Le serveur Icewarp

Configuration d'un annuaire LDAP

EPOS – v14

Janvier 2025

Sommaire

Configuration d'un annuaire LDAP

Introduction

Ce document décrit la création et l'utilisation d'un carnet d'adresses LDAP avec le serveur IceWarp.

L'objectif est de synchroniser les comptes créés sur le serveur IceWarp vers un annuaire LDAP. Dans le cas décrit ci-dessous, l'annuaire est créé spécifiquement sur le serveur mais il est possible aussi d'utiliser un annuaire externe préexistant.

Qu'est-ce que LDAP ?

LDAP est l'acronyme de **Lightweight Directory Access** Protocol. Il s'agit d'un protocole d'accès aux services d'annuaires.

LDAP permet de gérer des organisations, des personnes et d'autres ressources telles que fichiers ou matériels. Un annuaire LDAP peut donc constituer une base centrale de stockage pour ces objets. L'annuaire sera ensuite lu par d'autres logiciels pour retrouver des données selon des critères de recherche appropriés. Par exemple, il est facile de retrouver vos collègues dans un annuaire LDAP à partir de tout client mail supportant LDAP.

C'est dans ce cadre qu'intervient le couplage de IceWarp avec un annuaire LDAP.

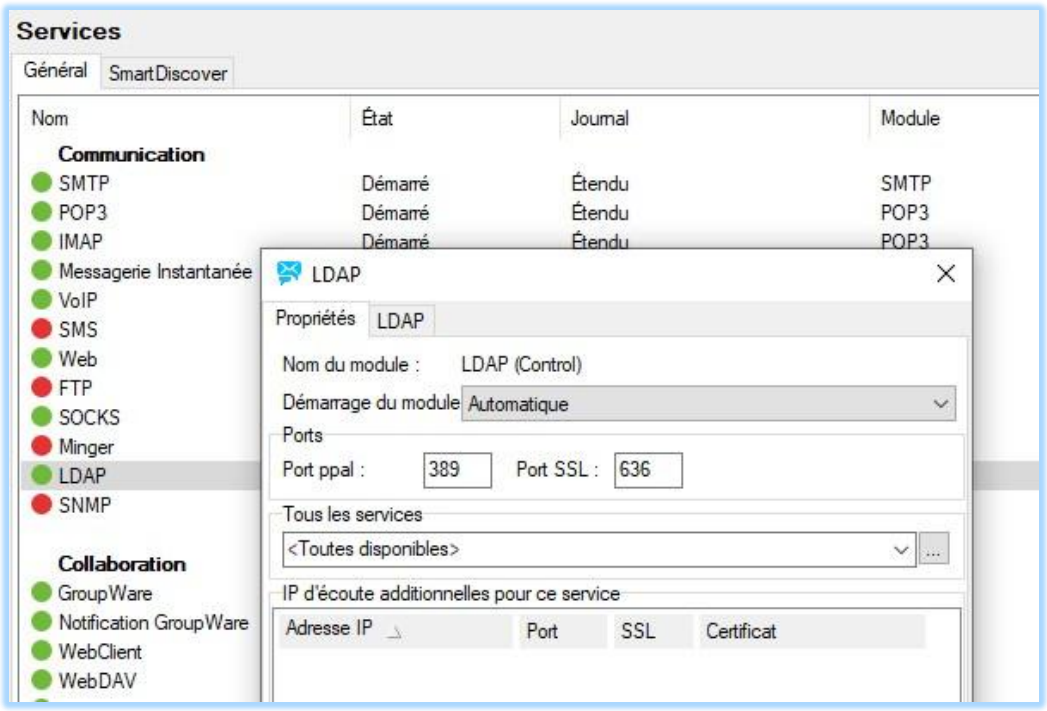
Dans la suite, nous exposons d'abord comment paramétrer l'annuaire LDAP utilisé avec IceWarp et nous terminons par l'utilisation faite de cet annuaire dans un client de messagerie (Outlook).

IceWarp et LDAP

Configuration de l'annuaire

Durant l'installation d'IceWarp, un annuaire LDAP est installé automatiquement. Il s'agit de OpenLDAP, une implémentation "open source" du protocole LDAP. Vous trouverez des informations sur le projet OpenLDAP à l'adresse suivante : openldap.org.

