PSTB – UPEC

TP SSO

Mise en place d'un service d'annuaire OpenLDAP

COTTENCEAU Donatien – VALENCELLE Luka
07/01/2026

Table des matières

Installation et mise en place du Serveur

Pour cette machine virtuelle, nous avons choisi la Machine Virtuelle Turnkey Linux afin d’obtenir directement le service OpenLDAP.

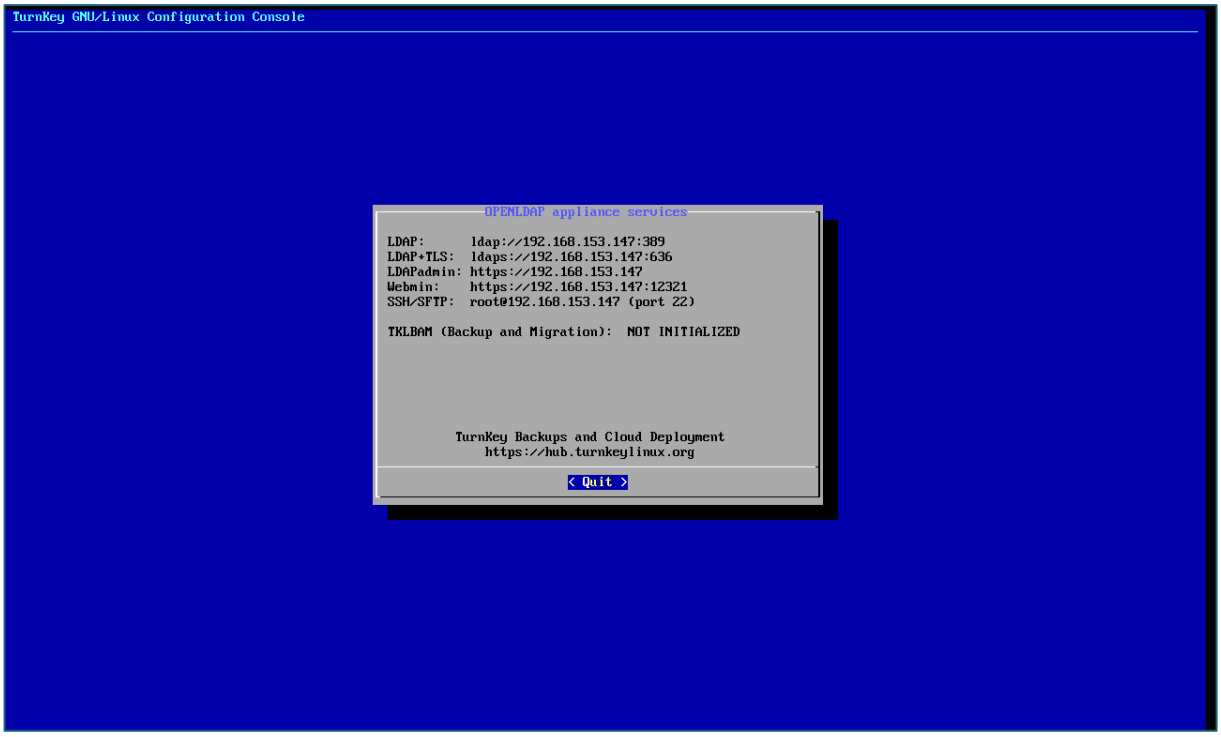

Figure 1 : Configuration réseau de la VM OpenLDAP

Nous voyons donc ci-dessus que notre VM a une adresse IP fixe (comme tout bon serveur qui se respecte xD) La carte réseau est configurée en NAT.

Accès à la page WEB

Une fois cette configuration réalisée, nous nous rendons sur notre machine hôte (Windows hébergeant la VM OpenLDAP via VmWare) et nous accédons à la page WEB d'OpenLDAP.

