DOCUMENTATION D'INSTALLATION ET CONFIGURATION OpenLdap SUR DEBIAN 13

Version: 1.0
Date: Février 2026
Système: Debian 13 (Trixie)
Domaine: ldap.techvault.fr

PRÉREQUIS

- Système Debian 13 (Trixie) fraîchement installé
- Accès root ou utilisateur avec privilèges sudo
- Connexion Internet fonctionnelle
- Nom de domaine DNS configuré (ex: ldap.techvault.fr)
- Compte OVH avec accès API pour génération automatique de certificats Let's Encrypt

1. INSTALLATION D'OPENLDAP

1.1 Installation des paquets

Installez OpenLDAP et ses outils :

⇨ *apt install slapd ldap-utils migrationtools -y*

```
root@Auth:~# apt install slapd ldap-utils migrationtools -y
Installation de :
  ldap-utils  migrationtools  slapd

Installation de dépendances :
  libargon2-1     libldap2  libodbc2    libsasl2-2        libsasl2-modules-db
  libldap-common  libltdl7  libodbccr2  libsasl2-modules  psmisc

Paquets suggérés :
  libsasl2-modules-gssapi-mit       odbc-postgresql  libsasl2-modules-ldap  libsasl2-modules-sql
  | libsasl2-modules-gssapi-heimdal  tdsodbc          libsasl2-modules-otp

Sommaire :
  Mise à niveau de : 0. Installation de : 13Supprimé : 0. Non mis à jour : 0
Taille du téléchargement : 2 898 kB
  Espace nécessaire : 9 061 kB / 29,0 GB disponible
```

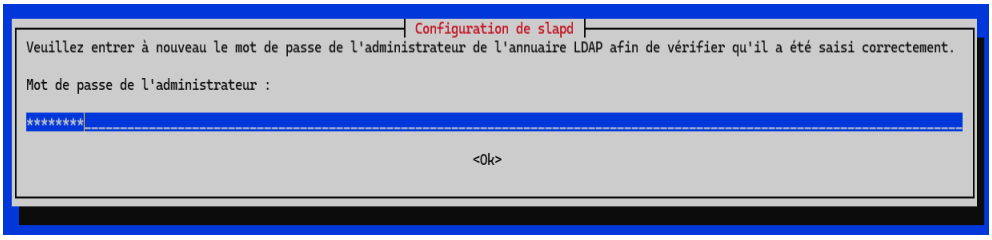
1.2 Configuration initiale de slapd

Pour configurer slapd après installation :

⇨ *dpkg-reconfigure slapd*

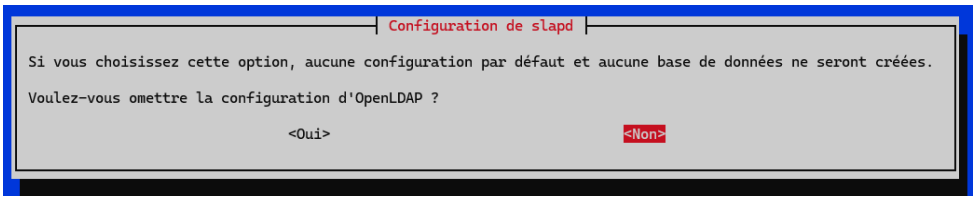
Étape 1 : Mot de passe administrateur

Saisie du mot de passe de l'administrateur LDAP



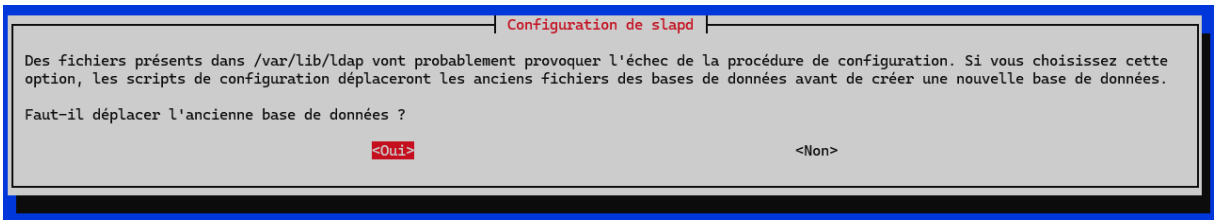
Étape 2 : Omission de la configuration par défaut