Par défaut, cet annuaire tourne sur le port 389 de la machine où IceWarp est installé (389 est le port par défaut selon la norme LDAP). S'il arrive que ce port soit déjà utilisé sur la machine (ce qui sera probablement le cas si Microsoft Active Directory est activé sur la même machine qu'IceWarp), on peut modifier le port de l'annuaire OpenLDAP utilisé par IceWarp. Pour cela, aller dans le menu Services, choisir le service 'LDAP', afficher ses propriétés, changer la valeur du port d'écoute de l'annuaire et redémarrer le service, dans cet exemple, c'est le port 389 qui est utilisé :



La configuration de l'annuaire est inscrite dans le fichier <répertoire d'installation de IceWarp> \config\ldap\etc \slapd.conf.

Ce fichier est aussi accessible à partir de l'interface IceWarp (onglet LDAP ci-dessus). Une explication détaillée de slapd.conf se trouve dans l'annexe A de ce document.

Nous avons défini les paramètres suivants pour l'annuaire : un nœud qui s'appelle 'dc=darnis, dc=com' et le compte administrateur qui s'appelle 'cn=manager'.

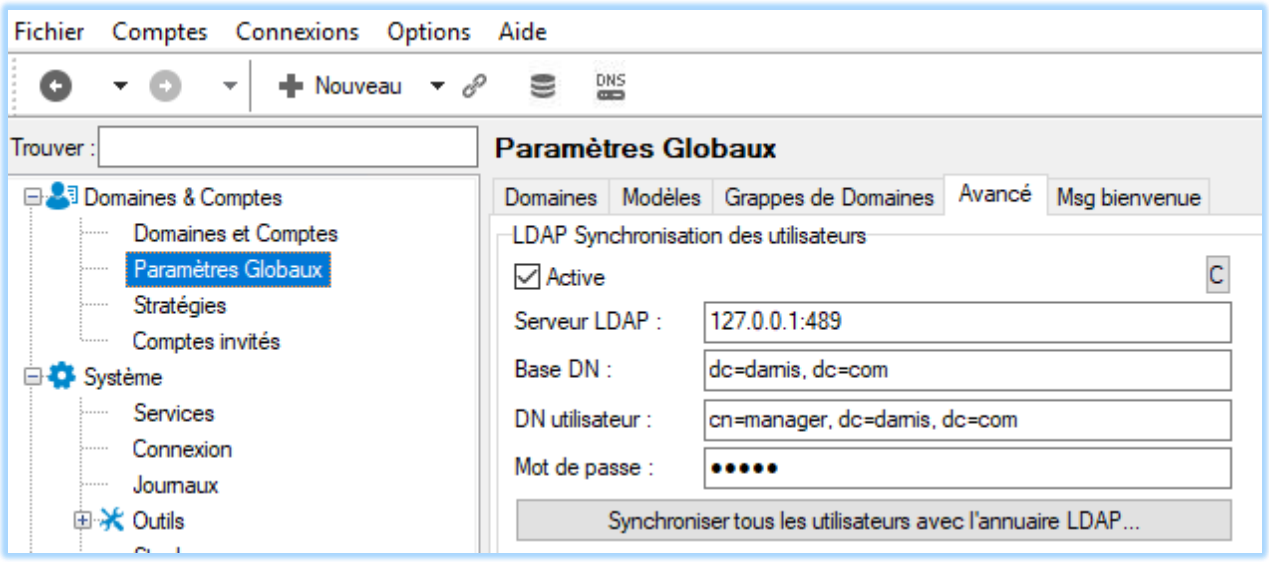
Un nœud supplémentaire : "ou=users " a été créé à l'aide d'un browser LDAP.

Configuration de la synchronisation

Une fois que le serveur LDAP est configuré, la prochaine étape consiste à configurer les paramètres de connexion pour la synchronisation des comptes.

Aller dans Gestion -> Paramètres Globaux -> onglet Avancé.

