

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	2
Accès à la page WEB	3
Premiers pas sur php LDAP admin	4
Création d'une OU	4
Création d'un Utilisateur.....	4
Création d'un Compte Admin.....	5
Serveur WEB	6
Première page WEB.....	6
Changement de la configuration du site.....	6
Page WEB protégée	7
Test de la protection de page WEB.....	7
Résultat	7

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.

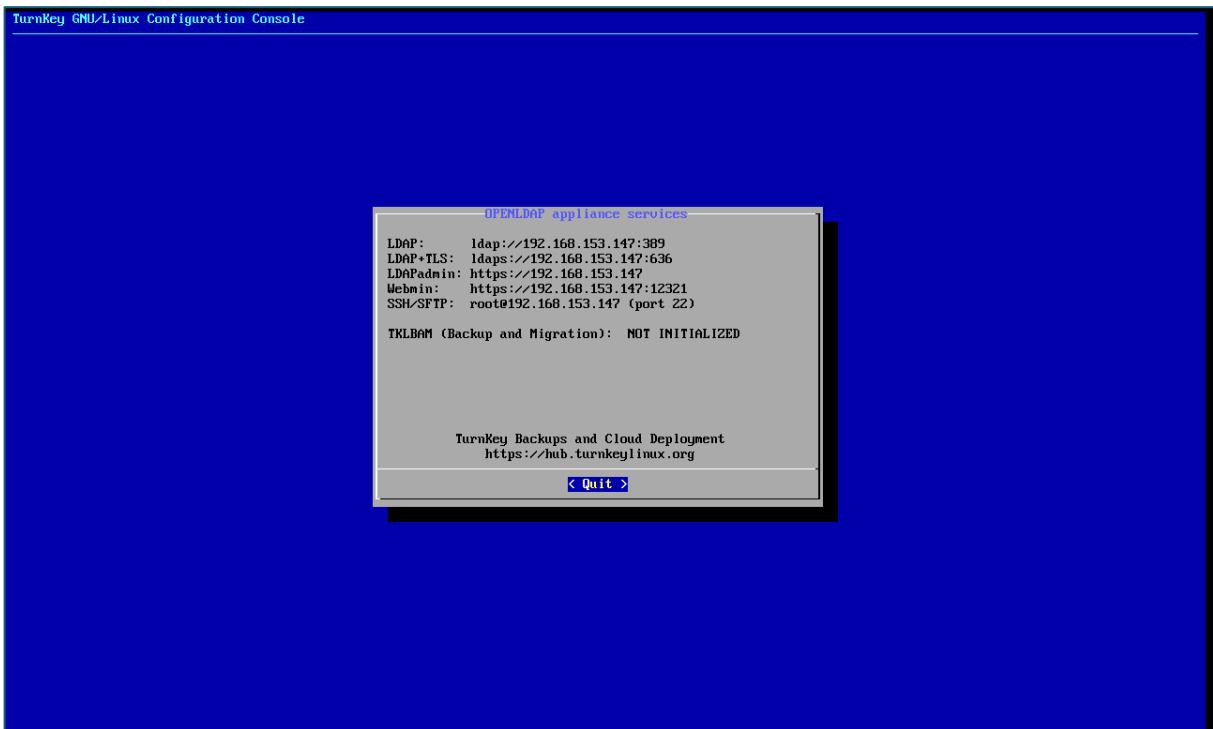


Figure 1 : Configuration réseau de la VM OpenLDAP

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.