: Question "Voulez-vous omettre la configuration d'OpenLDAP ?" - Sélectionner "Non"



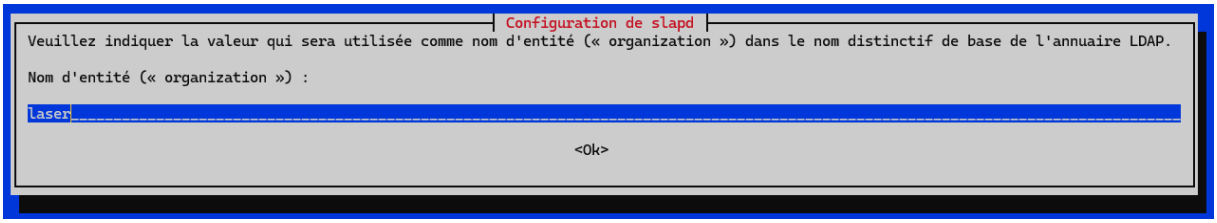
Étape 3 : Déplacement de l'ancienne base

Question sur le déplacement de l'ancienne base de données - Sélectionner "Oui"



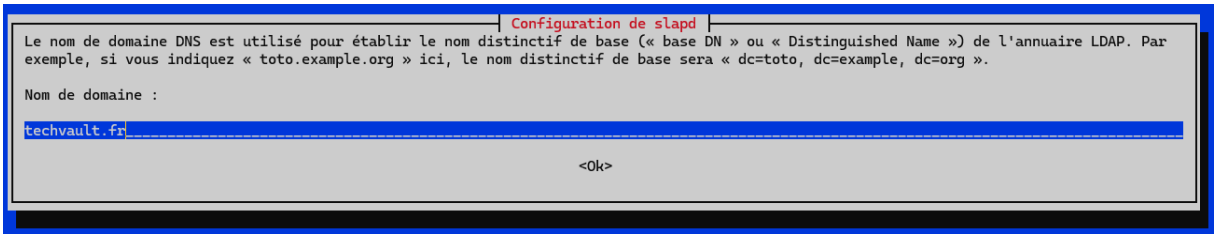
Étape 4 : Nom d'entité (organisation)

Saisie du nom d'organisation (ex: laser)



Étape 5 : Nom de domaine DNS

Saisie du nom de domaine (techvault.fr) qui deviendra dc=techvault,dc=fr



2. CRÉATION DE LA STRUCTURE DIT (DIRECTORY INFORMATION TREE)

2.1 Création du fichier base.ldif

Créez le fichier définissant la racine de l'annuaire :

⇨ *nano base.ldif*

Contenu du fichier base.ldif définissant dc=techvault,dc=fr avec OU=users et OU=groups

```
 GNU nano 8.4                                                    base.ldif *
dn: ou=users,dc=techvault,dc=fr
objectClass: organizationalUnit
ou: users

dn: ou=groups,dc=techvault,dc=fr
objectClass: organizationalUnit
ou: groups
```

Ajout des entrées à l'annuaire :

➪ *ldapadd -x -D "cn=admin,dc=techvault,dc=fr" -W -f base.ldif*

Ajout réussi des entrées OU=users et OU=groups

```
root@Auth:~/ldap-config# ldapadd -x -D "cn=admin,dc=techvault,dc=fr" -W -f base.ldif
Enter LDAP Password:
adding new entry "ou=users,dc=techvault,dc=fr"

adding new entry "ou=groups,dc=techvault,dc=fr"

root@Auth:~/ldap-config#
```

3. CRÉATION DES GROUPES

3.1 Création du fichier groups.ldif

Création du fichier définissant les groupes système :