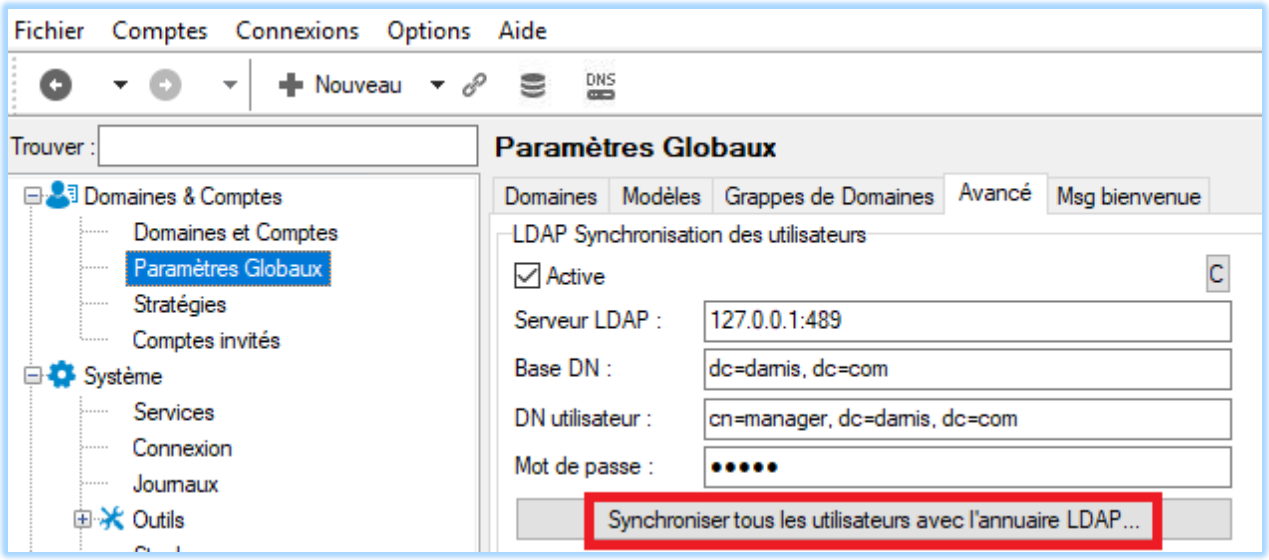
Cocher la case 'Active' et indiquer le nom/adresse IP de la machine et le compte pour se connecter à l'annuaire. Noter qu'il est nécessaire de spécifier le port, si différent du port standard (389).



Synchronisation

Il faut maintenant insérer les comptes existants sur IceWarp dans l'annuaire LDAP. Un objet LDAP sera créé pour chaque compte IceWarp de type 'User'.

Pour démarrer la synchronisation, aller dans Gestion -> Paramètres Globaux -> onglet Avancé et cliquer sur le bouton 'Synchroniser tous les Utilisateurs avec l'annuaire LDAP…'



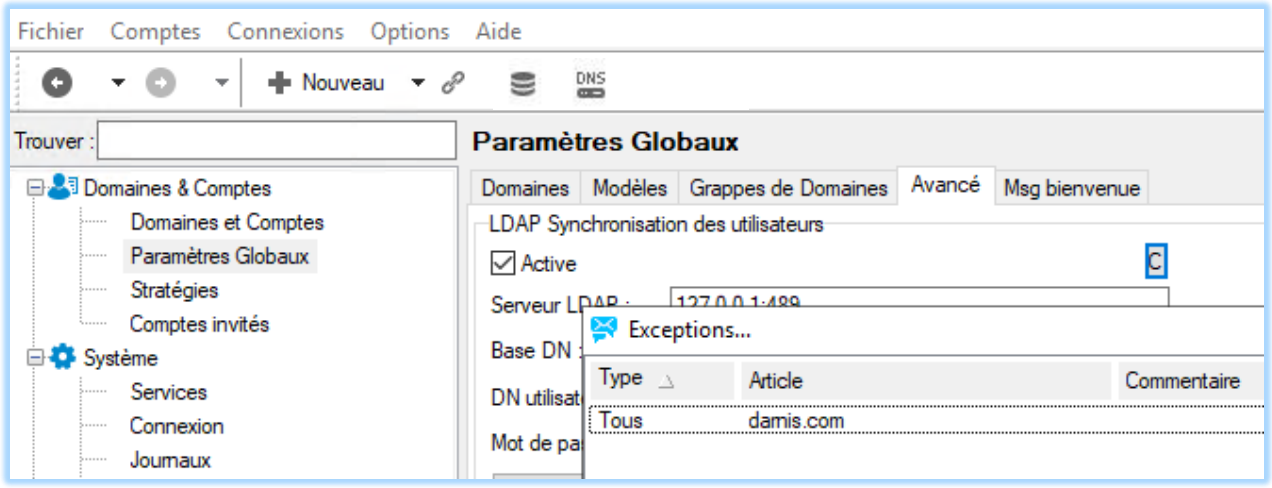
La première fois que ce bouton est activé, tous les comptes IceWarp sont synchronisés vers l'annuaire LDAP.

Par la suite, chaque fois qu'un changement survient sur un compte IceWarp, l'annuaire LDAP est mis à jour automatiquement.

Les changements pris en compte sont : création/suppression/modification.

