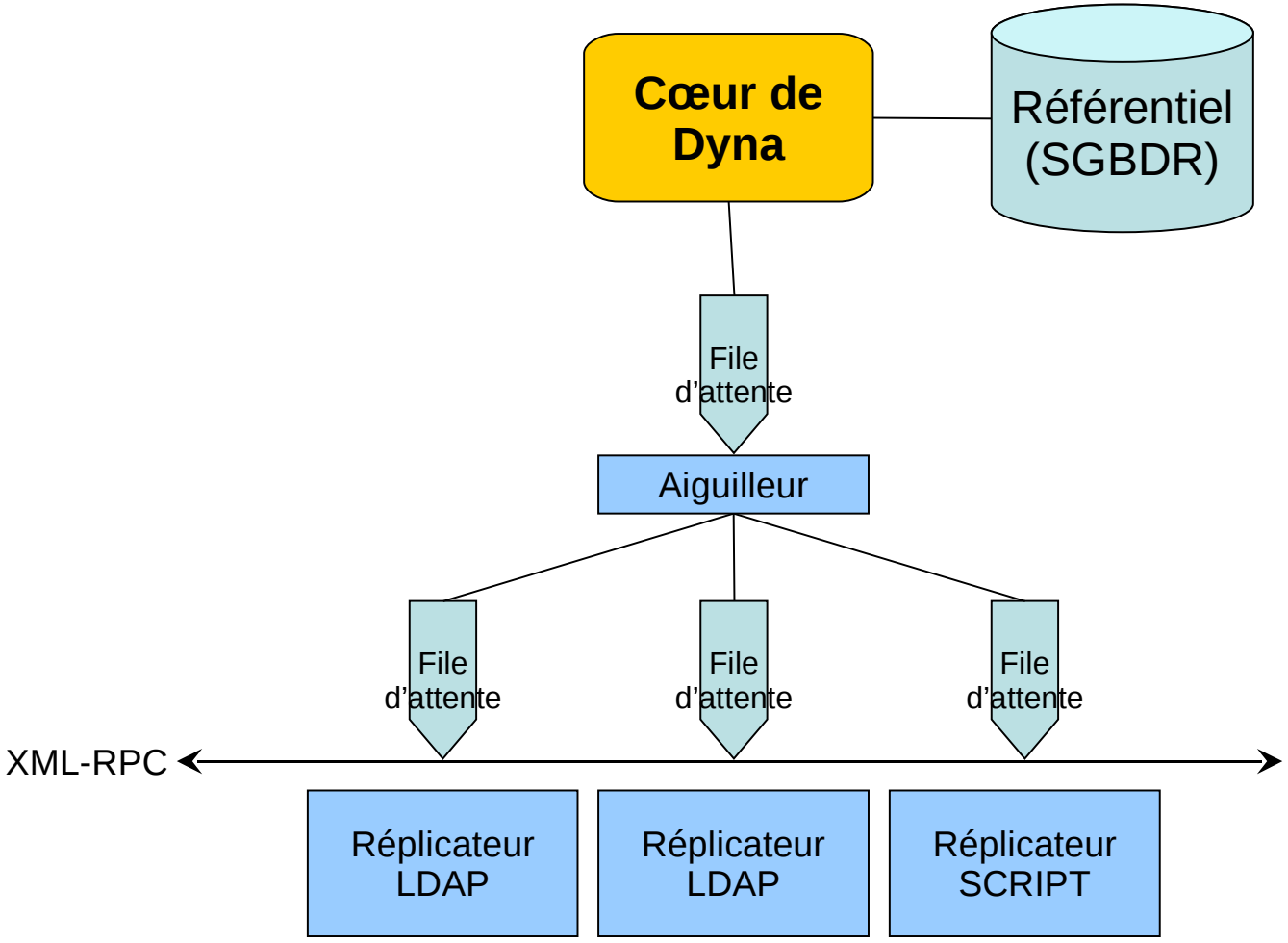
Les réplicateurs permettent de propager les modifications du référentiel dans les bases de données distantes notamment LDAP.

Les entrées en attente de réplication sont placées dans une file d'attente, avant d'être aiguillées vers des queues de réplication sérialisées dans la base de données du référentiel, à raison d'une queue par réplicateur.

Un réplicateur s'exécute dans un processus distinct. Il est invoqué par le cœur de Dyna via XML-RPC. Il peut s'exécuter sur une machine distincte du serveur Dyna.

Lorsqu'un réplicateur est indisponible ou qu'il échoue sur un erreur non fatale (p. ex. indisponibilité du serveur LDAP), le cœur de Dyna essaiera à nouveau de le contacter après un délai croissant. Il n'abandonnera qu'après plusieurs jours (analogie avec l'impression).

Les réplicateurs



Le réplicateur SUPANN

Ajouter un nouvel annuaire LDAP à répliquer par Dyna est une opération relativement simple :

- Soit les classes LDAP à implémenter sont standards (inetOrgPerson, posixAccount, etc.) : il suffit de configurer le réplicateur ;
- Soit les classes sont spécifiques comme avec SUPANN : on dérive la classe ReplicateurLDAP en indiquant pour chaque objet les attributs à positionner.

Les exploitants

Le provisionnement amont ne suffit pas :

- mots de passe perdus, etc.
- nouveaux utilisateurs à inscrire rapidement ;
- population en marge de l'Université, absente des bases amont.

Les exploitants Dyna, pour chaque composante ou laboratoire, sont habilités à gérer leurs utilisateurs à travers l'interface Web wwDyna.

wwDyna, écrit en PHP, communique avec le cœur de Dyna via le service XML-RPC.

Conclusion

- Le maître mot de Dyna : la réactivité. Il est condamné à évoluer en permanence afin de s'adapter aux nouveaux besoins des bases aval et d'être capable d'irriguer efficacement le système d'information.

- Il a permis de s'adapter rapidement à SUPANN 2008, avec un minimum d'effort de développement.