Álvaro Almellones Fernández

PRÁCTICA 12
SERVIDOR FREERADIUS. WPA2-ENTERPRISE. INTEGRACIÓN CON SERVIDOR LDAP

INSTALACIÓN DE SERVIDOR FREERADIUS SIN MYSQL NI LDAP

1. **(1,5 punto)** Realice la instalación del servidor FreeRadius en un nuevo equipo (radiuslapXXxx) (para evitar configuraciones de iptables, etc.) mediante S.O. Ubuntu Server en la zona WAN (bridge) para permitir el acceso a un cliente radius vía localhost para realizar pruebas (personalice la contraseña por defecto). Además, cree un usuario en la forma XXxx con la contraseña XXxx para pruebas locales. Evidencie:

a. Ficheros modificados y contenido de lo modificado.

```
  GNU nano 7.2                                /etc/freeradius/3.0/users
DEFAULT Hint == "SLIP"
        Framed-Protocol = SLIP

#
# Last default: rlogin to our main server.
#
#DEFAULT
#       Service-Type = Login-User,
#       Login-Service = Rlogin,
#       Login-IP-Host = shellbox.ispdomain.com

# #
# # Last default: shell on the local terminal server.
# #
# DEFAULT
#       Service-Type = Administrative-User


# On no match, the user is denied access.


############################################################
# You should add test accounts to the TOP of this file! #
# See the example user "bob" above.                      #
############################################################

almellonesfernandez   Cleartext-Password := "almellonesfernandez"
```

b. Servicio arrancado y comprobación de que está funcionando (systemctl, netstat, nmap)

```
root@almellonesfernandez-radiusldap:/home/almellonesfernandez# systemctl status freeradius
● freeradius.service - FreeRADIUS multi-protocol policy server
     Loaded: loaded (/usr/lib/systemd/system/freeradius.service; enabled; preset: enabled)
     Active: active (running) since Mon 2025-03-10 11:49:10 UTC; 6min ago
       Docs: man:radiusd(8)
             man:radiusd.conf(5)
             http://wiki.freeradius.org/
             http://networkradius.com/doc/
   Main PID: 2417 (freeradius)
     Status: "Processing requests"
      Tasks: 6 (limit: 4552)
     Memory: 43.4M (max: 2.0G available: 1.9G peak: 43.7M)
        CPU: 290ms
     CGroup: /system.slice/freeradius.service
             └─2417 /usr/sbin/freeradius -f

mar 10 11:49:10 almellonesfernandez-radiusldap freeradius[2415]: Compiling Post-Auth-Type Challenge for attr Post-Aut>
mar 10 11:49:10 almellonesfernandez-radiusldap freeradius[2415]: Compiling Post-Auth-Type Client-Lost for attr Post-A>
mar 10 11:49:10 almellonesfernandez-radiusldap freeradius[2415]: Compiling Auth-Type PAP for attr Auth-Type
mar 10 11:49:10 almellonesfernandez-radiusldap freeradius[2415]: Compiling Auth-Type CHAP for attr Auth-Type
mar 10 11:49:10 almellonesfernandez-radiusldap freeradius[2415]: Compiling Auth-Type MS-CHAP for attr Auth-Type
mar 10 11:49:10 almellonesfernandez-radiusldap freeradius[2415]:  # Skipping contents of 'if' as it is always 'false'>
mar 10 11:49:10 almellonesfernandez-radiusldap freeradius[2415]: Compiling Post-Auth-Type REJECT for attr Post-Auth-T>
mar 10 11:49:10 almellonesfernandez-radiusldap freeradius[2415]: radiusd: #### Skipping IP addresses and Ports ####
mar 10 11:49:10 almellonesfernandez-radiusldap freeradius[2415]: Configuration appears to be OK
mar 10 11:49:10 almellonesfernandez-radiusldap systemd[1]: Started freeradius.service - FreeRADIUS multi-protocol pol>
lines 1-25/25 (END)
```

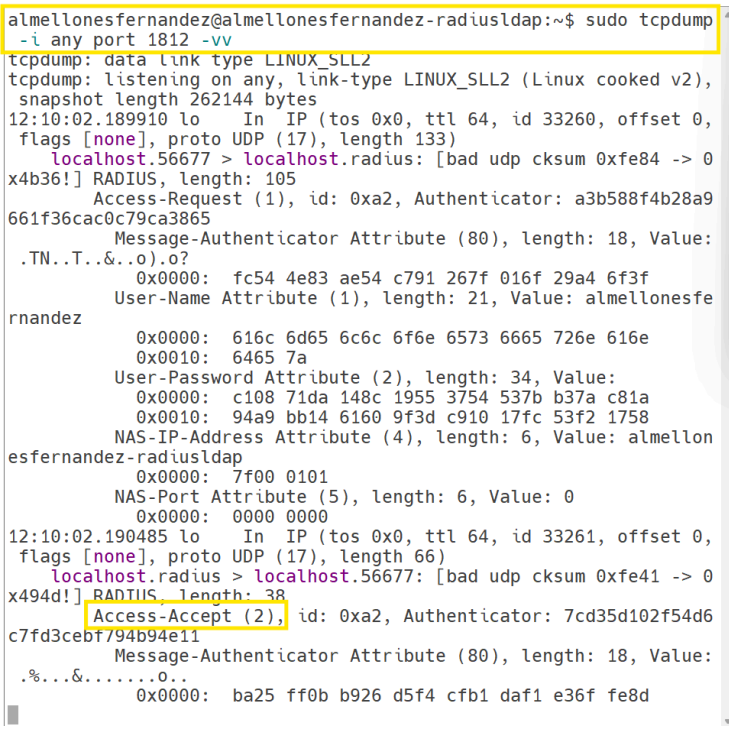
```
root@almellonesfernandez-radiusldap:/home/almellonesfernandez# netstat -putan
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      675/systemd-resolve
tcp        0      0 127.0.0.1:6010          0.0.0.0:*               LISTEN      1434/sshd: almellon
tcp        0      0 127.0.0.54:53           0.0.0.0:*               LISTEN      675/systemd-resolve
tcp6       0      0 :::22                   :::*                    LISTEN      1/init
tcp6       0      0 ::1:6010                :::*                    LISTEN      1434/sshd: almellon
tcp6       0      0 192.168.1.112:22        192.168.1.64:52044      ESTABLISHED 1379/sshd: almellon
tcp6       0     48 192.168.1.112:22        192.168.1.64:52037      ESTABLISHED 1357/sshd: almellon
udp        0      0 127.0.0.1:18120         0.0.0.0:*                           2417/freeradius
udp        0      0 0.0.0.0:38653           0.0.0.0:*                           2417/freeradius
udp        0      0 0.0.0.0:1812            0.0.0.0:*                           2417/freeradius
udp        0      0 0.0.0.0:1813            0.0.0.0:*                           2417/freeradius
udp        0      0 127.0.0.54:53           0.0.0.0:*                           675/systemd-resolve
udp        0      0 127.0.0.53:53           0.0.0.0:*                           675/systemd-resolve
udp        0      0 192.168.1.112:68        0.0.0.0:*                           655/systemd-network
udp6       0      0 fe80::20c:29ff:feb9:546 :::*                                655/systemd-network
udp6       0      0 :::48383                :::*                                2417/freeradius
udp6       0      0 :::1812                 :::*                                2417/freeradius
udp6       0      0 :::1813                 :::*                                2417/freeradius
root@almellonesfernandez-radiusldap:/home/almellonesfernandez#
```

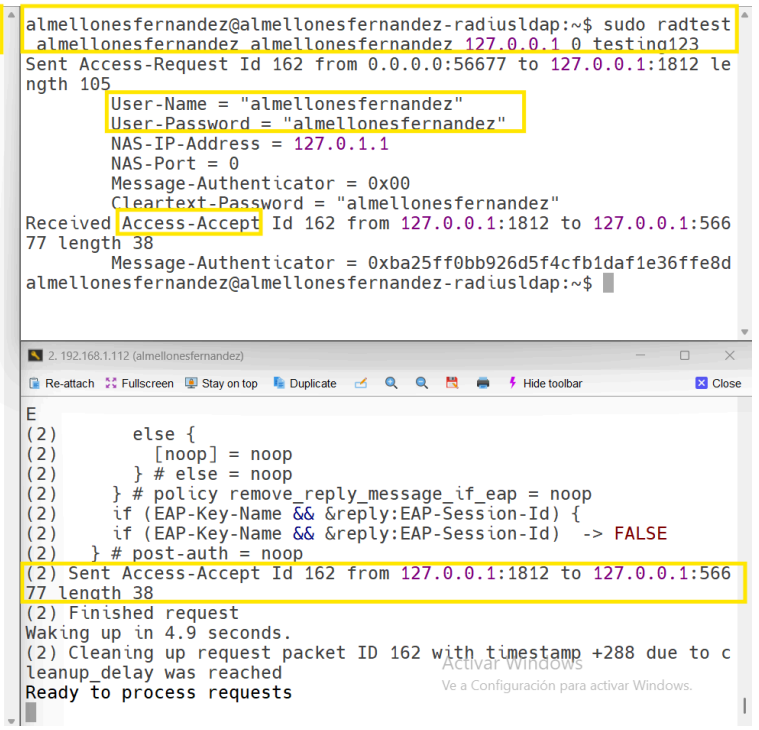
```
root@almellonesfernandez-radiusldap:/home/almellonesfernandez# nmap -sU  127.0.0.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-10 11:59 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.13s latency).
Not shown: 998 closed udp ports (port-unreach)
PORT     STATE         SERVICE
1812/udp open          radius
1813/udp open|filtered radacct

Nmap done: 1 IP address (1 host up) scanned in 2.37 seconds
root@almellonesfernandez-radiusldap:/home/almellonesfernandez#
```

c. Pare el servicio y arranque mediante comando freeradius -X y evidencie pruebas en modo local con comando radtest con el usuario/contraseña correctamente y la salida del comando freeradius -X. Capture el momento de la conexión con tcpdump.

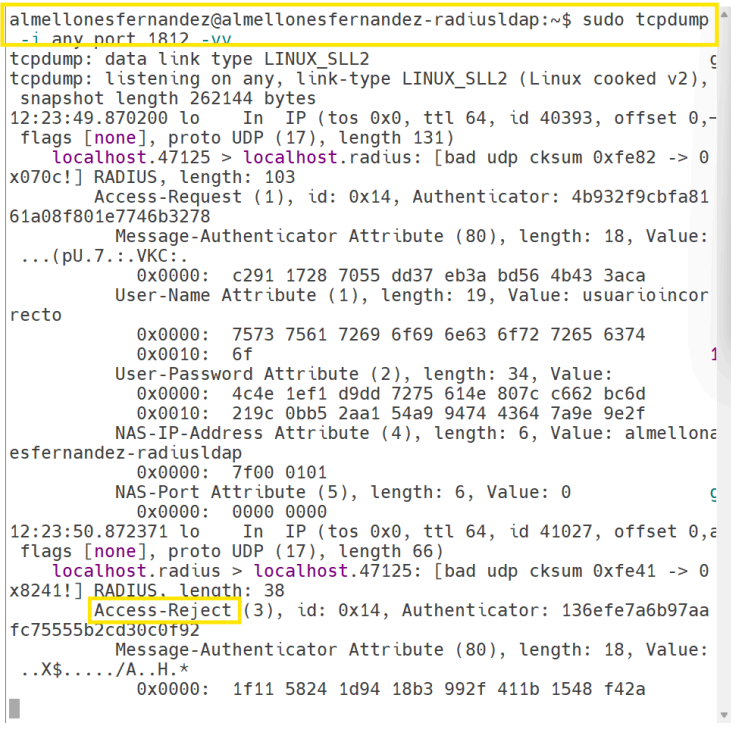
```
root@almellonesfernandez-radiusldap:/home/almellonesfernandez# sys
temctl stop freeradius
root@almellonesfernandez-radiusldap:/home/almellonesfernandez# fre
eradius -X
FreeRADIUS Version 3.2.5
Copyright (C) 1999-2023 The FreeRADIUS server project and contribu
tors
There is NO warranty; not even for MERCHANTABILITY or FITNESS FOR
A
PARTICULAR PURPOSE
You may redistribute copies of FreeRADIUS under the terms of the
GNU General Public License
For more information about these matters, see the file named COPYR
IGHT
Starting - reading configuration files ...
including dictionary file /usr/share/freeradius/dictionary
including dictionary file /usr/share/freeradius/dictionary.dhcp
including dictionary file /usr/share/freeradius/dictionary.vqp
including dictionary file /etc/freeradius/3.0/dictionary
including configuration file /etc/freeradius/3.0/radiusd.conf
including configuration file /etc/freeradius/3.0/proxy.conf
including configuration file /etc/freeradius/3.0/clients.conf
including files in directory /etc/freeradius/3.0/mods-enabled/
including configuration file /etc/freeradius/3.0/mods-enabled/chap
including configuration file /etc/freeradius/3.0/mods-enabled/expr
including configuration file /etc/freeradius/3.0/mods-enabled/prep
rocess
Listening on auth address * port 1812 bound to server default
Listening on acct address * port 1813 bound to server default
Listening on auth address :: port 1812 bound to server default
Listening on acct address :: port 1813 bound to server default
Listening on auth address 127.0.0.1 port 18120 bound to server inn
er-tunnel
Listening on proxy address * port 54852
Listening on proxy address :: port 57559
Ready to process requests
```

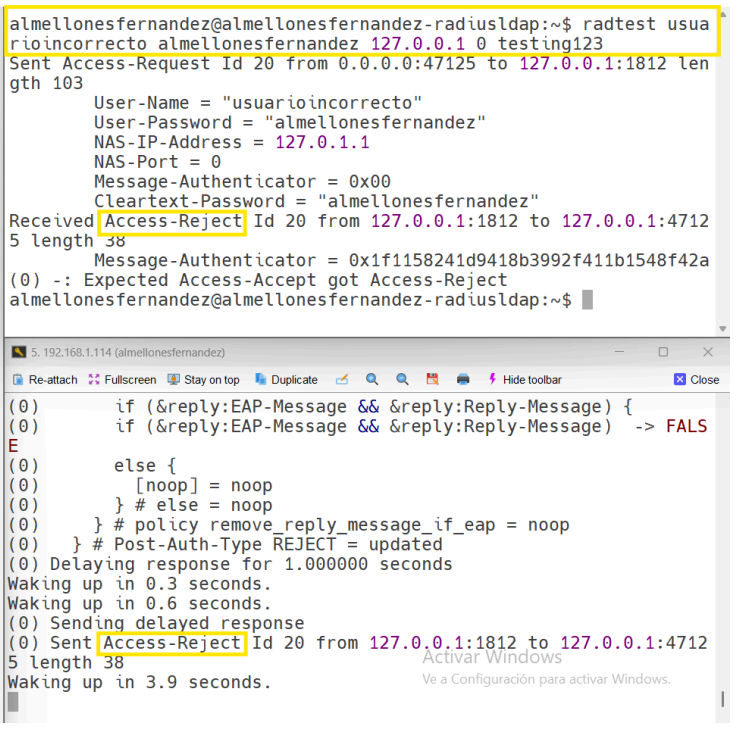
Álvaro Almellones Fernández





d. Evidencie pruebas en modo local con comando radtest, poniendo usuario mal, contraseña mal y contraseña del cliente mal.





Álvaro Almellones Fernández

```
almellonesfernandez@almellonesfernandez-radiusldap:~$ sudo tcpdump
 -i any port 1812 -vv
tcpdump: data link type LINUX_SLL2
tcpdump: listening on any, link-type LINUX_SLL2 (Linux cooked v2),
 snapshot length 262144 bytes
12:25:19.181284 lo    In  IP (tos 0x0, ttl 64, id 27261, offset 0,-
 flags [none], proto UDP (17), length 133)
    localhost.42637 > localhost.radius: [bad udp cksum 0xfe84 -> 0
xc88c!] RADIUS, length: 105
        Access-Request (1), id: 0x66, Authenticator: 40cc7c43ac2e0
4c6e7c30f39868621d3
          Message-Authenticator Attribute (80), length: 18, Value:
 c"...[H..v[..D..
            0x0000:  6322 c8ef be5b 48b3 1876 5b03 8844 9519
          User-Name Attribute (1), length: 21, Value: almellonesfe
rnandez
            0x0000:  616c 6d65 6c6c 6f6e 6573 6665 726e 616e
            0x0010:  6465 7a
          User-Password Attribute (2), length: 34, Value:
            0x0000:  a625 ae95 ef7b 9b1a 7d66 510b e62e 1e74
            0x0010:  7826 2e4b 0b9f ca37 a99f d591 7e89 11a4
          NAS-IP-Address Attribute (4), length: 6, Value: almellona
esfernandez-radiusldap
            0x0000:  7f00 0101
          NAS-Port Attribute (5), length: 6, Value: 0
            0x0000:  0000 0000
12:25:20.183391 lo    In  IP (tos 0x0, ttl 64, id 27730, offset 0,a
 flags [none], proto UDP (17), length 66)
    localhost.radius > localhost.42637: [bad udp cksum 0xfe41 -> 0
xa712!] RADIUS, length: 38
        Access-Reject (3), id: 0x66, Authenticator: 92c608296bf28a
b21f6f208bc6ea256a
          Message-Authenticator Attribute (80), length: 18, Value:
 ...A7.......1p..
            0x0000:  a81e f341 37ef f097 e813 feea 3170 bf02
```

```
almellonesfernandez@almellonesfernandez-radiusldap:~$ radtest alme
llonesfernandez contraseñaincorrecta 127.0.0.1 0 testing123
Sent Access-Request Id 102 from 0.0.0.0:42637 to 127.0.0.1:1812 le
ngth 105
        User-Name = "almellonesfernandez"
        User-Password = "contraseñaincorrecta"
        NAS-IP-Address = 127.0.1.1
        NAS-Port = 0
        Message-Authenticator = 0x00
        Cleartext-Password = "contraseñaincorrecta"
Received Access-Reject Id 102 from 127.0.0.1:1812 to 127.0.0.1:426
37 length 38
        Message-Authenticator = 0xa81ef34137eff097e813feea3170bf02
(0) -: Expected Access-Accept got Access-Reject
almellonesfernandez@almellonesfernandez-radiusldap:~$
```

```
5. 192.168.1.114 (almellonesfernandez)
Re-attach  Fullscreen  Stay on top  Duplicate  Hide toolbar  Close
(1)        else {
(1)          [noop] = noop
(1)        } # else = noop
(1)      } # policy remove_reply_message_if_eap = noop
(1)    } # Post-Auth-Type REJECT = updated
(1) Delaying response for 1.000000 seconds
Waking up in 0.3 seconds.
Waking up in 0.6 seconds.
(1) Sending delayed response
(1) Sent Access-Reject Id 102 from 127.0.0.1:1812 to 127.0.0.1:426
37 length 38
Waking up in 3.9 seconds.
(1) Cleaning up request packet ID 102 with timestamp +124 due to c
leanup_delay was reached
Ready to process requests
```

```
almellonesfernandez@almellonesfernandez-radiusldap:~$ sudo tcpdump
 -i any port 1812 -vv
tcpdump: data link type LINUX_SLL2
tcpdump: listening on any, link-type LINUX_SLL2 (Linux cooked v2),
 snapshot length 262144 bytes
12:26:48.567602 lo    In  IP (tos 0x0, ttl 64, id 40641, offset 0,-
 flags [none], proto UDP (17), length 133)
    localhost.59679 > localhost.radius: [bad udp cksum 0xfe84 -> 0
xd7ad!] RADIUS, length: 105
        Access-Request (1), id: 0x14, Authenticator: 2d59689a5fcdf
477c25d297e41d602ed
          Message-Authenticator Attribute (80), length: 18, Value:
 f..R..T..l..I:..
            0x0000:  66a2 9b52 2ee7 54d0 1e6c b785 493a 1080
          User-Name Attribute (1), length: 21, Value: almellonesfe
rnandez
            0x0000:  616c 6d65 6c6c 6f6e 6573 6665 726e 616e
            0x0010:  6465 7a
          User-Password Attribute (2), length: 34, Value:
            0x0000:  de30 e534 4db6 0af1 6e1d 18c8 61fc 629a
            0x0010:  babc 65da c906 437e b0b6 ba85 22d2 dd09
          NAS-IP-Address Attribute (4), length: 6, Value: almellona
esfernandez-radiusldap
            0x0000:  7f00 0101
          NAS-Port Attribute (5), length: 6, Value: 0
            0x0000:  0000 0000
12:26:53.573144 lo    In  IP (tos 0x0, ttl 64, id 41155, offset 0,a
 flags [none], proto UDP (17), length 133)
    localhost.59679 > localhost.radius: [bad udp cksum 0xfe84 -> 0
xd7ad!] RADIUS, length: 105
        Access-Request (1), id: 0x14, Authenticator: 2d59689a5fcdf
477c25d297e41d602ed
          Message-Authenticator Attribute (80), length: 18, Value:
 f..R..T..l..I:..
            0x0000:  66a2 9b52 2ee7 54d0 1e6c b785 493a 1080
          User-Name Attribute (1), length: 21, Value: almellonesfe
```

```
almellonesfernandez@almellonesfernandez-radiusldap:~$ radtest alme
llonesfernandez almellonesfernandez 127.0.0.1 0 contraseñaincorrec
tacliente
Sent Access-Request Id 20 from 0.0.0.0:59679 to 127.0.0.1:1812 len
gth 105
        User-Name = "almellonesfernandez"
        User-Password = "almellonesfernandez"
        NAS-IP-Address = 127.0.1.1
        NAS-Port = 0
        Message-Authenticator = 0x00
        Cleartext-Password = "almellonesfernandez"
Sent Access-Request Id 20 from 0.0.0.0:59679 to 127.0.0.1:1812 len
gth 105
        User-Name = "almellonesfernandez"
        User-Password = "almellonesfernandez"
        NAS-IP-Address = 127.0.1.1
```

```
5. 192.168.1.114 (almellonesfernandez)
Re-attach  Fullscreen  Stay on top  Duplicate  Hide toolbar  Close
 from 127.0.0.1 with invalid Message-Authenticator!  (Shared secre
t is incorrect.) (from client localhost)
Waking up in 0.3 seconds.
(3) Cleaning up request packet ID 20 with timestamp +218 due to do
ne
Ready to process requests
(4) Received Access-Request Id 20 from 127.0.0.1:59679 to 127.0.0.
1:1812 length 105
Dropping packet without response because of error: Received packet
 from 127.0.0.1 with invalid Message-Authenticator!  (Shared secre
t is incorrect.) (from client localhost)
Waking up in 0.3 seconds.
(4) Cleaning up request packet ID 20 with timestamp +223 due to do
ne
Ready to process requests
```

Álvaro Almellones Fernández

INSTALACIÓN DE SERVIDOR LDAP EN LINUX. OPENLDAP

2. **(1,5 punto)** Realice la instalación del servidor OpenLDAP en el mismo servidor que FreeRadius usando el nombre del dominio XXxx.com. Evidencie.