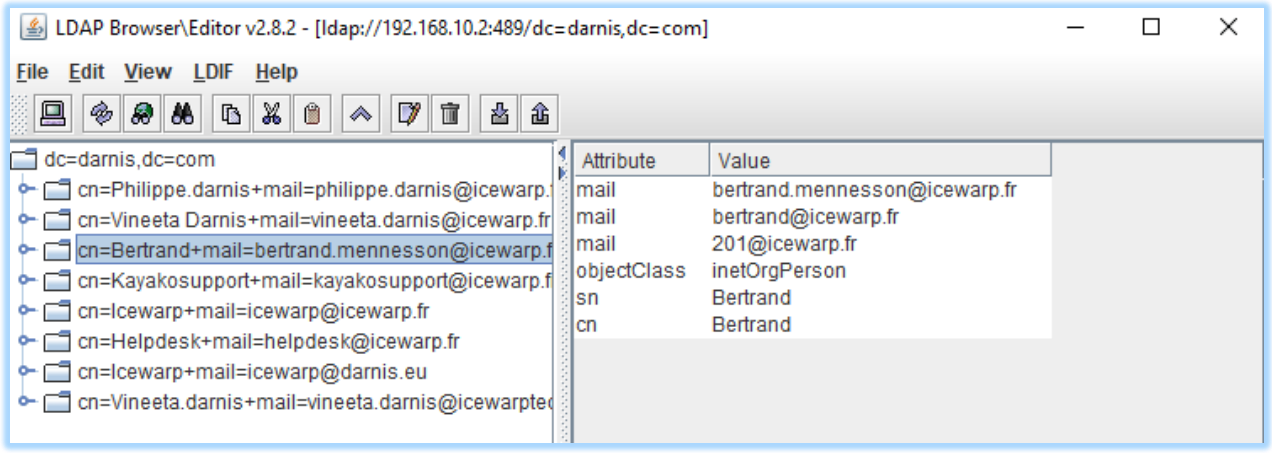
Il s'agit d'une synchronisation unidirectionnelle : IceWarp vers OpenLDAP. La clé de jointure est l'attribut CN de l'annuaire LDAP qui correspond au champ' Full name' de IceWarp.

Si on ne souhaite pas synchroniser certains comptes IceWarp vers l'annuaire, il faut indiquer ces comptes dans le fichier 'Contournement'. Le fichier Contournement contient des adresses mail et des domaines (une par ligne). Il est possible d'utiliser des masques. Ces adresses vont servir de critères d'exclusion pendant la synchronisation. Des explications détaillées sur le format du fichier de contournement sont fournies en annexe B de ce document.



Dans le cas présenté ici, le domaine darnis.com ne sera pas synchronisé vers l'annuaire LDAP.

Voici le résultat de la synchronisation visualisée dans browser LDAP :

