LABO SERVICES

DECOUVERTE DU SERVICE LDAP

INTRODUCTION

Nous allons utiliser une appliance ISO TurnkeyLinux OpenLDAP :

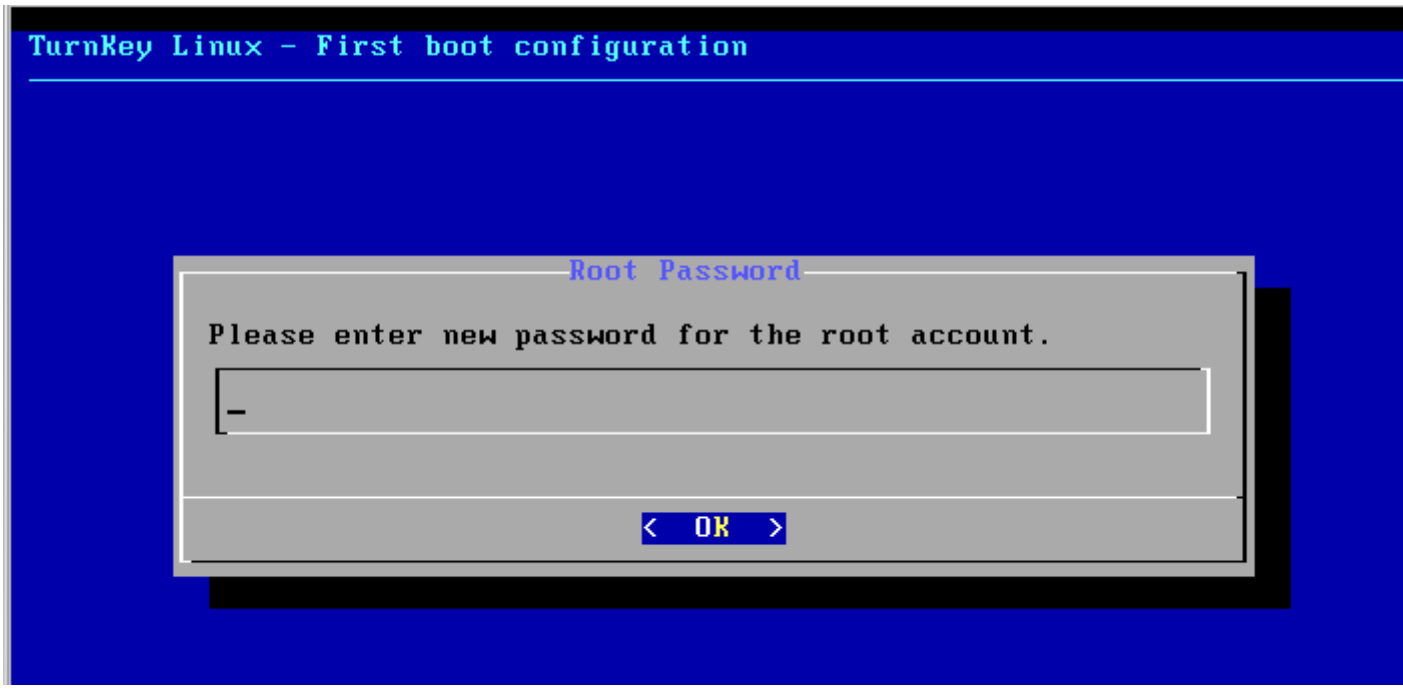
A récupérer dans la dropbox

PREMIER LANCEMENT DE LA VM TURNKEY OPENLDAP

LORS DE L'INSTALLATION :

