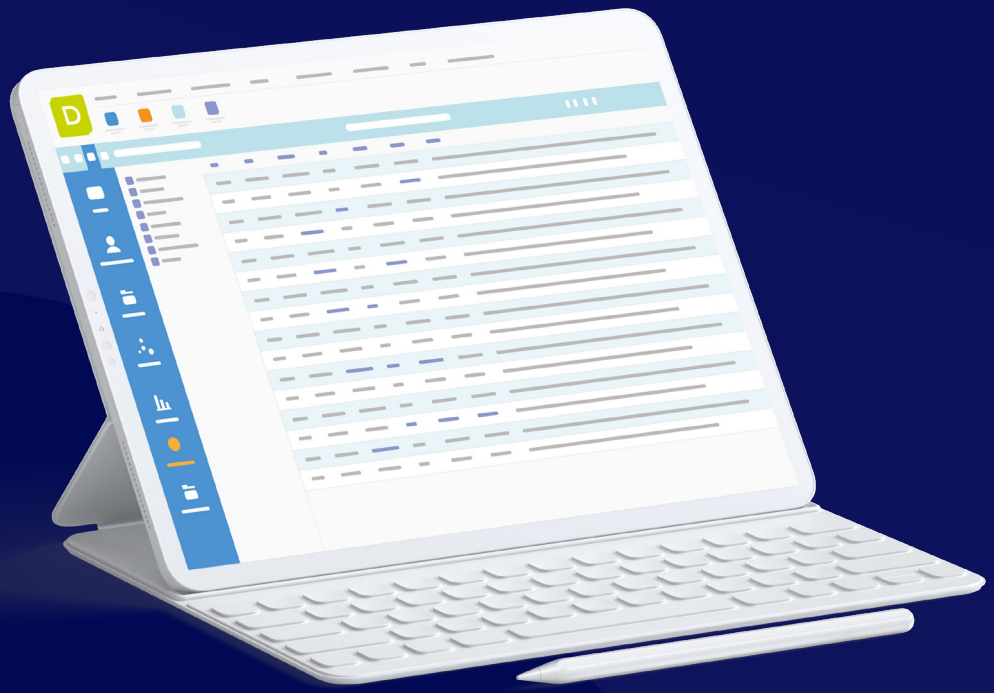


ACD

FICHE TECHNIQUE

ADMIN - LDAP : Mise en place

DIA CLIENT

Document mis à jour le 23 novembre 2023

FICHE TECHNIQUE

ADMIN - LDAP : MISE EN PLACE

Lightweight Directory Access Protocol (**LDAP**) est à l'origine un protocole permettant l'interrogation et la modification des services d'annuaire.

Ce protocole repose sur **TCP/IP**. Il a cependant évolué pour représenter une norme pour les systèmes d'annuaires, incluant un modèle de données, un modèle de nommage, un modèle fonctionnel basé sur le protocole **LDAP**, un modèle de sécurité et un modèle de réplication. Un **annuaire LDAP** respecte généralement le modèle **X.500** édicté par l'**UIT-T** : c'est une structure arborescente dont chacun des nœuds est constitué d'attributs associés à leurs valeurs.

Le nommage des éléments constituant l'arbre (racine, branches, feuilles) reflète souvent le modèle politique, géographique ou organisationnel de la structure représentée. La tendance actuelle est d'utiliser le nommage **DNS** pour les éléments de base de l'annuaire (racine et premières branches). Les branches plus profondes de l'annuaire peuvent représenter des personnes (people), des unités organisationnelles (*organizational units*), des groupes (*groups*).

SOMMAIRE

LIMITATION ET SÉCURITÉ

Lecture de l'Active Directory

Toutes les personnes connectée avec un **identifiant** et un **mot de passe** sur l'**Active Directory** sont en mesure de lister l'ensemble des machines déclarées en tant que **serveur MySQ**L. Elles peuvent également prendre connaissance des i**nformations propres à leur profil**.

À NOTER

Toutes personnes connectées au domaine peut lire les informations.

Écriture dans l'Active Directory

Afin de pouvoir créer les tags, l'utilisateur doit être identifié en tant qu'administrateur sur le contrôleur du domaine.

Pour pouvoir écrire dans l'**Active Directory**, il est nécessaire que l'utilisateur soit connecté en tant qu'administrateur du domaine.

À NOTER

Il faut être connecté en tant qu'administrateur sur le contrôleur du domaine pour écrire dans l'annuaire.

DÉCLARER UN SERVEUR MYSQL DANS L'ANNUAIRE LDAP

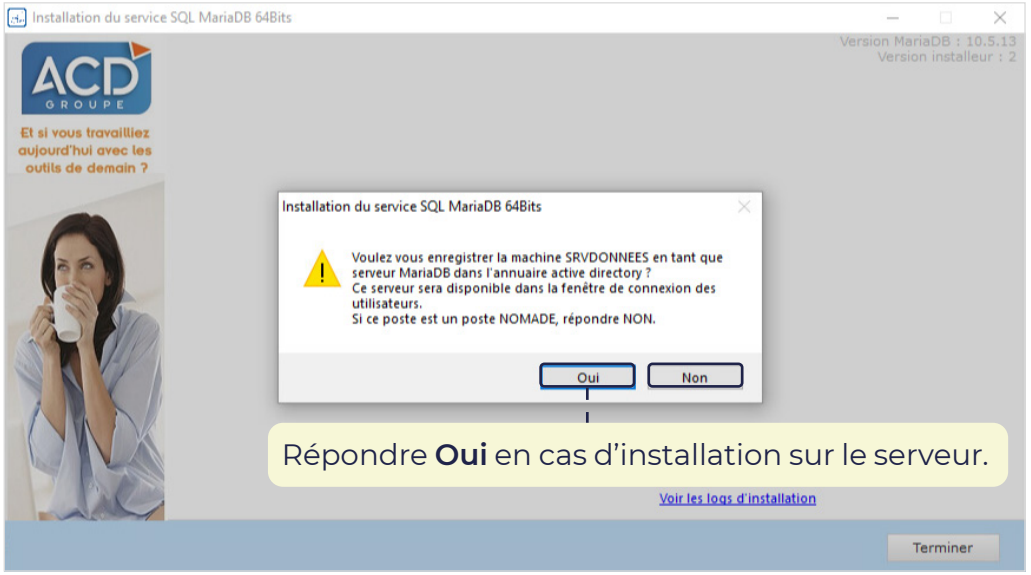
Lors de l'installation du **serveur MariaDB version 10.5**, l'enregistrement du serveur dans l'annuaire **LDAP** est proposé (identifier celui-ci en tant que machine avec le **Service MySQL** présent).