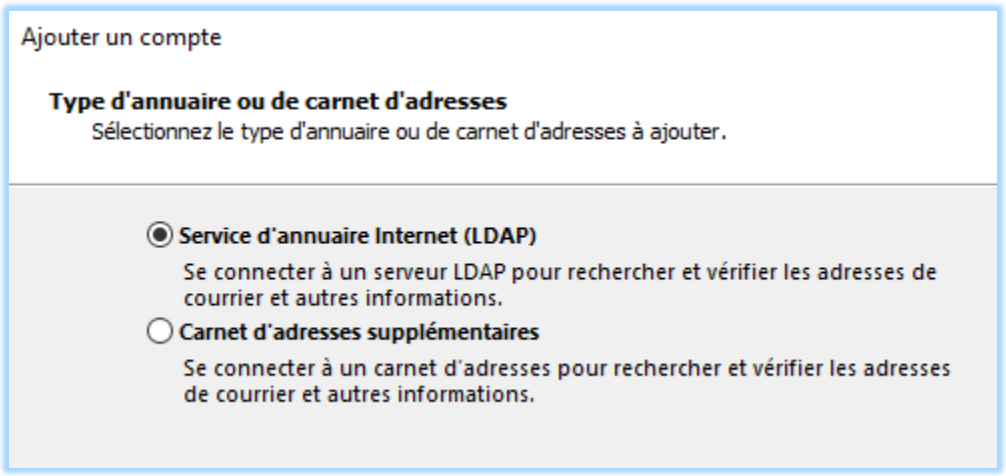


Utilisation depuis le client de messagerie Outlook

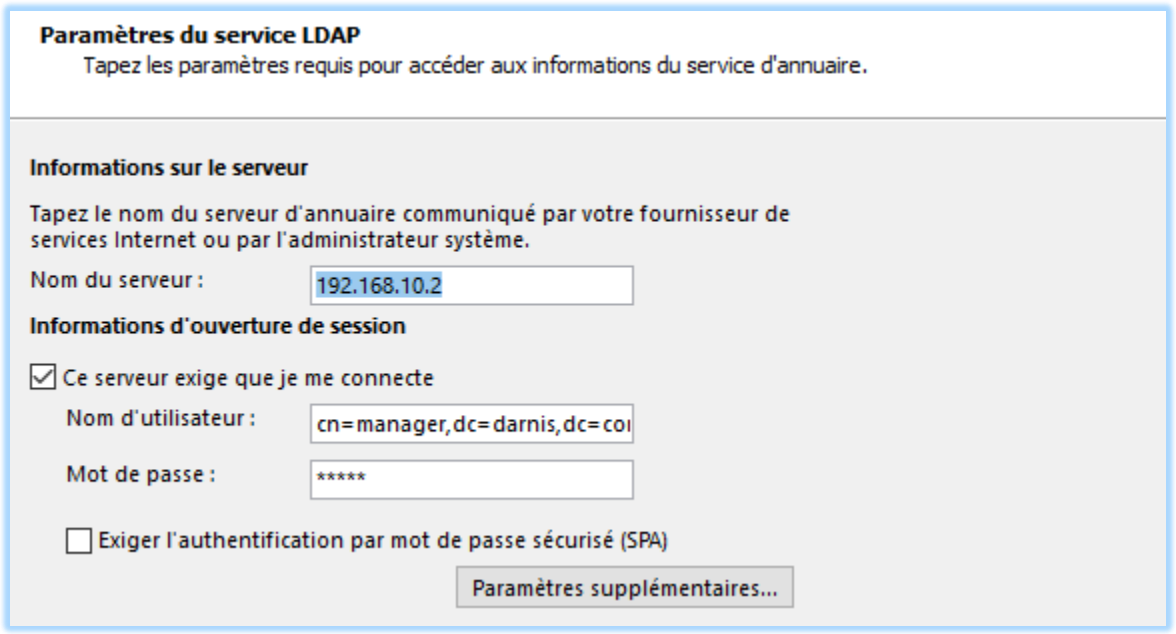
Une fois que les comptes IceWarp sont synchronisés avec l'annuaire externe, il sera possible d'utiliser cet annuaire lors de la composition des messages dans un client de messagerie.

Par la suite, on indique la façon de faire depuis le client Microsoft Outlook (2016). La manière d'intégrer un annuaire LDAP est en effet propre à chaque client de messagerie.

Ouvrez Fichier -> Paramètres du compte -> onglet Carnet d'adresses -> Nouveau…



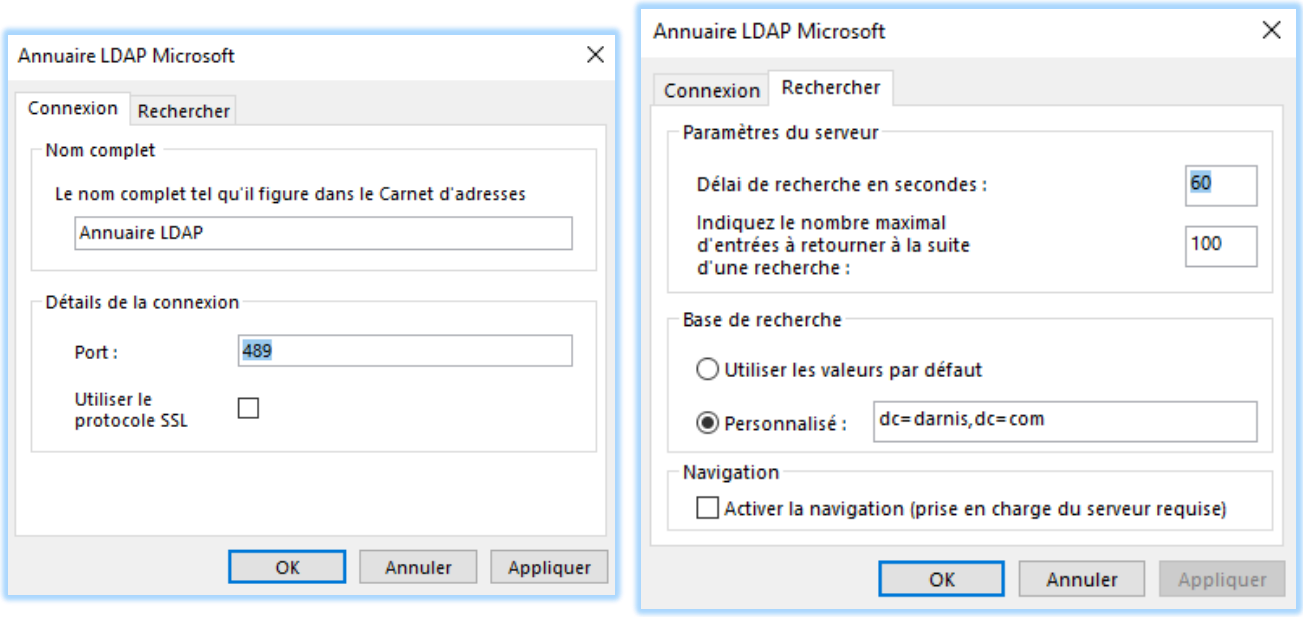
Sélectionnez 'Service d'annuaire Internet (LDAP)' et cliquer sur 'Suivant'.