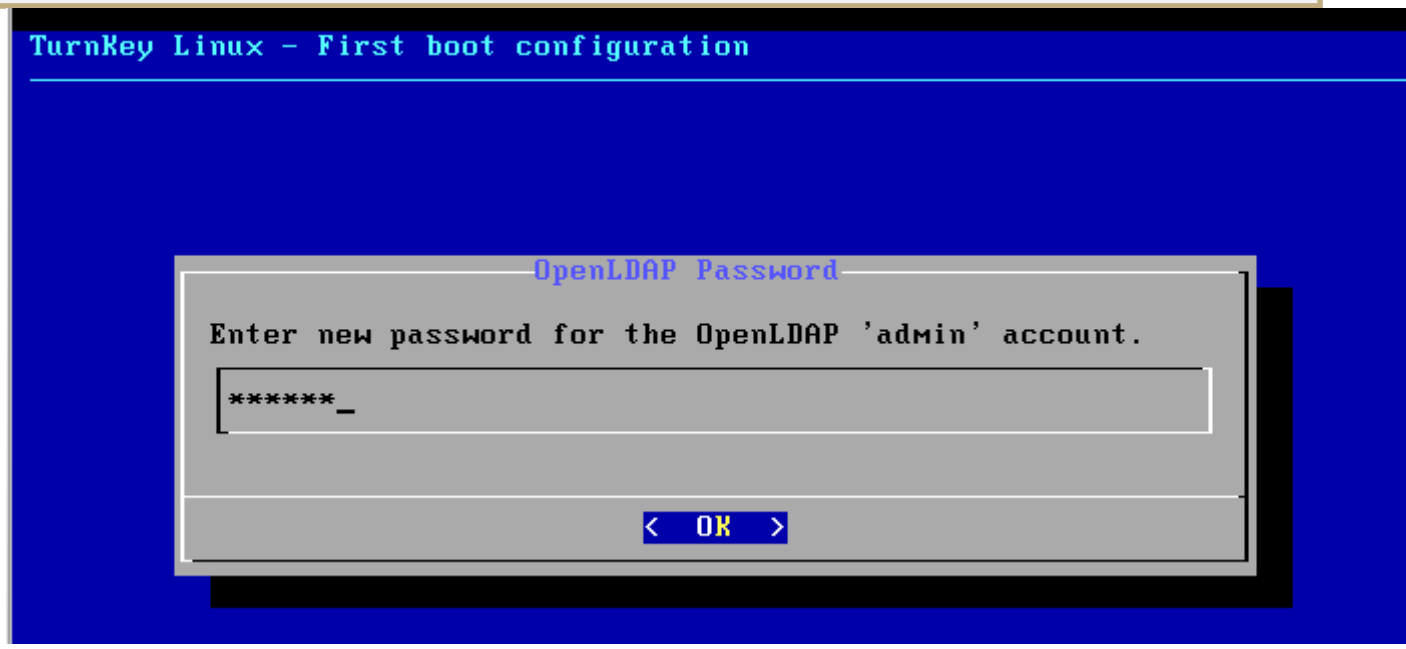
Renseigner le mot de passe du compte « root »

```
password = eleve1234
```



Renseigner le mot de passe du compte « admin OpenLdap »