Enregistrement du serveur

Le fait d'enregistrer un serveur **MySQL** dans l'annuaire **LDAP** le fera apparaître automatiquement dans la liste des serveurs. Cette liste est visible depuis la fenêtre de connexion de **Dia Client**.

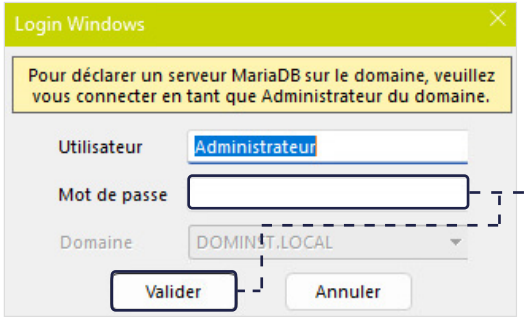
À NOTER

Répondre **Non** pour une installation sur un poste NOMADE.



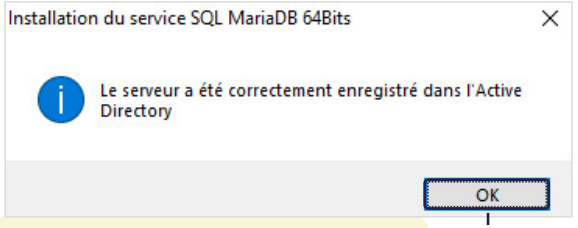
Autorisation de l'accès à l'Active Directory

La fenêtre d'identification **Login Windows** apparaît :



Saisir le **Mot de passe** de l'utilisateur Windows **Administrateur** puis cliquer sur **Valider**.

Un message s'affiche et confirme l'enregistrement dans l'**Active Directory**.

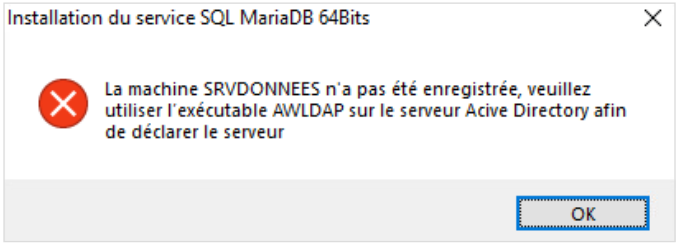


Cliquer sur **OK** pour fermer celui-ci.

FICHE TECHNIQUE

ADMIN - LDAP : MISE EN PLACE

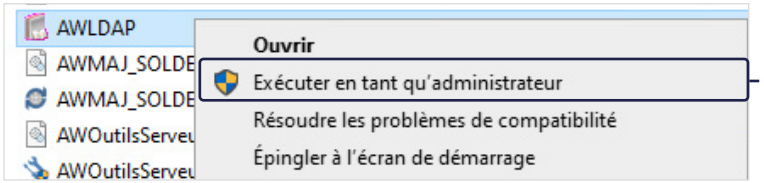
Si le message suivant apparaît :



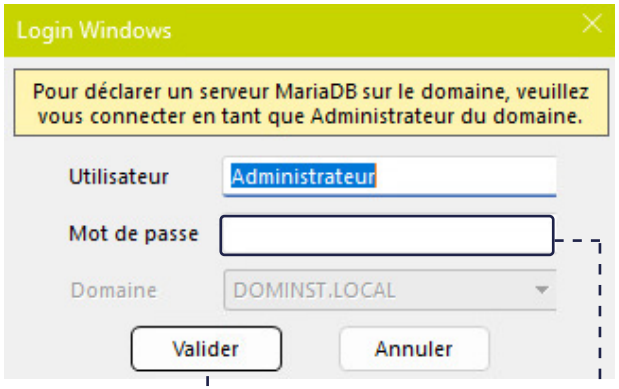
Le serveur sur lequel est installé le service **MariaDB** n'est pas contrôleur de domaine ou n'a pas le rôle de maître de schéma.
Dans ces deux cas, ouvrir une session sur le **serveur Contrôleur de domaine** (maître de schéma).

Exécuter à partir de ce serveur le fichier **Awldap.exe** en faisant un clic droit puis **Exécuter en tant qu'administrateur** soit :

- En installant les **Outils Serveur Mysql**
- En passant par le **partage C$ du serveur de données**.

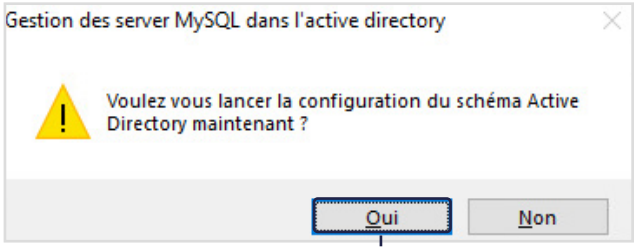


Se connecter en qu'**Administrateur du domaine**.



Saisir le **Mot de passe** puis cliquer sur **Valider**.