Il faut donner l'adresse ou le nom du serveur sur laquelle tourne le serveur LDAP mais il n'est pas nécessaire de fournir des informations d'ouverture de session car, par défaut, l'annuaire OpenLDAP permet une lecture en mode anonyme (sans connexion).

Cliquez sur 'Paramètres supplémentaires…' et remplir les deux onglets 'Connexion' et 'Rechercher' comme suivant

(Cliquez 'OK' sur la fenêtre de message demandant de quitter Outlook. On fera un redémarrage à la fin de la configuration).



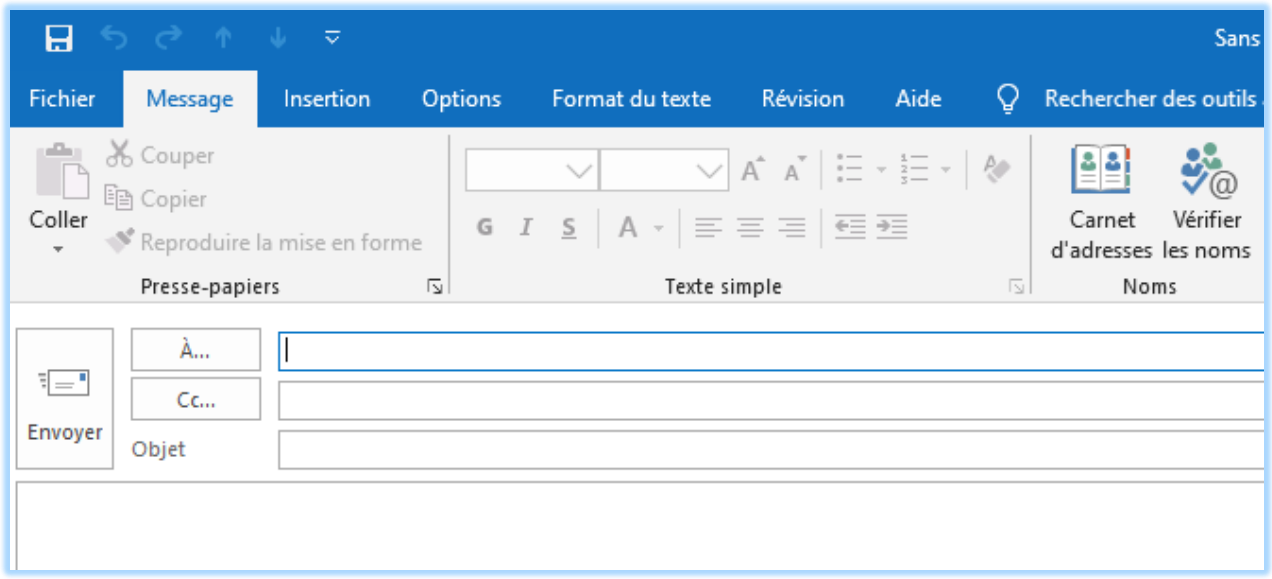
Le 'Nom complet' est celui qui apparaîtra dans la liste de choix pendant la rédaction d'un message.

Par défaut, le numéro de port est '389' pour une connexion non sécurisée ou '636' pour une connexion sécurisée (SSL). Indiquez ici la même valeur que celle de la configuration du service LDAP dans la console IceWarp.