➪ *nano groups.ldif*

Contenu de groups.ldif avec 3 groupes : cn=admins (gidNumber:5000), cn=students (gidNumber:5001), cn=guests (gidNumber:5002)

```
 GNU nano 8.4                                                    groups.ldif *
dn: cn=admins,ou=groups,dc=techvault,dc=fr
objectClass: posixGroup
cn: admins
gidNumber: 5000
description: Administrateurs systeme

dn: cn=students,ou=groups,dc=techvault,dc=fr
objectClass: posixGroup
cn: students
gidNumber: 5001
description: Etudiants authentifies

dn: cn=guests,ou=groups,dc=techvault,dc=fr
objectClass: posixGroup
cn: guests
gidNumber: 5002
description: Invites acces limite
```

Ajout des groupes à l'annuaire :

➪ *ldapadd -x -D "cn=admin,dc=techvault,dc=fr" -W -f groups.ldif*

Ajout réussi des trois groupes (admins, students, guests)

```
root@Auth:~/ldap-config# ldapadd -x -D "cn=admin,dc=techvault,dc=fr" -W -f groups.ldif
Enter LDAP Password:
adding new entry "cn=admins,ou=groups,dc=techvault,dc=fr"

adding new entry "cn=students,ou=groups,dc=techvault,dc=fr"

adding new entry "cn=guests,ou=groups,dc=techvault,dc=fr"

root@Auth:~/ldap-config#
```

3.2 Vérification des groupes

Vérification spécifique des groupes :

- ⇨ *ldapsearch -x -b "ou=groups,dc=techvault,dc=fr"*

Résultat ldapsearch affichant les 4 groupes : ou=groups, cn=admins(gid:5000), cn=guests(gid:5002), cn=etudiants(gid:5001) avec leurs descriptions

```
root@Auth:~/ldap-config# ldapsearch -x -b "ou=groups,dc=techvault,dc=fr"
# extended LDIF
#
# LDAPv3
# base <ou=groups,dc=techvault,dc=fr> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# groups, techvault.fr
dn: ou=groups,dc=techvault,dc=fr
objectClass: organizationalUnit
ou: groups

# admins, groups, techvault.fr
dn: cn=admins,ou=groups,dc=techvault,dc=fr
objectClass: posixGroup
cn: admins
gidNumber: 5000
description: Administrateurs systeme

# guests, groups, techvault.fr
dn: cn=guests,ou=groups,dc=techvault,dc=fr
objectClass: posixGroup
cn: guests
gidNumber: 5002
description: Invites acces limite

# etudiants, groups, techvault.fr
dn: cn=etudiants,ou=groups,dc=techvault,dc=fr
objectClass: posixGroup
cn: etudiants
gidNumber: 5001
description: Etudiants authentifies

# search result
search: 2
result: 0 Success

# numResponses: 5
# numEntries: 4
root@Auth:~/ldap-config#
```

3.3 Vérification de la base de données

Teste de la connectivité et listage la base complète :

- ⇨ *ldapsearch -x -b "dc=techvault,dc=fr"*

Résultat ldapsearch montrant l'arborescence complète : dc=techvault,dc=fr, ou=users, ou=groups, et les 3 groupes (admins, etudiants, guests) - numResponses: 7, numEntries: 6

```
root@Auth:~/ldap-config# ldapsearch -x -b "dc=techvault,dc=fr"
# extended LDIF
#
# LDAPv3
# base <dc=techvault,dc=fr> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# techvault.fr
dn: dc=techvault,dc=fr
objectClass: top
objectClass: dcObject
objectClass: organization
o: laser
dc: techvault

# users, techvault.fr
dn: ou=users,dc=techvault,dc=fr
objectClass: organizationalUnit
ou: users

# groups, techvault.fr
dn: ou=groups,dc=techvault,dc=fr
objectClass: organizationalUnit
ou: groups

# admins, groups, techvault.fr
dn: cn=admins,ou=groups,dc=techvault,dc=fr
objectClass: posixGroup
cn: admins
gidNumber: 5000
description: Administrateurs systeme

# etudiants, groups, techvault.fr
dn: cn=etudiants,ou=groups,dc=techvault,dc=fr
objectClass: posixGroup
cn: etudiants
gidNumber: 5001
description: Etudiants authentifies

# guests, groups, techvault.fr
dn: cn=guests,ou=groups,dc=techvault,dc=fr
objectClass: posixGroup
cn: guests
gidNumber: 5002
description: Invites acces limite

# search result
search: 2
result: 0 Success

# numResponses: 7
# numEntries: 6
root@Auth:~/ldap-config#
```