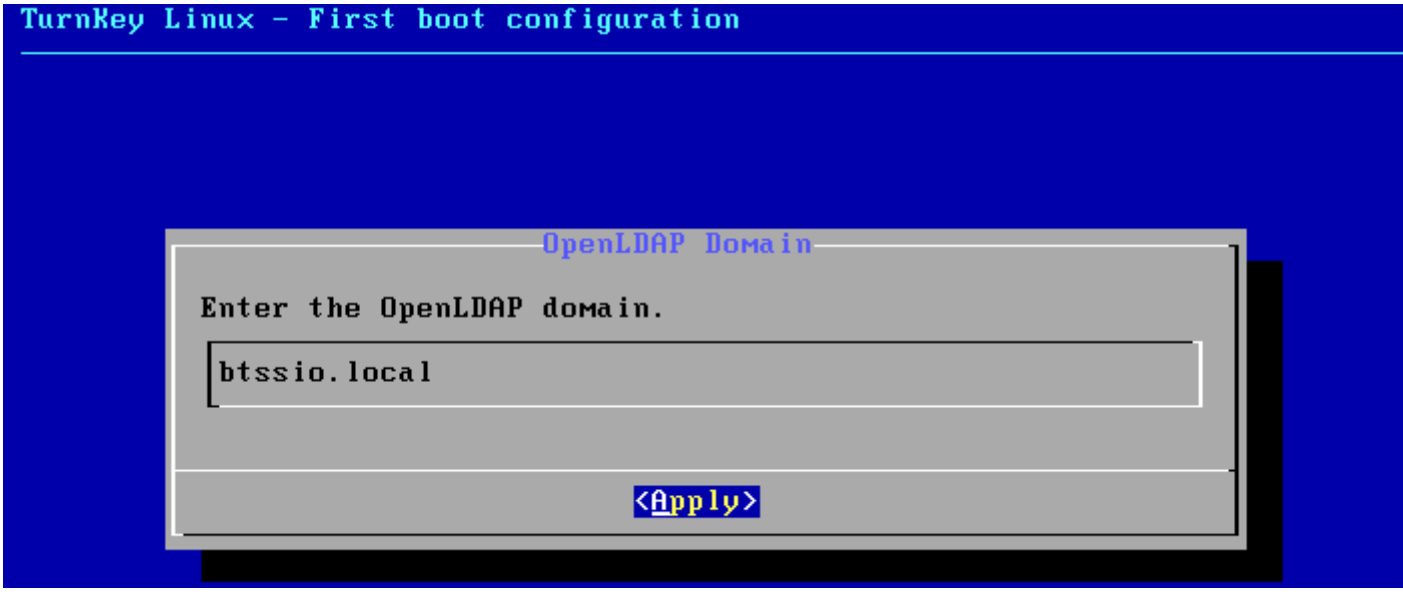
```
password = eleve1234
```



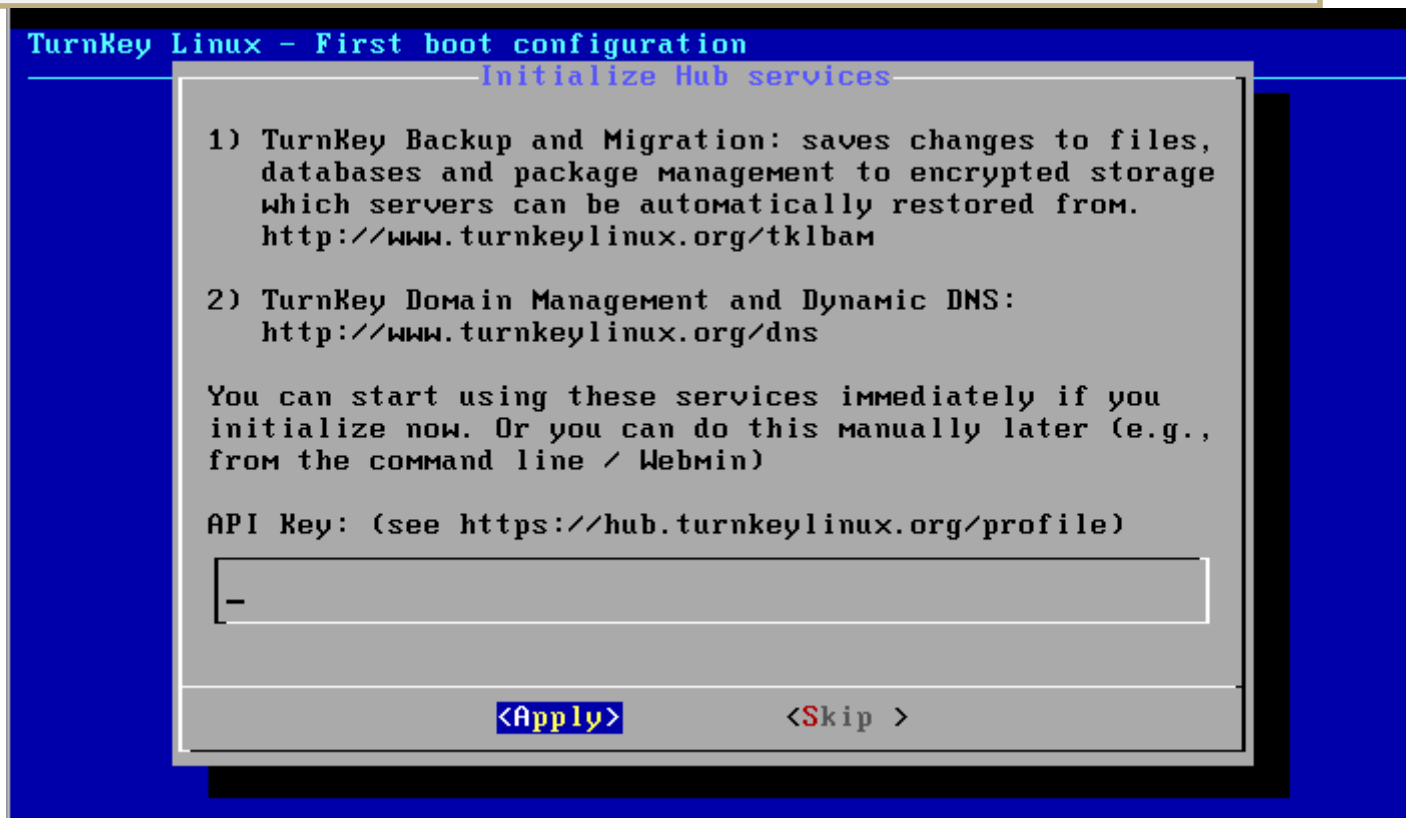
Renseigner le « domaine OpenLdap »

```
domaine OpenLdap = btssio.local
```