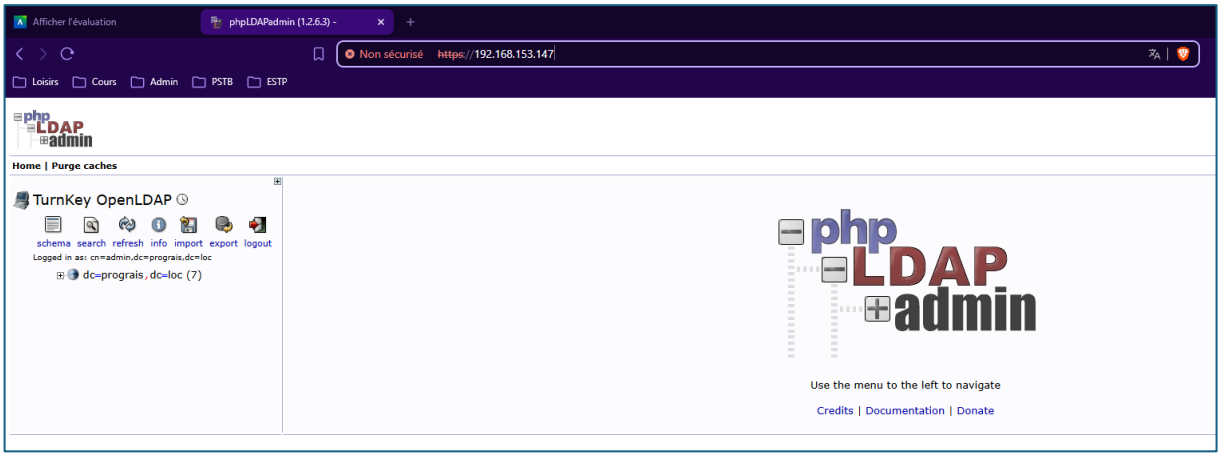

Figure 2 : Page WEB OpenLDAP via adresse IP

Nous accédons correctement à la page WEB depuis la machine hôte via l'IP vue précédemment dans notre configuration réseau.

