

Nerea Álvarez Justel

#### Instalación de Open LDAP en Ubuntu20.04.

Puede confirmar que la instalación se realizó correctamente mediante los comandos slapcat para generar el contenido de la base de datos SLAPD.

**sudo slapcat**

```
miadmin@NAJUSED:~$ sudo slapcat
dn: dc=nereaa,dc=local
objectClass: top
objectClass: dcObject
objectClass: organization
o: nereaa
dc: nereaa
structuralObjectClass: organization
entryUUID: e4e4bba6-fbd9-103a-8cf4-91387d45e652
creatorsName: cn=admin,dc=nereaa,dc=local
createTimestamp: 20210205084259Z
entryCSN: 20210205084259.088813Z#000000#000#000000
modifiersName: cn=admin,dc=nereaa,dc=local
modifyTimestamp: 20210205084259Z

dn: cn=admin,dc=nereaa,dc=local
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator
userPassword:: e1NTSEF9bnJlYUVGUEM5V0FmaDJldmJOOERtTXVPbkIvYk9NRFU=
structuralObjectClass: organizationalRole
entryUUID: e4e52316-fbd9-103a-8cf5-91387d45e652
creatorsName: cn=admin,dc=nereaa,dc=local
createTimestamp: 20210205084259Z
entryCSN: 20210205084259.091498Z#000000#000#000000
modifiersName: cn=admin,dc=nereaa,dc=local
modifyTimestamp: 20210205084259Z
```

**Paso 2:** agregar el dn base para los usuarios y grupos.

Lo siguiente es agregar un DN base para usuarios y grupos. Crear nombre de archivo basado. Idif con los siguientes contenidos.

**vim basedn.ldif**

```
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
GNU nano 4.8
Edit dn: ou=people,dc=nereaa,dc=local
      objectClass: organizationalUnit
Edit ou: people
      . 1
      dn: ou=groups,dc=nereaa,dc=local
      objectClass: organizationalUnit
      ou: groups
```

Ahora agregue el archivo ejecutando los comandos.

***ldapadd -x -D cn=admin,dc=nereaa,dc=local -W -f basedn.ldif***

```
Last login: Fri Feb 5 10:23:33 2021
miadmin@NAJLDAP:~$ ldapadd -x -D cn=admin,dc=nereaa,dc=local -W -f basedn.ldif
Enter LDAP Password:
adding new entry "ou=people,dc=nereaa,dc=local"

adding new entry "ou=groups,dc=nereaa,dc=local"

miadmin@NAJLDAP:~$
```

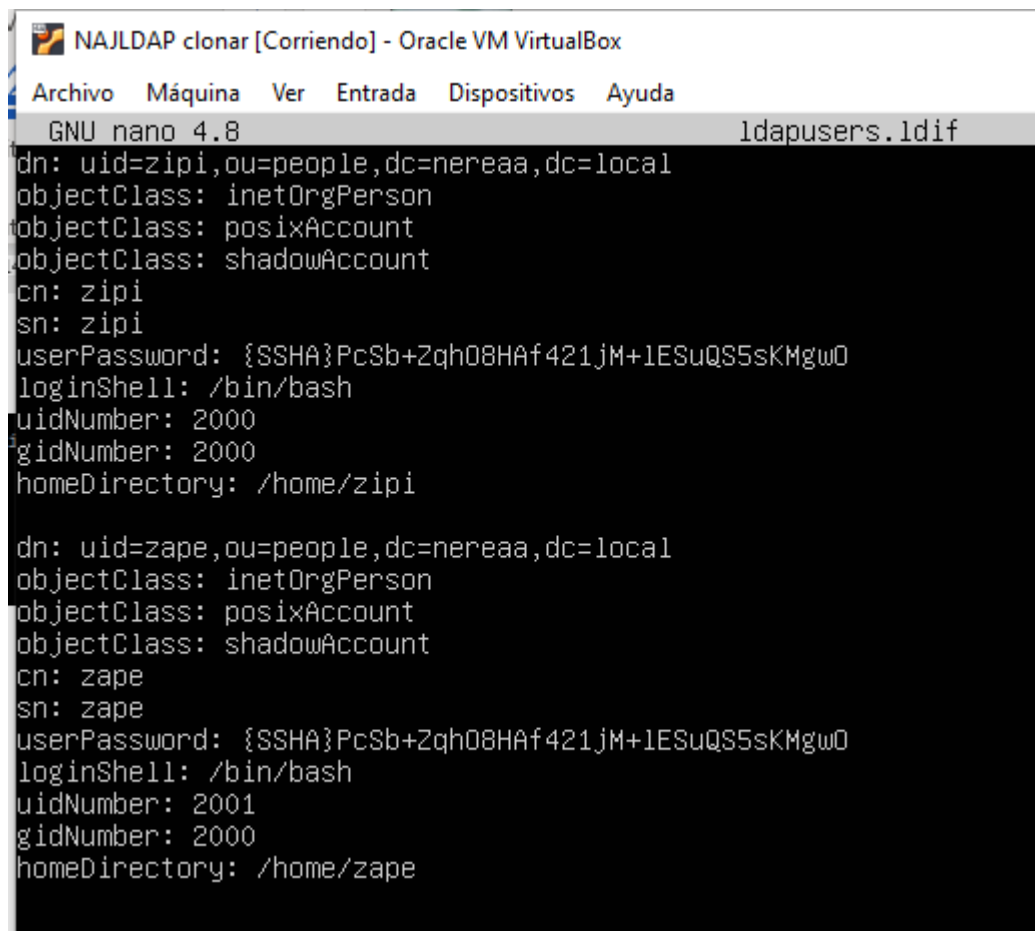
**Paso 3:** Agregar las cuentas de usuario y los grupos.

