

# Migration de Active Directory vers OpenLDAP

## **Préambule**

Nous souhaitons mettre en place une gestion centralisée des services réseaux, des ordinateurs, des utilisateurs, des groupes et des droits dans un réseau hétérogène comprenant des ordinateurs Windows et Linux. Active Directory est actuellement utilisé pour assurer ce service. Il a été décidé de migrer vers OpenLDAP.

L'objet de ce document est d'établir la la procédure de migration des comptes, la liste des fonctionnalités attendues et de proposer une maquette en évaluant les moyens techniques d'implémentation.

## **Contraintes**

Une unité organisationnelle (Staff) comporte une centaine d'utilisateur dans Active Directory.

## **Description de la maquette**

### ***Architecture Réseau***

Deux serveurs sont nécessaires pour la mise en place du contrôleur de domaine. Sur la première machine, Samba sera installé et fera office de serveur de fichier. Sur le deuxième serveur, openLDAP fournira le backend pour Samba et les outils d'administration seront installés.

Le serveur Active Directory, actuellement en place, sera ensuite utilisé comme réplica du premier serveur openLDAP lorsque les comptes auront été migrés et Active Directory retiré du réseau.

### ***Considérations sur l'architecture LDAP***

Pour tous les objets relatifs à la gestion du domaine Samba, nous nous baserons sur les schémas fournis par Samba.

### ***Logiciel serveur***

Le système d'exploitation utilisé est Debian GNU/Linux. Le serveur LDAP utilisé est openLDAP, suffisamment mature pour être utilisé en production.

## ***Outils d'administration.***

L'interface web Gosa est installée sur le serveur openLDAP. Le serveur web apache est nécessaire. Gosa permet la gestion des comptes utilisateurs et services. PhpLDAPadmin est aussi présent sur la machine. Cet outil permet une administration générale de l'annuaire LDAP.

## **Migration des données**

### ***Contraintes***

L'étude précédemment réalisée a fait ressortir la difficulté d'importer les mots de passe des utilisateurs à partir d'Active Directory. L'exécution de scripts (vbscript, perl) rend possible cette exportation mais cette solution n'est pas suffisamment fiable pour être utilisée.

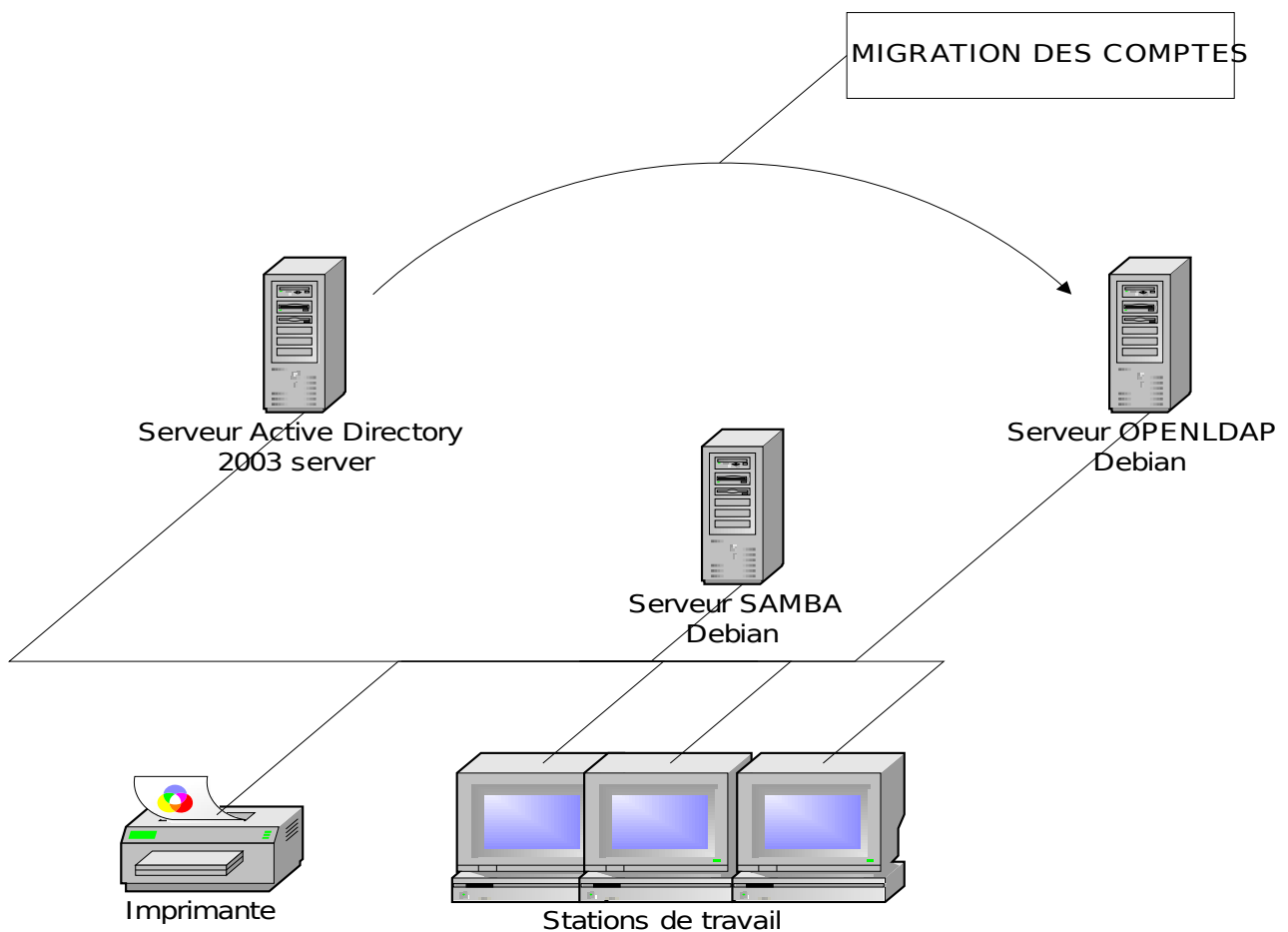
Il a donc été choisi de redéfinir des mots de passe pour les utilisateurs, de façon aléatoire. La liste des mots de passe sera accessible par l'administrateur et sera construite à partir d'un script d'exportation des données. Les utilisateurs seront invités à modifier leur mot de passe en passant par l'interface d'administration GOSA.