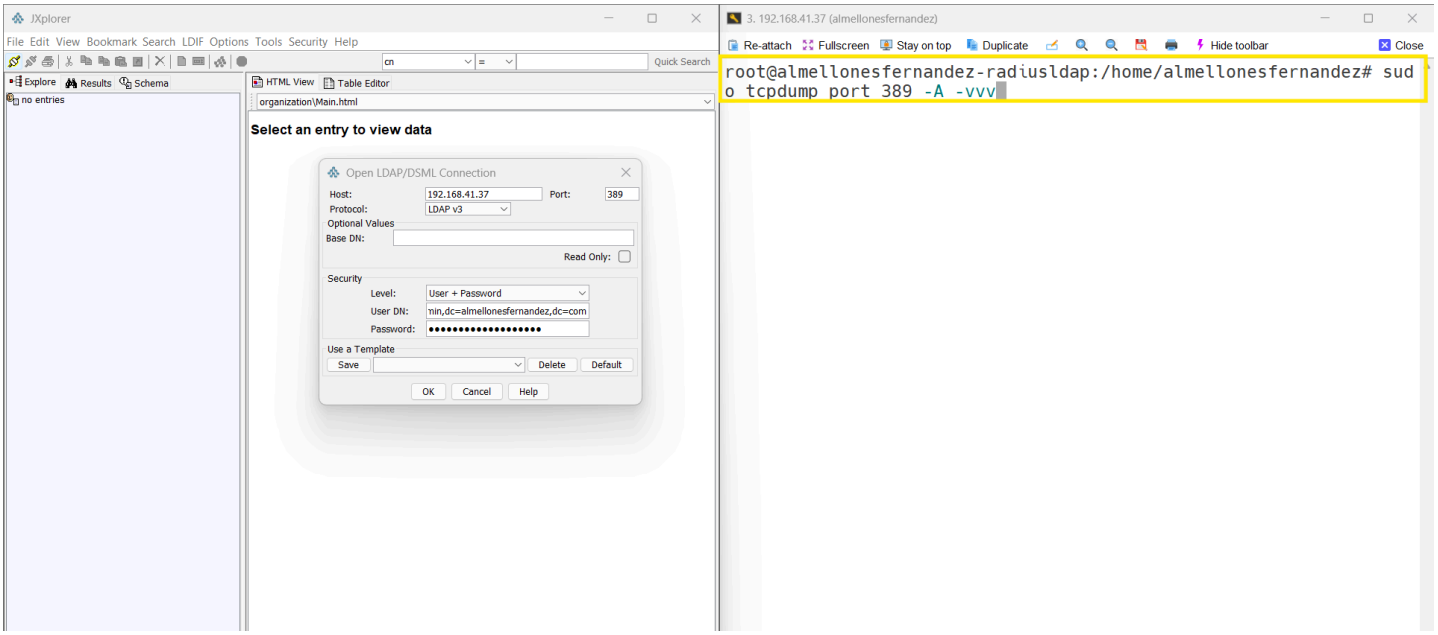
a. Servicio arrancado y comprobación de que está funcionando (systemctl, netstat, nmap)

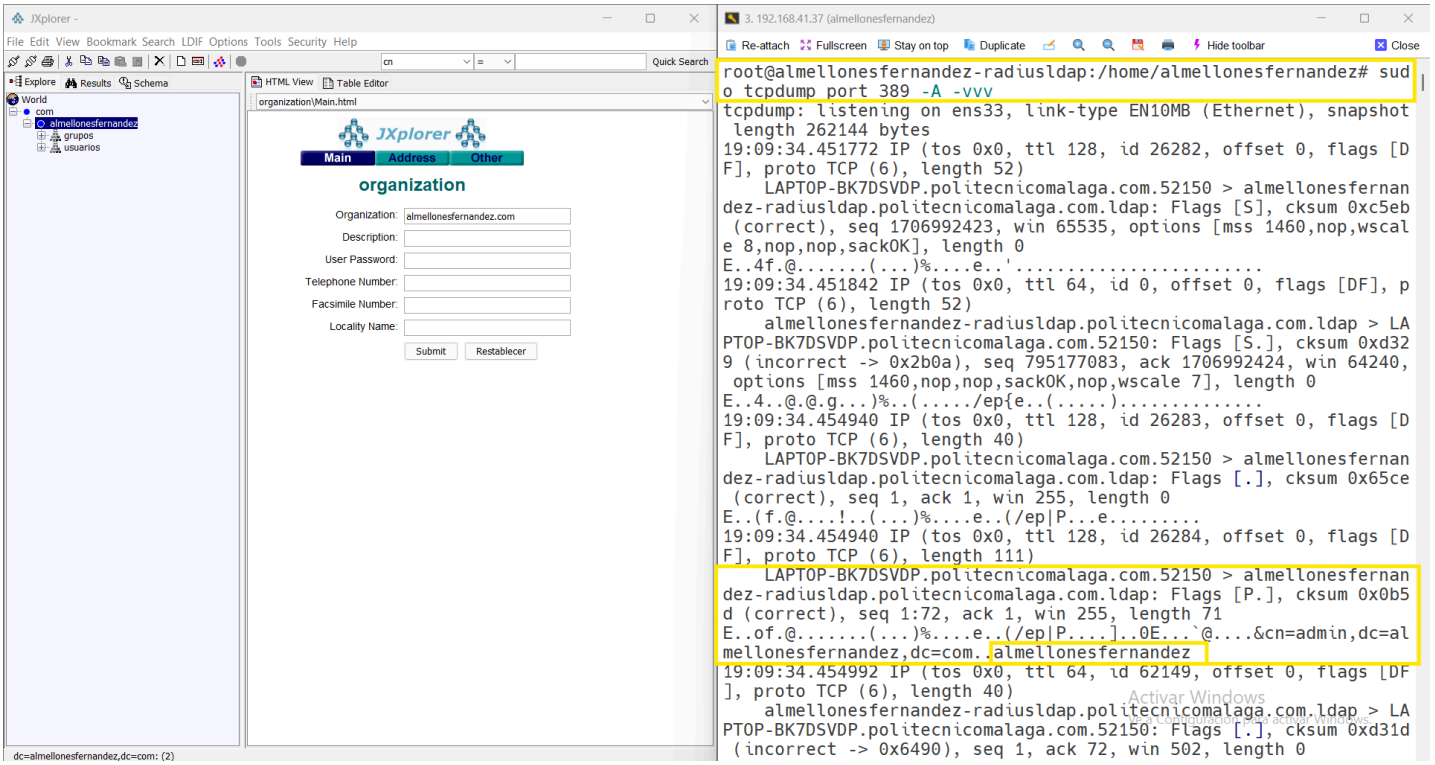
```
almellonesfernandez@almellonesfernandez-radiusldap:~$ sudo systemctl status slapd
● slapd.service - LSB: OpenLDAP standalone server (Lightweight Directory Access Protocol)
     Loaded: loaded (/etc/init.d/slapd; generated)
    Drop-In: /usr/lib/systemd/system/slapd.service.d
             └─slapd-remain-after-exit.conf
     Active: active (running) since Mon 2025-03-10 12:31:38 UTC; 1min 12s ago
       Docs: man:systemd-sysv-generator(8)
    Process: 2924 ExecStart=/etc/init.d/slapd start (code=exited, status=0/SUCCESS)
      Tasks: 3 (limit: 4552)
     Memory: 3.3M (peak: 4.3M)
        CPU: 27ms
     CGroup: /system.slice/slapd.service
             └─2931 /usr/sbin/slapd -h "ldap:/// ldapi:///" -g openldap -u openldap -F /etc/ldap/slapd.d

mar 10 12:31:38 almellonesfernandez-radiusldap systemd[1]: Starting slapd.service - LSB: OpenLDAP standalone server (Lightweight Direc>
mar 10 12:31:38 almellonesfernandez-radiusldap slapd[2924]:  * Starting OpenLDAP slapd
mar 10 12:31:38 almellonesfernandez-radiusldap slapd[2930]: @(#) $OpenLDAP: slapd 2.6.7+dfsg-1~exp1ubuntu8.2 (Dec  9 2024 02:50:18) $
                                                            Ubuntu Developers <ubuntu-devel-discuss@lists.ubuntu.com>
mar 10 12:31:38 almellonesfernandez-radiusldap slapd[2931]: slapd starting
mar 10 12:31:38 almellonesfernandez-radiusldap slapd[2924]:    ...done.
mar 10 12:31:38 almellonesfernandez-radiusldap systemd[1]: Started slapd.service - LSB: OpenLDAP standalone server (Lightweight Direct>
lines 1-20/20 (END)
```

```
almellonesfernandez@almellonesfernandez-radiusldap:~$ sudo netstat -putan | grep slapd
tcp        0      0 0.0.0.0:389             0.0.0.0:*               LISTEN      2931/slapd
tcp6       0      0 :::389                  :::*                    LISTEN      2931/slapd
almellonesfernandez@almellonesfernandez-radiusldap:~$ sudo nmap -p 389 127.0.0.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-10 12:34 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000053s latency).

PORT    STATE SERVICE
389/tcp open  ldap

Nmap done: 1 IP address (1 host up) scanned in 0.05 seconds
almellonesfernandez@almellonesfernandez-radiusldap:~$
```

b. Conexión mediante cliente JXPLORER en Windows, evidencia de conexión establecida y captura con el comando tcpdump que puede capturar usuario y contraseña en texto plano (ldap no seguro).

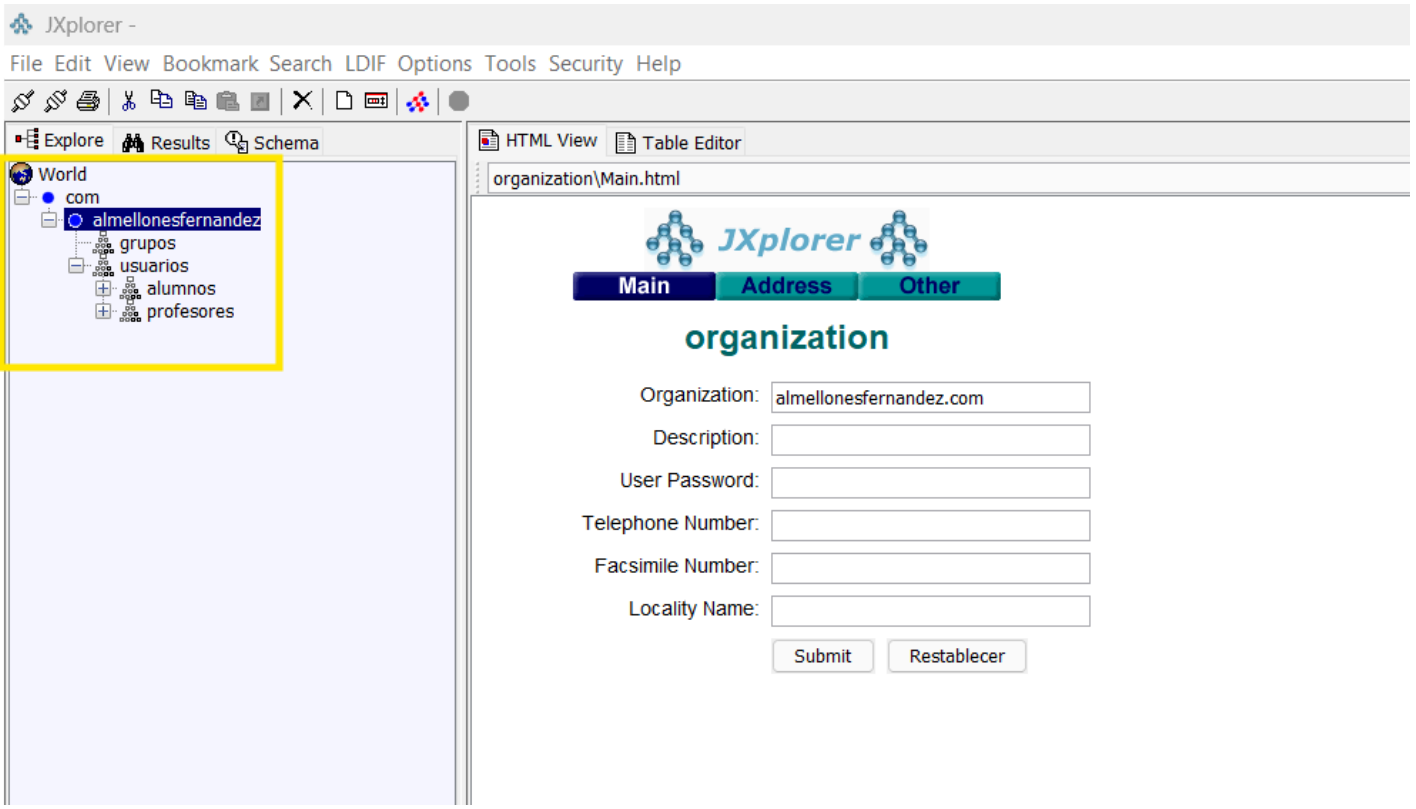
Álvaro Almellones Fernández





c.(fichero-ou.ldif) Añada una estructura mínima con cuatro unidades organizativas (usuarios, usuarios/alumnos, usuarios/profesores y grupos) mediante comando ldapadd. Compruebe mediante cliente GUI en Microsoft Windows SOFTERRA LDAP BROWSER.

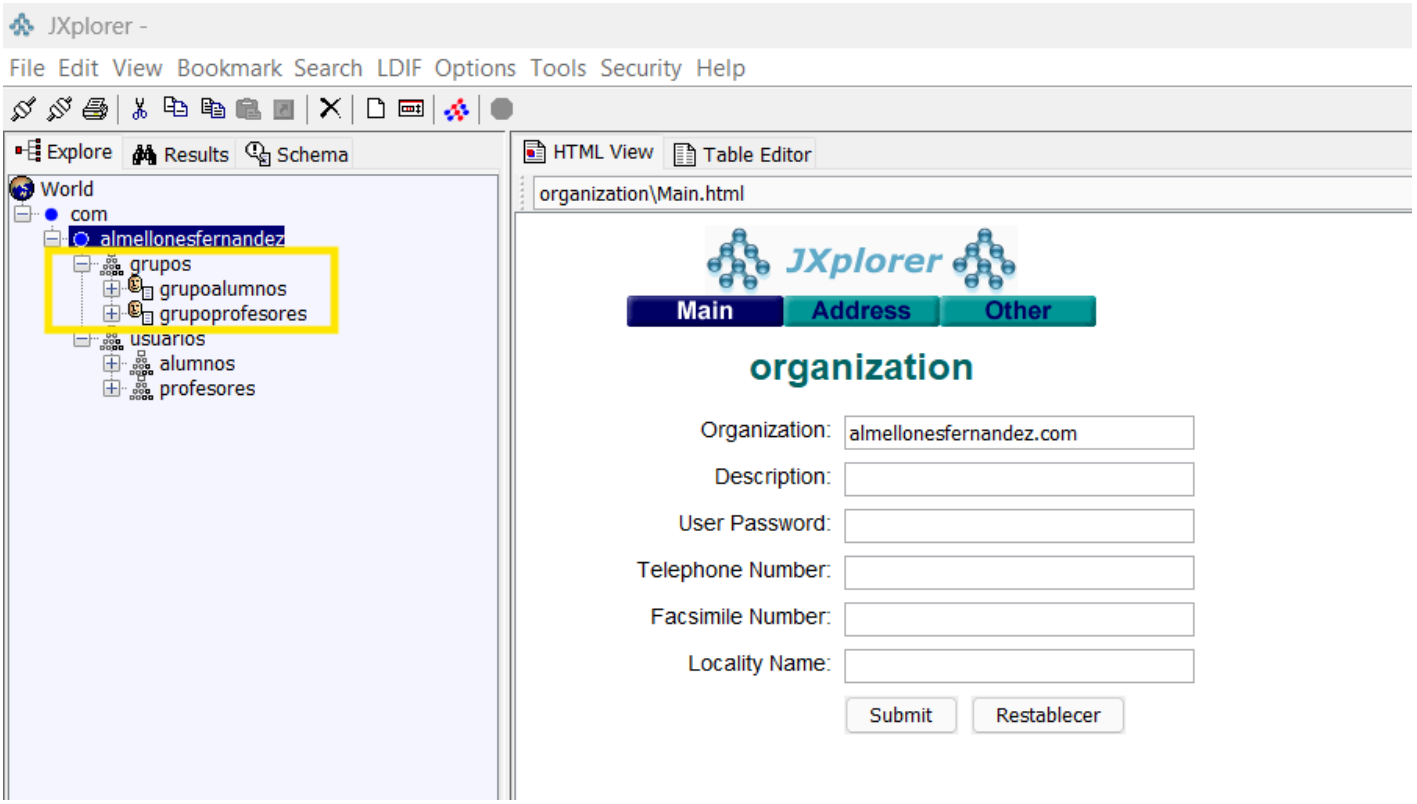
```
root@almellonesfernandez-radiusldap:~/scripts# cat ou.ldif
dn: ou=usuarios,dc=almellonesfernandez,dc=com
objectClass: organizationalUnit
ou: usuarios

dn: ou=alumnos,ou=usuarios,dc=almellonesfernandez,dc=com
objectClass: organizationalUnit
ou: alumnos

dn: ou=profesores,ou=usuarios,dc=almellonesfernandez,dc=com
objectClass: organizationalUnit
ou: profesores

dn: ou=grupos,dc=almellonesfernandez,dc=com
objectClass: organizationalUnit
ou: grupos
root@almellonesfernandez-radiusldap:~/scripts# ldapadd -x -D "cn=admin,dc=almellonesfernandez,dc=com" -W -f ou.ldif
Enter LDAP Password:
adding new entry "ou=usuarios,dc=almellonesfernandez,dc=com"

adding new entry "ou=alumnos,ou=usuarios,dc=almellonesfernandez,dc=com"

adding new entry "ou=profesores,ou=usuarios,dc=almellonesfernandez,dc=com"

adding new entry "ou=grupos,dc=almellonesfernandez,dc=com"

root@almellonesfernandez-radiusldap:~/scripts#
```



d. (fichero-grupos.ldif) Añada dos grupos de LINUX en la unidad organizativa grupos con los nombres grupoalumnos y grupoprofesores (adapte GID) mediante comando ldapadd. Compruebe mediante JXPLORER.