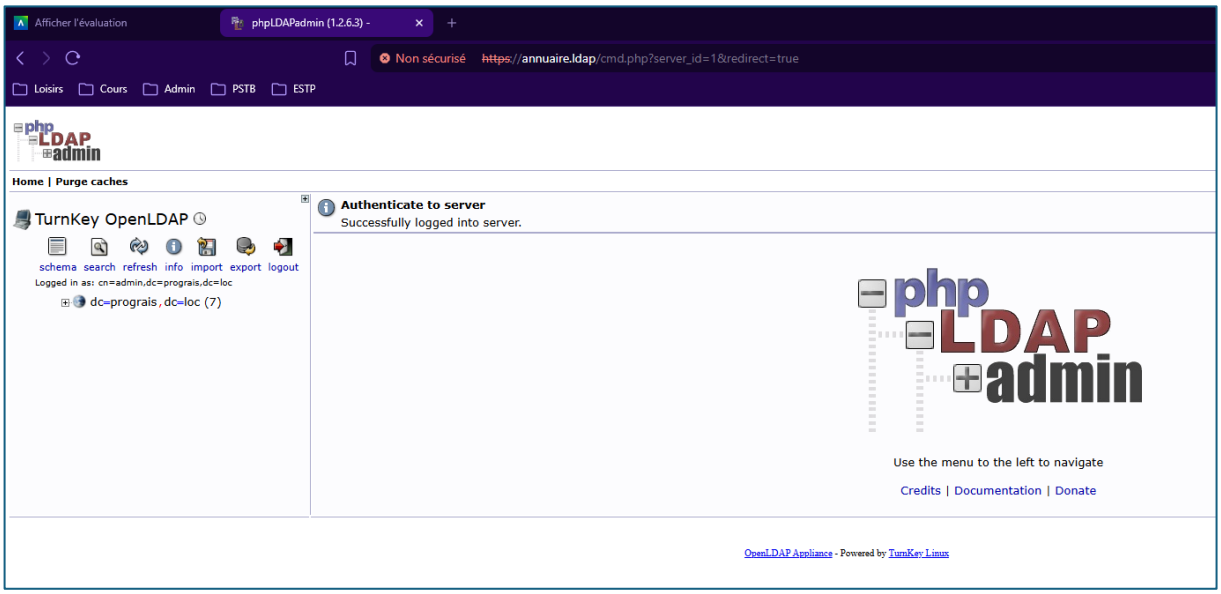

Figure 3 : Page WEB OpenLDAP via FQDN

Il est également possible d'accèder à cette même page via le FQDN ce qui rend l'expérience utilisateur plus agréable. Manipulation réalisée dans le fichier hosts de l'ordinateur hôte afin de simuler un « localhost » bien qu'il vienne d'une VM.

Premiers pas sur php LDAP admin

Création d'une OU

Une fois authentifiés, nous pouvons commencer à travailler comme nous le ferions sur son jumeau Windowsien, l'Active Directory !

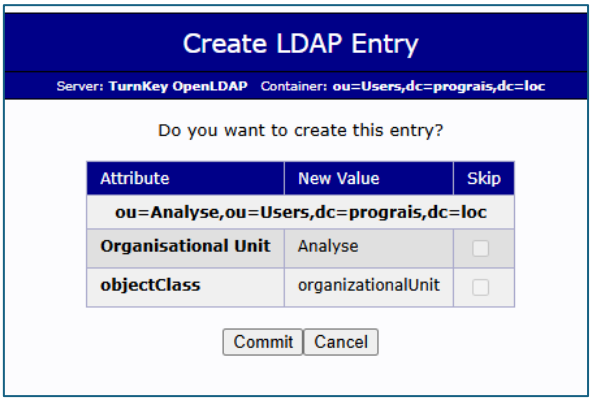

Figure 4 : Création d'une OU

Ici, nous venons de créer une Unité d'Organisation afin d'y intégrer nos futurs employés. Il s'agit ici de l'OU « Analyse », l'un des départements/services de l'entreprise.

Création d'un Utilisateur

Une OU sans User n'étant rien, nous créons donc des utilisateurs.

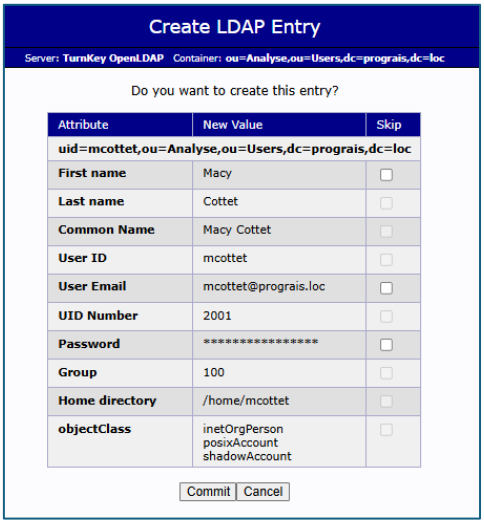

Figure 5 : Création d'un User

Nous avons créé un utilisateur appartenant à l'OU créée précédemment.

Création d'un Compte Admin

Dans une organisation, les utilisateurs n'ont pas tous les mêmes droits et les mêmes accès. C'est pourquoi nous avons ici créé un autre type de compte, un compte « admin » appartenant à un autre groupe.