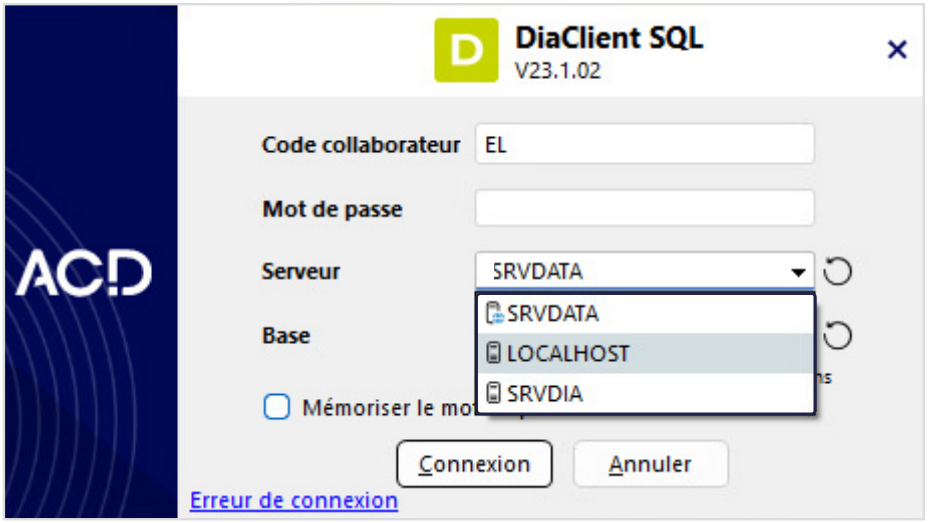
Un message de demande de configuration apparaît.



Cliquer sur **Oui**.

Il peut y avoir un délai entre la modification du schéma et la prise en compte des nouveaux objets . Cela demande un peu de temps pour que le serveur puisse être coché.

Cocher le serveur qui héberge le service **MariaDB**.



La liste déroulante propose la liste des serveurs saisis sur le poste local et la liste des serveurs déclarés dans l'annuaire **LDAP**.

L'icône représente les serveurs **MySQL** présents dans l'**Active Directory**. Les autres choix proviennent du fichier **awlazur.ini**.

Le bouton **Actualiser** permet de nettoyer la liste des serveurs provenant du fichier **awlazur.ini**.

À NOTER

Même en fonctionnement LDAP, la liste des serveurs est toujours saisissable sauf si la coche **base unique** a été sélectionnée lors de la liaison des collaborateurs au LDAP.

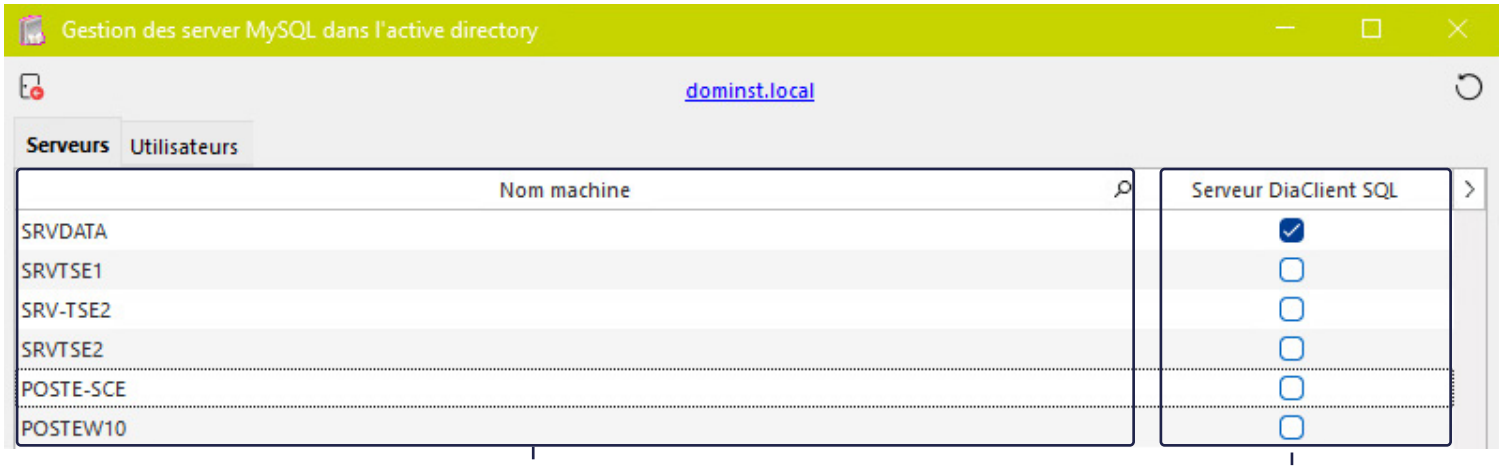
L'outil AWLDAP.exe

L'**outil AWLDAP.exe** est un utilitaire qui permet de gérer les serveurs déclarés dans l'Active Directory, ainsi que d'enregistrer ou de supprimer des serveurs de l'annuaire LDAP.

À NOTER

A lancer sur le contrôleur de domaine en tant qu'administrateur.

L'outil est installé avec les **Outils Serveur** et est accessible dans **C:\Program Files (x86)\ACDSuite\AWOutilsServeur.**



Liste des **Noms Machine** (objets de type Computer) déclarés au niveau de l'**Active Directory** (tout ordinateur associé au domaine).

Objets cochés déclarés en tant que **serveur MySQL** et qui apparaissent dans la liste des serveurs sur la fenêtre de connexion.