Álvaro Almellones Fernández

```
root@almellonesfernandez-radiusldap:~/scripts# cat grupos.ldif
dn: cn=grupoalumnos,ou=grupos,dc=almellonesfernandez,dc=com
objectClass: posixGroup
cn: grupoalumnos
gidNumber: 1001

dn: cn=grupoprofesores,ou=grupos,dc=almellonesfernandez,dc=com
objectClass: posixGroup
cn: grupoprofesores
gidNumber: 1002
root@almellonesfernandez-radiusldap:~/scripts# ldapadd -x -D "cn=admin,dc=almellonesfernandez,dc=com" -W -f grupos.ldi
f
Enter LDAP Password:
adding new entry "cn=grupoalumnos,ou=grupos,dc=almellonesfernandez,dc=com"

adding new entry "cn=grupoprofesores,ou=grupos,dc=almellonesfernandez,dc=com"

root@almellonesfernandez-radiusldap:~/scripts#
```



e. (fichero-usuarios.ldif) Añada 2 usuarios con uid profesorXXxx y alumnoXxxx con las siguientes características:

i. En su correspondiente unidad organizativa (usuarios/alumnos, usuarios/profesores)

ii. Que tenga Shell

iii. Con directorio de trabajo (/home/profesorXXxx, /home/alumnoXXxx)

iv. Con contraseña en formato SSHA (use comando slappasswd)

v. Adapte UID y GID (según sea profesor o alumno).

Álvaro Almellones Fernández

```
root@almellonesfernandez-radiusldap:~/scripts# cat usuarios.ldif
dn: uid=profesormelerolopez,ou=profesores,ou=usuarios,dc=almellonesfernandez,dc=com
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: top
uid: profesormelerolopez
cn: Profesor Melero Lopez
sn: Melero Lopez
userPassword: {SSHA}cChh4hhvjx1uTWwdafNjzgj8NePw/sbn
loginShell: /bin/bash
homeDirectory: /home/profesormelerolopez
uidNumber: 2001
gidNumber: 1002

dn: uid=alumnoalmellonesfernandez,ou=alumnos,ou=usuarios,dc=almellonesfernandez,dc=com
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: top
uid: alumnoalmellonesfernandez
cn: Alumno Almellones Fernandez
sn: Almellones Fernandez
userPassword: {SSHA}cChh4hhvjx1uTWwdafNjzgj8NePw/sbn
loginShell: /bin/bash
homeDirectory: /home/alumnoalmellonesfernandez
uidNumber: 2002
gidNumber: 1001
root@almellonesfernandez-radiusldap:~/scripts#
```

Evidencie:

vi. Contraseñas generadas.

```
root@almellonesfernandez-radiusldap:~/scripts# slappasswd
New password:
Re-enter new password:
{SSHA}cChh4hhvjx1uTWwdafNjzgj8NePw/sbn
root@almellonesfernandez-radiusldap:~/scripts#
```

Le he puesto la misma contraseña que uso siempre a los dos usuarios para que no se me olvide, pero si queremos generar más simplemente se vuelve a lanzar el comando y pones otra contraseña

vii. Su creación con comando ldapadd.

```
root@almellonesfernandez-radiusldap:~/scripts# ldapadd -x -D "cn=admin,dc=almellonesfernandez,dc=com" -W -f usuarios.l
dif
Enter LDAP Password:
adding new entry "uid=profesormelerolopez,ou=profesores,ou=usuarios,dc=almellonesfernandez,dc=com"

adding new entry "uid=alumnoalmellonesfernandez,ou=alumnos,ou=usuarios,dc=almellonesfernandez,dc=com"

root@almellonesfernandez-radiusldap:~/scripts#
```

viii. Uso del comando ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:///

```
root@almellonesfernandez-radiusldap:/home/almellonesfernandez# ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:///
dn: dc=almellonesfernandez,dc=com
objectClass: top
objectClass: dcObject
objectClass: organization
o: almellonesfernandez.com
dc: almellonesfernandez

dn: ou=grupos,dc=almellonesfernandez,dc=com
objectClass: organizationalUnit
ou: grupos

dn: ou=usuarios,dc=almellonesfernandez,dc=com
objectClass: organizationalUnit
ou: usuarios

dn: cn=grupoalumnos,ou=grupos,dc=almellonesfernandez,dc=com
objectClass: posixGroup
cn: grupoalumnos
gidNumber: 1001

dn: cn=grupoprofesores,ou=grupos,dc=almellonesfernandez,dc=com
objectClass: posixGroup
cn: grupoprofesores
gidNumber: 1002

dn: ou=alumnos,ou=usuarios,dc=almellonesfernandez,dc=com
objectClass: organizationalUnit
ou: alumnos

dn: ou=profesores,ou=usuarios,dc=almellonesfernandez,dc=com
objectClass: organizationalUnit
ou: profesores

dn: uid=alumnoalmellonesfernandez,ou=alumnos,ou=usuarios,dc=almellonesfernande
 z,dc=com
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: top
uid: alumnoalmellonesfernandez
cn: Alumno Almellones Fernandez
sn: Almellones Fernandez
loginShell: /bin/bash
homeDirectory: /home/alumnoalmellonesfernandez
uidNumber: 2002
gidNumber: 1001

dn: uid=profesormelerolopez,ou=profesores,ou=usuarios,dc=almellonesfernandez,d
 c=com
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: top
uid: profesormelerolopez
cn: Profesor Melero Lopez
sn: Melero Lopez
loginShell: /bin/bash
homeDirectory: /home/profesormelerolopez
uidNumber: 2001
gidNumber: 1002

root@almellonesfernandez-radiusldap:/etc#
```

ix. Uso del comando ldapsearch -x -H ldap://127.0.0.1 -b dc=XXxx,dc=com

Álvaro Almellones Fernández

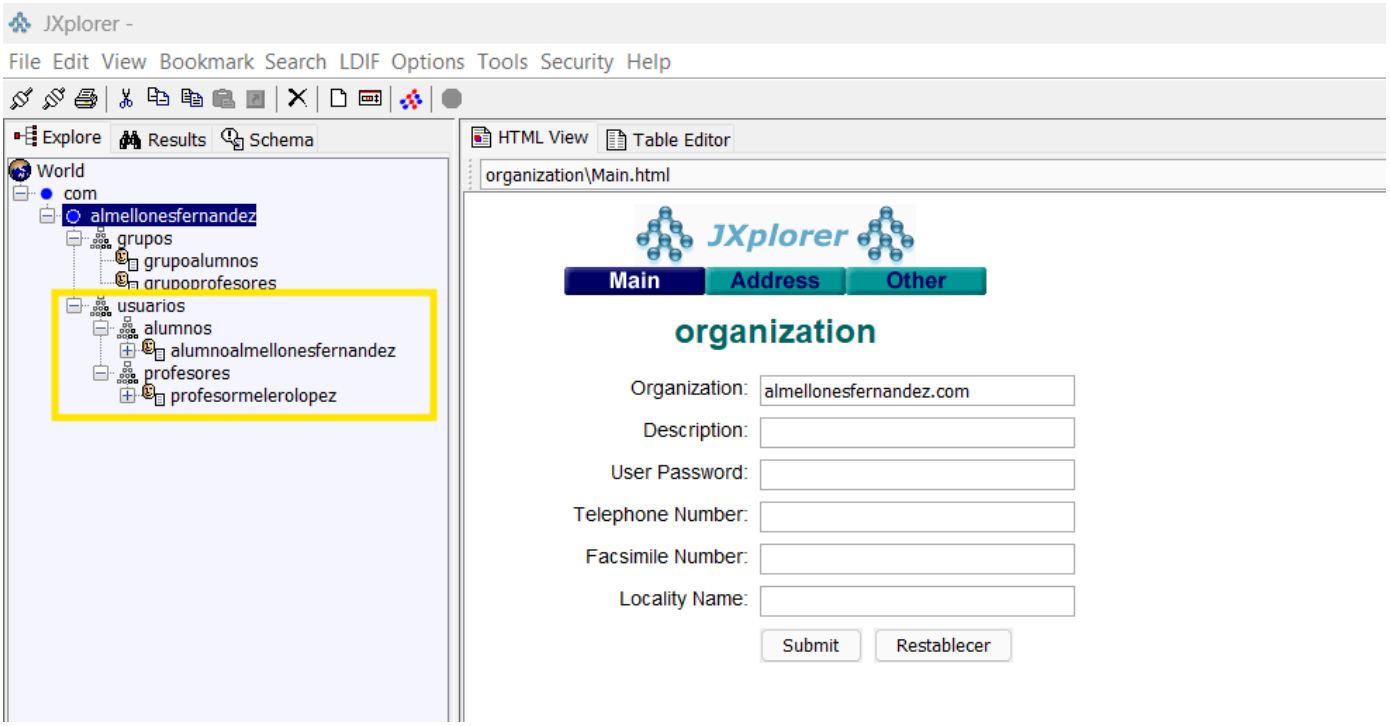
```
root@almellonesfernandez-radiusldap:~/scripts# ldapsearch -x -H ldap://127.0.0.1 -b dc=almellonesfernandez,dc=com
# extended LDIF
#
# LDAPv3
# base <dc=almellonesfernandez,dc=com> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# almellonesfernandez.com
dn: dc=almellonesfernandez,dc=com
objectClass: top
objectClass: dcObject
objectClass: organization
o: almellonesfernandez.com
dc: almellonesfernandez

# grupos, almellonesfernandez.com
dn: ou=grupos,dc=almellonesfernandez,dc=com
objectClass: organizationalUnit
ou: grupos

# usuarios, almellonesfernandez.com
dn: ou=usuarios,dc=almellonesfernandez,dc=com
objectClass: organizationalUnit
ou: usuarios

# grupoalumnos, grupos, almellonesfernandez.com
dn: cn=grupoalumnos,ou=grupos,dc=almellonesfernandez,dc=com
objectClass: posixGroup
cn: grupoalumnos
gidNumber: 1001
```



```
# grupoprofesores, grupos, almellonesfernandez.com
dn: cn=grupoprofesores,ou=grupos,dc=almellonesfernandez,dc=com
objectClass: posixGroup
cn: grupoprofesores
gidNumber: 1002

# alumnos, usuarios, almellonesfernandez.com
dn: ou=alumnos,ou=usuarios,dc=almellonesfernandez,dc=com
objectClass: organizationalUnit
ou: alumnos

# profesores, usuarios, almellonesfernandez.com
dn: ou=profesores,ou=usuarios,dc=almellonesfernandez,dc=com
objectClass: organizationalUnit
ou: profesores

# alumnoalmellonesfernandez, alumnos, usuarios, almellonesfernandez.com
dn: uid=alumnoalmellonesfernandez,ou=alumnos,ou=usuarios,dc=almellonesfernande
 z,dc=com
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: top
uid: alumnoalmellonesfernandez
cn: Alumno Almellones Fernandez
sn: Almellones Fernandez
loginShell: /bin/bash
homeDirectory: /home/alumnoalmellonesfernandez
uidNumber: 2002
gidNumber: 1001
```

```
# profesormelerolopez, profesores, usuarios, almellonesfernandez.com
dn: uid=profesormelerolopez,ou=profesores,ou=usuarios,dc=almellonesfernandez,d
 c=com
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: top
uid: profesormelerolopez
cn: Profesor Melero Lopez
sn: Melero Lopez
loginShell: /bin/bash
homeDirectory: /home/profesormelerolopez
uidNumber: 2001
gidNumber: 1002

# search result
search: 2
result: 0 Success

# numResponses: 10
# numEntries: 9
root@almellonesfernandez-radiusldap:~/scripts#
```

x. JXPLORER y la estructura de los diferentes usuarios creada tal y como aparece en el enunciado.



Álvaro Almellones Fernández

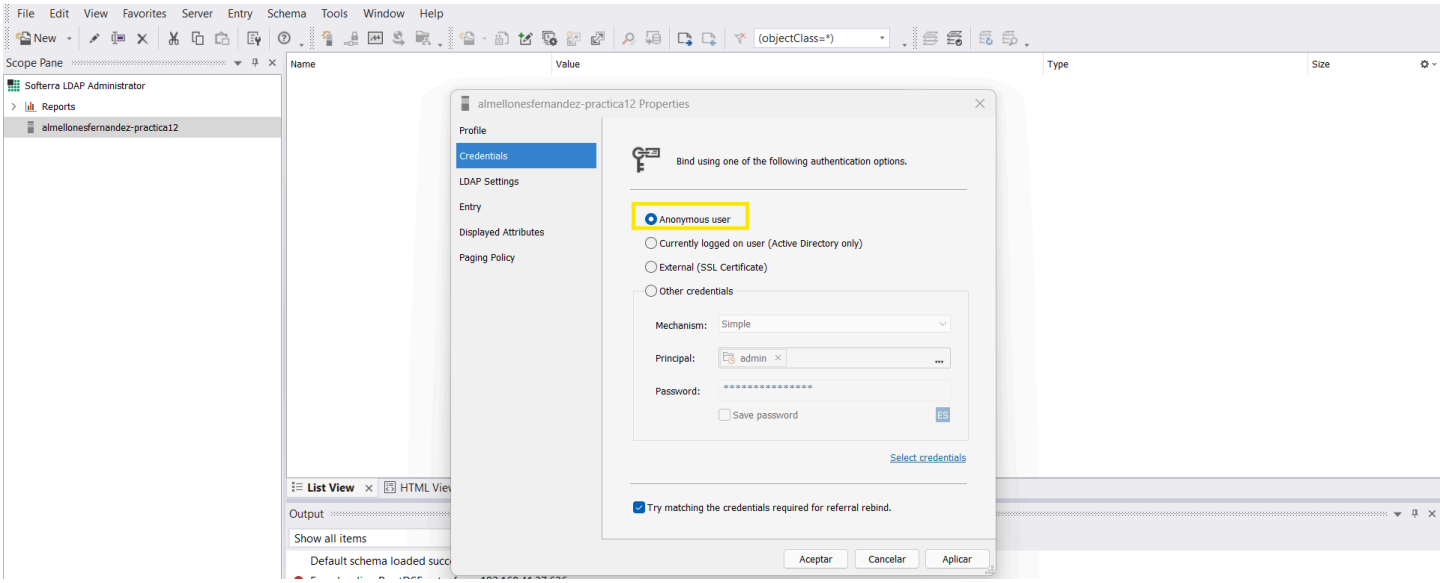
CONFIGURACIÓN SERVIDOR LDAP SEGURO (LDAPS)

3. **(1 punto)** Realice la configuración del servidor OpenLDAP para que la conexiones sean cifradas (puerto 636) usando para ello use el certificado autogenerado por nuestra CA en prácticas anteriores o creando uno para esta práctica (ldap.crt y ldap.key). Se debe evidenciar:

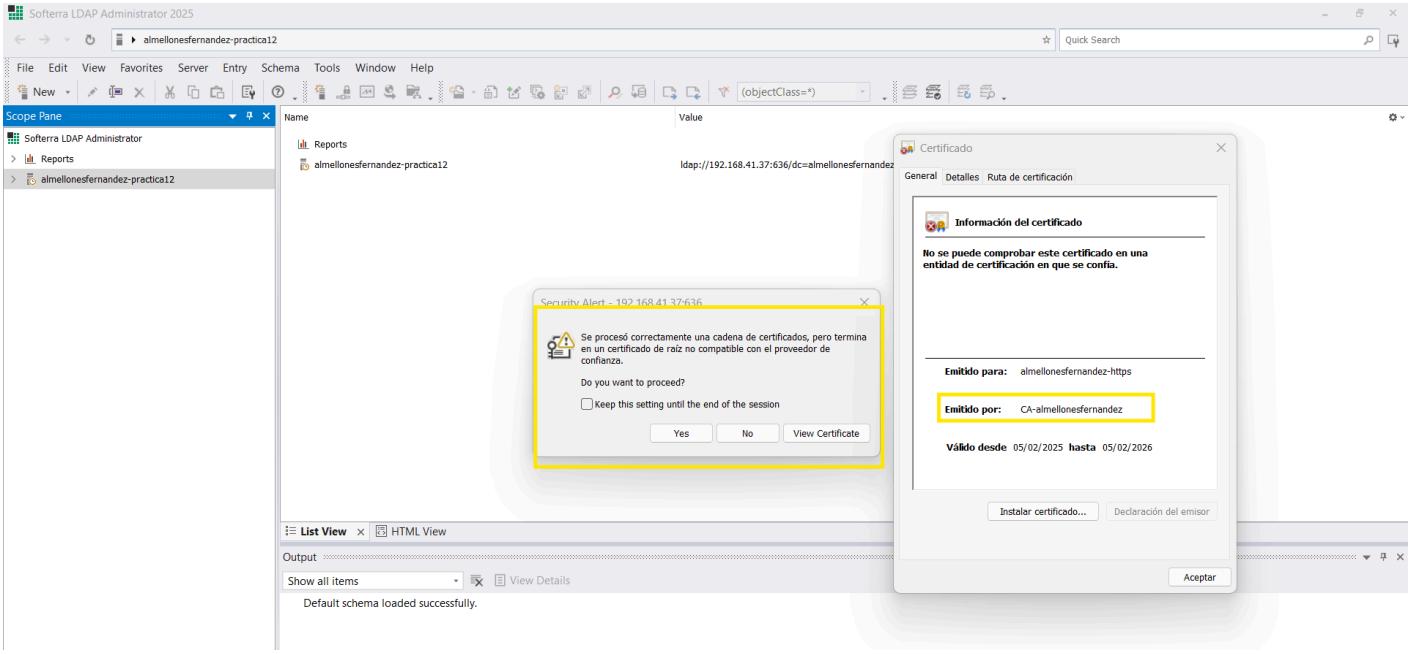
a. Netstat, ss, tcpdump e iptraf.

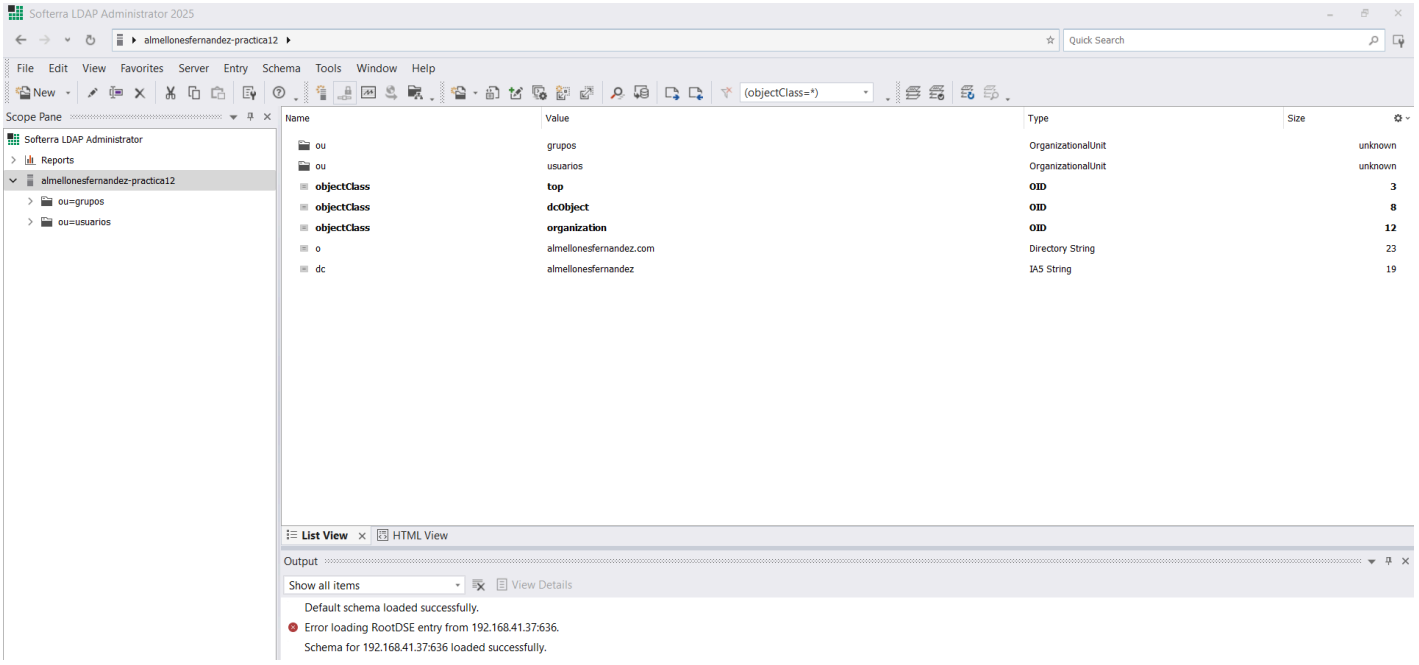
```
root@almellonesfernandez-radiusldap:/etc/default# sudo netstat -putan | grep slapd
tcp        0      0 0.0.0.0:389             0.0.0.0:*               LISTEN      1789/slapd
tcp        0      0 0.0.0.0:636             0.0.0.0:*               LISTEN      1789/slapd
tcp6       0      0 :::389                  :::*                    LISTEN      1789/slapd
tcp6       0      0 :::636                  :::*                    LISTEN      1789/slapd
root@almellonesfernandez-radiusldap:/etc/default#
```

b. Conexión con Softerra LDAP Browser de forma anónima y SSL+user+password por el puerto 636. Demostrar que te solicita descargar la llave pública y comprobar donde se guarda (mostrar información de ese certificado en el software).

