

Integrate asterisk schema and asterisk ldif to ldap

ldapadd -Y EXTERNAL ldapi:/// asterisk.schema

ldapadd -Y EXTERNAL ldapi:/// asterisk.ldif

sudo nano user.ldif

```
GNU nano 7.2
dn: uid=test,ou=users,ou=asterisk,dc=ldap,dc=com
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
objectClass: AsteriskSIPUser
uid: test
cn: test
sn: test
givenName: Test
uidNumber: 3001
gidNumber: 3001
homeDirectory: /home/test
loginShell: /bin/bahs
userPassword: {md5}d8e8fca2dc0f896fd7cb4cb0031ba249
```

ldapadd -x -D "cn=admin,dc=ldap,dc=com" -W -f user.ldif

-> problèmes rencontrés

a- les vm sont en mode terminal donc il n'est pas possible de faire copier/coller

→ installation proftpd pour transférer les fichiers entre les vms

b- le schema ldap ne fonctionne pas : erreur d'objectClass avec les classes Asterisk

→ modify slapd.conf -> include /etc/ldap/asterisk.schema (cc)

```
GNU nano 7.2
# This is the main slapd configuration file. See slapd.conf(5) for
# info on the configuration options.

#####
# Global Directives:

# Schema and objectClass definitions
include /etc/ldap/schema/core.schema
include /etc/ldap/schema/cosine.schema
include /etc/ldap/schema/nis.schema
include /etc/ldap/schema/inetorgperson.schema
include /etc/ldap/schema/asterisk.schema

# Where the pid file is put. The init.d script
# will not stop the server if you change this.
pidfile /var/run/slapd/slapd.pid

# List of arguments that were passed to the server
argsfile /var/run/slapd/slapd.args

# Read slapd.conf(5) for possible values
loglevel none

# Where the dynamically loaded modules are stored
modulepath /usr/lib/ldap
moduleload back_mdb
```

```

root@ldap:~# sftp ftpuser@192.168.104.90
The authenticity of host '192.168.104.90 (192.168.104.90)' can't be established.
ED25519 key fingerprint is SHA256:wo+yxfb6XzdCcaC4M20FP0rC0traIVQvQ/m3DVrhunY.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:1: [hashed name]
  ~/.ssh/known_hosts:4: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.104.90' (ED25519) to the list of known hosts.
ftpuser@192.168.104.90's password:
Connected to 192.168.104.90.
sftp> get asterisk.ldap-schema
Fetching /home/ftpuser/asterisk.ldap-schema to asterisk.ldap-schema
asterisk.ldap-schema                                100% 29KB 4.6
sftp> get asterisk.ldif
Fetching /home/ftpuser/asterisk.ldif to asterisk.ldif
asterisk.ldif                                       100% 29KB 10.2
sftp> exit
root@ldap:~# ls
asterisk.ldap-schema  asterisk.ldif
root@ldap:~# sudo cp asterisk.ldap-schema /etc/ldap/schema/asterisk.schema
root@ldap:~# sudo /etc/init.d/slaped restart
Restarting slapd (via systemctl): slapd.service.
root@ldap:~# sudo ldapadd -Y EXTERNAL -H ldapi:/// -f asterisk.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
adding new entry "cn=asterisk,cn=schema,cn=config"

```

Voip-Asterisk server

sudo apt install libldap-dev

./configure

make menuselect

→ vérifier que le modelu res_ldap.so est bien sélectionner

make install

sudo nano /etc/asterisk/modules.conf

=> preload => res_config_ldap.so

-> editer fichier /etc/asterisk/res_ldap.conf

```

[general]
;
; Specify one of either host and port OR url.  URL is preferred, as you can
; use more options.
server=ldap://192.168.104.90
port=389
;url=ldap://ldap3.mydomain.com:3890
protocol=3 ; Version of the LDAP protocol to use; default is 3.
basedn=dc=ldap,dc=com ; Base DN
user=cn=admin,dc=ldap,dc=com ; Bind DN
pass=root ; Bind password
binddn=cn=admin,dc=ldap,dc=com
bindpw=root
scope=sub
tls=no
password_attribute=userPassword

```

core restart now

realtime show ldap status

```

debian@CLI> core restart now
debian@CLI>
Disconnected from Asterisk server
Asterisk cleanly ending (0).
Executing last minute cleanups
root@debian:/usr/src/asterisk-22.2.0# asterisk -r
Asterisk 22.2.0, Copyright (C) 1999 - 2025, Sangoma Technologies Corporation and others.
Created by Mark Spencer <markster@digium.com>
Asterisk comes with ABSOLUTELY NO WARRANTY; type 'core show warranty' for details.
This is free software, with components licensed under the GNU General Public
License version 2 and other licenses; you are welcome to redistribute it under
certain conditions. Type 'core show license' for details.
=====
Connected to Asterisk 22.2.0 currently running on debian (pid = 24095)
debian@CLI> realtime show ldap status
Connected to 'ldap://192.168.104.90:389', baseDN dc=ldap,dc=com with username cn=admin,dc=ldap,dc=com for 18 seconds
debian@CLI>