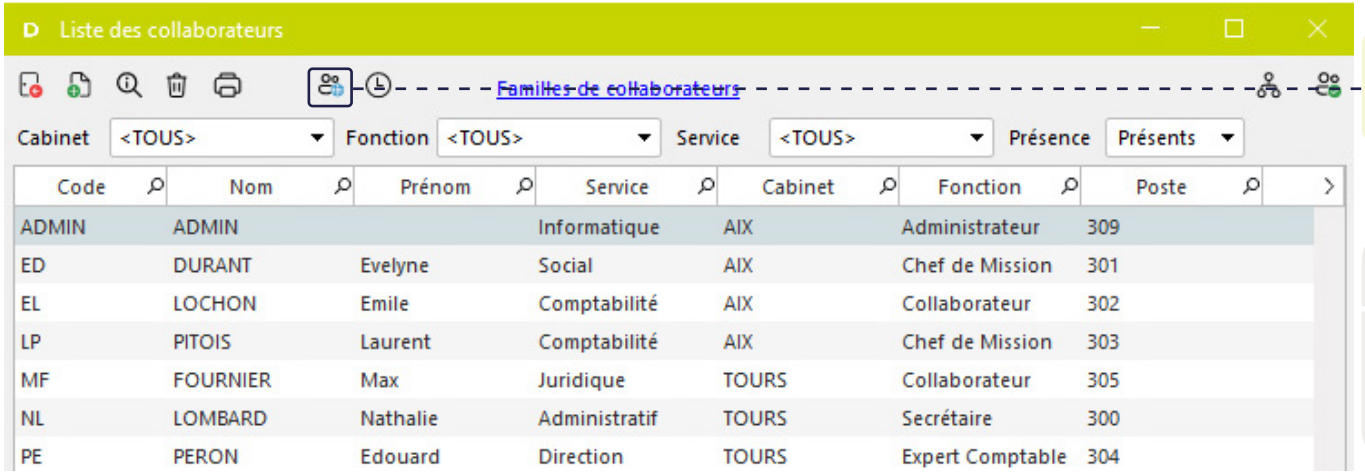
ASSOCIER UN UTILISATEUR DIA CLIENT À SON COMPTE WINDOWS (SSO)

L'**authentification unique** (ou identification unique ; en anglais **Single Sign-On** ou **SSO**) est une méthode permettant à un utilisateur de ne procéder qu'à une seule authentification pour accéder à plusieurs applications informatiques (ou sites web sécurisés).
Les objectifs sont multiples :

- **Simplifier pour l'utilisateur la gestion de ses mots de passe**
  Plus l'utilisateur doit gérer de mots de passe, plus il aura tendance à utiliser des mots de passe similaires ou simples à mémoriser, abaissant par la même occasion le niveau de sécurité.
- **Simplifier la gestion des données personnelles détenues par les différents services en ligne**, en les coordonnant par des mécanismes de type méta-annuaire.
- **Simplifier la définition et la mise en œuvre de politiques de sécurité**.

Cette déclaration se fait directement, dans la gestion des collaborateurs de **Dia Client** (menu **Généralités** - **Collaborateurs**).

La liste des collaborateurs apparaît :



Ce bouton permet d'accéder à la **gestion de l'intégration**.

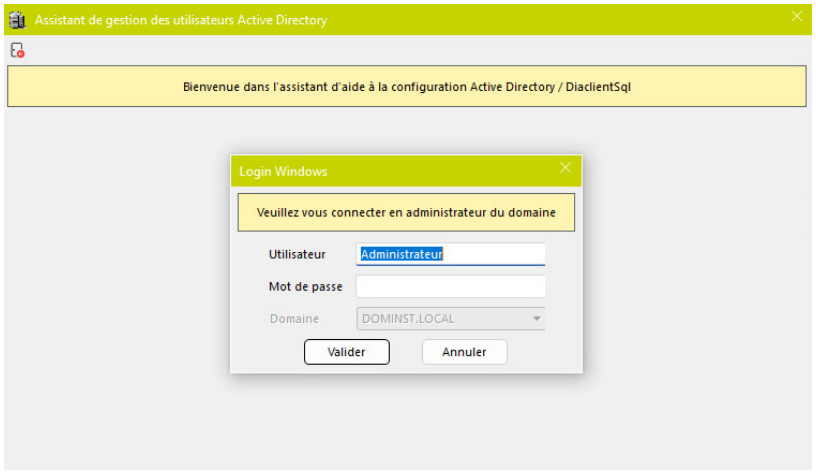
À NOTER

A lancer sur le contrôleur de domaine en tant qu'administrateur Windows et Dia Client.

ADMIN - LDAP : MISE EN PLACE

Lors de l'ouverture de la fenêtre de gestion, si vous êtes bien sur la session **Administrateur**, le mot de passe sera demandé.

Saisir le mot de passe en tant qu'administrateur du domaine (Login Windows) :



À NOTER

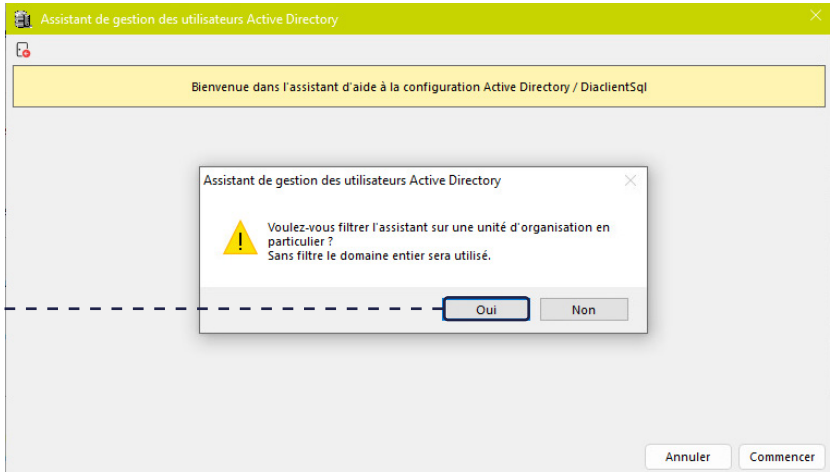
Si le mot de passe renseigné est erroné, la fenêtre reste grisée.

En cliquant **Oui**, il est possible de choisir la branche concernée de l'**Active Directory** (Unité Organisationnelle (O.U)) à partir de laquelle les utilsateurs doivent être importés.