4. CONFIGURATION DES ACL (ACCESS CONTROL LISTS)

4.1 Création du fichier ACL

Création du fichier définissant les règles d'accès :

⇨ *nano acl.ldif*

Configuration complète des ACL avec règles pour userPassword, shadowLastChange, accès self write, group admins write, et différents niveaux d'accès par OU

```
  GNU nano 8.4                                                  acl.ldif *
dn: olcDatabase={1}mdb,cn=config
changetype: modify
replace: olcAccess
olcAccess: {0}to attrs=userPassword,shadowLastChange
  by self write
  by anonymous auth
  by group.exact="cn=admins,ou=groups,dc=techvault,dc=fr" write
  by * none
olcAccess: {1}to dn.subtree="ou=users,dc=techvault,dc=fr"
  by self write
  by group.exact="cn=admins,ou=groups,dc=techvault,dc=fr" write
  by group.exact="cn=etudiants,ou=groups,dc=techvault,dc=fr" read
  by * none
olcAccess: {2}to dn.base="ou=groups,dc=techvault,dc=fr"
  by group.exact="cn=admins,ou=groups,dc=techvault,dc=fr" write
  by users read
  by * none
olcAccess: {3}to attrs=cn,sn,givenName,mail
  by self write
  by group.exact="cn=admins,ou=groups,dc=techvault,dc=fr" write
  by group.exact="cn=etudiants,ou=groups,dc=techvault,dc=fr" read
  by group.exact="cn=guests,ou=groups,dc=techvault,dc=fr" read
  by * none
olcAccess: {4}to *
  by group.exact="cn=admins,ou=groups,dc=techvault,dc=fr" write
  by self read
  by * none
```

Les règles définies :

- Accès aux mots de passe : self write, anonymous auth, admins write
- Accès à la base racine : lecture publique
- Accès à ou=users : self write, admins write, students read
- Accès à ou=groups : admins write, users read
- Accès aux attributs (cn, sn, givenName, mail) : self write, admins write, students et guests read

Application des ACL :

- ⇨ *ldapmodify -Y EXTERNAL -H ldapi:/// -f acl.ldif*

Application réussie de la configuration ACL (SASL/EXTERNAL authentication, modifying entry "olcDatabase={1}mdb,cn=config")

```
root@Auth:/etc/ldap# nano acl.ldif
root@Auth:/etc/ldap# ldapmodify -Y EXTERNAL -H ldapi:/// -f acl.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "olcDatabase={1}mdb,cn=config"
```

5. INSTALLATION DES OUTILS DE BASE

5.1 Installation de Curl

Installez curl pour télécharger ACME.sh :

- ⇨ *apt install curl*

Installation du paquet curl

```
root@Auth:~# apt install curl
Installation de :
  curl

Installation de dépendances :
  libcurl4t64

Sommaire :
  Mise à niveau de : 0. Installation de : 2Supprimé : 0. Non mis à jour : 1
Taille du téléchargement : 661 kB
  Espace nécessaire : 1 542 kB / 28,5 GB disponible
```

6. CONFIGURATION DES CERTIFICATS TLS/SSL VIA ACME.SH

6.1 Installation d'ACME.sh

Téléchargement et installation du client ACME.sh *depuis GitHub (archive master.tar.gz)*