Aucun changement ne devra être effectué durant la phase de migration. Le temps d'interruption de service dépend du volume de données et des temps de traitement.

## Déroulement de la migration

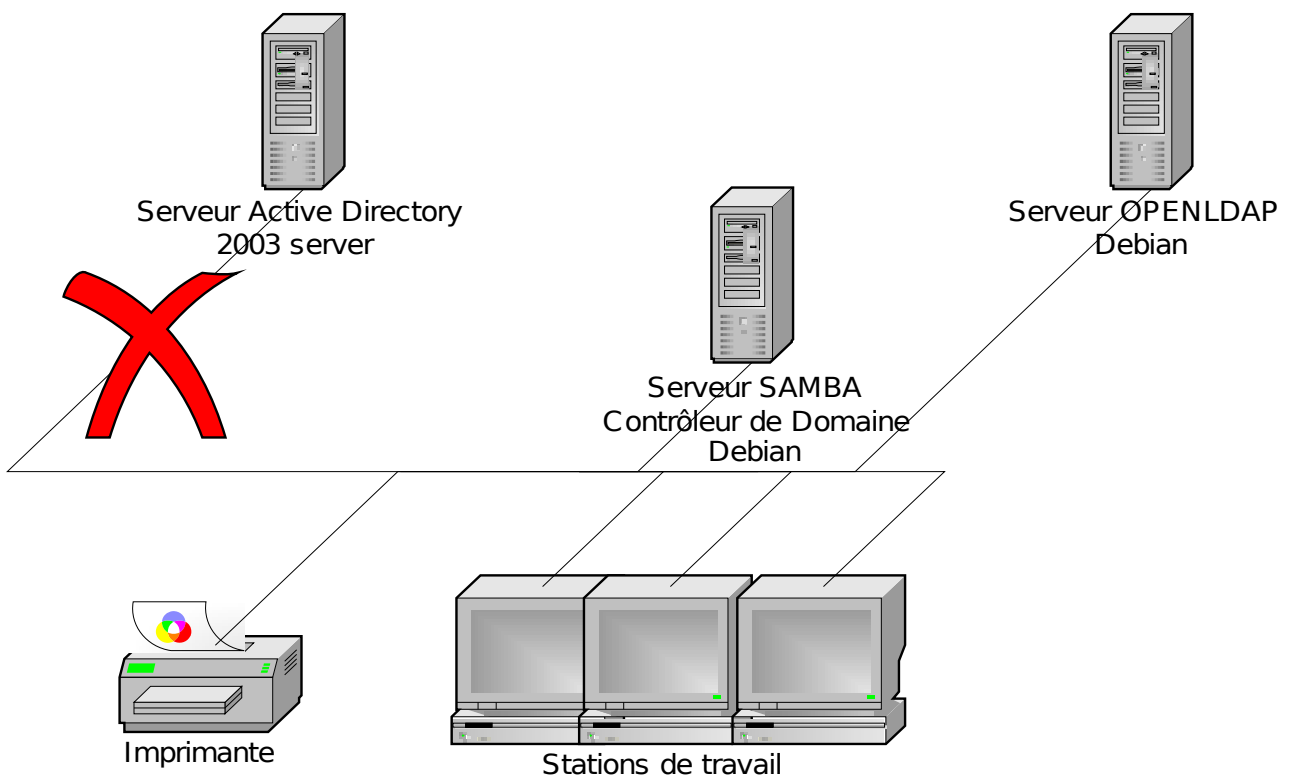
### Installation des services et préparation des données