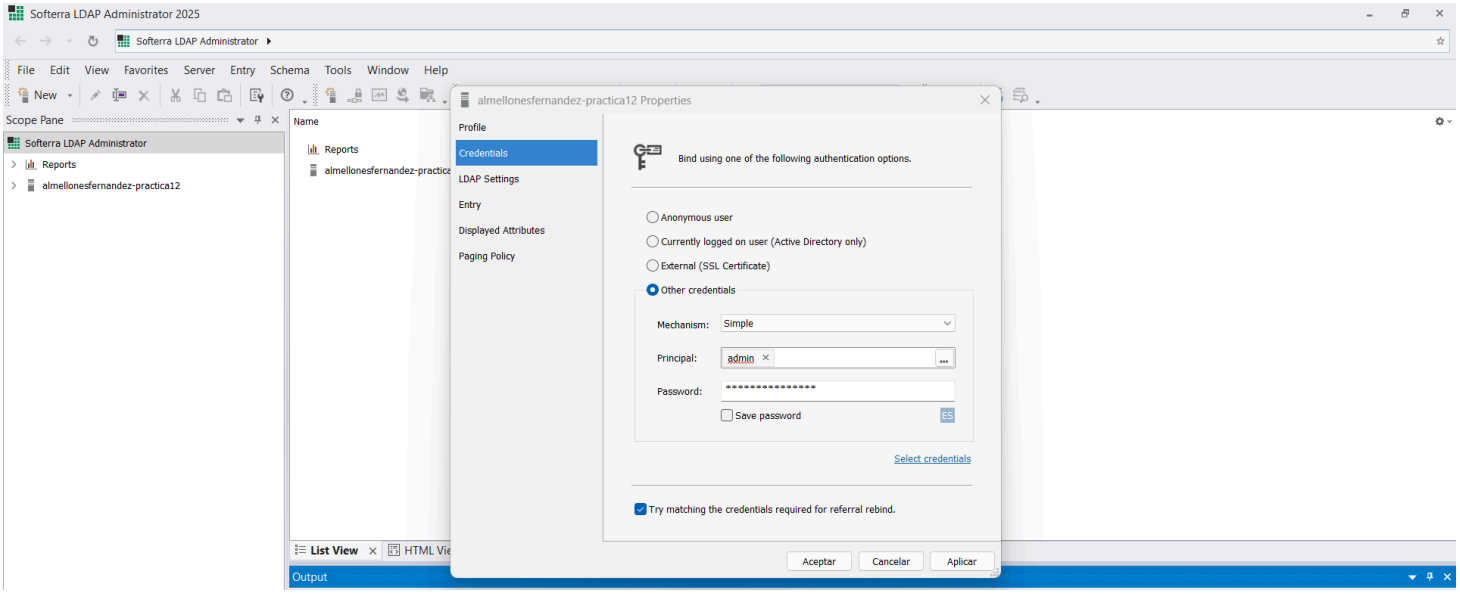


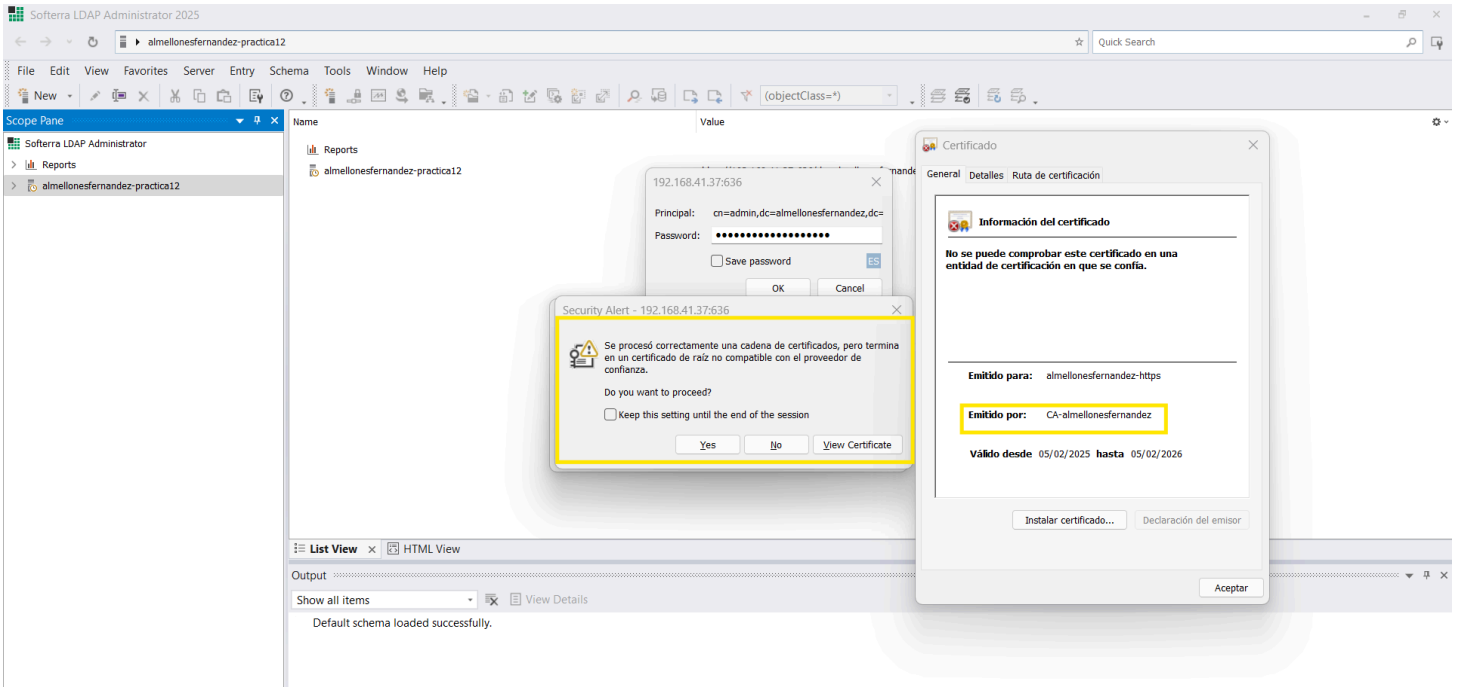
Álvaro Almellones Fernández



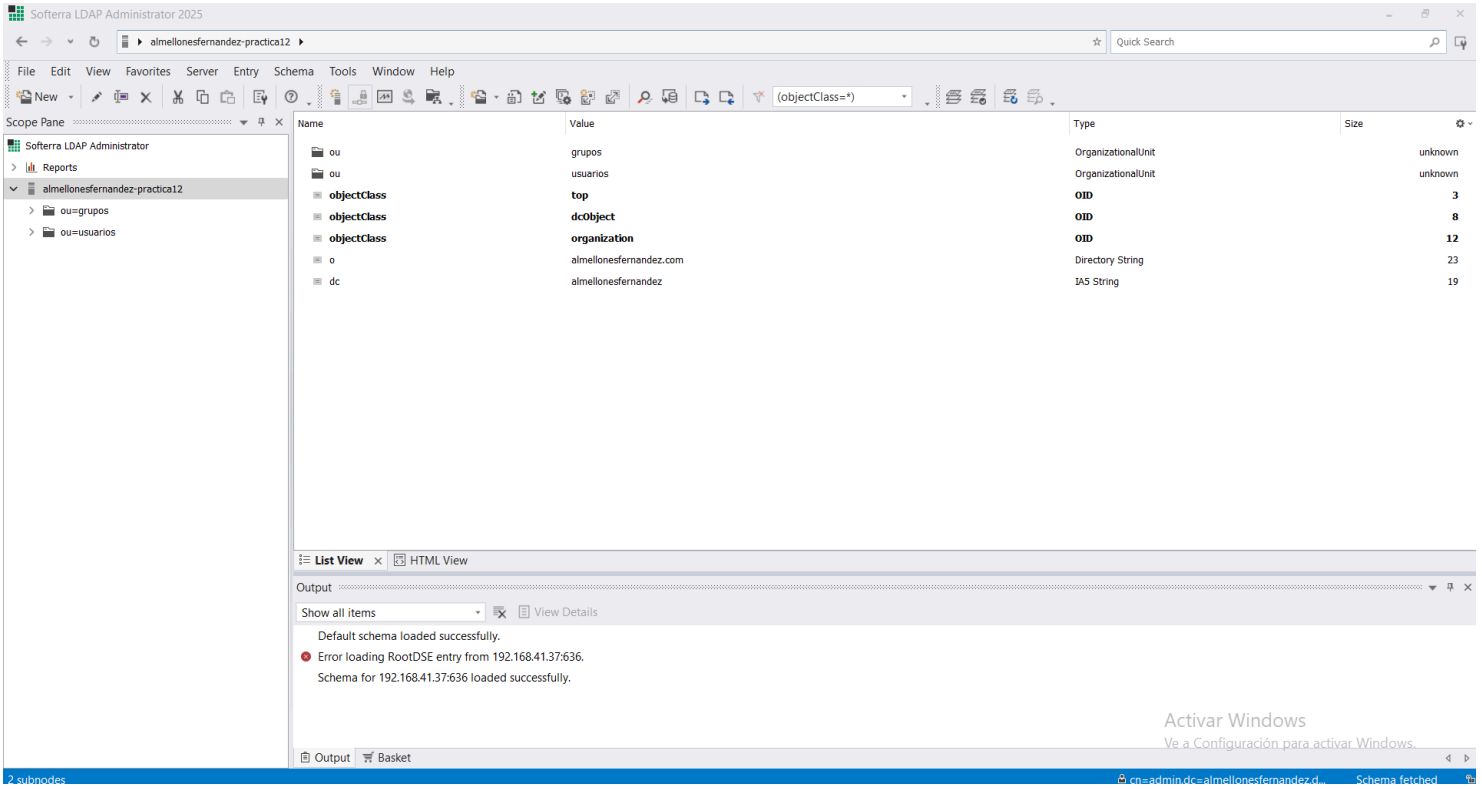


Álvaro Almellones Fernández





Álvaro Almellones Fernández




```
root@almellonesfernandez-radiusldap:/home/almellonesfernandez# netstat -putan | grep slapd
tcp        0      0 0.0.0.0:636             0.0.0.0:*               LISTEN      1179/slapd
tcp        0      0 0.0.0.0:389             0.0.0.0:*               LISTEN      1179/slapd
tcp        0      0 192.168.41.37:636       192.168.40.141:52356    ESTABLISHED 1179/slapd
tcp6       0      0 :::636                  :::*                    LISTEN      1179/slapd
tcp6       0      0 :::389                  :::*                    LISTEN      1179/slapd
root@almellonesfernandez-radiusldap:/home/almellonesfernandez#
```

c. No es posible capturar la información de conexión con usuario cn=admin, al realizar la conexión (SSL+user+password) de forma segura.

```
root@almellonesfernandez-radiusldap:/home/almellonesfernandez# sudo tcpdump port 636 -A -vvv
tcpdump: listening on ens33, link-type EN10MB (Ethernet), snapshot length 262144 bytes
18:46:12.065511 IP (tos 0x0, ttl 128, id 1809, offset 0, flags [DF], proto TCP (6), length 52)
    LAPTOP-BK7DSVDP.politecnicomalaga.com.52036 > 192.168.1.114.ldaps: Flags [S], cksum 0x3988 (correct), seq 11941614
82, win 65535, options [mss 1460,nop,wscale 8,nop,nop,sackOK], length 0
E..4..@...Hc..(....r.D.|G-uJ........9.............
18:46:13.072579 IP (tos 0x0, ttl 128, id 1810, offset 0, flags [DF], proto TCP (6), length 52)
    LAPTOP-BK7DSVDP.politecnicomalaga.com.52036 > 192.168.1.114.ldaps: Flags [S], cksum 0x3988 (correct), seq 11941614
82, win 65535, options [mss 1460,nop,wscale 8,nop,nop,sackOK], length 0
E..4..@...Hb..(....r.D.|G-uJ........9.............
18:46:15.077171 IP (tos 0x0, ttl 128, id 1811, offset 0, flags [DF], proto TCP (6), length 52)
    LAPTOP-BK7DSVDP.politecnicomalaga.com.52036 > 192.168.1.114.ldaps: Flags [S], cksum 0x3988 (correct), seq 11941614
82, win 65535, options [mss 1460,nop,wscale 8,nop,nop,sackOK], length 0
E..4..@...Ha..(....r.D.|G-uJ........9.............
18:46:19.080981 IP (tos 0x0, ttl 128, id 1812, offset 0, flags [DF], proto TCP (6), length 52)
    LAPTOP-BK7DSVDP.politecnicomalaga.com.52036 > 192.168.1.114.ldaps: Flags [S], cksum 0x3988 (correct), seq 11941614
82, win 65535, options [mss 1460,nop,wscale 8,nop,nop,sackOK], length 0
E..4..@...H`..(....r.D.|G-uJ........9.............
18:46:27.087059 IP (tos 0x0, ttl 128, id 1813, offset 0, flags [DF], proto TCP (6), length 52)
    LAPTOP-BK7DSVDP.politecnicomalaga.com.52036 > 192.168.1.114.ldaps: Flags [S], cksum 0x3988 (correct), seq 11941614
82, win 65535, options [mss 1460,nop,wscale 8,nop,nop,sackOK], length 0
E..4..@...H_..(....r.D.|G-uJ........9.............
18:46:33.111650 IP (tos 0x0, ttl 128, id 1814, offset 0, flags [DF], proto TCP (6), length 52)
    LAPTOP-BK7DSVDP.politecnicomalaga.com.52040 > 192.168.1.114.ldaps: Flags [S], cksum 0xa5f4 (correct), seq 39984952
2, win 65535, options [mss 1460,nop,wscale 8,nop,nop,sackOK], length 0
E..4..@...H^..(....r.H.|..82.....................
18:46:34.127001 IP (tos 0x0, ttl 128, id 1815, offset 0, flags [DF], proto TCP (6), length 52)
```

```
E..4..@.@.....)...)%.H.|.....zh.....@......
.3....8.
18:47:46.002014 IP (tos 0x0, ttl 64, id 40992, offset 0, flags [DF], proto TCP (6), length 569)
    ldapradiuscova.politecnicomalaga.com.39240 > almellonesfernandez-radiusldap.politecnicomalaga.com.ldaps: Flags [P.
], cksum 0x592e (correct), seq 1:518, ack 1, win 502, options [nop,nop,TS val 2503208089 ecr 3872930024], length 517
E..9. @.@.....)...)%.H.|.....zh.....Y......
.3....8............#}.u. ..j....\.<..{.p....(..... 8K....8s...]U.)..+N.#       ...U{xm.y.........3.9.5./.,.0........
...........].a.W.S.+./.............\.`.V.R.$.(.k.j.s.w.....#.'.g.@.r.v.....
...8.....       ...2.E.D.......Q.......P.=...<.....A..............
.........................#.............*.(...........   .
.............................+.........-.....3.&.$... ........sN,.....$.......:.1..X.b.................................
.....................................................................................................
18:47:46.002054 IP (tos 0x0, ttl 64, id 32650, offset 0, flags [DF], proto TCP (6), length 52)
    almellonesfernandez-radiusldap.politecnicomalaga.com.ldaps > ldapradiuscova.politecnicomalaga.com.39240: Flags [.]
, cksum 0xd3ab (incorrect -> 0x3ec8), seq 1, ack 518, win 506, options [nop,nop,TS val 3872930025 ecr 2503208089], len
gth 0
E..4..@.@.....)%..)..|.H.zh.................
..8..3..
18:47:46.002271 IP (tos 0x0, ttl 64, id 32651, offset 0, flags [DF], proto TCP (6), length 179)
    almellonesfernandez-radiusldap.politecnicomalaga.com.ldaps > ldapradiuscova.politecnicomalaga.com.39240: Flags [P.
], cksum 0xd42a (incorrect -> 0xd4bf), seq 1:128, ack 518, win 506, options [nop,nop,TS val 3872930026 ecr 2503208089]
, length 127
E.....@.@..4..)%..)..|.H.zh..........*.....
..8..3......z...v......n ~...s..p(a-..)..|.@....... 8K....8s...]U.)..+N.#       ...U{xm.y.......3.$... .*ZV#egh....1=@
...'+\b1).6.....B.+....
```

d. Deshabilite ahora que se pueda loguear mediante LDAP no seguro (389) pero si funcione mediante LDAP seguro (636). Deje al final que se puedan permitir la conexión con LDAP y LDAPS.