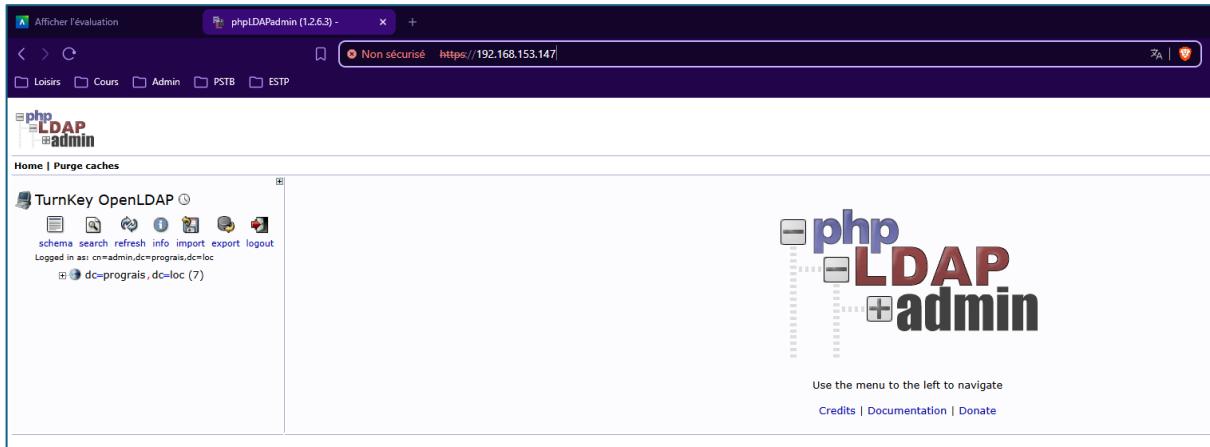


Figure 2 : Page WEB OpenLDAP via adresse IP

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

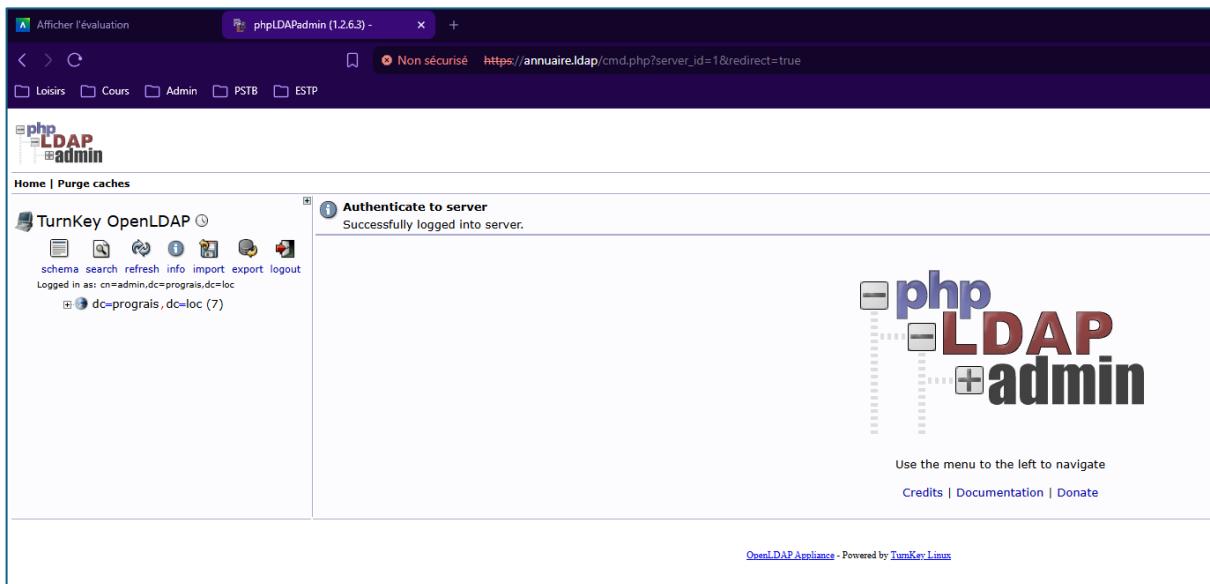


Figure 3 : Page WEB OpenLDAP via FQDN

Il est également possible d'accéder 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 !

The screenshot shows a 'Create LDAP Entry' dialog box. At the top, it says 'Server: TurnKey OpenLDAP Container: ou=Users,dc=prograis,dc=loc'. Below that, a question 'Do you want to create this entry?' is asked. A table lists attributes and their values:

Attribute	New Value	Skip
ou	Analyse,ou=Users,dc=prograis,dc=loc	<input type="checkbox"/>
Organisational Unit	Analyse	<input type="checkbox"/>
objectClass	organizationalUnit	<input type="checkbox"/>

At the bottom are 'Commit' and 'Cancel' buttons.

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.

The screenshot shows a 'Create LDAP Entry' dialog box. At the top, it says 'Server: TurnKey OpenLDAP Container: ou=Analyse,ou=Users,dc=prograis,dc=loc'. Below that, a question 'Do you want to create this entry?' is asked. A table lists attributes and their values:

Attribute	New Value	Skip
uid	mcottet,ou=Analyse,ou=Users,dc=prograis,dc=loc	<input type="checkbox"/>
First name	Macy	<input type="checkbox"/>
Last name	Cottet	<input type="checkbox"/>
Common Name	Macy Cottet	<input type="checkbox"/>
User ID	mcottet	<input type="checkbox"/>
User Email	mcottet@prograis.loc	<input type="checkbox"/>
UID Number	2001	<input type="checkbox"/>
Password	*****	<input type="checkbox"/>
Group	100	<input type="checkbox"/>
Home directory	/home/mcottet	<input type="checkbox"/>
objectClass	inetOrgPerson posixAccount shadowAccount	<input type="checkbox"/>

At the bottom are 'Commit' and 'Cancel' buttons.