Les serveurs installés et paramétrés sont intégrés dans le réseau existant (pas dans le domaine). Les données utilisateurs sont exportées d'Active Directory et converties en format Idif. Le résultat est importé dans openLDAP.



## Deuxième étape

La configuration de samba est modifiée et paramétrée en tant que contrôleur de domaine.  
Active Directory est enlevé du réseau.

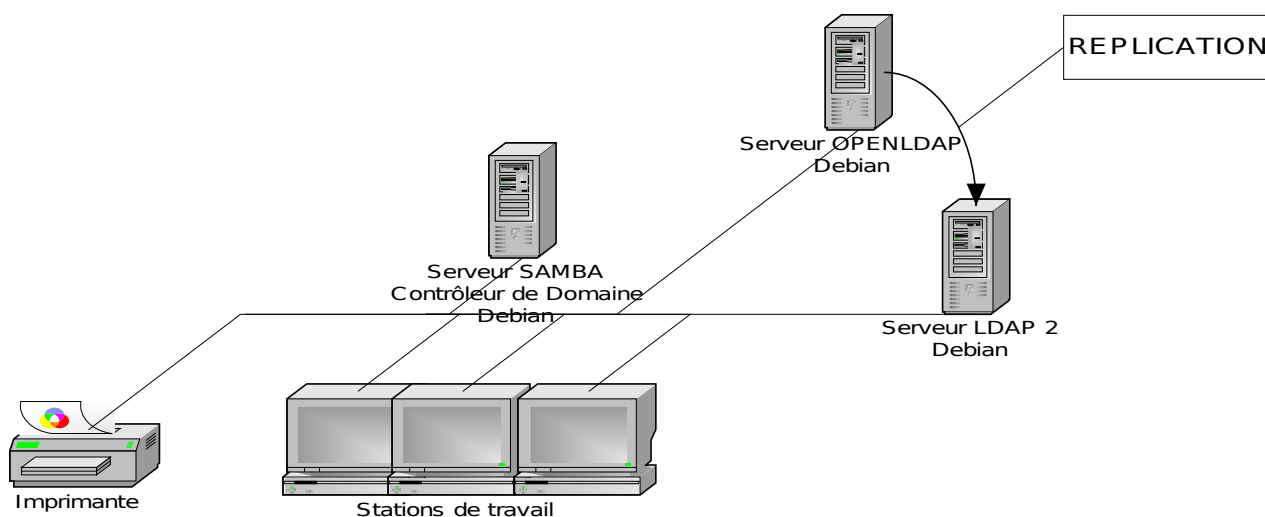


## Troisième étape

Configuration des clients et mise en place du réplica LDAP.

Pour chaque machine Windows, il est créé un compte dans la base LDAP. Cette action doit être réalisée à partir du poste client.

Pour les clients Linux : les comptes POSIX sont dans l'annuaire LDAP. Il faut que le système puisse interroger l'annuaire afin que chaque compte apparaisse de manière transparente comme étant un compte POSIX standard (présent dans /etc/passwd et /etc/group). Ceci se fait par l'intermédiaire de nsswitch et de la librairie libnss\_ldap (www.padl.com)



## Mise en place du réplica

Une fois le domaine samba opérationnel, il faut mettre en oeuvre le réplica OpenLDAP.

## Description des lots

Philippe Clément	Jean-françois Ferry
Installation Active Directory + comptes	Installation des serveurs Debian

Export des données Import dans openLDAP Configuration Clients Test Rédaction documents	Installation OpenLDAP + Samba Installation outils d'administration Tests outils administration Rédaction documents
--	---

## **Fonctionnalités après mise en oeuvre**

- Gestion des comptes Windows/Unix par une interface web.  
Deux niveaux de sécurité : administrateur et utilisateur.
- partage de fichiers, d'imprimantes
- Définition de niveaux d'accès aux ressources.
- Evolutivité des services réseaux et indépendance au niveau des éditeurs.
- Coût réduit du fait des licences d'utilisations.

## **Fonctionnalités non présentes par rapport à Active Directory**

- On ne peut pas appliquer les configurations logicielles particulières à Microsoft (stratégies de groupe)