Introduzca la contraseña de la cuenta de usuario y confírmela.

```
miadmin@NAJLDAP:~$ slappasswd
New password:
Re-enter new password:
{SSHA}PcSb+ZqhO8HAf421jM+1ESuQS5sKMgwO
miadmin@NAJLDAP:~$
```

Cree un archivo ldif para agregar usuarios.

***vim ldapusers.ldif***



The screenshot shows a terminal window titled "NAJLDAP clonar [Corriendo] - Oracle VM VirtualBox". The terminal is running the GNU nano 4.8 editor, editing the file "ldapusers.ldif". The file contains two LDAP entry definitions for users "zipi" and "zape". Both entries are of type "inetOrgPerson" and "posixAccount", with a "shadowAccount" object class. They share the same password "{SSHA}PcSb+ZqhO8HAf421jM+1ESuQS5sKMgwO" and login shell "/bin/bash". The "zipi" user has uid 2000 and home directory "/home/zipi". The "zape" user has uid 2001 and home directory "/home/zape".

```
GNU nano 4.8 ldapusers.ldif
dn: uid=zipi,ou=people,dc=nereaa,dc=local
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: zipi
sn: zipi
userPassword: {SSHA}PcSb+ZqhO8HAf421jM+1ESuQS5sKMgwO
loginShell: /bin/bash
uidNumber: 2000
gidNumber: 2000
homeDirectory: /home/zipi

dn: uid=zape,ou=people,dc=nereaa,dc=local
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: zape
sn: zape
userPassword: {SSHA}PcSb+ZqhO8HAf421jM+1ESuQS5sKMgwO
loginShell: /bin/bash
uidNumber: 2001
gidNumber: 2000
homeDirectory: /home/zape
```

Una vez que haya terminado con la edición, agregue la cuenta ejecutando.

***ldapadd -x -D cn=admin,dc=nereaa,dc=local -W -f ldapusers.ldif***

```
miadmin@NAJLDAP:~$ ldapadd -x -D cn=admin,dc=nereaa,dc=local -W -f ldapusers.ldif
Enter LDAP Password:
adding new entry "uid=zipi,ou=people,dc=nereaa,dc=local"

adding new entry "uid=zape,ou=people,dc=nereaa,dc=local"
```

Haz lo mismo con el grupo.