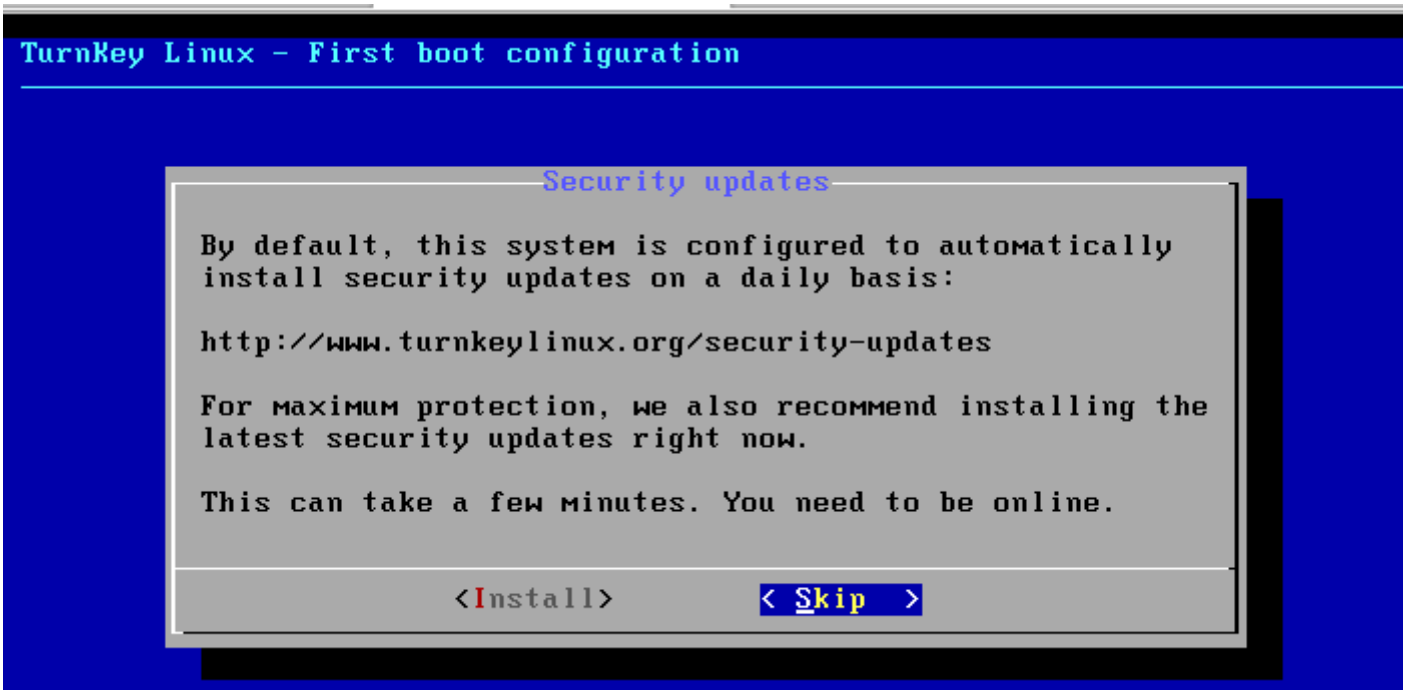
Attention, vous travaillez en QWERTY !!



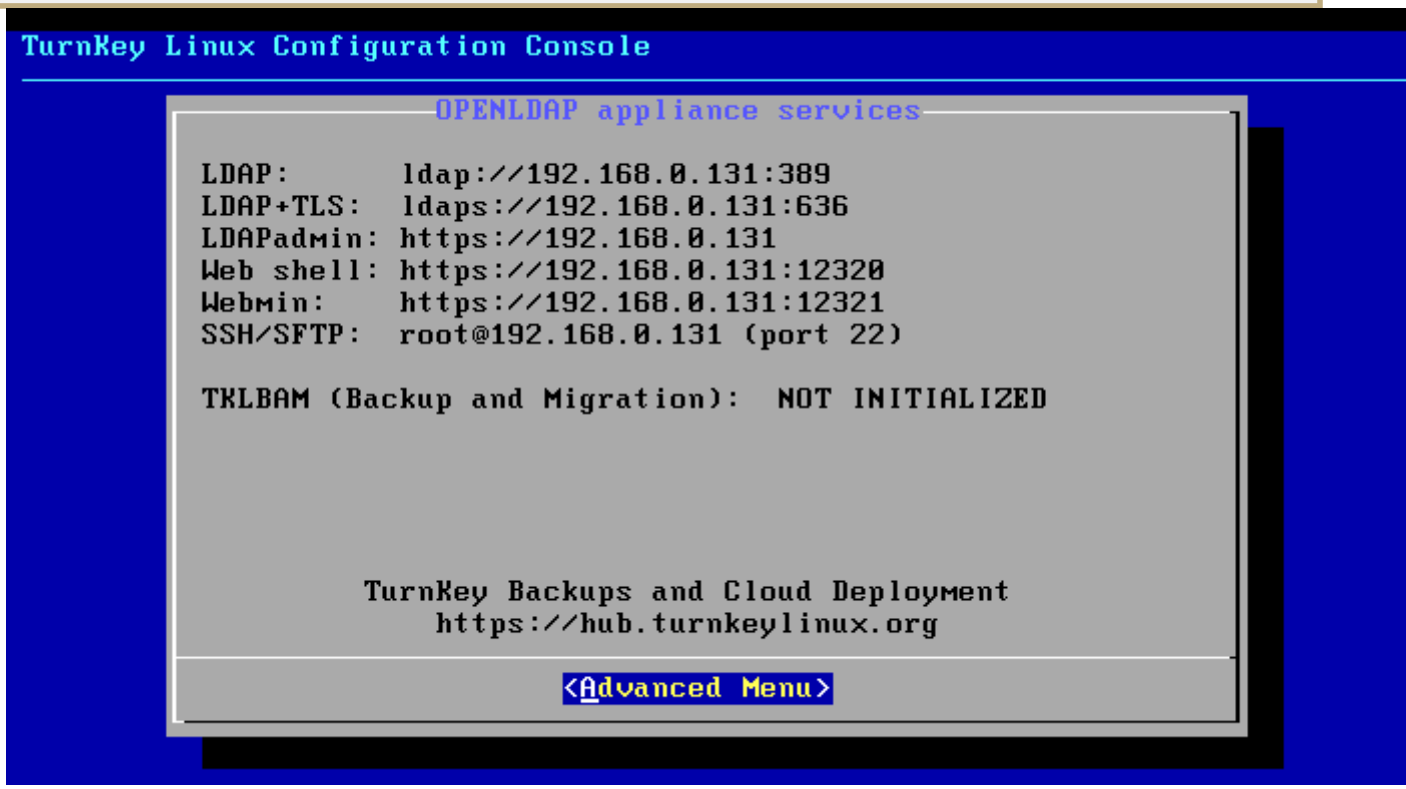
Vous pouvez sauter l'étape infra :



