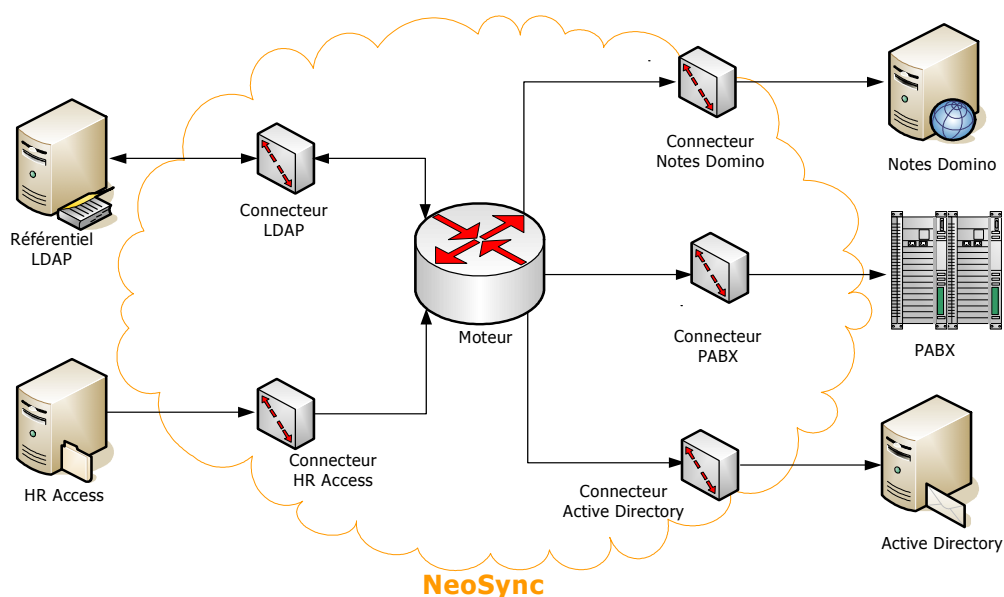


Nos solutions de synchronisation d'annuaires

ADUNEO forte de nombreuses expériences dans le domaine des méta annuaires (France Telecom, PSA, Société Générale, SDV/Bolloré, Bureau Veritas, Muséum National d'Histoire Naturelle, PMU, ..) propose une gamme de produits de synchronisation d'annuaire et de gestion d'identité qu'elle a développés et maintient auprès de ses clients.

- Une solution complète **NeoSync®** permettant toutes synchronisations
- Un logiciel limité à la synchronisation des mots de passe entre Active Directory et LDAP (**NeoPass®**).
- Un logiciel de workflow permettant la gestion des habilitations **NeoFlow®**
- Un logiciel de consultation d'annuaire et d'administration déléguée **NeoPage®**

Exemple d'architecture de synchronisation via NeoSync® :



Solution NeoSync®

NeoSync® est une plate forme permettant le développement aisé des synchronisations d'annuaires. Il intègre **un moteur**, un **planificateur** et des **outils d'aide à l'exploitation** (console d'administration web , gestion des logs et des alertes, etc.). Il fonctionne avec un système de connecteurs gérant l'interface avec les bases, et avec un système de tâches effectuant les traitements de synchronisation (recherche des éléments à modifier, créer, supprimer, prise en compte des règles de gestion, etc.). Il existe ainsi un certain nombre de **connecteurs** pour s'interfacer avec le système d'informations : LDAP, Active Directory, bases de données (Oracle, SQL Server, etc.), Lotus Domino, PABX, fichiers plats, fichiers XML, etc ...

La partie traitements est développée spécifiquement pour chaque projet afin de s'adapter aux besoins de chaque client.

Grâce à ce framework, le développeur peut alors se concentrer sur la programmation effective des différents traitements et règles de gestion spécifiques à chaque projet.

En effet, les synchronisations sont très souvent complexes. On donne quelques exemples de cette complexité :

- les synchronisations doivent être efficaces et sûres : NeoSync® dispose ainsi d'un certain nombre d'algorithmes éprouvés de recherche de différentiel pour ne modifier que les entrées le nécessitant et pour s'assurer que toutes les modifications sont bien effectuées ;

- la mise en relation des entrées à synchroniser peut demander des traitements particuliers ;

- on doit souvent filtrer les entrées à synchroniser ;

- les formats de données n'étant pas toujours homogènes, on doit retraiter les informations (ajout/suppression d'accents, travail sur la casse, concaténations, voire opérations bien plus complexes avec des corrélations avec des bases externes) ;

- on doit parfois s'interfacer avec des applications complémentaires (déclenchement d'alertes par Web Service, démarrage de workflow, etc.) ;

- on doit souvent mettre en place des règles de bon fonctionnement, par exemple sur le nombre d'entrées que l'on peut supprimer en une seule fois pour se prémunir d'une mauvaise configuration où l'ensemble de l'annuaire serait effacé... ;

- on doit bien penser la reprise sur incident (problème d'accès aux données,

- les fichiers manipulés doivent être gérés (archivage automatique, suppression des archives les plus anciennes, etc.) ;

- on doit aussi gérer les accès aux fichiers (récupération par FTP, SFTP ou autre système) ;

- la liste n'est évidemment pas exhaustive.