- ⇨ *curl https://get.acme.sh | sh*

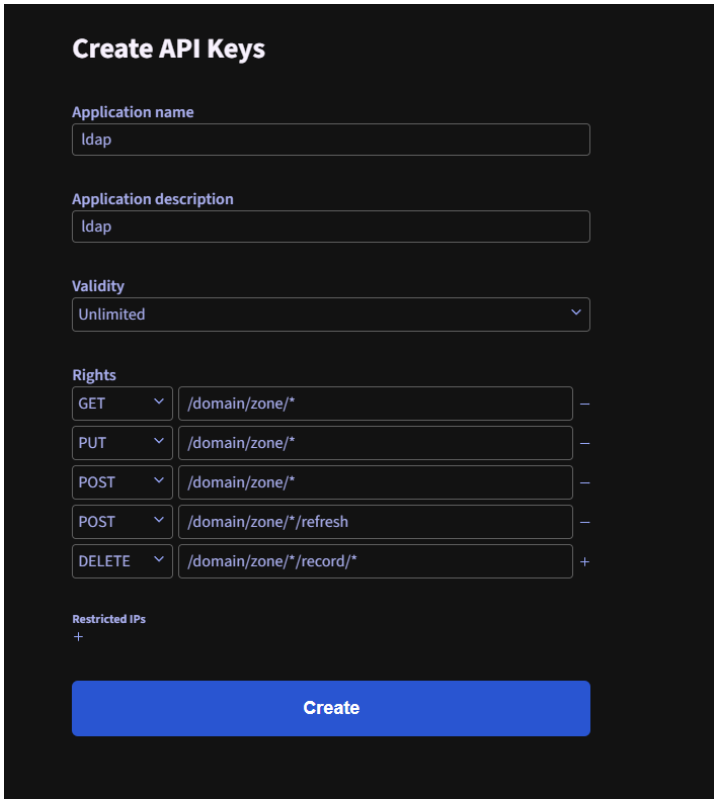
```
root@Auth:~# curl https://get.acme.sh | sh
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  1032    0  1032    0     0  12160      0 --:--:-- --:--:-- --:--:-- 12285
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  229k  100  229k    0     0  6298k      0 --:--:-- --:--:-- --:--:-- 6383k
[jeu. 12 févr. 2026 14:14:59 CET] Installing from online archive.
[jeu. 12 févr. 2026 14:14:59 CET] Downloading https://github.com/acmesh-official/acme.sh/archive/master.tar.gz
[jeu. 12 févr. 2026 14:15:00 CET] Extracting master.tar.gz
[jeu. 12 févr. 2026 14:15:00 CET] Installing to /root/.acme.sh
[jeu. 12 févr. 2026 14:15:00 CET] Installed to /root/.acme.sh/acme.sh
[jeu. 12 févr. 2026 14:15:00 CET] Installing alias to '/root/.bashrc'
[jeu. 12 févr. 2026 14:15:00 CET] Close and reopen your terminal to start using acme.sh
[jeu. 12 févr. 2026 14:15:00 CET] Installing cron job
no crontab for root
no crontab for root
[jeu. 12 févr. 2026 14:15:00 CET] bash has been found. Changing the shebang to use bash as preferred.
[jeu. 12 févr. 2026 14:15:00 CET] OK
[jeu. 12 févr. 2026 14:15:00 CET] Install success!
```

6.2 Configuration des clés API OVH (www.ovhcloud.com/fr)

Créez des clés API sur le portail OVH avec les droits suivants :

- GET /domain/zone/*
- PUT /domain/zone/*
- POST /domain/zone/*
- POST /domain/zone/*/refresh
- DELETE /domain/zone//*record/*

Interface de création des API keys OVH avec droits configurés



Créez un fichier temporaire pour stocker les clés :

⇨ *nano /tmp/ovh_keys.sh*

Contenu du fichier avec export des variables OVH_AK, OVH_AS, OVH_CK

NB : il faut mettre les valeurs de chaque variable dans le fichier

Définissez les permissions :

- ⇨ *chmod 600 /tmp/ovh_keys.sh*

```
root@Auth:~# chmod 600 /tmp/ovh_keys.sh
```