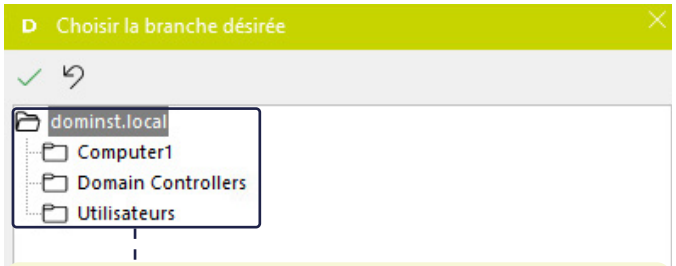
À NOTER

En cliquant **Non**, c'est le domaine complet qui est utilisé.

Une fois le mot de passe validé, la fenêtre suivante apparaît :

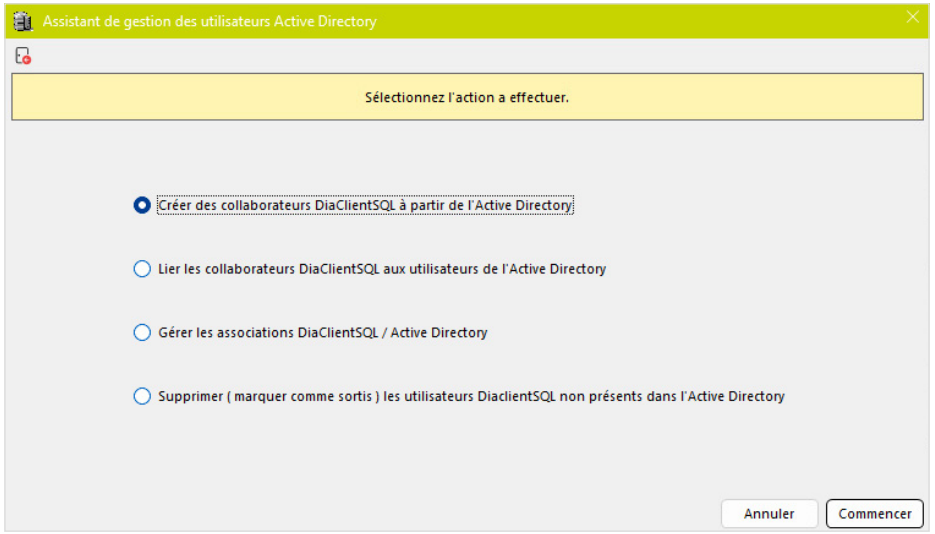


Choisir l'**O.U.** ou double-cliquer pour faire apparaître les sous-dossiers.



L'ensemble des utilisateurs est récupéré à partir de l'**O.U.** sélectionnée ainsi que ceux des sous **O.U**.

La fenêtre suivante apparaît :

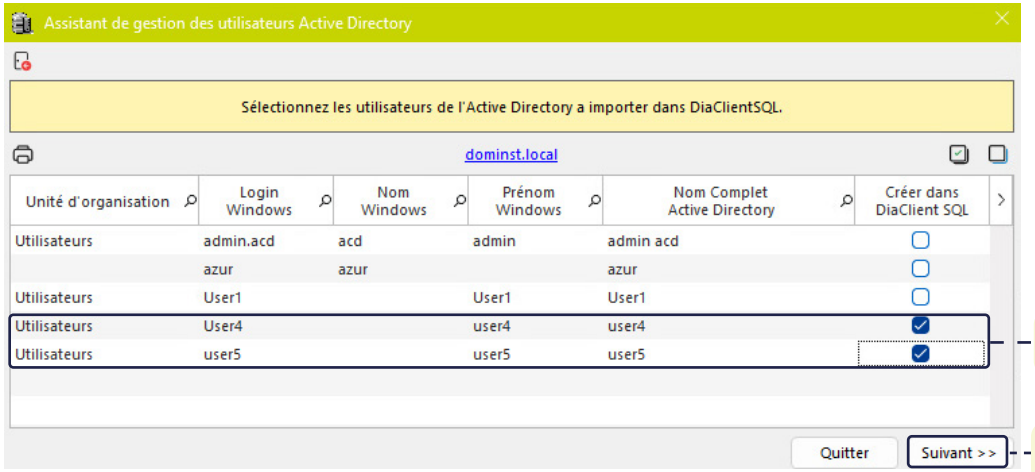


Quatre choix sont proposés :

- Créer des collaborateurs DiaClientSQL à partir de l'Active Directory
  Sélectionner ce choix pour une nouvelle installation afin de créer automatiquement les collaborateurs **Dia Client** à partir des utilisateurs Windows de l'Active Directory.
- Lier les collaborateurs DiaClientSQL aux utilisateurs de l'Active Directory
  Cocher cette option pour une installation existante afin d'associer des collaborateurs existants dans **Dia Client** à des utilisateurs **Windows** de l'**Active Directory**.
- Gérer les associations DiaClientSQL / Active Directory
  Dissocier / synchroniser les collaborateurs **Dia Client** avec l'**Active Directory**.
- Supprimer (marquer comme sortis) les utilisateurs DiaClientSQL non présents dans l'Active Directory
  Classer les collaborateurs **Dia Client** en fonction de l'**Active Directory** en marquant ceux- ci comme sortis si non trouvés dans l'**Active Directory**.