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.

The screenshot shows the TurnKey OpenLDAP web interface. On the left, there's a sidebar with various icons and a tree view of the LDAP schema. The main area is titled 'cn=admin'. It shows a form for creating a child entry. The 'objectClass' dropdown is set to 'inetOrgPerson' and 'posixAccount'. The 'gidNumber' field is set to '200'. There are also fields for 'cn' (set to 'admin') and 'uidNumber' (set to '100'). A note says '200' is the value for an administrator. At the bottom right, there's a 'Create' button.

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

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

Attribut	Nouvelle valeur	Sauter
uid=ljemou,ou=Informatique,ou=Gestion,ou=Users,dc=prograis,dc=loc		
First name	Line	<input type="checkbox"/>
Last name	Jemou	<input type="checkbox"/>
Common Name	Line Jemou	<input type="checkbox"/>
User ID	ljemou	<input type="checkbox"/>
User Email	ljemou@prograis.loc	<input type="checkbox"/>
UID Number	2004	<input type="checkbox"/>
Password	*****	<input type="checkbox"/>
Group	200	<input type="checkbox"/>
Home directory	/home/ljemou	<input type="checkbox"/>
objectClass	inetOrgPerson posixAccount shadowAccount	<input type="checkbox"/>

Figure 7 : Crédit 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.

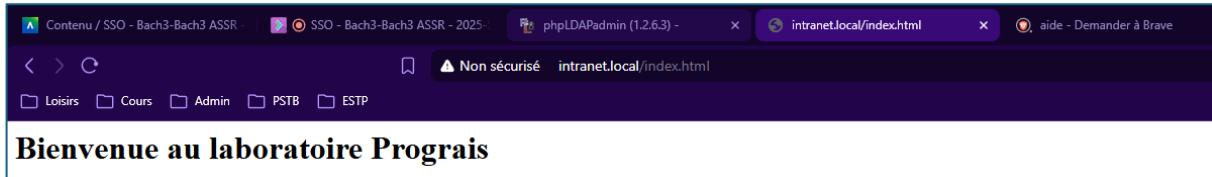


Figure 8 : Page d'accueil Serveur WEB

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 "P0seldorf"

        # 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.

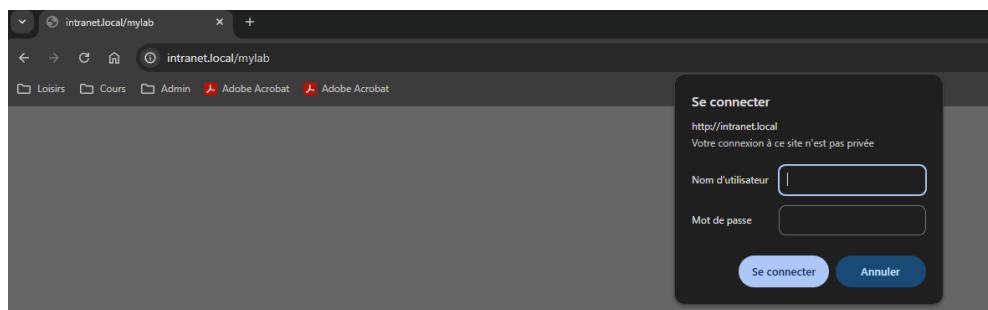
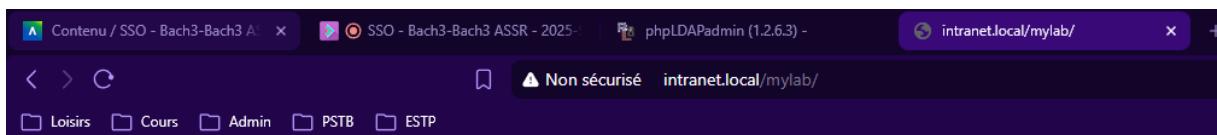


Figure 11 : Pop-up authentication page WEB

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.



Zone protegee du laboratoire Prograis

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.