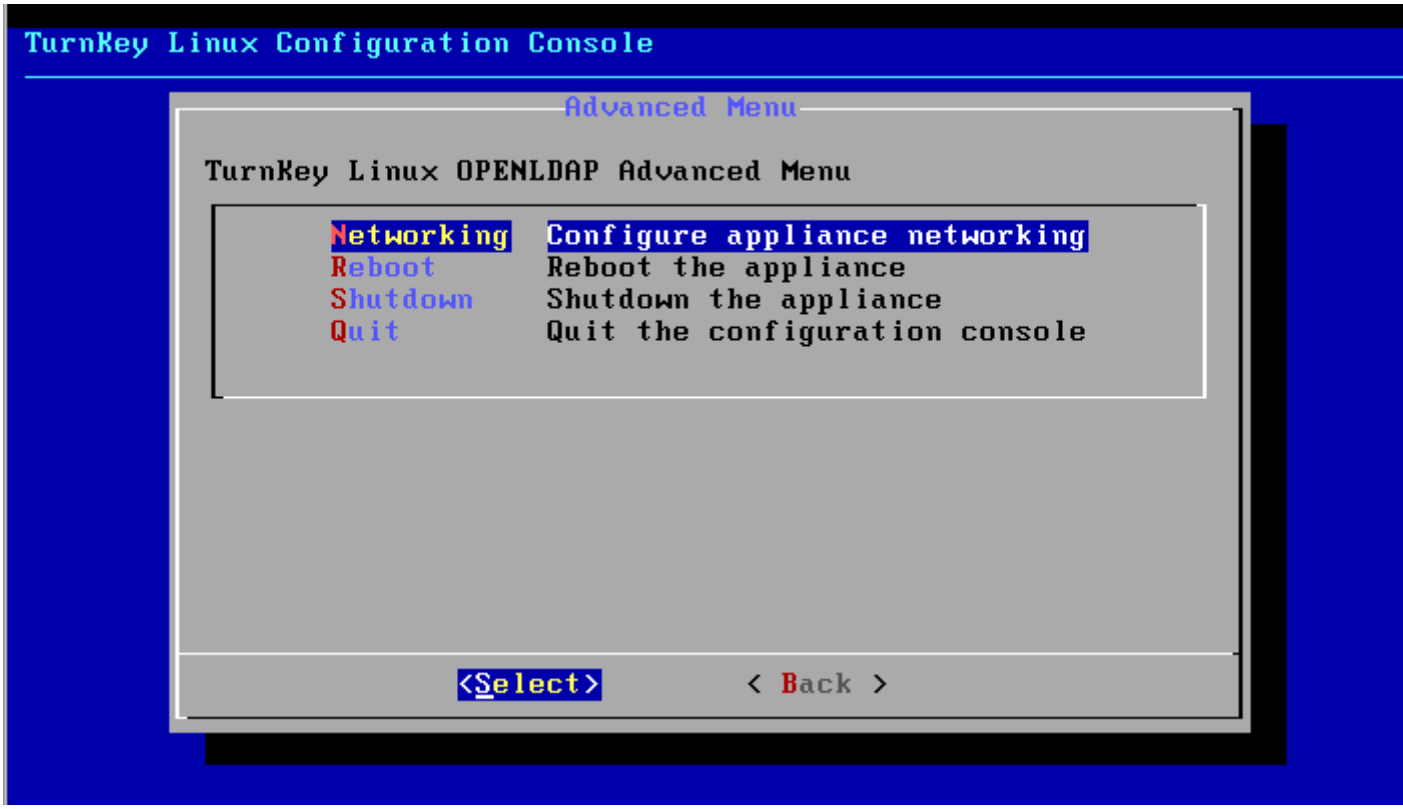
Vous pouvez sauter l'étape infra :