```

sudo nano /etc/asterisk/pjsip.conf

```
[global]
type=global
user_agent=Asterisk

[transport-udp]
type=transport
protocol=udp
bind=0.0.0.0:5060

[2001]
type=auth
auth_type=userpass
username=2001
password=ldap://2001@192.168.104.90

[2001]
type=endpoint
transport=transport-udp
context=Internal
aors=2001
auth=2001
direct_media=no

[2001]
type=aor
max_contacts=1
contact=sip:2001@192.168.104.90
```

sudo nano /etc/asterisk/extensions.conf

```
exten => 6001,1,Dial(PJSIP/6001)
exten => 6002,1,Dial(PJSIP/6002)
exten => 820,1,Dial(PJSIP/ilona)
exten => 821,1,Dial(PJSIP/104)
exten => 821,n,Hangup()
exten => 2001,1,Dial(PJSIP/2001)
```

sudo nano /etc/asterisk/extn.config

```
;
[settings]
sipusers => ldap,"ou=ldap,dc=ldap,dc=com",sip
sippeers => ldap,"ou=ldap,dc=ldap,dc=com",sip
extensions => ldap,"ou=extensions,dc=ldap,dc=com",extensions
;
```

-> failure to authenticate

```
Connected to Asterisk 22.2.0 currently running on debian (pid=678)
(Feb 21 10:41:25) NOTICE[706]: res_pjsip/pjsip_distributor.c:688 log_failed_request: Request 'REGISTER' from '<sip:2001@192.168.104.21>' failed for '192.168.104.31:40138' (callid: HX_390pccENWdClnhSy2UQ..) - Failed to authenticate
(Feb 21 10:42:18) NOTICE[706]: res_pjsip/pjsip_distributor.c:688 log_failed_request: Request 'REGISTER' from '<sip:2001@192.168.104.21>' failed for '192.168.104.31:40138' (callid: cFns6bf4neY3Qmzun2-oIg..) - Failed to authenticate
debian*CLI>
```

=> Asterisk 22 ne parvient pas à lire le mot de passe en hash md5 bien que ce soit ce format qui est recommandé par la documentation et slapd ne permet pas de stocker les mots de passe en clair
solution: utiliser une autre base de données plus simple à implémenter avec asterisk tel que MySQL

Bash Script :

Lire le fichier csv

- Créer un fichier \$uid.ldif
- remplir les données nécessaire avec les variables

→ Modifier fichier pjsip.conf pour ajouter le endpoint

→ Modifier extension.conf pour ajouter le dialplan

```
GNU nano 7.2 adduser.sh *
#!/usr/bin/bash
#Lecture du fichier CSV
CSV_FILE="user.csv"
while IFS=";" read uid gid passwd; do
    if [ "$uid" = "uid" ]; then
        continue
    fi
    if [ "$uid" != "" ]; then
        printf "\ndn: uid=$uid,ou=users,ou=asterisk,dc=ldap,dc=com\nobjectClass: inetOrgPerson\nobjectClass: posixAccount\nobjectClass: shadowAccount\nobjectClass: user\nuid=$uid\npassword=$passwd\nuidNumber=$gid\nhomeDirectory=/\nloginShell=/bin/bash\n" >> /etc/asterisk/pjsip.conf
        printf "[\$uid]\ntype=ao\nmax_contacts=1\ncontact=ssip:$uid@192.168.104.90\n" >> /etc/asterisk/pjsip.conf
        printf "exten => \$uid,1,Dial(PJSIP/\$uid)" >> /etc/asterisk/extensions.conf
        ldapadd -x -H ldap://192.168.104.90 -w root -D "cn=admin,dc=ldap,dc=com" -f $uid.ldif
    else
        echo "L'utilisateur $uid existe déjà"
    fi
    asterisk -rx 'pjsip reload'
    asterisk -rx 'dialplan reload'
    asterisk -rx 'pjsip show endpoints'
```

→ ldapadd -x -w mdp -H ldap://192,168,104,90 -D 'cn=admin,dc=ldap,dc=com' -f \$uid.ldif

→ reload asterisk avec :

- asterisk -rx 'pjsip reload'
- asterisk -rx 'dialplan reload'

=> permet de ne pas avoir à rentrer dans le CLI de asterisk ou de devoir utiliser sudo systemctl restart et avoir à mettre le mdp sudo

on vérifie en essayant de faire ldapadd manuellement

```
root@debian:~# ldapadd -x -w root -H ldap://192.168.104.90 -D "cn=admin,dc=ldap,dc=com" -f 2002.ldif
adding new entry "uid=2002,ou=users,ou=asterisk,dc=ldap,dc=com"
ldap_add: Already exists (68)
root@debian:~#
```

→ L'entrée existe déjà donc l'utilisateur a bien été enregistré dans l'annuaire ldap.