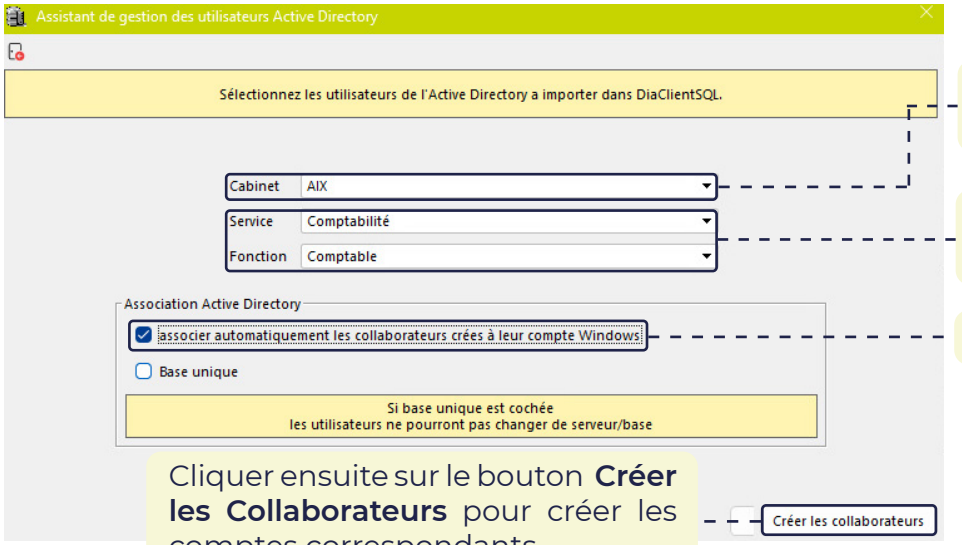
Créer des collaborateurs Dia Client à partir de l'Active Directory

La fenêtre liste des utilisateurs **LDAP**.



Les utilisateurs cochés sont ensuite créés dans **Dia Client**.

Cliquer sur **Suivant**.



Attribuer ensuite le **cabinet de rattachement principal** des collaborateurs (**obligatoire**).

Le service et la fonction sont facultatifs. Cela permet d'initialiser ces zones dans la fiche collaborateur.

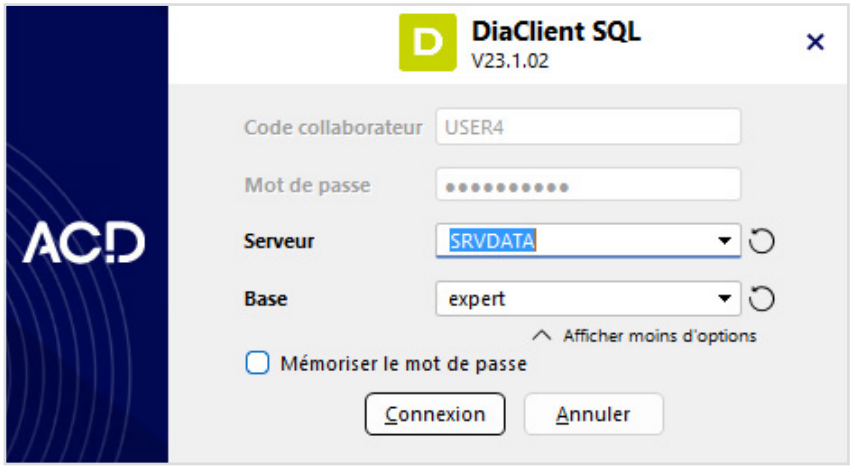
Liaison avec l'**annuaire LDAP**.

Par défaut tous les collaborateurs ont accès à l'ensemble des fiches de tous les cabinets. La limitation d'accès d'un collaborateur sur un ou plusieurs cabinet(s) se paramètre dans la fiche **Collaborateur** de **Dia Client**.

Cliquer ensuite sur le bouton **Créer les Collaborateurs** pour créer les comptes correspondants.

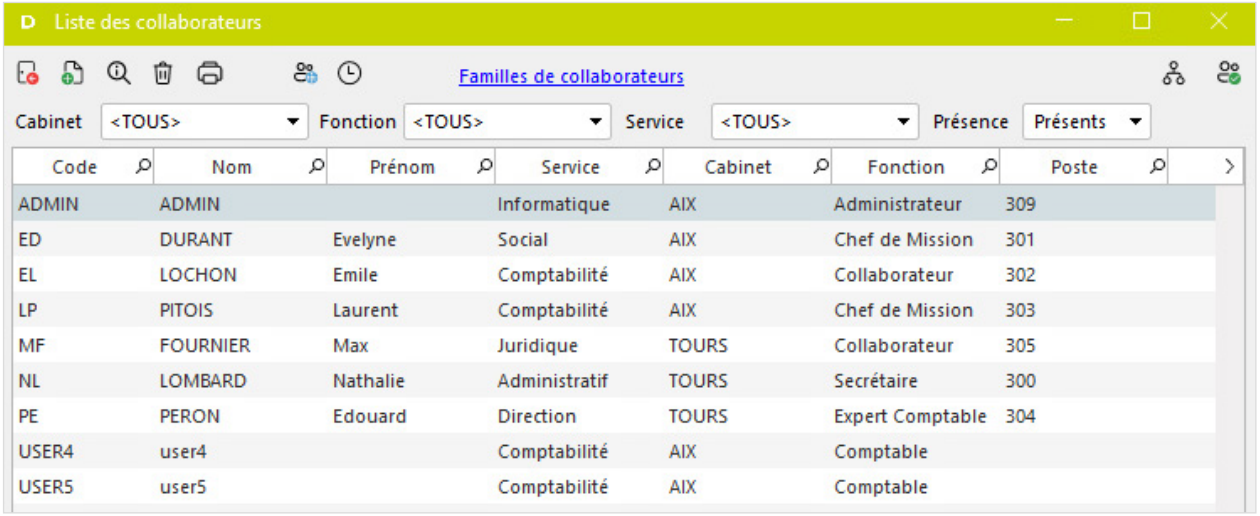
FICHE TECHNIQUE

ADMIN - LDAP : MISE EN PLACE

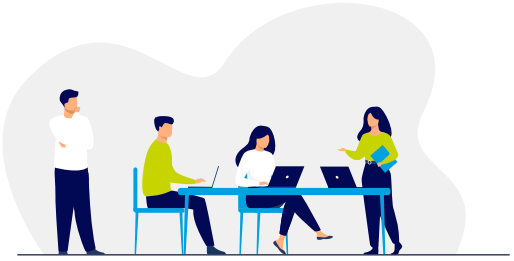


Deux cas sont possibles :