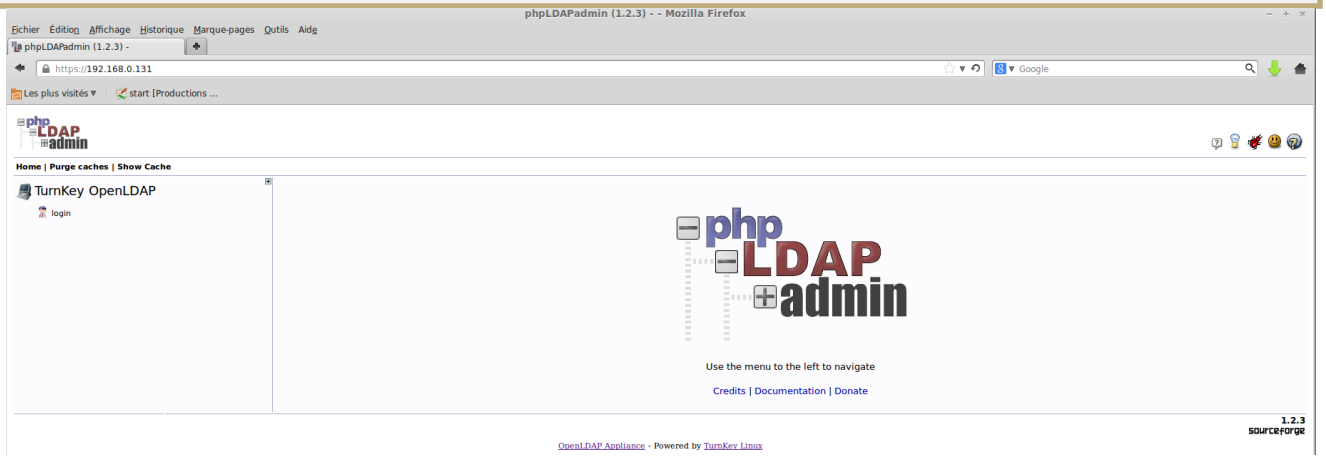
Après installation vous devez obtenir quelque chose comme ça :



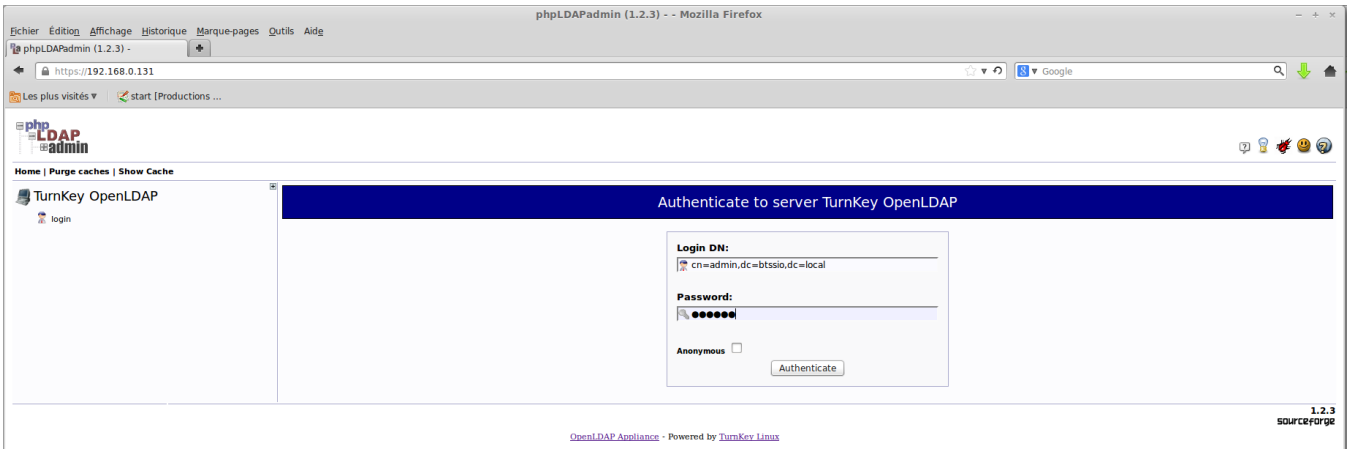
Le « menu avancé » peut être utile…



Vous pouvez maintenant accéder au serveur OpenLDAP à partir de n'importe quel navigateur d'une machine cliente :