NeoSync® est un produit ouvert dans lequel on peut aisément rajouter de nouveaux connecteurs et de nouvelles tâches de synchronisation. Il est programmable en **Java 5 ou 6.0**.

Les tâches gérées par NeoSync® sont principalement des tâches de synchronisation, mais il peut aussi s'agir d'autres tâches : transmission des fichiers, activation/désactivation automatique des comptes, gestion des logs et des archives, etc.

La définition des tâches de synchronisation peut se faire de trois manières :

- les tâches simples ne nécessitant pas de traitements particuliers peuvent être définies dans un simple fichier de configuration ;
- pour les tâches un peu plus complexes, on peut rajouter du code Java dans le fichier de configuration pour s'occuper de traitements particuliers ;
- dans le cas des tâches complexes, il est préférable de programmer la tâche directement en Java, en s'appuyant sur les différents outils mis à disposition par NeoSync® (accès aux données, traitement des données, algorithme de différentiel, etc.).

Les tâches définies par fichier de configuration sont ensuite automatiquement compilées en Java pour obtenir des performances optimales.

Une tâche de synchronisation simple demande par exemple l'écriture de quelques dizaines de lignes de code, avec une structuration forte.

En effet, une tâche de synchronisation entre un annuaire A et un annuaire B correspond aux éléments suivants :

- définition de la liste des entrées à sélectionner dans l'annuaire A (par la fourniture d'une requête), avec la liste des attributs ;
- définition de la liste des entrées à sélectionner dans l'annuaire B (par la fourniture d'une requête), avec la liste des attributs ;
- définition des champs de mise en relation, avec les options associées (prise en compte de la casse par exemple) ;
- définition des correspondances entre les attributs (mapping) avec les règles de comparaison (prise en compte de la casse, comparaison de type chaîne, nombre ou date, prise en compte de l'ordre des valeurs multiples) ;
- traitements à effectuer lors de la lecture d'une entrée dans l'annuaire A ;
- traitements à effectuer lors de la lecture d'une entrée dans l'annuaire B ;
- traitements à effectuer pour une entrée trouvée dans l'annuaire A mais pas dans l'annuaire B (souvent création dans B ou suppression dans A) ;
- traitements à effectuer pour une entrée trouvée dans l'annuaire B mais pas dans l'annuaire A (souvent création dans A ou suppression dans B) ;
- traitements à effectuer lorsqu'une entrée de A est identique à celle de B (souvent rien) ;
- traitements à effectuer lorsqu'il est détecté des différences entre une entrée de A et une entrée de B, dans le sens d'une modification de A vers B (souvent modification de l'entrée B) ;
- traitements à effectuer lorsqu'il est détecté des différences entre une entrée de A et une entrée de B, dans le sens d'une modification de B vers A (souvent modification de l'entrée A).

Synchronisation des mots de passe avec Active Directory

NeoSync® intègre un module de synchronisation des mots de passe provenant d'Active Directory. Par l'installation sur tous les contrôleurs de domaine Windows d'un composant Microsoft standard, toutes les modifications de mots de passe (effectuées par les administrateurs ou directement par les utilisateurs) sont transmises de façon sécurisée (authentification par hash et chiffrement 3DES) au moteur NeoSync® pour être mises à disposition des tâches. Leur rôle est alors de propager ces mots de passe dans les bases qu'elles doivent synchroniser.

NeoSync® contient un système de communication par messages s'assurant que si l'annuaire destination n'est pas disponible alors qu'il faut effectuer une modification du mot de passe, cette dernière sera réalisée ultérieurement.

Environnement haute disponibilité

NeoSync permet un fonctionnement en haute disponibilité par l'installation d'un cluster NeoSync à deux nœuds.

Ce cluster fonctionne en actif/passif et ne requiert aucun logiciel supplémentaire, les fonctions de cluster étant prises en charge directement par NeoSync. La seule fonctionnalité qui n'est pas gérée en propre par NeoSync est l'accès à l'interface web d'administration. Sur une plate forme Linux/Unix, il est cependant facile d'ajouter la gestion d'une adresse IP virtuelle activée par le nœud actif du cluster.