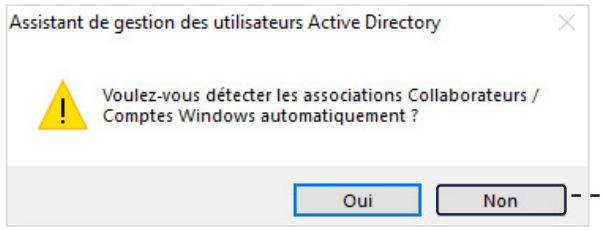
- Si l'option **Associer automatiquement les collaborateurs créés à leur compte Windows** est cochée, alors le code collaborateur et le mot de passe ne sont plus saisissables car dépendants de l'identification Windows.
- Si l'option **Base unique** est aussi cochée, la fenêtre de connexion habituelle de Dia Client ci-contre n'apparaîtra plus. Le collaborateur ne pouvant plus sélectionner de serveur ou de base, la connexion est transparente.



Code	Nom	Prénom	Service	Cabinet	Fonction	Poste
ADMIN	ADMIN		Informatique	AIX	Administrateur	309
ED	DURANT	Evelyne	Social	AIX	Chef de Mission	301
EL	LOCHON	Emile	Comptabilité	AIX	Collaborateur	302
LP	PITOIS	Laurent	Comptabilité	AIX	Chef de Mission	303
MF	FOURNIER	Max	Juridique	TOURS	Collaborateur	305
NL	LOMBARD	Nathalie	Administratif	TOURS	Secrétaire	300
PE	PERON	Edouard	Direction	TOURS	Expert Comptable	304
USER4	user4		Comptabilité	AIX	Comptable	
USER5	user5		Comptabilité	AIX	Comptable	



Lier les collaborateurs Dia Client aux utilisateurs de l'Active Directory



Lors du lancement de cette option, un assistant associe automatiquement un utilisateur Windows à un utilisateur Dia Client, à l'aide du compte Windows nom/prénom.

En répondant **Non**, il sera possible de procéder manuellement à l'affectation.

Cliquer dans la colonne pour sélectionner le collaborateur à l'aide de la liste déroulante.

À NOTER

Si la coche **Base unique** est sélectionnée, la fenêtre de connexion n'apparaîtra plus. Le collaborateur ne pouvant plus sélectionner de serveur/base, la connexion se fait de manière transparente.

Lors de l'association, un nouveau mot de passe est généré pour le collaborateur sélectionné.
Cliquer sur le bouton **Associer** pour terminer la procédure.

À NOTER

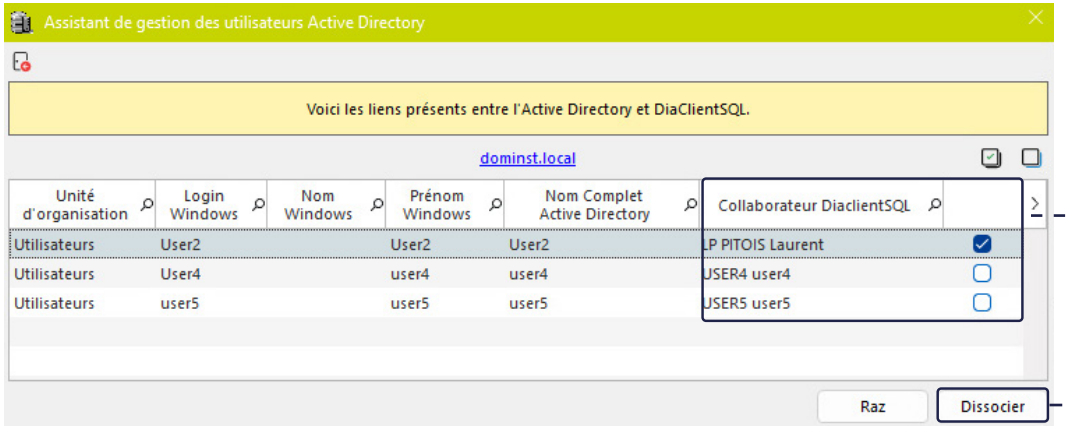
Le **Code collaborateur** et le **Mot de passe** ne sont plus saisissables car ils sont dépendants de l'identification Windows.

Le serveur et la base restent modifiables car, dans ce cas de figure, la coche **Base unique** n'a pas été sélectionnée.

Suite au traitement, la fenêtre de connexion à **Dia Client** se présente comme dans l' exemple ci-contre :

Gérer les associations Dia Client / Active Directory

Cet écran liste les utilisateurs de l'Active Directory marqués comme appartenant à une base **Dia Client**.
Le code collaborateur associé est affiché.

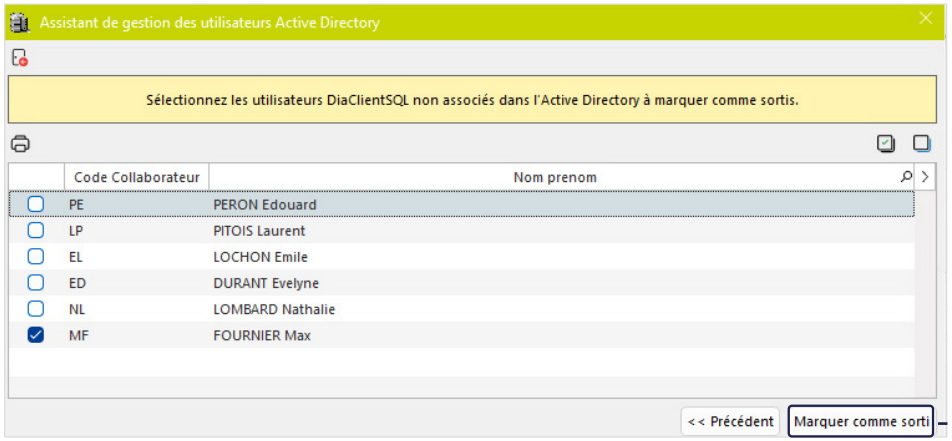


1/ Sélectionner le ou les comptes à dissocier.