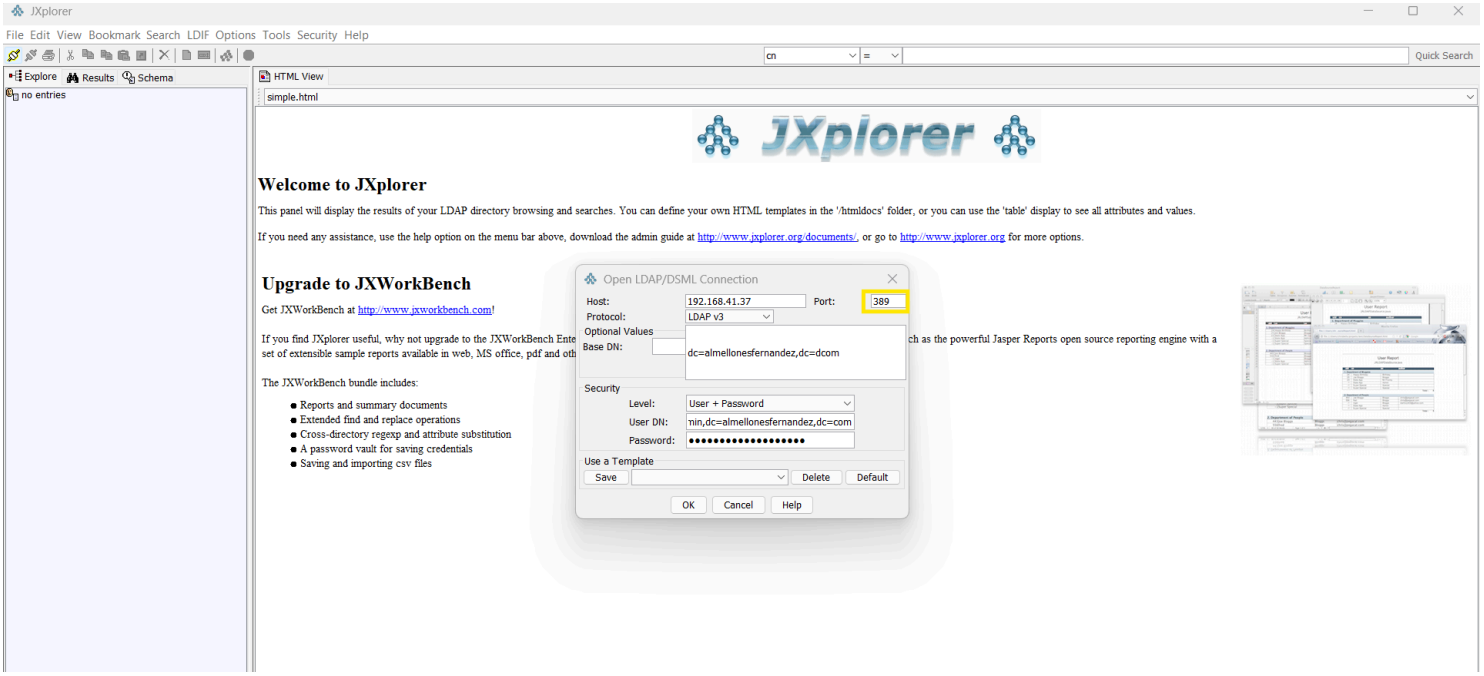
```
root@almellonesfernandez-radiusldap:/home/almellonesfernandez# netstat -putan | grep 389
tcp        0      0 0.0.0.0:389             0.0.0.0:*               LISTEN      1179/slapd
tcp6       0      0 :::389                  :::*                    LISTEN      1179/slapd
root@almellonesfernandez-radiusldap:/home/almellonesfernandez# nano /etc/default/slapd
root@almellonesfernandez-radiusldap:/home/almellonesfernandez# systemctl restart slapd
root@almellonesfernandez-radiusldap:/home/almellonesfernandez# netstat -putan | grep 389
root@almellonesfernandez-radiusldap:/home/almellonesfernandez#
```

Álvaro Almellones Fernández

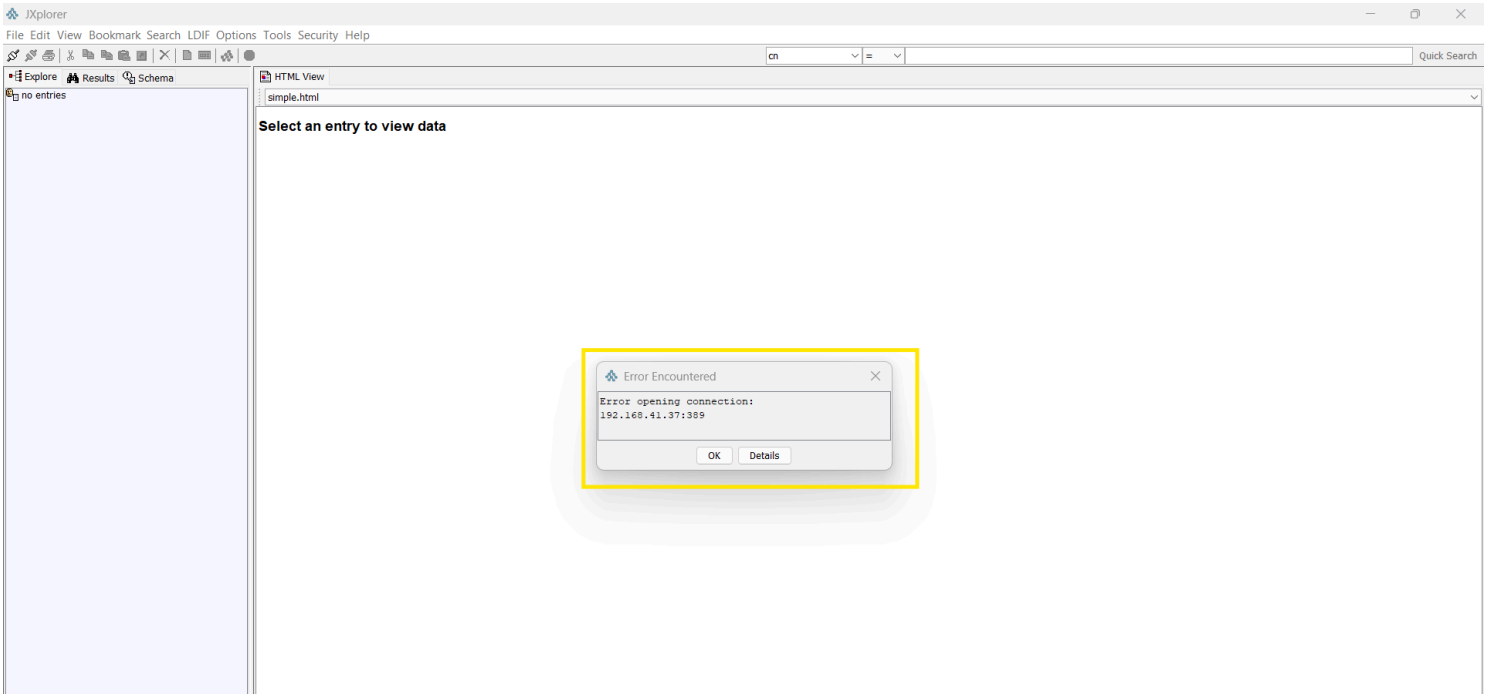
```
  GNU nano 7.2                                    /etc/default/slapd
# Default location of the slapd.conf file or slapd.d cn=config directory. If
# empty, use the compiled-in default (/etc/ldap/slapd.d with a fallback to
# /etc/ldap/slapd.conf).
SLAPD_CONF=

# System account to run the slapd server under. If empty the server
# will run as root.
SLAPD_USER="openldap"

# System group to run the slapd server under. If empty the server will
# run in the primary group of its user.
SLAPD_GROUP="openldap"

# Path to the pid file of the slapd server. If not set the init.d script
# will try to figure it out from $SLAPD_CONF (/etc/ldap/slapd.d by
# default)
SLAPD_PIDFILE=

# slapd normally serves ldap only on all TCP-ports 389. slapd can also
# service requests on TCP-port 636 (ldaps) and requests via unix
# sockets.
# Example usage:
# SLAPD_SERVICES="ldap://127.0.0.1:389/ ldaps:/// ldapi:///"
SLAPD_SERVICES=" ldapi:/// ldaps:///"

# If SLAPD_NO_START is set, the init script will not start or restart
# slapd (but stop will still work).  Uncomment this if you are
# starting slapd via some other means or if you don't want slapd normally
# started at boot.
#SLAPD_NO_START=1

# If SLAPD_SENTINEL_FILE is set to path to a file and that file exists,
```

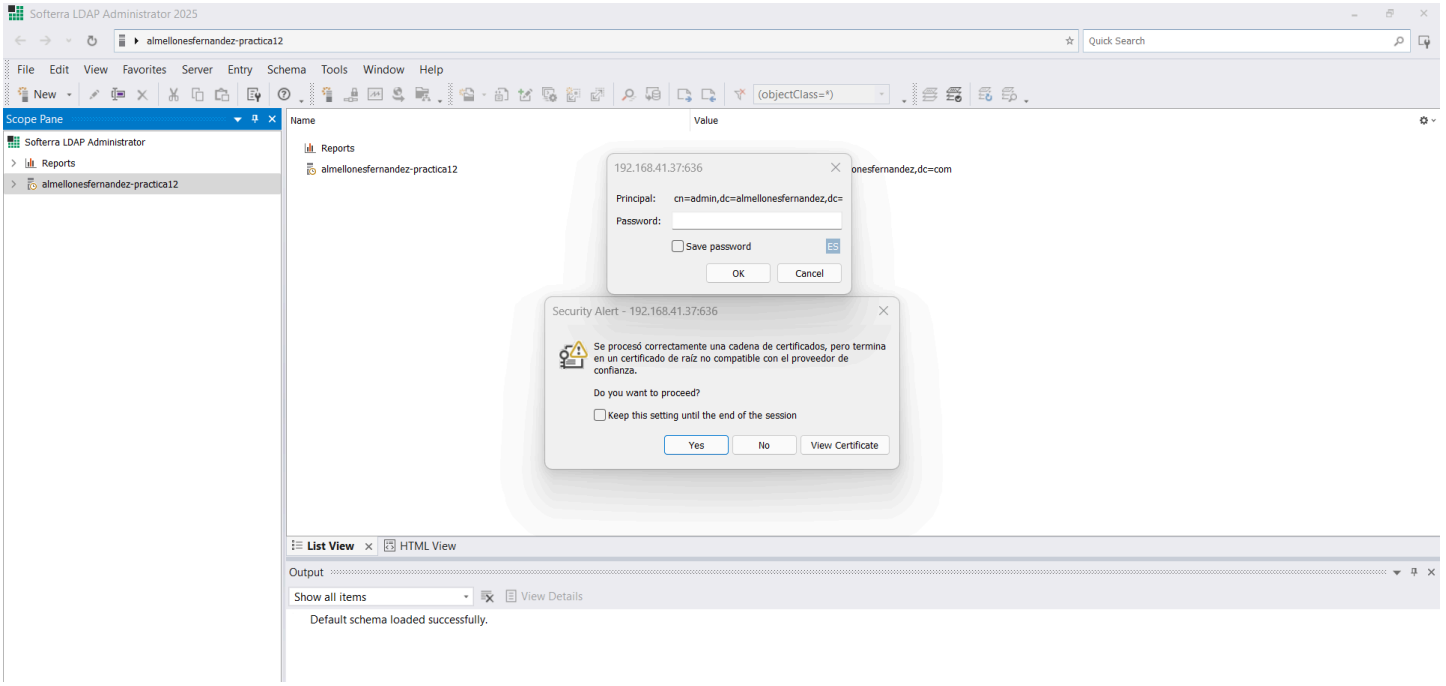
Elimino ldap:/// de SLAPD_SERVICE para deshabilitar ldap de forma no segura

```
root@almellonesfernandez-radiusldap:/home/almellonesfernandez# netstat -putan | grep 389
root@almellonesfernandez-radiusldap:/home/almellonesfernandez# netstat -putan | grep 636
tcp        0      0 0.0.0.0:636             0.0.0.0:*               LISTEN      1818/slapd
tcp6       0      0 :::636                  :::*                    LISTEN      1818/slapd
root@almellonesfernandez-radiusldap:/home/almellonesfernandez#
```

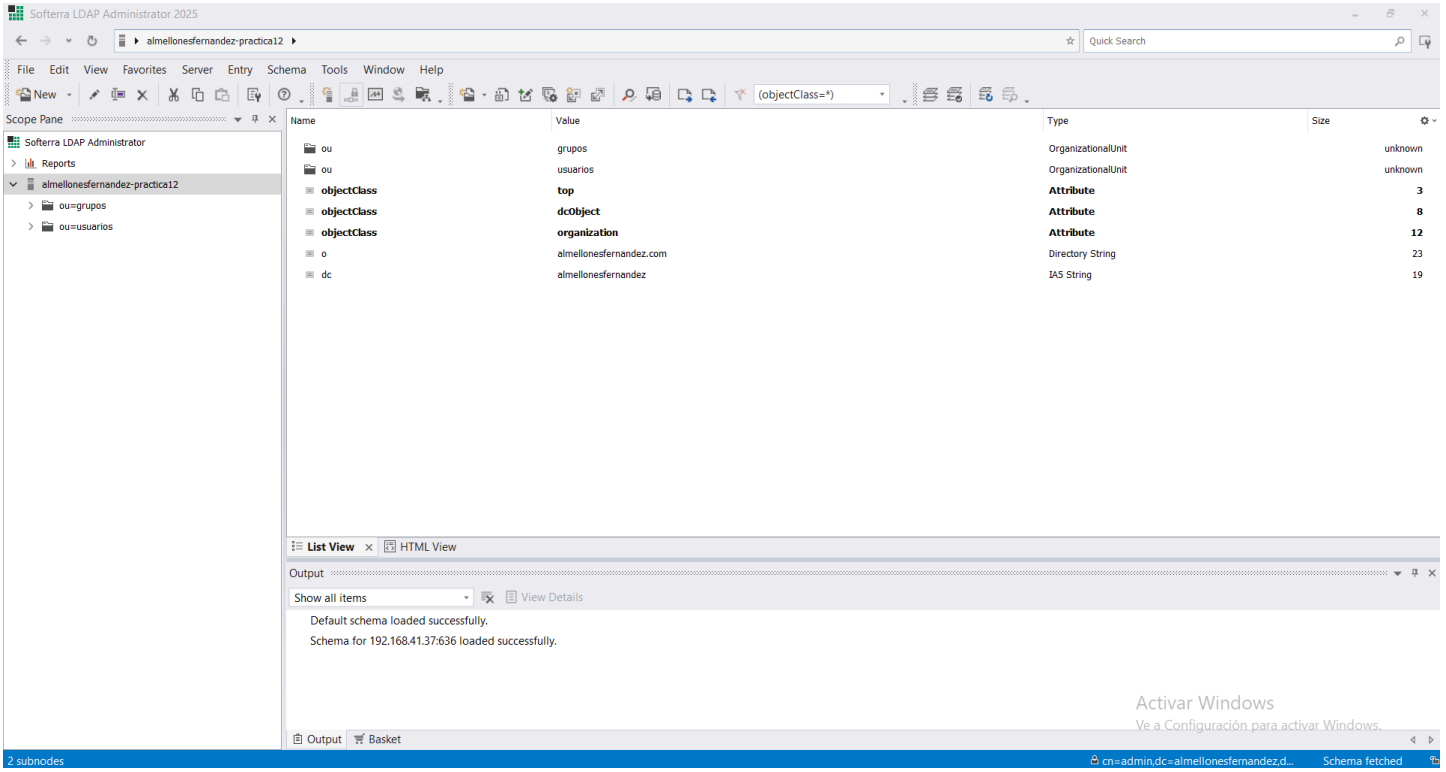


Álvaro Almellones Fernández





Álvaro Almellones Fernández




```
root@almellonesfernandez-radiusldap:/home/almellonesfernandez# netstat -putan | grep slapd
tcp        0      0 0.0.0.0:636             0.0.0.0:*               LISTEN      1818/slapd
tcp        0      0 192.168.41.37:636       192.168.40.141:52744    ESTABLISHED 1818/slapd
tcp6       0      0 :::636                  :::*                    LISTEN      1818/slapd
root@almellonesfernandez-radiusldap:/home/almellonesfernandez#
```

NO USAR JXPLORER ya que tiene problemas con SSL.

Álvaro Almellones Fernández

AUTENTIFICACIÓN EN FREERADIUS A TRAVÉS DE SERVIDOR OPENLDAP

4. **(1,5 punto)** Realice la integración de FreeRadius con el servidor OpenLDAP (inicialmente 389). Se debe evidenciar:

a. Configuración realizada en servidor FreeRadius inicialmente con puerto 389 para la integración.

```
  GNU nano 7.2                                  /etc/freeradius/3.0/mods-available/ldap
#
ldap {
        #  Note that this needs to match the name(s) in the LDAP server
        #  certificate, if you're using ldaps.  See OpenLDAP documentation
        #  for the behavioral semantics of specifying more than one host.
        #
        #  Depending on the libldap in use, server may be an LDAP URI.
        #  In the case of OpenLDAP this allows additional the following
        #  additional schemes:
        #  - ldaps:// (LDAP over SSL)
        #  - ldapi:// (LDAP over Unix socket)
        #  - ldapc:// (Connectionless LDAP)
        server = 'localhost'
#       server = 'ldap.rrdns.example.org'
#       server = 'ldap.rrdns.example.org'

        #  Port to connect on, defaults to 389, will be ignored for LDAP URIs.
        port = 389

        #  Administrator account for searching and possibly modifying.
        #  If using SASL + KRB5 these should be commented out.
#       identity = 'cn=admin,dc=example,dc=org'
        identity = 'cn=admin,dc=almellonesfernandez,dc=com'
#       password = mypass
        password = almellonesfernandez

        #  Unless overridden in another section, the dn from which all
        #  searches will start from.
        base_dn = 'dc=almellonesfernandez,dc=com'

        #
        #  You can run the 'ldapsearch' command line tool using the
```

```
  GNU nano 7.2                                  /etc/freeradius/3.0/sites-enabled/default
        #  Read the 'users' file.  In v3, this is located in
        #  raddb/mods-config/files/authorize
        files

        #
        #  Look in an SQL database.  The schema of the database
        #  is meant to mirror the "users" file.
        #
        #  See "Authorization Queries" in mods-available/sql
        -sql

        #
        #  If you are using /etc/smbpasswd, and are also doing
        #  mschap authentication, the un-comment this line, and
        #  configure the 'smbpasswd' module.
#       smbpasswd

        #
        #  The ldap module reads passwords from the LDAP database.
        ldap

        #
```

Álvaro Almellones Fernández

```
 GNU nano 7.2                                /etc/freeradius/3.0/sites-enabled/default

        #  Uncomment it if you want to use ldap for authentication
        #
        #  Note that this means "check plain-text password against
        #  the ldap database", which means that EAP won't work,
        #  as it does not supply a plain-text password.
        #
        #  We do NOT recommend using this.  LDAP servers are databases.
        #  They are NOT authentication servers.  FreeRADIUS is an
        #  authentication server, and knows what to do with authentication.
        #  LDAP servers do not.
        #
        #  However, it is necessary for Active Directory, because
        #  Active Directory won't give the passwords to FreeRADIUS.
        #
        Auth-Type LDAP {
                ldap
        }
```

b. Haciendo uso del arranque de freeradius con la opción -X y del comando radtest, realice las siguientes comprobaciones.

• Prueba de funcionamiento en modo local con usuario alumnoXXxx y contraseña correctamente.

```
almellonesfernandez@almellonesfernandez-radiusldap ~$ radtest alumnoalmellonesfernandez almellonesfernandez localhost
0 testing123
Sent Access-Request Id 126 from 0.0.0.0:33856 to 127.0.0.1:1812 length 111
        User-Name = "alumnoalmellonesfernandez"
        User-Password = "almellonesfernandez"
        NAS-IP-Address = 127.0.1.1
        NAS-Port = 0
        Message-Authenticator = 0x00
        Cleartext-Password = "almellonesfernandez"
Received Access-Accept Id 126 from 127.0.0.1:1812 to 127.0.0.1:33856 length 38
        Message-Authenticator = 0x2631eb4317654fa1651136a22436475a
```

```
(0)     [logintime] = noop
(0) pap: Converted: &control:Password-With-Header -> &control:SSHA1-Password
(0) pap: Removing &control:Password-With-Header
(0) pap: Normalizing SSHA1-Password from base64 encoding, 32 bytes -> 24 bytes
(0)     [pap] = updated
(0)   } # authorize = updated
(0) Found Auth-Type = PAP
(0) # Executing group from file /etc/freeradius/3.0/sites-enabled/default
(0)   Auth-Type PAP {
(0) pap: Login attempt with password
(0) pap: Comparing with "known-good" SSHA-Password
(0) pap: User authenticated successfully
(0)     [pap] = ok
(0)   } # Auth-Type PAP = ok
(0) # Executing section post-auth from file /etc/freeradius/3.0/sites-enabled/default
(0)   post-auth {
(0)     if (session-state:User-Name && reply:User-Name && request:User-Name && (reply:User-Name == request:User-Name))
 {
(0)     if (session-state:User-Name && reply:User-Name && request:User-Name && (reply:User-Name == request:User-Name))
  -> FALSE
(0)     update {
(0)       No attributes updated for RHS &session-state:
(0)     } # update = noop
(0)     [exec] = noop
(0)     policy remove_reply_message_if_eap {
(0)       if (&reply:EAP-Message && &reply:Reply-Message) {
(0)       if (&reply:EAP-Message && &reply:Reply-Message)  -> FALSE
(0)       else {
(0)         [noop] = noop
(0)       } # else = noop
(0)     } # policy remove_reply_message_if_eap = noop
(0)     if (EAP-Key-Name && &reply:EAP-Session-Id) {
(0)     if (EAP-Key-Name && &reply:EAP-Session-Id)  -> FALSE
(0)   } # post-auth = noop
(0) Sent Access-Accept Id 126 from 127.0.0.1:1812 to 127.0.0.1:33856 length 38
(0) Finished request
```


• Apague el servidor Openldap y realice prueba de funcionamiento en modo local con usuario (alumnoXXxx) y contraseña correctamente. ¿Qué ocurre ahora?