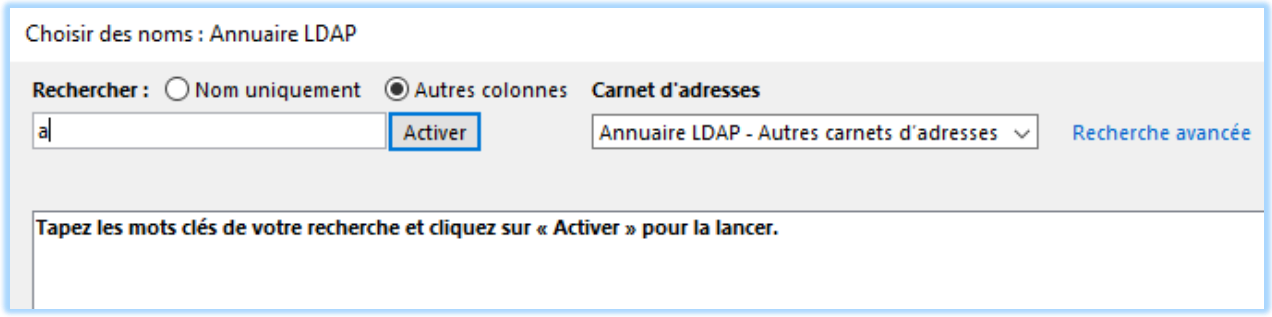
Le nœud principal sous lequel la recherche sera effectuée est 'dc=root' par défaut, il faut donc le modifier dans notre cas.

Cliquez sur 'Appliquer'. Il est nécessaire de redémarrer Outlook pour une prise en compte complète.

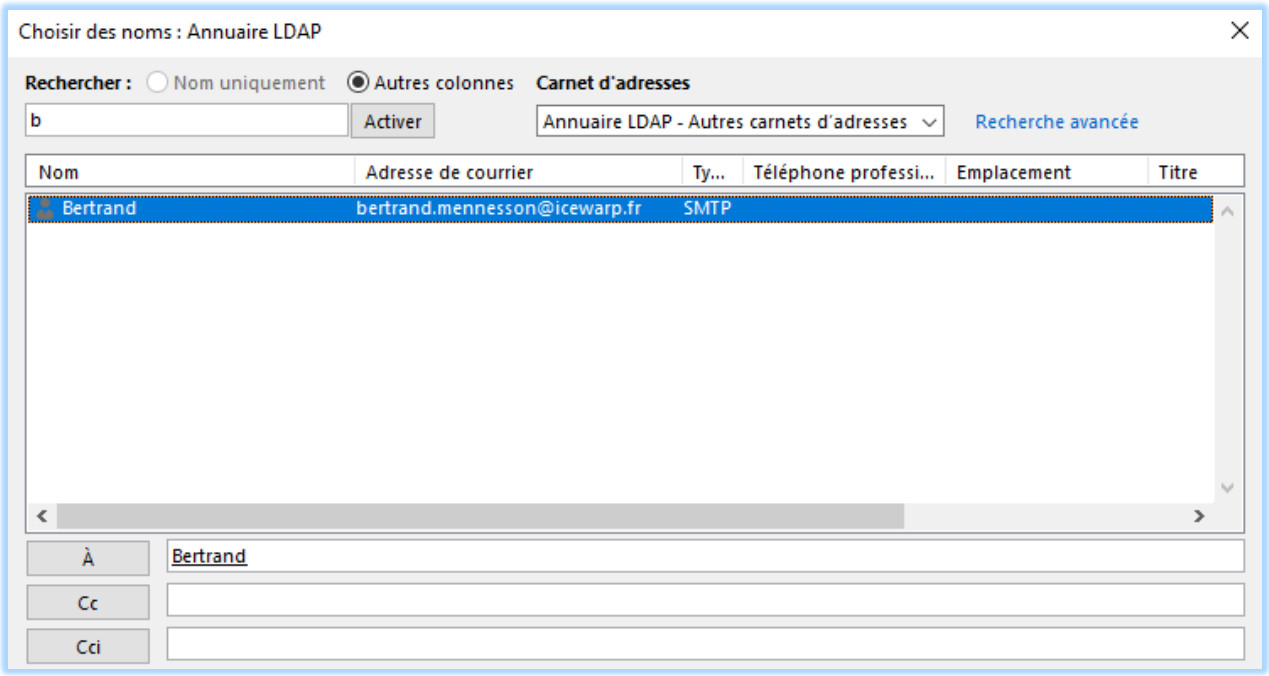
Commencer la rédaction d'un nouveau message.