***vim ldapgroups.ldif***

```
miadmin@NAJLDAP: ~
GNU nano 4.8                                ldapgroups.ldif
cn: cn=gemelos,ou=groups,dc=nereaa,dc=local
objectClass: posixGroup
cn: gemelos
gidNumber: 2000
memberUid:
```

***ldapadd -x -D cn=admin,dc=nereaa,dc=local -W -f ldapgroups.ldif***

```
miadmin@NAJLDAP:~$ ldapadd -x -D cn=admin,dc=nereaa,dc=local -W -f ldapgroups.ldif
Enter LDAP Password:
adding new entry "cn=gemelos,ou=groups,dc=nereaa,dc=local"
```

```
miadmin@NAJLDAP:~$ sudo slapcat
[sudo] password for miadmin:
dn: dc=nereaa,dc=local
objectClass: top
objectClass: dcObject
objectClass: organization
o: nereaa
dc: nereaa
structuralObjectClass: organization
entryUUID: e4e4bba6-fbd9-103a-8cf4-91387d45e652
creatorsName: cn=admin,dc=nereaa,dc=local
createTimestamp: 20210205084259Z
entryCSN: 20210205084259.088813Z#000000#000#000000
modifiersName: cn=admin,dc=nereaa,dc=local
modifyTimestamp: 20210205084259Z

dn: cn=admin,dc=nereaa,dc=local
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator
userPassword:: e1NTSEF9bnJlYUVGUEM5V0FmaDJldmJOOERtTXVPbkIvYk9NRFU=
structuralObjectClass: organizationalRole
entryUUID: e4e52316-fbd9-103a-8cf5-91387d45e652
creatorsName: cn=admin,dc=nereaa,dc=local
createTimestamp: 20210205084259Z
entryCSN: 20210205084259.091498Z#000000#000#000000
modifiersName: cn=admin,dc=nereaa,dc=local
modifyTimestamp: 20210205084259Z

dn: ou=people,dc=nereaa,dc=local
objectClass: organizationalUnit
ou: people
structuralObjectClass: organizationalUnit
entryUUID: 82e4bb86-fbe8-103a-92fe-a78843c53695
creatorsName: cn=admin,dc=nereaa,dc=local
createTimestamp: 20210205102737Z
entryCSN: 20210205102737.123064Z#000000#000#000000
modifiersName: cn=admin,dc=nereaa,dc=local
modifyTimestamp: 20210205102737Z

dn: ou=groups,dc=nereaa,dc=local
objectClass: organizationalUnit
ou: groups
structuralObjectClass: organizationalUnit
entryUUID: 82e6b5f8-fbe8-103a-92ff-a78843c53695
creatorsName: cn=admin,dc=nereaa,dc=local
createTimestamp: 20210205102737Z
entryCSN: 20210205102737.136039Z#000000#000#000000
modifiersName: cn=admin,dc=nereaa,dc=local
modifyTimestamp: 20210205102737Z
```

```
dn: uid=zipi,ou=people,dc=nereaa,dc=local
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: zipi
sn: zipi
userPassword:: e1NTSEF9UGNTYitacWhPOEhBZjQyMWpNK2xFU3VRUzVzS0lnd08=
loginShell: /bin/bash
uidNumber: 2000
gidNumber: 2000
homeDirectory: /home/zipi
structuralObjectClass: inetOrgPerson
uid: zipi
entryUUID: ba74f6c8-fbe9-103a-9300-a78843c53695
creatorsName: cn=admin,dc=nereaa,dc=local
createTimestamp: 20210205103619Z
entryCSN: 20210205103619.839727Z#000000#000#000000
modifiersName: cn=admin,dc=nereaa,dc=local
modifyTimestamp: 20210205103619Z
```

```
dn: uid=zape,ou=people,dc=nereaa,dc=local
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: zape
sn: zape
userPassword:: e1NTSEF9UGNTYitacWhPOEhBZjQyMWpNK2xFU3VRUzVzS0lnd08=
loginShell: /bin/bash
uidNumber: 2001
gidNumber: 2000
homeDirectory: /home/zape
structuralObjectClass: inetOrgPerson
uid: zape
entryUUID: ba7634b6-fbe9-103a-9301-a78843c53695
creatorsName: cn=admin,dc=nereaa,dc=local
createTimestamp: 20210205103619Z
entryCSN: 20210205103619.847866Z#000000#000#000000
modifiersName: cn=admin,dc=nereaa,dc=local
modifyTimestamp: 20210205103619Z
```

```
dn: cn=gemelos,ou=groups,dc=nereaa,dc=local
objectClass: posixGroup
cn: gemelos
gidNumber: 2000
memberUid:
structuralObjectClass: posixGroup
entryUUID: 6728dc4a-fbea-103a-9302-a78843c53695
creatorsName: cn=admin,dc=nereaa,dc=local
createTimestamp: 20210205104109Z
entryCSN: 20210205104109.586811Z#000000#000#000000
modifiersName: cn=admin,dc=nereaa,dc=local
modifyTimestamp: 20210205104109Z
```