Álvaro Almellones Fernández

```
almellonesfernandez@almellonesfernandez-radiusldap:~$ radtest alumnoalmellonesfernandez almellonesfernandez localhost
0 testing123
Sent Access-Request Id 126 from 0.0.0.0:33856 to 127.0.0.1:1812 length 111
        User-Name = "alumnoalmellonesfernandez"
        User-Password = "almellonesfernandez"
        NAS-IP-Address = 127.0.1.1
        NAS-Port = 0
        Message-Authenticator = 0x00
        Cleartext-Password = "almellonesfernandez"
Received Access-Accept Id 126 from 127.0.0.1:1812 to 127.0.0.1:33856 length 38
        Message-Authenticator = 0x2631eb4317654fa1651136a22436475a
almellonesfernandez@almellonesfernandez-radiusldap:~$ sudo systemctl stop slapd
almellonesfernandez@almellonesfernandez-radiusldap:~$ radtest alumnoalmellonesfernandez almellonesfernandez localhost
0 testing123
Sent Access-Request Id 114 from 0.0.0.0:47163 to 127.0.0.1:1812 length 111
        User-Name = "alumnoalmellonesfernandez"
        User-Password = "almellonesfernandez"
        NAS-IP-Address = 127.0.1.1
        NAS-Port = 0
        Message-Authenticator = 0x00
        Cleartext-Password = "almellonesfernandez"
Received Access-Reject Id 114 from 127.0.0.1:1812 to 127.0.0.1:47163 length 38
        Message-Authenticator = 0x0cb6450662a0e26a2c0e947ede2ecdb8
(0) -: Expected Access-Accept got Access-Reject
almellonesfernandez@almellonesfernandez-radiusldap:~$
```

```
(1) ldap: Waiting for search result...
ber_get_next failed, errno=0.
rlm_ldap (ldap): Reconnecting (5)
rlm_ldap (ldap): Connecting to ldap://localhost:389
rlm_ldap (ldap): Bind with cn=admin,dc=almellonesfernandez,dc=com to ldap://localhost:389 failed: Can't contact LDAP s
erver
rlm_ldap (ldap): Closing connection (5) - Failed to reconnect
rlm_ldap (ldap): Failed to reconnect (5), no free connections are available
(1) ldap: ERROR: Failed performing search: Can't contact LDAP server
(1)     [ldap] = fail
(1)   } # authorize = fail
(1) Using Post-Auth-Type Reject
(1) # Executing group from file /etc/freeradius/3.0/sites-enabled/default
(1)   Post-Auth-Type REJECT {
(1) attr_filter.access_reject: EXPAND %{User-Name}
(1) attr_filter.access_reject:    --> alumnoalmellonesfernandez
(1) attr_filter.access_reject: Matched entry DEFAULT at line 11
(1)     [attr_filter.access_reject] = updated
(1)     [eap] = noop
(1)     policy remove_reply_message_if_eap {
(1)       if (&reply:EAP-Message && &reply:Reply-Message) {
(1)       if (&reply:EAP-Message && &reply:Reply-Message)  -> FALSE
(1)       else {
(1)         [noop] = noop
(1)       } # else = noop
(1)     } # policy remove_reply_message_if_eap = noop
(1)   } # Post-Auth-Type REJECT = updated
(1) Delaying response for 1.000000 seconds
Waking up in 0.3 seconds.
Waking up in 0.6 seconds.
(1) Sending delayed response
(1) Sent Access-Reject Id 114 from 127.0.0.1:1812 to 127.0.0.1:47163 length 38
Waking up in 3.9 seconds.
(1) Cleaning up request packet ID 114 with timestamp +75 due to cleanup_delay was reached
Ready to process requests
```


Al detener OpenLDAP nos rechaza el acceso ya que freeradius no puede preguntarle a ldap por los usuarios que tiene

• Evidencia de conexionado en modo local con usuario alumnoXXxx y contraseña incorrectamente.

Álvaro Almellones Fernández

```
almellonesfernandez@almellonesfernandez-radiusldap:~$ radtest alumnoalmellonesfernandez almellonesfernandez localhost 0 testing123
Sent Access-Request Id 188 from 0.0.0.0:51655 to 127.0.0.1:1812 length 111
        User-Name = "alumnoalmellonesfernandez"
        User-Password = "almellonesfernandez"
        NAS-IP-Address = 127.0.1.1
        NAS-Port = 0
        Message-Authenticator = 0x00
        Cleartext-Password = "almellonesfernandez"
Received Access-Accept Id 188 from 127.0.0.1:1812 to 127.0.0.1:51655 length 38
        Message-Authenticator = 0x8590158e91aa29b42da50fbb49d0ca2e
almellonesfernandez@almellonesfernandez-radiusldap:~$ radtest alumnoalmellonesfernandez contraseñaincorrecta localhost 0 testing123
Sent Access-Request Id 223 from 0.0.0.0:55040 to 127.0.0.1:1812 length 111
        User-Name = "alumnoalmellonesfernandez"
        User-Password = "contraseñaincorrecta"
        NAS-IP-Address = 127.0.1.1
        NAS-Port = 0
        Message-Authenticator = 0x00
        Cleartext-Password = "contraseñaincorrecta"
Received Access-Reject Id 223 from 127.0.0.1:1812 to 127.0.0.1:55040 length 38
        Message-Authenticator = 0x540b2a20cb2504ec5431fe3033370e5d
(0) -: Expected Access-Accept got Access-Reject
almellonesfernandez@almellonesfernandez-radiusldap:~$
```

• Evidencia de conexionado en modo local con usuario profesorXXxx y contraseña incorrectamente.

```
almellonesfernandez@almellonesfernandez-radiusldap:~$ radtest profesormelerolopez almellonesfernandez localhost 0 testing123
Sent Access-Request Id 175 from 0.0.0.0:57498 to 127.0.0.1:1812 length 105
        User-Name = "profesormelerolopez"
        User-Password = "almellonesfernandez"
        NAS-IP-Address = 127.0.1.1
        NAS-Port = 0
        Message-Authenticator = 0x00
        Cleartext-Password = "almellonesfernandez"
Received Access-Accept Id 175 from 127.0.0.1:1812 to 127.0.0.1:57498 length 38
        Message-Authenticator = 0x7540b9c98bcf52ae2886864d9deb73e3
almellonesfernandez@almellonesfernandez-radiusldap:~$ radtest profesormelerolopez contraseñaincorrecta localhost 0 testing123
Sent Access-Request Id 84 from 0.0.0.0:35570 to 127.0.0.1:1812 length 105
        User-Name = "profesormelerolopez"
        User-Password = "contraseñaincorrecta"
        NAS-IP-Address = 127.0.1.1
        NAS-Port = 0
        Message-Authenticator = 0x00
        Cleartext-Password = "contraseñaincorrecta"
Received Access-Reject Id 84 from 127.0.0.1:1812 to 127.0.0.1:35570 length 38
        Message-Authenticator = 0xd4ac6810bb6985f8150f03681cb3dcde
(0) -: Expected Access-Accept got Access-Reject
almellonesfernandez@almellonesfernandez-radiusldap:~$
```

c. Configuración realizada en servidor FreeRadius inicialmente con puerto 636

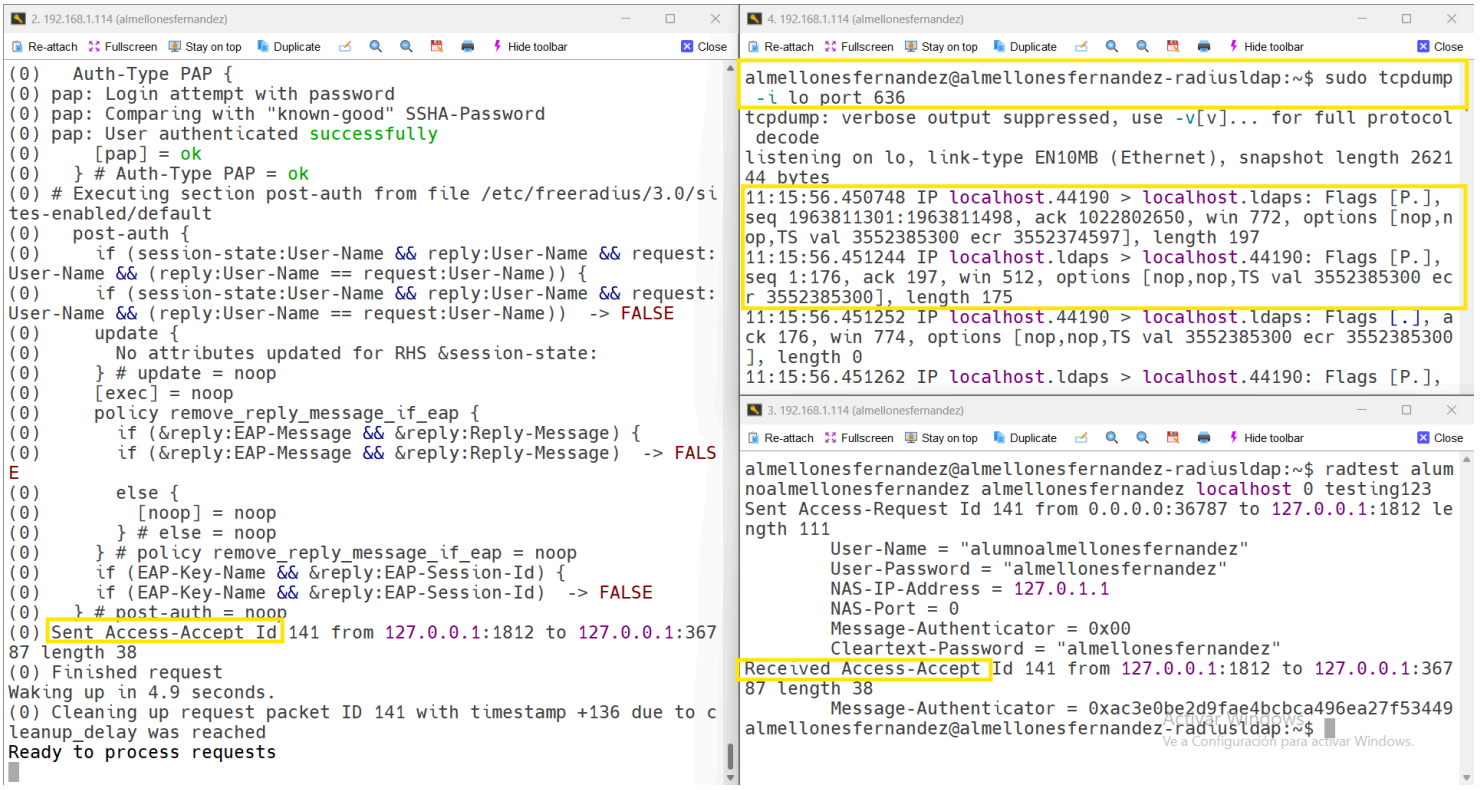
```
 GNU nano 7.2                          /etc/freeradius/3.0/mods-available/ldap
# -*- text -*-
#
#  $Id: d5838ffa01a880fdb516159d9a289d9578acffd8 $

#
#  Lightweight Directory Access Protocol (LDAP)
#
ldap {
        #  Note that this needs to match the name(s) in the LDAP server
        #  certificate, if you're using ldaps.  See OpenLDAP documentation
        #  for the behavioral semantics of specifying more than one host.
        #
        #  Depending on the libldap in use, server may be an LDAP URI.
        #  In the case of OpenLDAP this allows additional the following
        #  additional schemes:
        #  - ldaps:// (LDAP over SSL)
        #  - ldapi:// (LDAP over Unix socket)
        #  - ldapc:// (Connectionless LDAP)
        server = 'localhost'
#       server = 'ldap.rrdns.example.org'
#       server = 'ldap.rrdns.example.org'

        #  Port to connect on, defaults to 389, will be ignored for LDAP URIs.
#       port = 389
        port = 636

        #  Administrator account for searching and possibly modifying.
        #  If using SASL + KRB5 these should be commented out.
#       identity = 'cn=admin,dc=example,dc=org'
        identity = 'cn=admin,dc=almellonesfernandez,dc=com'
#       password = mypass
        password = almellonesfernandez
```

```
 GNU nano 7.2                          /etc/freeradius/3.0/mods-available/ldap
        #
        tls {
                # Set this to 'yes' to use TLS encrypted connections
                # to the LDAP database by using the StartTLS extended
                # operation.
                #
                # The StartTLS operation is supposed to be
                # used with normal ldap connections instead of
                # using ldaps (port 636) connections
#               start_tls = yes
#               ca_file = ${certdir}/cacert.pem
#               ca_path = ${certdir}
                ca_file = /home/almellonesfernandez/keys/ca.crt
                certificate_file = /home/almellonesfernandez/keys/almellonesfernandez-https.crt
                private_key_file = /home/almellonesfernandez/keys/almellonesfernandez-https.key
#               random_file = /dev/urandom

                #  Certificate Verification requirements.  Can be:
                #    'never' (do not even bother trying)
                #    'allow' (try, but don't fail if the certificate
                #                cannot be verified)
                #    'demand' (fail if the certificate does not verify)
                #    'hard'  (similar to 'demand' but fails if TLS
                #             cannot negotiate)
                #
                #  The default is libldap's default, which varies based
                #  on the contents of ldap.conf.
#               require_cert    = 'demand'
                require_cert    = 'allow'
```

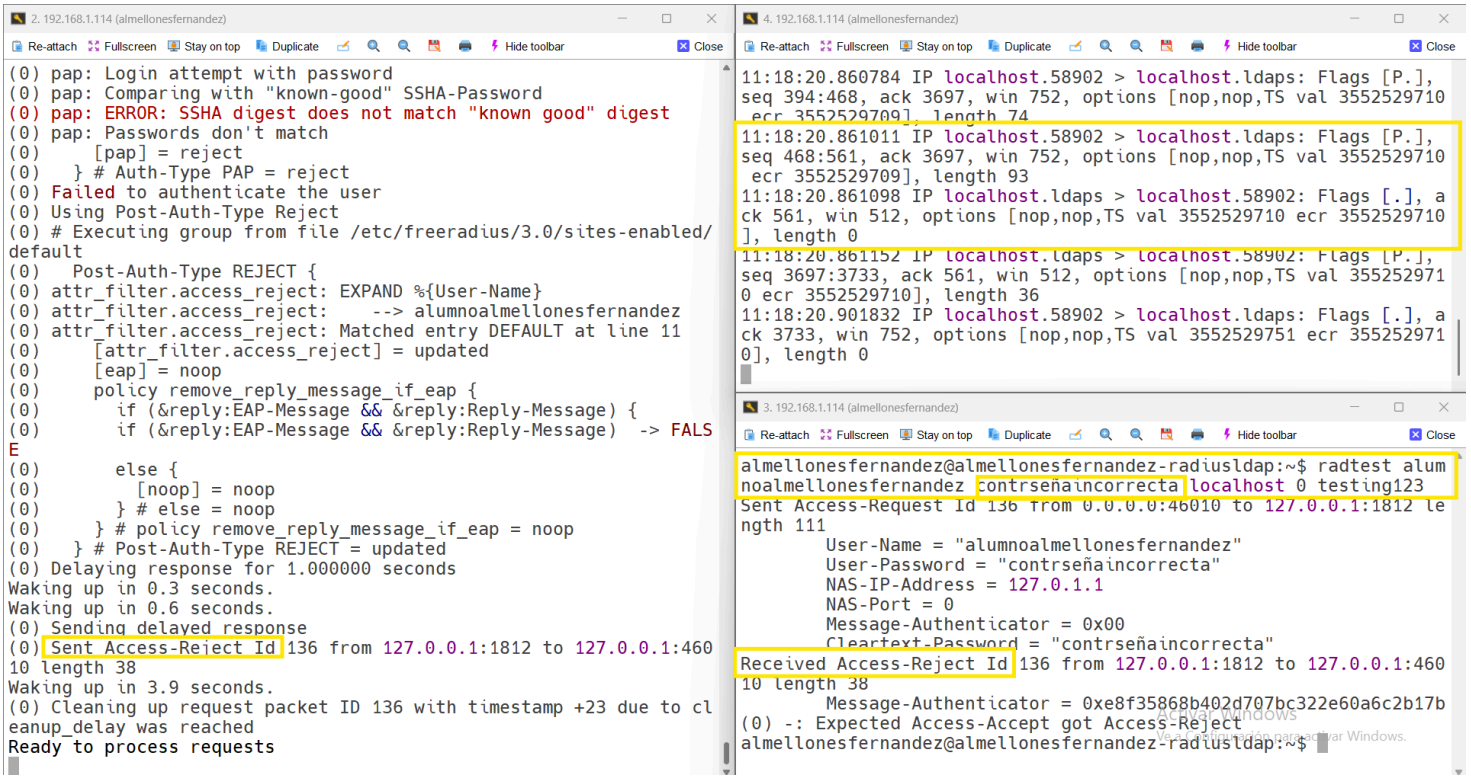
d. Haciendo uso del arranque de freeradius con la opción -X y del comando radtest, realice las siguientes comprobaciones.

i. Prueba de funcionamiento en modo local con usuario alumnoXXxx correctamente.

Álvaro Almellones Fernández



ii. Prueba de funcionamiento en modo local con usuario alumnoXXxx incorrectamente.



iii. Prueba de funcionamiento en modo local con usuario profesorXXxx correctamente.