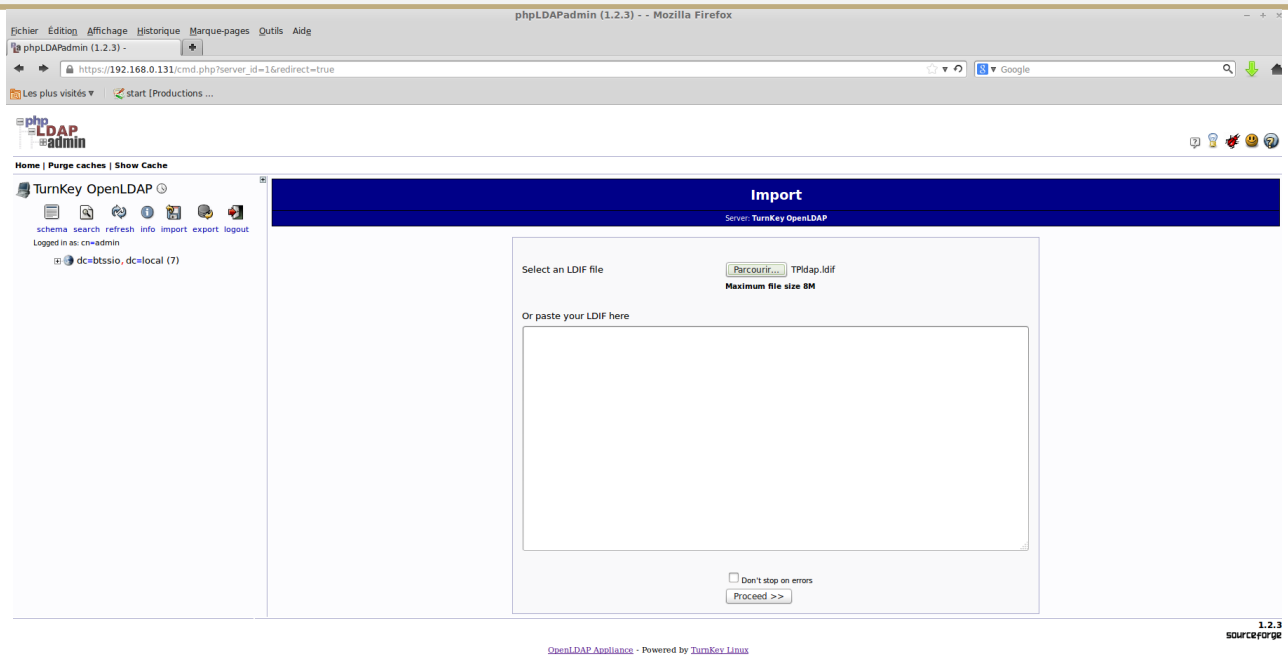


Vous pouvez vous authentifier auprès du serveur OpenLDAP :



Télécharger depuis la dropbox le fichier tpladap.ldif :

Importer le fichier tpldap.ldif sur le serveur OpenLDAP :



Vous pouvez maintenant accéder à distance au serveur OpenLDAP par connexion ssh ou encore en initialisant une connexion https.

RECHERCHE D'INFORMATIONS AVEC LA COMMANDE LDAPSEARCH

La commande ldapsearch permet d'effectuer des requêtes sur un annuaire LDAP et de récupérer le résultat au format LDIF.

Le cas le plus simple consiste à demander localement (directement sur le serveur) l'export total de toutes les informations d'un annuaire et on utilise souvent cette possibilité pour vérifier la présence d'un objet ou simplement que l'annuaire répond bien aux requêtes.

Syntaxe de la commande ldapsearch pour exporter toutes les informations publiques d'un annuaire :

```
ldapsearch -x -b contexte
```

Export avec ldapsearch : options et paramètres	
-x	Utilise une authentification simple (cas général).
-b contexte	Réalise la recherche à partir du DN du conteneur contexte.

Syntaxe de la commande ldapsearch pour récupérer des informations précises selon critères de recherche :

```
ldapsearch -x -D dn_admin -W -h ip_serveur -b contexte -s sub attribut=valeur
```

Recherche avec ldapsearch : options et paramètres	
-D dn_admin	Fait l'authentification avec le nom distinctif dn_admin.
-W	Demande interactivement le mot de passe. Peut être remplacé par -w (minuscule) suivi du mot de passe en clair dans la ligne de commande.
-h ip_serveur	S'adresse au serveur dont l'adresse est ip_serveur.
-s sub	Réalise une recherche récursive dans tous les niveaux subordonnés au contexte de recherche.
attribut	Le nom de l'attribut qui sera le critère de recherche.
valeur	La valeur de l'attribut recherché. Le caractère « * » représente n'importe quelle valeur existante.

REMARQUE : ici, toutes les connexions aux serveurs LDAP sont effectuées avec l'option -x indiquant une authentification en texte clair. Cela constitue naturellement un risque en matière de sécurité. La connexion avec authentification SASL permettrait de remédier à cette situation. Toutefois, sa complexité de mise en œuvre et le fait que la plupart des consultations se font en mode anonyme font que l'authentification SASL est rarement utilisée.