Chargez les variables d'environnement :

- ⇨ *source /tmp/ovh_keys.sh*

```
root@Auth:~# source /tmp/ovh_keys.sh
```

6.3 Génération du certificat Let's Encrypt

Générez le certificat avec validation DNS automatique :

- ⇨ *~/.acme.sh/acme.sh --issue --dns dns_ovh -d ldap.techvault.fr --email mail@gmail.com*

Processus de génération terminé avec succès - certificats disponibles

```
acme.sh --issue --dns dns_ovh -d ldap.techvault.fr --email nasuialex@gmail.com
```

Emplacement des certificats générés dans /root/.acme.sh/.techvault.fr_ecc/*

```
-----END CERTIFICATE-----
[jeu. 12 févr. 2026 15:03:05 CET] Your cert is in: /root/.acme.sh/*.techvault.fr_ecc/*.techvault.fr.cer
[jeu. 12 févr. 2026 15:03:05 CET] Your cert key is in: /root/.acme.sh/*.techvault.fr_ecc/*.techvault.fr.key
[jeu. 12 févr. 2026 15:03:05 CET] The intermediate CA cert is in: /root/.acme.sh/*.techvault.fr_ecc/ca.cer
[jeu. 12 févr. 2026 15:03:05 CET] And the full-chain cert is in: /root/.acme.sh/*.techvault.fr_ecc/fullchain.cer
root@Auth:/tmp#
```

7. CONFIGURATION TLS/SSL DANS OPENLDAP

7.1 Copie des certificats

Créez le répertoire et copiez les certificats :

- ⇨ *mkdir -p /etc/ldap/certs*
- ⇨ *cp /root/.acme.sh/*.techvault.fr_ecc/fullchain.cer /etc/ldap/certs/*
- ⇨ *cp /root/.acme.sh/*.techvault.fr_ecc/*.techvault.fr.key /etc/ldap/certs/*
- ⇨ *cp /root/.acme.sh/*.techvault.fr_ecc/ca.cer /etc/ldap/certs/*

Copie des fichiers de certificats dans /etc/ldap/certs/

```
root@Auth:/tmp# mkdir -p /etc/ldap/certs
root@Auth:/tmp# cp ~/.acme.sh/\*.techvault.fr_ecc/fullchain.cer /etc/ldap/certs/
root@Auth:/tmp# cp ~/.acme.sh/\*.techvault.fr_ecc/\*.techvault.fr.key /etc/ldap/certs/
root@Auth:/tmp# cp ~/.acme.sh/\*.techvault.fr_ecc/ca.cer /etc/ldap/certs/
root@Auth:/tmp#
```

Modification des permissions :

- ⇨ *chown openldap:openldap /etc/ldap/certs/**
- ⇨ *chmod 600 /etc/ldap/certs/*.key*
- ⇨ *chmod 644 /etc/ldap/certs/*.certs*

```
root@Auth:/tmp# chown openldap:openldap /etc/ldap/certs/*
root@Auth:/tmp# chmod 600 /etc/ldap/certs/*.key
root@Auth:/tmp# chmod 644 /etc/ldap/certs/*.cer
root@Auth:/tmp#
```

7.2 Utilisation des certificats pour la sécurisation de ldap

Création du fichier ldap_tls.ldif :

- ⇨ *nano ldap_tls.ldif*

Contenu du fichier ldap_tls.ldif avec configuration TLS

```
 GNU nano 8.4                                                    ldap_tls.ldif *
dn: cn=config
changetype: modify
replace: olcTLSCACertificateFile
olcTLSCACertificateFile: /etc/ldap/certs/ca.cer
-
replace: olcTLSCertificateFile
olcTLSCertificateFile: /etc/ldap/certs/fullchain.cer
-
replace: olcTLSCertificateKeyFile
olcTLSCertificateKeyFile: /etc/ldap/certs/*.techvault.fr.key
-
replace: olcTLSCipherSuite
olcTLSCipherSuite: ECDHE+AESGCM:ECDHE+CHACHA20:DHE+AESGCM:DHE+CHACHA20:!aNULL:!MD5:!DSS
```