Álvaro Almellones Fernández

```
(0)   Auth-Type PAP {
(0) pap: Login attempt with password
(0) pap: Comparing with "known-good" SSHA-Password
(0) pap: User authenticated successfully
(0)     [pap] = ok
(0)   } # Auth-Type PAP = ok
(0) # Executing section post-auth from file /etc/freeradius/3.0/si
tes-enabled/default
(0)   post-auth {
(0)     if (session-state:User-Name && reply:User-Name && request:
User-Name && (reply:User-Name == request:User-Name)) {
(0)     if (session-state:User-Name && reply:User-Name && request:
User-Name && (reply:User-Name == request:User-Name))  -> FALSE
(0)     update {
(0)       No attributes updated for RHS &session-state:
(0)     } # update = noop
(0)     [exec] = noop
(0)     policy remove_reply_message_if_eap {
(0)       if (&reply:EAP-Message && &reply:Reply-Message) {
(0)       if (&reply:EAP-Message && &reply:Reply-Message)  -> FALS
E
(0)       else {
(0)         [noop] = noop
(0)       } # else = noop
(0)     } # policy remove_reply_message_if_eap = noop
(0)     if (EAP-Key-Name && &reply:EAP-Session-Id) {
(0)     if (EAP-Key-Name && &reply:EAP-Session-Id)  -> FALSE
(0)   } # post-auth = noop
(0) Sent Access-Accept Id 132 from 127.0.0.1:1812 to 127.0.0.1:418
28 length 38
(0) Finished request
Waking up in 4.9 seconds.
(0) Cleaning up request packet ID 132 with timestamp +31 due to cl
eanup_delay was reached
Ready to process requests
```

```
almellonesfernandez@almellonesfernandez-radiusldap:~$ sudo tcpdump
 -i lo port 636
tcpdump: verbose output suppressed, use -v[v]... for full protocol
 decode
listening on lo, link-type EN10MB (Ethernet), snapshot length 2621
44 bytes
11:20:32.950853 IP localhost.52734 > localhost.ldaps: Flags [P.],
seq 1737987002:1737987193, ack 4076783501, win 752, options [nop,n
op,TS val 3552661800 ecr 3552629829], length 191
11:20:32.951426 IP localhost.ldaps > localhost.52734: Flags [P.],
seq 1:173, ack 191, win 512, options [nop,nop,TS val 3552661800 ec
r 3552661800], length 172
11:20:32.951435 IP localhost.52734 > localhost.ldaps: Flags [.], a
ck 173, win 774, options [nop,nop,TS val 3552661800 ecr 3552661800
], length 0
11:20:32.951458 IP localhost.ldaps > localhost.52734: Flags [P.],
```

```
3. 192.168.1.114 (almellonesfernandez)
Re-attach  Fullscreen  Stay on top  Duplicate  Hide toolbar  Close
almellonesfernandez@almellonesfernandez-radiusldap:~$ radtest prof
esormelerolopez almellonesfernandez localhost 0 testing123
Sent Access-Request Id 132 from 0.0.0.0:41828 to 127.0.0.1:1812 le
ngth 105
        User-Name = "profesormelerolopez"
        User-Password = "almellonesfernandez"
        NAS-IP-Address = 127.0.1.1
        NAS-Port = 0
        Message-Authenticator = 0x00
        Cleartext-Password = "almellonesfernandez"
Received Access-Accept Id 132 from 127.0.0.1:1812 to 127.0.0.1:418
28 length 38
        Message-Authenticator = 0xfbf2815818b9e61e40e7dc8fb92c19e9
almellonesfernandez@almellonesfernandez-radiusldap:~$
```

Álvaro Almellones Fernández

INTEGRACIÓN DE RADIUS CON MYSQL

5. **(1 puntos)** Realice la integración de FreeRadius con un servidor Mysql. Se deja al alumno que presente las evidencias que desee para comprobar su funcionalidad. Puede valer los mismos apartados que ejercicios anteriores.

```
root@almellonesfernandez-radiusldap:/# systemctl status mysql
● mysql.service - MySQL Community Server
     Loaded: loaded (/usr/lib/systemd/system/mysql.service; enabled; preset: enabled)
     Active: active (running) since Sun 2025-03-23 12:22:30 UTC; 3min 18s ago
    Process: 10929 ExecStartPre=/usr/share/mysql/mysql-systemd-start pre (code=exited, status=0/SUCCESS)
   Main PID: 10937 (mysqld)
     Status: "Server is operational"
      Tasks: 37 (limit: 4552)
     Memory: 364.1M (peak: 378.2M)
        CPU: 3.561s
     CGroup: /system.slice/mysql.service
             └─10937 /usr/sbin/mysqld

mar 23 12:22:30 almellonesfernandez-radiusldap systemd[1]: Starting mysql.service - MySQL Community Server...
mar 23 12:22:30 almellonesfernandez-radiusldap systemd[1]: Started mysql.service - MySQL Community Server.
root@almellonesfernandez-radiusldap:/# netstat -putan | grep mysql
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      10937/mysqld
tcp        0      0 127.0.0.1:33060         0.0.0.0:*               LISTEN      10937/mysqld
root@almellonesfernandez-radiusldap:/#
```

```
root@almellonesfernandez-radiusldap:/# mysql -u root -p radius < /etc/freeradius/3.0/mods-config/sql/main/mysql/schema.sql
Enter password:
root@almellonesfernandez-radiusldap:/# sudo mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 10
Server version: 8.0.41-0ubuntu0.24.04.1 (Ubuntu)

Copyright (c) 2000, 2025, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> USE radius;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> SHOW TABLES;
+------------------+
| Tables_in_radius |
+------------------+
| nas              |
| nasreload        |
| radacct          |
| radcheck         |
| radgroupcheck    |
| radgroupreply    |
| radpostauth      |
| radreply         |
| radusergroup     |
+------------------+
9 rows in set (0,00 sec)
```

```
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> USE radius;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> SHOW TABLES;
+------------------+
| Tables_in_radius |
+------------------+
| nas              |
| nasreload        |
| radacct          |
| radcheck         |
| radgroupcheck    |
| radgroupreply    |
| radpostauth      |
| radreply         |
| radusergroup     |
+------------------+
9 rows in set (0,00 sec)

mysql> SELECT * FROM radcheck;
+----+--------------------------+--------------------+----+--------------------+
| id | username                 | attribute          | op | value              |
+----+--------------------------+--------------------+----+--------------------+
|  1 | usuario1                 | Cleartext-Password | := | contraseña1        |
|  2 | msqlalmellonesfernandez | Cleartext-Password | := | almellonesfernandez |
+----+--------------------------+--------------------+----+--------------------+
2 rows in set (0,00 sec)

mysql>
```

```
 GNU nano 7.2                                /etc/freeradius/3.0/mods-enabled/sql
        #       postgresql
        #       sqlite
        #       mongo
        #
        dialect = "mysql"

        #
        #  The driver module used to execute the queries.  Since we
        #  don't know which SQL drivers are being used, the default is
        #  "rlm_sql_null", which just logs the queries to disk via the
        #  "logfile" directive, below.
        #
        #  In order to talk to a real database, delete the next line,
        #  and uncomment the one after it.
        #
        #  If the dialect is "mssql", then the driver should be set to
        #  one of the following values, depending on your system:
        #
        #       rlm_sql_db2
        #       rlm_sql_firebird
        #       rlm_sql_freetds
        #       rlm_sql_iodbc
        #       rlm_sql_unixodbc
        #
        driver = "rlm_sql_mysql"
#       driver = "rlm_sql_${dialect}"

        "
```

Álvaro Almellones Fernández

```
 GNU nano 7.2                                  /etc/freeradius/3.0/mods-enabled/sql
                #  The application name to use.
                #
                appname = "freeradius"

                #
                #  The TLS parameters here map directly to the Mongo TLS configuration
                #
                tls {
                        certificate_file = /path/to/file
                        certificate_password = "password"
                        ca_file = /path/to/file
                        ca_dir = /path/to/directory
                        crl_file = /path/to/file
                        weak_cert_validation = false
                        allow_invalid_hostname = false
                }
        }

        # Connection info:
        #
        server = "localhost"
        port = 3306
        login = "freeradius"
        password = "almellonesfernandez"

        # Connection info for Mongo
        # Authentication Without SSL
        #       server = "mongodb://USER:PASSWORD@192.16.0.2:PORT/DATABASE?authSource=admin&ssl=false"

        # Authentication With SSL
        #       server = "mongodb://USER:PASSWORD@192.16.0.2:PORT/DATABASE?authSource=admin&ssl=true"
```

```
almellonesfernandez@almellonesfernandez-radiusldap:~$ radtest msqlalmellonesfernandez almellonesfernandez 127.0.0.1 0 testing123
Sent Access-Request Id 80 from 0.0.0.0:56948 to 127.0.0.1:1812 length 109
        User-Name = "msqlalmellonesfernandez"
        User-Password = "almellonesfernandez"
        NAS-IP-Address = 127.0.1.1
        NAS-Port = 0
        Message-Authenticator = 0x00
        Cleartext-Password = "almellonesfernandez"
Received Access-Accept Id 80 from 127.0.0.1:1812 to 127.0.0.1:56948 length 38
        Message-Authenticator = 0x3c2ccae75e4beac3b09c383a60002eb2
almellonesfernandez@almellonesfernandez-radiusldap:~$ radtest msqlalmellonesfernandez contraseñaincorrecta 127.0.0.1 0 testing123
Sent Access-Request Id 22 from 0.0.0.0:39792 to 127.0.0.1:1812 length 109
        User-Name = "msqlalmellonesfernandez"
        User-Password = "contraseñaincorrecta"
        NAS-IP-Address = 127.0.1.1
        NAS-Port = 0
        Message-Authenticator = 0x00
        Cleartext-Password = "contraseñaincorrecta"
Received Access-Reject Id 22 from 127.0.0.1:1812 to 127.0.0.1:39792 length 38
        Message-Authenticator = 0x05d61d89db3864090f4f892bed1adf4a
(0) -: Expected Access-Accept got Access-Reject
almellonesfernandez@almellonesfernandez-radiusldap:~$
```

Álvaro Almellones Fernández

```
(1)     [logintime] = noop
(1)     [pap] = updated
(1)   } # authorize = updated
(1) Found Auth-Type = PAP
(1) # Executing group from file /etc/freeradius/3.0/sites-enabled/default
(1)   Auth-Type PAP {
(1) pap: Login attempt with password
(1) pap: Comparing with "known good" Cleartext-Password
(1) pap: User authenticated successfully
(1)     [pap] = ok
(1)   } # Auth-Type PAP = ok
(1) # Executing section post-auth from file /etc/freeradius/3.0/sites-enabled/default
(1)   post-auth {
(1)     if (session-state:User-Name && reply:User-Name && request:User-Name && (reply:User-Name == request:User-Name)) {
(1)     if (session-state:User-Name && reply:User-Name && request:User-Name && (reply:User-Name == request:User-Name))  -> FALSE
(1)     update {
(1)       No attributes updated for RHS &session-state:
(1)     } # update = noop
(1) sql: EXPAND .query
(1) sql:    --> .query
(1) sql: Using query template 'query'
rlm_sql (sql): Reserved connection (4)
(1) sql: EXPAND %{User-Name}
(1) sql:    --> msqlalmellonesfernandez
(1) sql: SQL-User-Name set to 'msqlalmellonesfernandez'
(1) sql: EXPAND INSERT INTO radpostauth (username, pass, reply, authdate ) VALUES ( '%{SQL-User-Name}', '%{%{User-Password}:-%{Chap-Pas
sword}}', '%{reply:Packet-Type}', '%S.%M' )
(1) sql:    --> INSERT INTO radpostauth (username, pass, reply, authdate ) VALUES ( 'msqlalmellonesfernandez', 'almellonesfernandez', '
Access-Accept', '2025-03-23 13:15:02.825857' )
(1) sql: Executing query: INSERT INTO radpostauth (username, pass, reply, authdate ) VALUES ( 'msqlalmellonesfernandez', 'almellonesfer
nandez', 'Access-Accept', '2025-03-23 13:15:02.825857' )
(1) sql: SQL query returned: success
(1) sql: 1 record(s) updated
rlm_sql (sql): Released connection (4)
(1)     [sql] = ok
(1)     [exec] = noop
```



```
rlm_ldap (ldap): Connecting to ldap://localhost:636
rlm_ldap (ldap): Waiting for bind result...
rlm_ldap (ldap): Bind successful
(2)     [ldap] = notfound
(2)     [expiration] = noop
(2)     [logintime] = noop
(2)     [pap] = updated
(2)   } # authorize = updated
(2) Found Auth-Type = PAP
(2) # Executing group from file /etc/freeradius/3.0/sites-enabled/default
(2)   Auth-Type PAP {
(2) pap: Login attempt with password
(2) pap: Comparing with "known good" Cleartext-Password
(2) pap: ERROR: Cleartext password does not match "known good" password
(2) pap: Passwords don't match
(2)     [pap] = reject
(2)   } # Auth-Type PAP = reject
(2) Failed to authenticate the user
(2) Using Post-Auth-Type Reject
(2) # Executing group from file /etc/freeradius/3.0/sites-enabled/default
(2)   Post-Auth-Type REJECT {
(2) sql: EXPAND .query
(2) sql:    --> .query
(2) sql: Using query template 'query'
rlm_sql (sql): Reserved connection (5)
(2) sql: EXPAND %{User-Name}
(2) sql:    --> msqlalmellonesfernandez
(2) sql: SQL-User-Name set to 'msqlalmellonesfernandez'
(2) sql: EXPAND INSERT INTO radpostauth (username, pass, reply, authdate ) VALUES ( '%{SQL-User-Name}', '%{%{User-Password}:-%{Chap-Pas
sword}}', '%{reply:Packet-Type}', '%S.%M' )
(2) sql:    --> INSERT INTO radpostauth (username, pass, reply, authdate ) VALUES ( 'msqlalmellonesfernandez', 'contraseñaincorrecta',
'Access-Reject', '2025-03-23 13:15:17.406688' )
(2) sql: Executing query: INSERT INTO radpostauth (username, pass, reply, authdate ) VALUES ( 'msqlalmellonesfernandez', 'contraseñainc
orrecta', 'Access-Reject', '2025-03-23 13:15:17.406688' )
(2) sql: SQL query returned: success
(2) sql: 1 record(s) updated
```

```
almellonesfernandez@almellonesfernandez-radiusldap:~$ radtest msqlalmellonesfernandez almellonesfernandez 127.0.0.1 0 testing123
Sent Access-Request Id 86 from 0.0.0.0:51514 to 127.0.0.1:1812 length 109
        User-Name = "msqlalmellonesfernandez"
        User-Password = "almellonesfernandez"
        NAS-IP-Address = 127.0.1.1
        NAS-Port = 0
        Message-Authenticator = 0x00
        Cleartext-Password = "almellonesfernandez"
Received Access-Accept Id 86 from 127.0.0.1:1812 to 127.0.0.1:51514 length 38
        Message-Authenticator = 0x5f0dae5320fcafc755c7a7100a9c715a
almellonesfernandez@almellonesfernandez-radiusldap:~$ systemctl stop mysql
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ====
Authentication is required to stop 'mysql.service'.
Authenticating as: almellonesfernandez
Password:
==== AUTHENTICATION COMPLETE ====
almellonesfernandez@almellonesfernandez-radiusldap:~$ radtest msqlalmellonesfernandez almellonesfernandez 127.0.0.1 0 testing123
Sent Access-Request Id 140 from 0.0.0.0:36870 to 127.0.0.1:1812 length 109
        User-Name = "msqlalmellonesfernandez"
        User-Password = "almellonesfernandez"
        NAS-IP-Address = 127.0.1.1
        NAS-Port = 0
        Message-Authenticator = 0x00
        Cleartext-Password = "almellonesfernandez"
Received Access-Reject Id 140 from 127.0.0.1:1812 to 127.0.0.1:36870 length 38
        Message-Authenticator = 0x865b60b9e2121b3142b34c275d542b77
(0) -: Expected Access-Accept got Access-Reject
almellonesfernandez@almellonesfernandez-radiusldap:~$
```

Álvaro Almellones Fernández

INTEGRACIÓN DE SQUID CON SERVIDOR FREERADIUS

6. **(1 punto)** Realice la integración del servidor squid (modo no transparente) con el servidor FreeRadius. Se deja al alumno que presente las evidencias que desee para comprobar su funcionalidad. Puede valer los mismos apartados que ejercicios anteriores.

```
root@almellonesfernandez-radiusldap:/home/almellonesfernandez# systemctl status squid
● squid.service - Squid Web Proxy Server
     Loaded: loaded (/usr/lib/systemd/system/squid.service; enabled; preset: enabled)
     Active: active (running) since Sun 2025-03-23 17:01:06 UTC; 2min 6s ago
       Docs: man:squid(8)
    Process: 2238 ExecStartPre=/usr/sbin/squid --foreground -z (code=exited, status=0/SUCCESS)
   Main PID: 2242 (squid)
      Tasks: 4 (limit: 4552)
     Memory: 17.8M (peak: 18.6M)
        CPU: 164ms
     CGroup: /system.slice/squid.service
             ├─2242 /usr/sbin/squid --foreground -sYC
             ├─2245 "(squid-1)" --kid squid-1 --foreground -sYC
             ├─2246 "(logfile-daemon)" /var/log/squid/access.log
             └─2247 "(pinger)"

mar 23 17:01:06 almellonesfernandez-radiusldap squid[2245]: Using Least Load store dir selection
mar 23 17:01:06 almellonesfernandez-radiusldap squid[2245]: Set Current Directory to /var/spool/squid
mar 23 17:01:06 almellonesfernandez-radiusldap squid[2245]: Finished loading MIME types and icons.
mar 23 17:01:06 almellonesfernandez-radiusldap squid[2245]: HTCP Disabled.
mar 23 17:01:06 almellonesfernandez-radiusldap squid[2245]: Pinger socket opened on FD 14
mar 23 17:01:06 almellonesfernandez-radiusldap systemd[1]: Started squid.service - Squid Web Proxy Server.
mar 23 17:01:06 almellonesfernandez-radiusldap squid[2245]: Squid plugin modules loaded: 0
mar 23 17:01:06 almellonesfernandez-radiusldap squid[2245]: Adaptation support is off.
mar 23 17:01:06 almellonesfernandez-radiusldap squid[2245]: Accepting HTTP Socket connections at conn3 local=[::]:3128 remote=[::] FD >
                                                                listening port: 3128
mar 23 17:01:07 almellonesfernandez-radiusldap squid[2245]: storeLateRelease: released 0 objects

root@almellonesfernandez-radiusldap:/home/almellonesfernandez# netstat -putan | grep squid
tcp6       0      0 :::3128                 :::*                    LISTEN      2245/(squid-1)
udp        0      0 0.0.0.0:48873           0.0.0.0:*                           2245/(squid-1)
udp6       0      0 ::1:42722               ::1:49096               ESTABLISHED 2245/(squid-1)
udp6       0      0 :::45611                :::*                                2245/(squid-1)
root@almellonesfernandez-radiusldap:/home/almellonesfernandez#
```



```
 GNU nano 7.2                          /etc/squid/radius.conf
server 127.0.0.1
secret testing123
identifier squid
port 1812
```

```
 GNU nano 7.2                          /etc/squid/conf.d/radiussquidalvaro.conf
http_port 3128


# Configuración del helper RADIUS
auth_param basic program /usr/lib/squid/basic_radius_auth -f /etc/squid/radius.conf
auth_param basic children 5
auth_param basic realm "Proxy Autenticado"
auth_param basic credentialsttl 2 hours

# ACL para usuarios autenticados
acl usuarios_autenticados proxy_auth REQUIRED
http_access allow usuarios_autenticados

# Denegar el acceso a cualquier otro usuario no autenticado
http_access deny all
```

Álvaro Almellones Fernández

```
root@almellonesfernandez-radiusldap /home/almellonesfernandez# curl -x http://alumnoalmellonesfernandez:almellonesfernandez@192.168.1.114:3128 http://example.com
<!doctype html>
<html>
<head>
    <title>Example Domain</title>

    <meta charset="utf-8" />
    <meta http-equiv="Content-type" content="text/html; charset=utf-8" />
    <meta name="viewport" content="width=device-width, initial-scale=1" />
    <style type="text/css">
    body {
        background-color: #f0f0f2;
        margin: 0;
        padding: 0;
        font-family: -apple-system, system-ui, BlinkMacSystemFont, "Segoe UI", "Open Sans", "Helvetica Neue", Helvetica
Arial, sans-serif;

    }
    div {
        width: 600px;
        margin: 5em auto;
        padding: 2em;
        background-color: #fdfdff;
        border-radius: 0.5em;
        box-shadow: 2px 3px 7px 2px rgba(0,0,0,0.02);
    }
    a:link, a:visited {
        color: #38488f;
        text-decoration: none;
    }
```



```
(0) sql: Using query template 'query'
rlm_sql (sql): Reserved connection (2)
(0) sql: EXPAND %{User-Name}
(0) sql:    --> alumnoalmellonesfernandez
(0) sql: SQL-User-Name set to 'alumnoalmellonesfernandez'
(0) sql: EXPAND INSERT INTO radpostauth (username, pass, reply, authdate ) VALUES ( '%{SQL-User-Name}', '%{%{User-Pass
word}:-%{Chap-Password}}', '%{reply:Packet-Type}', '%S.%M' )
(0) sql:    --> INSERT INTO radpostauth (username, pass, reply, authdate ) VALUES ( 'alumnoalmellonesfernandez', 'alme
llonesfernandez', 'Access-Accept', '2025-03-23 18:22:10.725206' )
(0) sql: Executing query: INSERT INTO radpostauth (username, pass, reply, authdate ) VALUES ( 'alumnoalmellonesfernand
ez', 'almellonesfernandez', 'Access-Accept', '2025-03-23 18:22:10.725206' )
(0) sql: SQL query returned: success
(0) sql: 1 record(s) updated
rlm_sql (sql): Released connection (2)
(0)     [sql] = ok
(0)     [exec] = noop
(0)     policy remove_reply_message_if_eap {
(0)       if (&reply:EAP-Message && &reply:Reply-Message) {
(0)       if (&reply:EAP-Message && &reply:Reply-Message)  -> FALSE
(0)       else {
(0)         [noop] = noop
(0)       } # else = noop
(0)     } # policy remove_reply_message_if_eap = noop
(0)     if (EAP-Key-Name && &reply:EAP-Session-Id) {
(0)     if (EAP-Key-Name && &reply:EAP-Session-Id)  -> FALSE
(0)   } # post-auth = ok
(0) Sent Access-Accept Id 5 from 127.0.0.1:1812 to 127.0.0.1:55154 length 38
(0) Finished request
Waking up in 4.9 seconds.
(0) Cleaning up request packet ID 5 with timestamp +6 due to cleanup_delay was reached
Ready to process requests
```