Le cluster NeoSync fonctionne de la manière suivante :

- NeoSync est installé sur deux serveurs différents ;
- On ne peut avoir plus d'un nœud actif à la fois (mais il est possible qu'aucun nœud ne soit actif si le serveur de quorum est indisponible) ;
- Le nœud inactif surveille le nœud actif ;
- Si le nœud actif n'est plus visible par le nœud inactif, ce dernier (après vérifications) tente de se rendre actif ;
- Pour cela, il contacte le serveur de quorum pour vérifier qu'il peut bien s'activer ;
- La réplication des fichiers (configuration et données) est effectuée par rsync.

Le serveur de quorum est un serveur qui permet de décider quel nœud peut être actif. En effet, il est possible que des conditions particulières fassent que les deux nœuds décident en même temps de s'activer (cas de split-brain). Le serveur de quorum est une base de données partagée par les deux nœuds leur permettant de décider lequel des nœuds doit être actif (on définit un nœud actif de préférence en mode nominal).

On choisit comme base de données une des sources ou des destinations des synchronisations. On s'assure ainsi que le quorum est toujours disponible quand on en a besoin (si la source ou la destination n'est pas accessible, la synchronisation est impossible et il n'est donc pas besoin d'activer de nœud).

Le serveur actif fait régulièrement une écriture sur le serveur de quorum. Lorsque le serveur inactif n'arrive plus à communiquer avec le serveur actif (perte de heartbeat), il se connecte au serveur de quorum et regarde la date de la dernière écriture. Si cette dernière est trop ancienne, il décide alors de s'activer.

Module d'audit

NeoSync dispose d'un module d'audit permettant de tracer l'ensemble des opérations effectuées sur les sources pour les données synchronisées. On peut ainsi par exemple suivre le cycle de vie d'un utilisateur de son arrivée dans le système jusqu'à sa suppression. Les informations sont enregistrées dans une base de données et consultables dans l'interface d'administration en faisant une recherche sur l'objet.

Il est alors présenté l'ensemble des opérations avec la date, les sources de données impliquées et un descriptif.

On peut ainsi mieux identifier les incohérences dans les données et remonter à leur source pour correction.

Interfaces d'administration

L'administration de NeoSync® peut se faire soit directement dans les fichiers de configuration et par une console en mode texte, soit par une interface web d'administration.

Cette interface est sécurisée par :

- le chiffrement du flux en SSL ;
- la restriction de l'accès par adresses IP ;
- l'authentification des utilisateurs.

Elle permet de réaliser les opérations suivantes :

- modification de la configuration ;
- déclenchement manuel des tâches ;
- consultation des logs et des rapports ;
- consultation du statut du serveur et des tâches ;
- lancement de commandes particulière.

L'interface d'administration est entièrement personnalisable, tant au point de vue de l'esthétique que des fonctionnalités. Il s'agit d'une application servlet/JSP que l'on peut modifier à loisir.

Aduneo NeoSync 3.0

Configuration
Paramètres

Commandes
Tâches
Terminal

Logs
Normaux
Complets
Archives

Statut
Résumé

Configuration
Configuration de base du framework NeoSync

Paramètre	Valeur	Aide
<input checked="" type="checkbox"/> administration.web.port	443	Port de l'interface d'administration
<input checked="" type="checkbox"/> administration.web.secure	true	Indique si on utilise un protocole sécurisé (chiffrement)
<input checked="" type="checkbox"/> administration.web.secure.protocol	SSL	Protocole de sécurisation utilisé (si administration.web.secure est à true)
<input checked="" type="checkbox"/> administration.web.keyStore	config/certs	Fichier où se trouvent les certificats (pour les protocoles sécurisés)
<input checked="" type="checkbox"/> administration.web.keystore.password	••••••	Mot de passe du fichier de certificats (pour les protocoles sécurisés)
<input checked="" type="checkbox"/> administration.web.keystore.key.password	••••••	Mot de passe de la clé privée (pour les protocoles sécurisés)
application.server.port	4444	Port du serveur d'administration raw telnet
<input checked="" type="checkbox"/> application.server.internaluser.login	admin	Login de l'utilisateur interne
<input checked="" type="checkbox"/> application.server.internaluser.password	••••	Mot de passe de l'utilisateur interne
<input checked="" type="checkbox"/> application.server.internalUser.authorizedIP	127.0.0.1	Liste des adresses IP pouvant se connecter à l'interface raw telnet ; les adresses sont séparées par des virgules
<input checked="" type="checkbox"/> application.smtp.host	smtp.aduneo.com	Nom du serveur de messagerie utilisé pour envoyer les messages de notification
<input checked="" type="checkbox"/> application.mail.sender	NeoSync <neosync@...>	Adresse utilisée comme expéditeur des messages de notification
<input checked="" type="checkbox"/> application.mail.debug	false	Mode de debug de l'envoi de messages
<input type="checkbox"/> application.taskdeactivation.timeout	30	Délai maximal d'attente de l'arrêt d'une tâche en désactivation de l'instance (en secondes)

Valider