Application de la configuration :

- ⇨ *ldapmodify -Y EXTERNAL -H ldapi:/// -f ldap_tls.ldif*

Application réussie de la configuration TLS

```
root@Auth:/etc/ldap# ldapmodify -Y EXTERNAL -H ldapi:/// -f ldap_tls.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "cn=config"
```

7.3 Activation du port LDAPS (636) et désactivation du port 389

Éditez le fichier de configuration du service :

- ⇨ *nano /etc/default/slapd*

Modifiez la ligne ‘SLAPD_SERVICES’ en y ajoutant :

- ⇨ *SLAPD_SERVICES="ldaps:/// ldapi:///" »*

Configuration SLAPD_SERVICES activant uniquement ldaps:/// et ldapi:///

```
  GNU nano 8.4                                                /etc/default/slapd *
SLAPD_SERVICES="ldaps:/// ldapi:///"
```

Redémarrage du service :

- ⇨ *systemctl restart slapd*

7.4 Vérification du port d'écoute

Vérifiez que slapd écoute bien sur le port 636 :

- ⇨ *ss -tlnp | grep slapd*

Processus slapd écoutant sur 0.0.0.0:636 et [::]:636 (IPv4 et IPv6)

```
root@Auth:/etc/ldap#  ss -tlnp | grep slapd
LISTEN 0      2048                             0.0.0.0:636       0.0.0.0:*    users:(("slapd",pid=25905,fd=7))
LISTEN 0      2048                                [::]:636          [::]:*    users:(("slapd",pid=25905,fd=8))
```

7.5 Test de connexion TLS/SSL

Teste de la connexion LDAPS avec OpenSSL :

- ⇨ *openssl s_client -connect localhost:636 </dev/null*

Validation de la chaîne de certificats (ISRG Root X1 → Let's Encrypt E8 → *.techvault.fr) avec dates de validité*

```
root@Auth:/etc/ldap# openssl s_client -connect localhost:636 </dev/null
Connecting to ::1
CONNECTED(00000003)
Can't use SSL_get_servername
depth=2 C=US, O=Internet Security Research Group, CN=ISRG Root X1
verify return:1
depth=1 C=US, O=Let's Encrypt, CN=E8
verify return:1
depth=0 CN=*.techvault.fr
verify return:1
---
Certificate chain
 0 s:CN=*.techvault.fr
   i:C=US, O=Let's Encrypt, CN=E8
   a:PKEY: EC, (prime256v1); sigalg: ecdsa-with-SHA384
   v:NotBefore: Feb 12 13:04:34 2026 GMT; NotAfter: May 13 13:04:33 2026 GMT
 1 s:C=US, O=Let's Encrypt, CN=E8
   i:C=US, O=Internet Security Research Group, CN=ISRG Root X1
   a:PKEY: EC, (secp384r1); sigalg: sha256WithRSAEncryption
   v:NotBefore: Mar 13 00:00:00 2024 GMT; NotAfter: Mar 12 23:59:59 2027 GMT
```

8. CONFIGURATION DU PARE-FEU

8.1 Configuration nftables

Éditez la configuration du pare-feu :

Règles nftables avec autorisation des ports :

- ✓ *lo (localhost)*
- ✓ *LDAPS (636)*
- ✓ *SSH (22)*
- ✓ *DNS (53)*
- ✓ *Kerberos (88,464)*
- ✓ *NFS (111,2049,32765-32768)*
- ✓ *Flask/Nginx (80,443)*

```
 GNU nano 8.4
#!/usr/sbin/nft -f

flush ruleset

table inet filter {
    chain input {
        type filter hook input priority 0; policy drop;

        # Connexions établies
        ct state established,related accept

        # Localhost
        iif "lo" accept

        # SSH
        tcp dport 22 accept

        # DNS
        udp dport 53 accept
        tcp dport 53 accept

        #LDAP
        tcp dport 636 accept

        #KERBEROS
        tcp dport { 88, 464 } accept
        udp dport { 88, 464 } accept

        #NFS
        tcp dport { 111, 2049, 32765-32768 } accept
        udp dport { 111, 2049, 32765-32768 } accept

        #Flask/Nginx
        tcp dport 80 accept
        tcp dport 443 accept

    }

    chain forward {
        type filter hook forward priority 0; policy drop;
        ct state established,related accept
    }

    chain output {
        type filter hook output priority 0; policy accept;
    }
}
```