2/ Cliquer sur **Dissocier**.

Supprimer/marquer comme sortis les utilisateurs Dia Client non présents dans l'Active Directory

Cette fenêtre liste les codes collaborateur associés à aucun utilisateur LDAP.



Cliquer sur ce bouton pour **Marquer comme sortis** les utilisateurs sélectionnés dans **Dia Client**.

CHANGEMENT DE SERVEUR MYSQL

Problématique

Suite à un changement de serveur MySQL, alors les utilisateurs ne peuvent plus se connecter du fait que les collaborateurs sont liés au login **Active Directory** et de la configuration de la **Base unique**.

En effet, les collaborateurs sont configurés pour rechercher un serveur MySQL et une base de données identifiée. De plus, ils n'ont plus accès à la modification de ces options au login **Dia Client**.

Solution

Se référer à la procédure Déclarer un serveur MySQL dans l'annuaire LDAP (page 5).

1/ Utiliser l'outil **AWLDAP.exe** (répertoire d'installation des outils sur les serveurs MySQL).

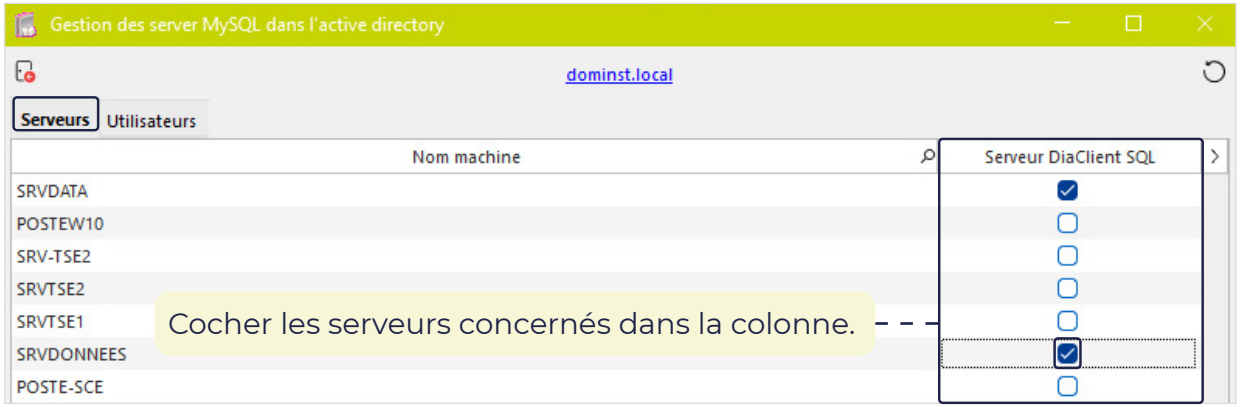
2/ Installer **MySQL** sur le nouveau serveur. Il est de la même version que sur l'ancien serveur.

À la question **Voulez-vous enregistrer le serveur MySQL dans l'active directory ?** , répondre **Oui**. Si le serveur existe déjà et qu'il n'a pas été enregistré dans l'AD, on peut aussi l'enregistrer avec **AWLDAP.exe**.

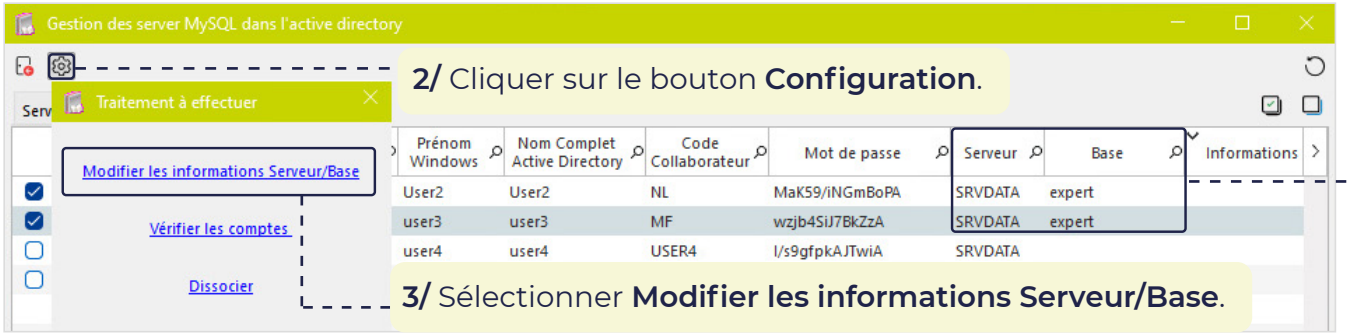
3/ Ouvrir l'outil **AWLDAP.exe**.

Dans l'onglet **Serveur**, la liste des serveurs enregistrés apparaît.

Si nécessaire, on peut enregistrer un **serveur MySQL** s'il a été préalablement installé sans avoir été validé dans l'**AD**.



Dans l'onglet **Utilisateurs**, indiquer le nouveau serveur MYSQL ou la nouvelle base :



2/ Cliquer sur le bouton **Configuration**.

1/ Les utilisateurs **Base unique** sont indiqués avec leur serveur et leur base.

3/ Sélectionner **Modifier les informations Serveur/Base**.

Indiquer le **nouveau serveur** ou la **nouvelle base**.

Attention
Si l'un des paramètres ne doit pas changer, ne pas laisser **à vide**, cocher **Conserver existant**.