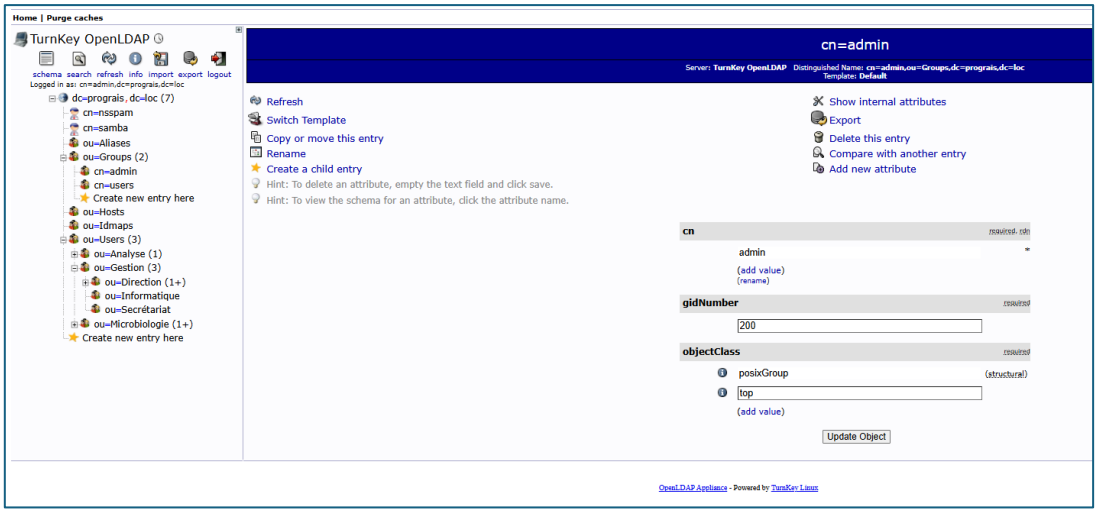

Figure 6 : Création d'un type de compte : Admin

Ce type de compte « admin » aura donc un gidNumber différent car compte « privilégié » (100 = user et 200 = admin)

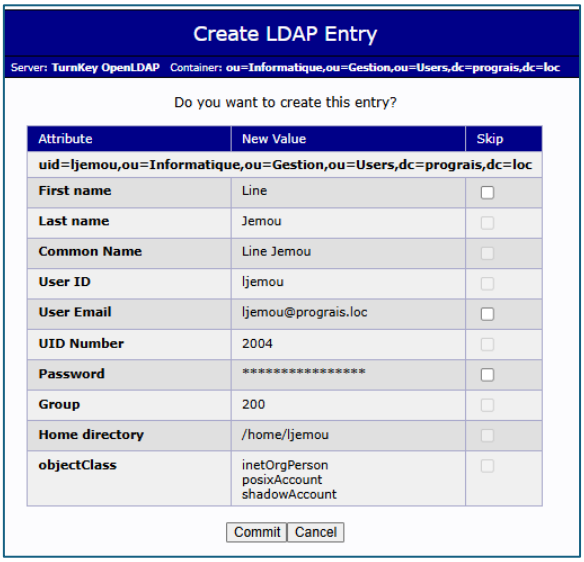

Figure 7 : Création d'un User « admin »

Ci-dessus une application de ce dont nous venons de traiter.

Serveur WEB

Première page WEB

Afin de tester notre annuaire LDAP, nous allons chercher à protéger certaines pages de notre Serveur WEB.

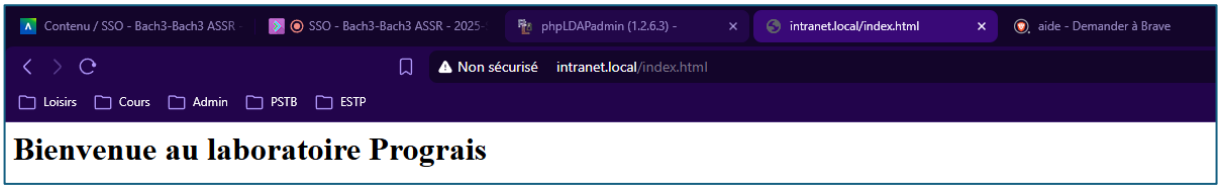

Figure 8 : Page d'accueil Serveur WEB

Voici donc la page d'accueil de notre site accessible par les utilisateurs du même réseau. Nous allons à présent chercher à inclure notre Annuaire LDAP dedans afin de bloquer les pages que nous souhaitons protéger.

