



Authentification LDAP client Ubuntu

>>> Ubuntu 16.04.2

Description :

Le but de cet article est de configurer un client Ubuntu afin d'utiliser OpenLDAP pour authentifier les utilisateurs.

Authentification LDAP client Ubuntu

>>> Ubuntu 16.04.2

Sommaire :

- I) Introduction
- II) Installation
- III) Configuration
- IV) Test de connexion

I) Introduction

Dans l'article 326, j'ai expliqué comment configurer le serveur OpenLDAP et comment peupler la base.

Je vais maintenant expliquer comment configurer un client Ubuntu pour utiliser la base d'utilisateurs LDAP.

Voici la configuration de mon LAB utilisé pour l'article :

- Serveur LDAP :
 - Machine virtuelle : Debian 8.7.1
 - Hostname : deb-idum-lab2
 - Adresse IP : 10.10.10.11/24
- Client Ubuntu :
 - Machine virtuelle : Ubuntu 16.04.2
 - Hostname : ubu-idum-lab2
 - Adresse IP : 10.10.10.12/24

II) Installation

- Commencez par l'installation des paquets "**libnss-ldap**", "**libpam-ldap**" et "**nscd**".

```
aptitude install libpam-ldap ldap-utils
```

- Remplacez "**ldapi** ://" par "**ldap** ://**ldap.idum.eu**" :

Configuration de ldap-auth-config

Please enter the URI of the LDAP server to use. This is a string in the form of ldap://<hostname or IP>:<port>/. ldaps:// or ldapi:// can also be used. The port number is optional.

Note: It is usually a good idea to use an IP address because it reduces risks of failure in the event name service problems.

LDAP server Uniform Resource Identifier:

ldap://ldap.idum.eu

<Ok>

- Définissez votre domaine :

Configuration de ldap-auth-config

Please enter the distinguished name of the LDAP search base. Many sites use the components of their domain names for this purpose. For example, the domain "example.net" would use "dc=example,dc=net" as the distinguished name of the search base.

Distinguished name of the search base:

dc=idum,dc=eu

<Ok>

- Sélectionnez la version 3 de LDAP :

Configuration de ldap-auth-config

Please enter which version of the LDAP protocol should be used by ldapns. It is usually a good idea to set this to the highest available version.

LDAP version to use:

3
2

<Ok>

- Répondez "Oui"

This option will allow you to make password utilities that use pam to behave like you would be changing local passwords.

The password will be stored in a separate file which will be made readable to root only.

If you are using NFS mounted /etc or any other custom setup, you should disable this.

Make local root Database admin:

<Oui>

<Non>

- Répondez "**Non**"



- Saisissez le nom de l'administrateur OpenLDAP. Dans l'article sur la configuration du serveur OpenLDAP nous avons créé un utilisateur "**manager**".



- Saisissez le mot de passe de l'administrateur OpenLDAP.



Les paquets sont installés.

Si vous avez fait une erreur pendant la saisie, vous pouvez reconfigurer le paquet :

```
dpkg-reconfigure ldap-auth-config
```

Les résultats de la boîte de dialogue peuvent être vus dans /etc/ldap.conf. Si votre serveur requiert des options qui ne sont pas dans le menu, éditez ce fichier en conséquence.

III) Configuration

- Activer "**auth-client-config**" dans le profil LDAP.

- **-t** : Ne modifie que le fichier /etc/nsswitch.conf.
- **-p** : Le nom du profil à activer, désactiver, etc.
- **lac_ldap** : Le profil auth-client-config qui fait partie du paquet ldap-auth-config.

```
auth-client-config -t nss -p lac_ldap
```

- Ensuite, l'utilitaire **pam-auth-update**, configure le système pour utiliser LDAP pour l'authentification :

- Dans le menu pam-auth-update, choisissez LDAP et les autres mécanismes d'authentification dont vous avez besoin.

```
pam-auth-update
```

- Vous devez obtenir ceci :



- Pour finir, éditez le fichier "**common-session**" :

```
vim /etc/pam.d/common-session
```

- Ajoutez la ligne ci-dessous afin de créer automatiquement les répertoires personnels des utilisateurs.

```
session required pam_mkhome.so skel=/etc/skel umask=0022
```

IV) Test de connexion

Vous devriez maintenant être capable de vous connecter en utilisant les identifiants d'utilisateurs stockés dans le répertoire LDAP. Ainsi qu'avec les identifiants d'utilisateurs stockés en local sur le client.

19 juin 2017 -- N.Salmon -- article_327.pdf



Idum