Cliquer sur l'un des boutons 'A...' ou 'Cc...' et la fenêtre suivante s'ouvre :



Choisir l'annuaire LDAP, remplir les critères de recherche et cliquez sur 'Activer', on obtient quelque chose comme :



Le filtre présenté ci-dessus va rechercher dans l'annuaire tous les objets tels qu'un de leurs attributs LDAP commence par la chaîne 'ber'. La recherche ne tient pas compte de la casse.

La correspondance entre les champs disponibles dans Outlook et IceWarp est la suivante :

Outlook	**IceWarp**	**Annuaire LDAP d'IceWarp**
Nom complet	Full name	cn
Prénom	Premier mot de Full name (ou vide si un seul mot dans Full name)	givenname
Nom	Les mots suivants de Full name (ou premier mot si un seul mot)	sn
Adresse	email et alias	mail

Annexe A

Configuration du fichier **slapd.conf** situé dans "<répertoire d'installation de IceWarp>\config\ldap\etc\" qui est le fichier de configuration général du serveur LDAP.

Cette annexe contient seulement le minimum pour faire tourner un serveur LDAP.

Voici les lignes actives du fichier (les lignes commençant par # sont des commentaires) :

```
# Schemas used for database.
ucdata-path     ./ucdata
include         ./schema/core.schema
include         ./schema/cosine.schema
include         ./schema/inetorgperson.schema
include         ./iwlog.conf

pidfile         ./run/slapd.pid
argsfile        ./run/slapd.args

# BDB database definitions
database        bdb
suffix          "dc=darnis,dc=com"
rootdn          "cn=manager,dc=darnis,dc=com"
rootpw          admin

 # ACL
access to *
        by self  write
        by users         read
        by anonymous  auth
        by *             none
directory       ./data

# Indices to maintain
index   default        pres,eq
index    objectClass      eq
index   uniqueMember    eq
```

Explications détaillées :

include

Ces lignes permettent d'inclure la définition des schémas LDAP. Tous les fichiers de définition des schémas LDAP sont dans le répertoire <répertoire d'installation de IceWarp>\ldap\Schema. Vous pouvez créer votre propre fichier de définition ou modifier les fichiers existants. La syntaxe de ces fichiers doit être scrupuleusement respectée, sinon le service ne démarre pas. Si vous n'êtes pas familier des schémas LDAP et de la syntaxe OpenLdap, contentez-vous d'utiliser les fichiers existants.

Iwlog.conf est un fichier qui indique où se trouve le fichier log, il contient une ligne comme :

```
logfile   "F:/Messagerie/logs/slapd.log"
```

Le fichier log est réinitialisé à chaque redémarrage du service LDAP (donc de Control/web).

Database

IceWarp utilise Ldbm ou bdb comme base de données pour stocker les données.

Suffix

Cette ligne identifie le nœud principal de l'arbre sous lequel les données vont être stockées. Toutes les connexions client devront utiliser ce suffixe pour se connecter. Si vous voulez changer de suffixe, la base complète doit être recréée sous ce nouveau suffixe. D'habitude, le suffixe correspond au nom de domaine.

Rootdn

Cette ligne identifie l'utilisateur administrateur de l'annuaire LDAP. Il n'a pas besoin de figurer dans l'annuaire, mais permet de faire toutes les actions comme : ajouter, modifier, supprimer des enregistrements. Il doit toujours contenir le suffixe à la fin de son nom.

Rootpw

Cette ligne contient le mot de passe pour l'administrateur déclaré dans rootdn. Il est conseillé de modifier le mot de passe par défaut.

Directory

Indique le répertoire où sont stockées les données. C'est le chemin relatif par rapport à <répertoire d'installation de IceWarp>\ldap

Index

Ces lignes permettent de spécifier les attributs qui doivent être indexés. Par défaut, aucun attribut n'est indexé, il est recommandé de spécifier au moins un index d'égalité sur l'attribut 'objectclass'.

Annexe B

Configuration du fichier **Bypass** dans le cas du serveur LDAP (bouton "C" de la console dans Domaines & Comptes -> Paramètres Globaux -> onglet Avancé). Les lignes commençant par // sont des commentaires. Par exemple :

```
icewarp.com
bill@microsoft.com
192.168.*.*
{c:\Data\Bypass\allbypass.dat}
```

Le **fichier Bypass** contient des adresses mail, des domaines et des adresses IP (une par ligne). Il est possible d'utiliser des masques. Ces adresses vont servir de critères de traitement pour la synchronisation.

"{" ...nom de fichier..."}" spécifie un fichier qui contient des adresses IP, des noms de domaines... pour le bypass.