Afficher tous les utilisateurs dont le prénom est « Regis »

```
root@openldap# ldapsearch -x -D cn=admin,dc=btssio,dc=local -w Eleve1234  -h
192.168.0.119 -b dc=btssio,dc=local -s sub givenName=Regis
```

Que renvoie la commande suivante ?

```
root@openldap# ldapsearch -x -D cn=admin,dc=btssio,dc=local -w Eleve1234 -h
192.168.0.119 -b ou=profs,dc=btssio,dc=local -s sub givenName=Regis
```

AJOUT D'OBJETS DANS L'ANNUAIRE LDAP AVEC LA COMMANDE LDAPADD

Pour l'essentiel, la commande ldapadd va lire le contenu d'un fichier au format LDIF contenant les données à modifier, et les ajouter à l'annuaire. La construction du fichier se doit d'être rigoureuse mais ne présente pas de difficulté.

Syntaxe simplifiée de la commande ldapadd :

```
ldapadd -x -D dn_admin -W -h ip_serveur -f fichier_ldif
```

Pourquoi cette commande ne renvoie aucun utilisateur de l'annuaire ? Quel paramètres faut-il modifier pour lister les utilisateurs ayant comme prénom « alain » ?

ldappadd : options et paramètres	
-x	Utilise une authentification simple (cas général).
-D dn_admin	Fait l'authentification avec le nom distinctif dn_admin.
-W	Demande interactivement le mot de passe. Peut être remplacé par -w (minuscule) suivi du mot de passe en clair dans la ligne de commande.
-h ip_serveur	S'adresse au serveur dont l'adresse est ip_serveur.
-f fichier_ldif	Ajoute les objets référencés dans le fichier fichier_ldif.

Créer le fichier LDIF suivant appelé « thierry.ldif » :

```
dn: cn=thierry,ou=profs,dc=btssio,dc=local

objectClass: person
```

```
cn: thierry

sn: lemaitre

telephoneNumber: 0555455600
```

Ajouter maintenant l'utilisateur Thierry dans l'annuaire OpenLDAP :

```
root@openldap# ldapadd -D cn=admin,dc=btssio,dc=local -W -h 192.168.0.119 -f
thierry.ldif
```

Dans quelle OU, Thierry est-il intégré ?

MODIFICATION D'OBJET EXISTANT AVEC LA COMMANDE LDAPMODIFY

La commande ldapmodify va également être utilisée avec un fichier ldif comme argument, et ses paramètres d'utilisation sont les mêmes que ceux de la commande ldapadd.

Syntaxe simplifiée de la commande ldapmodify :

```
ldapmodify -D dn_admin -W -h ip_serveur -f fichier_ldif
```

Modifier le numéro de téléphone de l'utilisateur Thierry.

Créez le fichier ldif suivant :

```
dn: cn=thierry,ou=profs,dc=btssio,dc=local

changetype: modify

replace: telephoneNumber

telephoneNumber: 0555455610
```

Lancer la commande ldapmodify avec les bons paramètres.

Vérifier en mode commande d'abord, puis avec PHP-LDAP-Admin que l'insertion s'est bien déroulée.

Lancer la commande ldapmodify avec, comme paramètre, le fichier ldif qui suit :

```
dn: cn=thierry,ou=profs,dc=btssio,dc=local

changetype: modify

delete: telephoneNumber
```

Vérifier en mode commande d'abord, puis avec PHP-LDAP-Admin que l'insertion s'est bien déroulée.

SUPPRESSION D'OBJET AVEC LA COMMANDE ldapdelete

La commande ldapdelete peut s'employer directement sans passer par un fichier ldif.

Testez la commande suivante :

```
root@openldap# ldapdelete -D cn=admin,dc=btssio,dc=local -w Eleve1234 -h
192.168.0.119 -x cn=thierry,ou=profs,dc=btssio,dc=local
```

MODIFICATION DE MOT DE PASSE AVEC LA COMMANDE LDAPPASSWD

La commande ldappasswd permet d'affecter un mot de passe encrypté à un objet utilisateur présent dans l'annuaire.

Syntaxe simplifiée de la commande ldappasswd :

```
ldappasswd -x -D dn_admin -W -h ip_serveur -s motdepasse dn_utilisateur
```

ldappasswd : options et paramètres	
-s motdepasse	Le mot de passe que l'on souhaite affecter au nouvel utilisateur. Peut être remplacé par -S (majuscule) pour une frappe interactive du nouveau mot de passe.
dn_utilisateur	Le nom distinctif de l'utilisateur dont il faut modifier le mot de passe.

Passez la commande :

```
root@openldap# ldappasswd -x -D cn=admin,dc=btssio,dc=local -w Eleve1234 -h
192.168.0.119 -s siosio cn=Jean-Bernard\ DODEMONT,ou=profs,dc=btssio,dc=local
```

A quoi sert le caractère « \ » incorporé dans le cn de l'utilisateur « Jean-Bernard DODEMONT » ?

Passez la commande :

```
root@openldap# ldapsearch -x -D cn=admin,dc=btssio,dc=local -w Eleve1234 -h
192.168.0.119 -s sub -b dc=btssio,dc=local cn=Jean-Bernard\ DODEMONT
```

A quoi sert cette commande ? Vérifiez la présence d'un mot de passe ? Sous quelle forme apparaît ce mot de passe ?