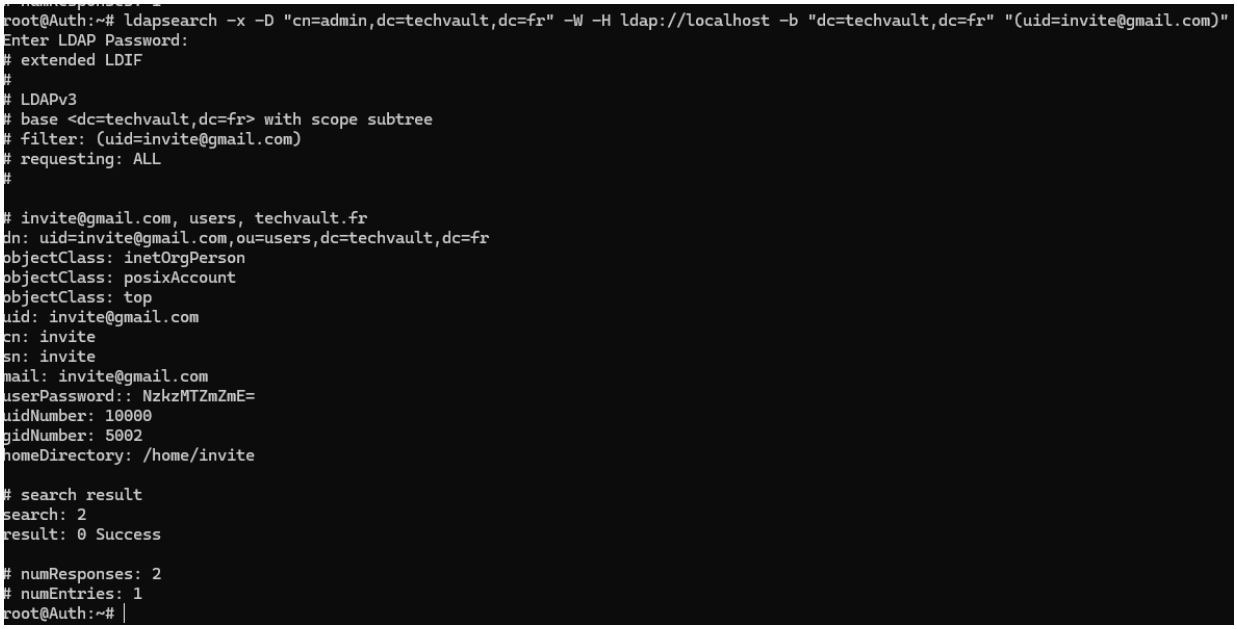
*A*pplication de la configuration:

- ⇨ *nft flush ruleset*
- ⇨ *nft -f /etc/nftables.conf*
- ⇨ *systemctl enable nftables*

Teste de fonctionnement de la base de données Ldap.

La commande qui suit permet de rechercher dans la base de données ldap un utilisateur déjà enregistré :

➔ *ldapsearch -x -D « cn=admin,dc=tecvault,dc=fr" -W -H ldap://localhost -b " dc=techvault,dc=fr" "(uid=invite@gmail.com)"*



ANNEXES

Ports utilisés

- 636/tcp : LDAPS (LDAP over TLS/SSL)
- 389/tcp : LDAP clair (désactivé)

Références

- Documentation officielle OpenLDAP : https://www.openldap.org/doc/
- Documentation Debian : https://wiki.debian.org/LDAP
- acme.sh : https://github.com/acmesh-official/acme.sh