Changement de la configuration du site

Plusieurs paramètres sont intéressants à ajouter dans notre fichier de configuration du site.

```
root@vls24lampcott:/etc/apache2/sites-enabled# cat 000-default.conf
<VirtualHost *:80>
    ServerName prograis.loc
    DocumentRoot /var/www/html

    <Directory "/var/www/html/mylab">
        # Type d'authentification
        AuthType Basic
        # Nom du domaine protégé affiché à l'utilisateur
        AuthName "Ressource Protégée"
        # Utilisation du fournisseur d'authentification LDAP
        AuthBasicProvider ldap

        # URL de recherche LDAP
        AuthLDAPURL "ldap://annuaire.ldap:389/dc=prograis,dc=loc?uid?sub?(objectClass=*)"

        AuthLDAPBindDN "cn=admin,dc=prograis,dc=loc"
        AuthLDAPBindPassword "P0se1don"

        # Accès autorisé à tout utilisateur valide dans l'annuaire
        Require valid-user
    </Directory>
</VirtualHost>
```

Figure 9 : Fichier 000-default.conf

Le fichier 000-default.conf est donc modifié, nous y ajoutons l'URL de recherche de notre LDAP ainsi qu'un compte ayant accès à l'annuaire LDAP afin d'assurer la liaison. Nous sommes d'accord que cela n'est pas sécurisé mais après tout, nous sommes en HTTP…

Page WEB protégée

Il nous faut à présent créer la page WEB qui sera protégée par une authentification LDAP.

```
root@vls24lampcott:/var/www/html/mylab# cat index.html
<h1>Zone protegee du laboratoire Prograis</h1>
root@vls24lampcott:/var/www/html/mylab#
```

Figure 10 : Contenu page WEB protégée

Le contenu de cette dernière est très sommaire mais nous avons simplement besoin de savoir si cela fonctionne ou pas.

Test de la protection de page WEB

Ultime test, nous essayons d'accéder à la page WEB protégée ultérieurement.

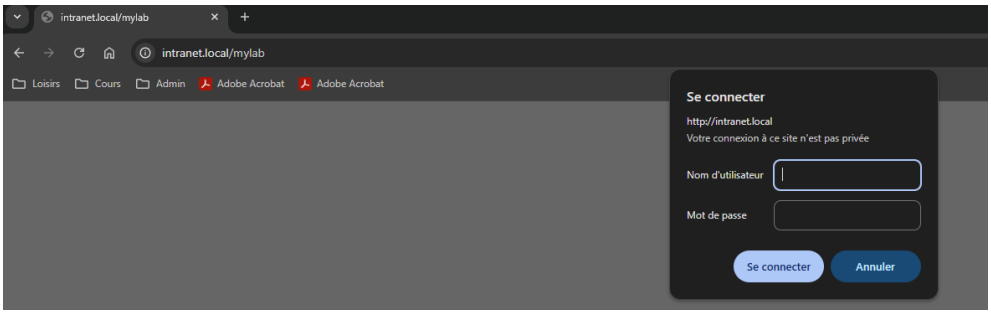

Figure 11 : Pop-up authentication page WEB

Une pop-up nous demandant de rentrer notre login & mot de passe d'un utilisateur de notre annuaire LDAP apparaît. Nous rentrons donc nos informations.

Résultat

Une fois ces informations rentrées, le pop-up disparaît et laisse apparaître la page WEB protégée.

Figure 12 : Page WEB protégée

Bonne nouvelle, notre page WEB apparaît. Nous avons réussi.

Conclusion :

Cette activité s’inscrit dans la continuité de notre session avec Monsieur Pôl-Quentin plus tôt dans l’année pour la partie Serveur WEB. L’utilisation d’un annuaire LDAP nous donne l’opportunité de nous familiariser avec cette technologie. Aucun problème rencontré au cours de ce TP.