Álvaro Almellones Fernández

```
root@almellonesfernandez-radiusldap /home/almellonesfernandez# curl -x http://alumnoalmellonesfernandez:contraseñamal@1
.168.1.114:3128 http://example.com
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">
<html><head>
<meta type="copyright" content="Copyright (C) 1996-2021 The Squid Software Foundation and contributors">
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<title>ERROR: Cache Access Denied</title>
<style type="text/css"><!--
 /*
 * Copyright (C) 1996-2023 The Squid Software Foundation and contributors
 *
 * Squid software is distributed under GPLv2+ license and includes
 * contributions from numerous individuals and organizations.
 * Please see the COPYING and CONTRIBUTORS files for details.
 */

/*
 Stylesheet for Squid Error pages
 Adapted from design by Free CSS Templates
 http://www.freecsstemplates.org
 Released for free under a Creative Commons Attribution 2.5 License
*/

/* Page basics */
* {
        font-family: verdana, sans-serif;
}

html body {
        margin: 0;
        padding: 0;
        background: #efefef;
```



```
word}:-%{Chap-Password}}', '%{reply:Packet-Type}', '%S.%M' )
(3) sql:     --> INSERT INTO radpostauth (username, pass, reply, authdate ) VALUES ( 'alumnoalmellonesfernandez', 'cont
raseñamal', 'Access-Reject', '2025-03-23 18:18:40.529904' )
(3) sql: Executing query: INSERT INTO radpostauth (username, pass, reply, authdate ) VALUES ( 'alumnoalmellonesfernand
ez', 'contraseñamal', 'Access-Reject', '2025-03-23 18:18:40.529904' )
(3) sql: SQL query returned: success
(3) sql: 1 record(s) updated
rlm_sql (sql): Released connection (8)
(3)     [sql] = ok
(3) attr_filter.access_reject: EXPAND %{User-Name}
(3) attr_filter.access_reject:    --> alumnoalmellonesfernandez
(3) attr_filter.access_reject: Matched entry DEFAULT at line 11
(3)     [attr_filter.access_reject] = updated
(3)     [eap] = noop
(3)     policy remove_reply_message_if_eap {
(3)       if (&reply:EAP-Message && &reply:Reply-Message) {
(3)       if (&reply:EAP-Message && &reply:Reply-Message)  -> FALSE
(3)       else {
(3)         [noop] = noop
(3)       } # else = noop
(3)     } # policy remove_reply_message_if_eap = noop
(3)   } # Post-Auth-Type REJECT = updated
(3) Delaying response for 1.000000 seconds
Waking up in 0.3 seconds.
Waking up in 0.6 seconds.
(3) (3) Discarding duplicate request from client localhost port 55154 - ID: 4 due to delayed response
(3) Sending delayed response
(3) Sent Access-Reject Id 4 from 127.0.0.1:1812 to 127.0.0.1:55154 length 38
Waking up in 3.9 seconds.
(3) Cleaning up request packet ID 4 with timestamp +856 due to cleanup_delay was reached
Ready to process requests
```



```
root@almellonesfernandez-radiusldap:/home/almellonesfernandez# sudo tail -f /var/log/squid/access.log
1742753155.380    216 ::1 TCP_MISS/200 788 HEAD http://www.google.com/ - HIER_DIRECT/142.250.201.68 text/html
1742753394.238    408 ::1 TCP_MISS/200 1634 GET http://example.com/ - HIER_DIRECT/23.192.228.80 text/html
1742753415.525      0 ::1 TCP_MEM_HIT/200 1644 GET http://example.com/ - HIER_NONE/- text/html
1742753445.520      0 ::1 TCP_MEM_HIT/200 1644 GET http://example.com/ - HIER_NONE/- text/html
1742753477.947    492 ::1 TCP_MISS/200 924 HEAD http://www.httpforever.com/ - HIER_DIRECT/146.190.62.39 text/html
1742753750.312     80 192.168.1.114 TCP_MEM_HIT/200 1645 GET http://example.com/ almellonesfernandez HIER_NONE/- text/h
l
1742753758.593   1062 192.168.1.114 TCP_DENIED/407 4079 GET http://example.com/ almellonesfernandez HIER_NONE/- text/ht
1742753835.390     46 192.168.1.114 TCP_MEM_HIT/200 1645 GET http://example.com/ alumnoalmellonesfernandez HIER_NONE/-
xt/html
1742753921.559   1045 192.168.1.114 TCP_DENIED/407 4097 GET http://example.com/ alumnoalmellonesfernandez HIER_NONE/- t
t/html
1742754130.754     49 192.168.1.114 TCP_MEM_HIT/200 1645 GET http://example.com/ alumnoalmellonesfernandez HIER_NONE/-
xt/html
```

Álvaro Almellones Fernández

INTEGRACIÓN DE UBUNTU SERVER (SSH, SU) CON SERVIDOR FREERADIUS. PAM

7. **(1,5 punto)** Realice la integración de un sistema operativo Ubuntu Server (puede hacerse vía localhost para no tener que usar otro sistema operativo) con FreeRadius (que a su vez ya está integrado con servidor LDAP). Se deja al alumno que realice las capturas oportunas para demostrar que se ha integrado correctamente el S.O.

a. Ficheros modificados para su integración con PAM.

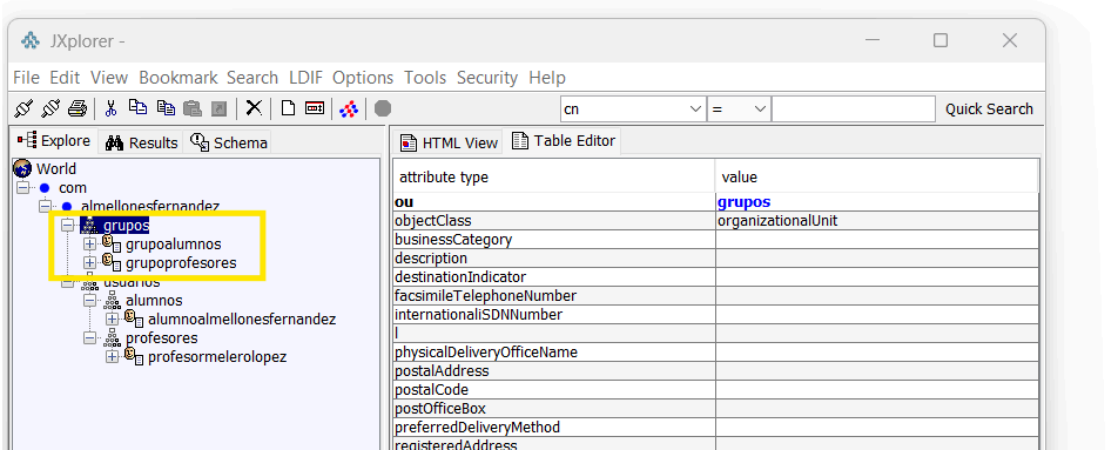
```
  GNU nano 7.2                                    /etc/ldap.conf

# The distinguished name of the search base.
base dc=almellonesfernandez,dc=com

# Another way to specify your LDAP server is to provide an
#uri ldapi:///almellonesfernandez.com
# Unix Domain Sockets to connect to a local LDAP Server.
uri ldap://127.0.0.1/
uri ldaps://127.0.0.1/
#uri ldapi://%2fvar%2frun%2fldapi_sock/
# Note: %2f encodes the '/' used as directory separator

# The LDAP version to use (defaults to 3
# if supported by client library)
ldap_version 3

# The distinguished name to bind to the server with.
# Optional: default is to bind anonymously
binddn cn=almellonesfernandez,dc=almellonesfernandez,dc=com

# The credentials to bind with.
# Optional: default is no credential.
bindpw almellonesfernandez

# The distinguished name to bind to the server with
# if the effective user ID is root. Password is
# stored in /etc/ldap.secret (mode 600)
rootbinddn cn=admin,dc=almellonesfernandez,dc=com


# The port.
# Optional: default is 389.
port 389
```

Álvaro Almellones Fernández

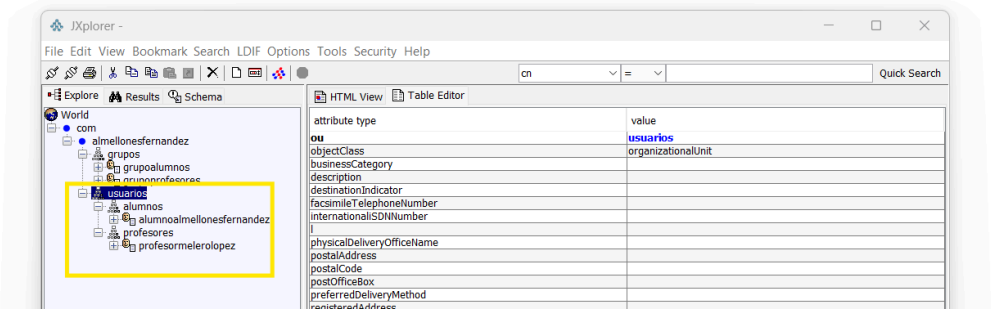
```
 GNU nano 7.2                                  /etc/nsswitch.conf
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality.
# If you have the `glibc-doc-reference' and `info' packages installed, try:
# `info libc "Name Service Switch"' for information about this file.

passwd:         files systemd ldap
group:          files systemd ldap
shadow:         files systemd ldap
gshadow:        files systemd

hosts:          files ldap dns
networks:       files

protocols:      db files
services:       ldap db files
ethers:         db files
rpc:            db files

netgroup:       nis
```

b. Uso de comandos tipo getent, tanto con usuarios, grupos, hosts y equipos, para demostrar que la integración es correcta

```
root@almellonesfernandez-radiusldap:~/scripts# getent group | grep grupo
grupoalumnos:*:10001:
grupoprofesores:*:10002:
root@almellonesfernandez-radiusldap:~/scripts#
```



```
root@almellonesfernandez-radiusldap:~/scripts# getent passwd | grep alumno
alumnoalmellonesfernandez:*:20002:10001:AlumnoAlmellonesFernandez:/home/alumnoalmellonesfernandez:/bin/bash
root@almellonesfernandez-radiusldap:~/scripts# getent passwd | grep profesor
profesormelerolopez:*:20001:10002:ProfesorMeleroLopez:/home/profesormelerolopez:/bin/bash
root@almellonesfernandez-radiusldap:~/scripts#
```



c. Inicio de sesión con usuario de freeradius directamente y un usuario alumno/profesor mediante comando switch user (su).

```
root@almellonesfernandez-radiusldap:~/scripts# su alumnoalmellonesfernandez
groups: cannot find name for group ID 10001
I have no name!@almellonesfernandez-radiusldap:/root/scripts$ exit
exit
root@almellonesfernandez-radiusldap:~/scripts# su profesormelerolopez
groups: cannot find name for group ID 10002
I have no name!@almellonesfernandez-radiusldap:/root/scripts$ exit
exit
root@almellonesfernandez-radiusldap:~/scripts#
```

No he conseguido solucionar este error. Me da error de que no encuenta el nombre para los grupos con los identificadores de mi ldap y entra en una especie de usuario llamado "I have no name"

d. Inicio de sesión con usuario de freeradius directamente y un usuario alumno/profesor mediante comando ssh.

```
root@almellonesfernandez-radiusldap:~/scripts# ssh alumnoalmellonesfernandez@localhost
alumnoalmellonesfernandez@localhost's password:
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.8.0-55-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of mar 25 mar 2025 13:15:40 UTC

  System load:  0.07              Processes:             234
  Usage of /:   52.2% of 9.75GB   Users logged in:       1
  Memory usage: 19%               IPv4 address for ens33: 192.168.1.114
  Swap usage:   0%
```

Álvaro Almellones Fernández

```
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Could not chdir to home directory /home/alumnoalmellonesfernandez: No such file or direct
$
```

```
root@almellonesfernandez-radiusldap:~/scripts# ssh profesormelerolopez@localhost
profesormelerolopez@localhost's password:
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.8.0-55-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of mar 25 mar 2025 13:17:09 UTC

  System load:  0.01              Processes:              237
  Usage of /:   52.2% of 9.75GB   Users logged in:        1
  Memory usage: 19%               IPv4 address for ens33: 192.168.1.114
  Swap usage:   0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

El mantenimiento de seguridad expandido para Applications está desactivado

Se pueden aplicar 132 actualizaciones de forma inmediata.
Para ver estas actualizaciones adicionales, ejecute: apt list --upgradable
```

```
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Could not chdir to home directory /home/profesormelerolopez: No such file or directory
$
```

En este ejercicio me pasa lo mismo, hace la acción de entrar pero me entra sin usuario

Álvaro Almellones Fernández

INVESTIGACIÓN

8. **(2 puntos)** Ejercicio número 8. Investigación

• Portal Cautivo con FreeRADIUS, OpenLDAP y CoovaChilli. **(Frank Castello, Alvaro, Jose Luis)**

• Integración de FreeRADIUS + OpenLDAP con VPN (OpenVPN).(**Frank Moreno, Eugenia, Hernan).**

• Implementar autenticación multifactor (2FA) para reforzar la seguridad de los accesos mediante OTP (One-Time Passwords).
(Covadonga, Miguel, Alvaro, Alberto)

• Bloqueo de Usuarios tras Múltiples Intentos Fallidos (Fail2Ban + FreeRADIUS) **(Cristian, David).**

Álvaro Almellones Fernández

```
Do you want authentication tokens to be time-based (y/n) y
Warning: pasting the following URL into your browser exposes the OTP secret to Google:
  https://www.google.com/chart?chs=200x200&chld=M|0&cht=qr&chl=otpauth://totp/almellonesfernandez@almellonesfernan
dez-radiusldap%3Fsecret%3DDFNKK3S3CRTU43QZNBVIVM72OQ%26issuer%3Dalmellonesfernandez-radiusldap
```

```
Your new secret key is: DFNKK3S3CRTU43QZNBVIVM72OQ
Enter code from app (-1 to skip):
```

```
Code confirmation skipped
Your emergency scratch codes are:
  70828665
  93525410
  47041611
  82174314
  83611842

Do you want me to update your "/home/almellonesfernandez/.google_authenticator" file? (y/n) y

Do you want to disallow multiple uses of the same authentication
token? This restricts you to one login about every 30s, but it increases
your chances to notice or even prevent man-in-the-middle attacks (y/n) n

By default, a new token is generated every 30 seconds by the mobile app.
In order to compensate for possible time-skew between the client and the server,
we allow an extra token before and after the current time. This allows for a
time skew of up to 30 seconds between authentication server and client. If you
experience problems with poor time synchronization, you can increase the window
from its default size of 3 permitted codes (one previous code, the current
code, the next code) to 17 permitted codes (the 8 previous codes, the current
code, and the 8 next codes). This will permit for a time skew of up to 4 minutes
between client and server.
Do you want to do so? (y/n) y

If the computer that you are logging into isn't hardened against brute-force
login attempts, you can enable rate-limiting for the authentication module.
By default, this limits attackers to no more than 3 login attempts every 30s.
Do you want to enable rate-limiting? (y/n) y
almellonesfernandez@almellonesfernandez-radiusldap:~$
```

```
  GNU nano 7.2                                    /etc/pam.d/radiusd
#
# /etc/pam.d/radiusd - PAM configuration for FreeRADIUS
#

auth    required   pam_google_authenticator.so forward_pass
account required   pam_permit.so


# We fall back to the system default in /etc/pam.d/common-*
#

@include common-auth
@include common-account
@include common-password
@include common-session
```

```
root@almellonesfernandez-radiusldap:/etc/freeradius/3.0/mods-enabled# pwd
/etc/freeradius/3.0/mods-enabled
root@almellonesfernandez-radiusldap:/etc/freeradius/3.0/mods-enabled# ls
always       detail.log       echo        files      mschap     passwd      replicate  unix
attr_filter  digest           exec        ldap       ntlm_auth  preprocess  soh        unpack
chap         dynamic_clients  expiration  linelog    pam        radutmp     sql        utf8
detail       eap              expr        logintime  pap        realm       sradutmp
root@almellonesfernandez-radiusldap:/etc/freeradius/3.0/mods-enabled#
```

Álvaro Almellones Fernández

```
  GNU nano 7.2                                                pam
# -*- text -*-
#
#  $Id: f4a91a948637bb2f42f613ed9faa6f9ae9ae6099 $


# Pluggable Authentication Modules
#
#  For Linux, see:
#       http://www.kernel.org/pub/linux/libs/pam/index.html
#
#  WARNING: On many systems, the system PAM libraries have
#           memory leaks!  We STRONGLY SUGGEST that you do not
#           use PAM for authentication, due to those memory leaks.
#
pam {
        #
        #  The name to use for PAM authentication.
        #  PAM looks in /etc/pam.d/${pam_auth_name}
        #  for it's configuration.  See 'redhat/radiusd-pam'
        #  for a sample PAM configuration file.
        #
        #  Note that any Pam-Auth attribute set in the 'authorize'
        #  section will over-ride this one.
        #
        pam_auth = radiusd
}

                                [ Read 26 lines ]
```

```
  GNU nano 7.2                  /etc/freeradius/3.0/sites-enabled/default
#  the post-auth section is for.
#
authenticate {
        #
        #  PAP authentication, when a back-end database listed
        #  in the 'authorize' section supplies a password.  The
        #  password can be clear-text, or encrypted.
#       Auth-Type PAP {
#               pap
#       }

       Auth-Type PAP {
               pam
       }

        #
        #  Most people want CHAP authentication
        #  A back-end database listed in the 'authorize' section
        #  MUST supply a CLEAR TEXT password.  Encrypted passwords
        #  won't work.
        Auth-Type CHAP {
                chap
        }

        #
        #  MSCHAP authentication.
        Auth-Type MS-CHAP {
```

```
almellonesfernandez@almellonesfernandez-radiusldap:/home$ radtest almellonesfernandez almellonesfernandez101527 12
7.0.0.1 0 testing123
Sent Access-Request Id 251 from 0.0.0.0:53971 to 127.0.0.1:1812 length 105
        User-Name = "almellonesfernandez"
        User-Password = "almellonesfernandez101527"
        NAS-IP-Address = 127.0.1.1
        NAS-Port = 0
        Message-Authenticator = 0x00
        Cleartext-Password = "almellonesfernandez101527"
Received Access-Reject Id 251 from 127.0.0.1:1812 to 127.0.0.1:53971 length 38
        Message-Authenticator = 0xcccc7dfe447b5c3c0ce6a92dada35e7c
(0) -: Expected Access-Accept got Access-Reject
almellonesfernandez@almellonesfernandez-radiusldap:/home$
```

Álvaro Almellones Fernández

```
rlm_ldap (ldap): Opening additional connection (5), 1 of 27 pending slots used
rlm_ldap (ldap): Connecting to ldap://localhost:636
rlm_ldap (ldap): Waiting for bind result...
rlm_ldap (ldap): Bind successful
(0)     [ldap] = notfound
(0)     [expiration] = noop
(0)     [logintime] = noop
(0)     [pap] = updated
(0)   } # authorize = updated
(0) Found Auth-Type = PAP
(0) # Executing group from file /etc/freeradius/3.0/sites-enabled/default
(0)   Auth-Type PAP {
(0) pam: Using pamauth string "radiusd" for pam.conf lookup
(0) pam: ERROR: pam_authenticate failed: Authentication failure
(0)     [pam] = reject
(0)   } # Auth-Type PAP = reject
(0) Failed to authenticate the user
(0) Using Post-Auth-Type Reject
(0) # Executing group from file /etc/freeradius/3.0/sites-enabled/default
(0)   Post-Auth-Type REJECT {
(0) sql: EXPAND .query
(0) sql:    --> .query
(0) sql: Using query template 'query'
rlm_sql (sql): Reserved connection (2)
(0) sql: EXPAND %{User-Name}
(0) sql:    --> almellonesfernandez
(0) sql: SQL-User-Name set to 'almellonesfernandez'
(0) sql: EXPAND INSERT INTO radpostauth (username, pass, reply, authdate ) VALUES ( '%{SQL-User-Name}', '%{%{User-
Password}:-%{Chap-Password}}', '%{reply:Packet-Type}', '%S.%M' )
(0) sql:    --> INSERT INTO radpostauth (username, pass, reply, authdate ) VALUES ( 'almellonesfernandez', 'almell
onesfernandez569994', 'Access-Reject', '2025-03-25 11:09:26.168609' )
(0) sql: Executing query: INSERT INTO radpostauth (username, pass, reply, authdate ) VALUES ( 'almellonesfernandez
```


Segun chatgpt y algunas paginas que he visitado , estos son los pasos que hay que seguir para integrar google-authenticator a freeradius pero no he conseguido que me funcione correctamente