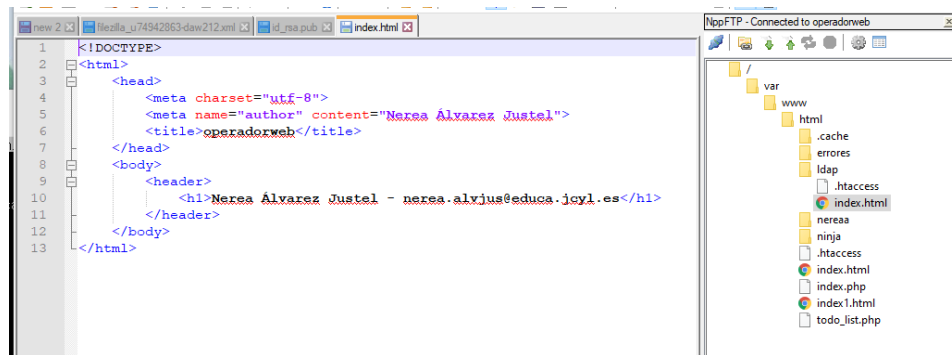
Ahora crearemos el fichero en el servidor de DESARROLLO para la autenticación del usuario ZIPI.  
Daremos la información de conexión para el servidor LDAP.

```

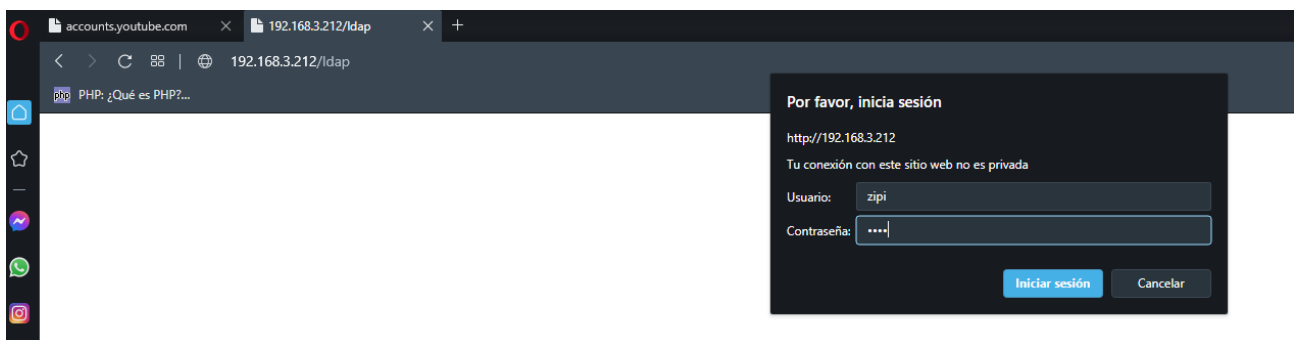
$-nereaa,dc=local?uid?sub?(objectClass=*)
NAJUSED [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
GNU nano 4.8 /var/www/html/ldap/.htaccess
AuthType Basic
AuthBasicProvider ldap
AuthName "login..."
AuthLDAPURL "ldap://192.168.3.112/dc=nereaa,dc=local?uid?sub?(objectClass=*)"
AuthLDAPBindDN "cn=admin,dc=nereaa,dc=local"
AuthLDAPBindPassword paso
Require ldap-user zipi

```

Aquí veremos la ruta y que veremos al dar un USUARIO y CONTRASEÑA correcta.



Comprobación de su funcionamiento.



# php LDAP admin

Instalaremos php LDAP admin, con esto podremos crear tanto usuarios como grupos de forma visual.

Esto se instalará en el servidor LDAP mediante el siguiente comando:

```
sudo apt-get install phpldapadmin -y
```

Se comprobará su instalación en el navegador, escribimos <http://IP/phpldapadmin/>. Nos pedirá información para el login, usuario y contraseña

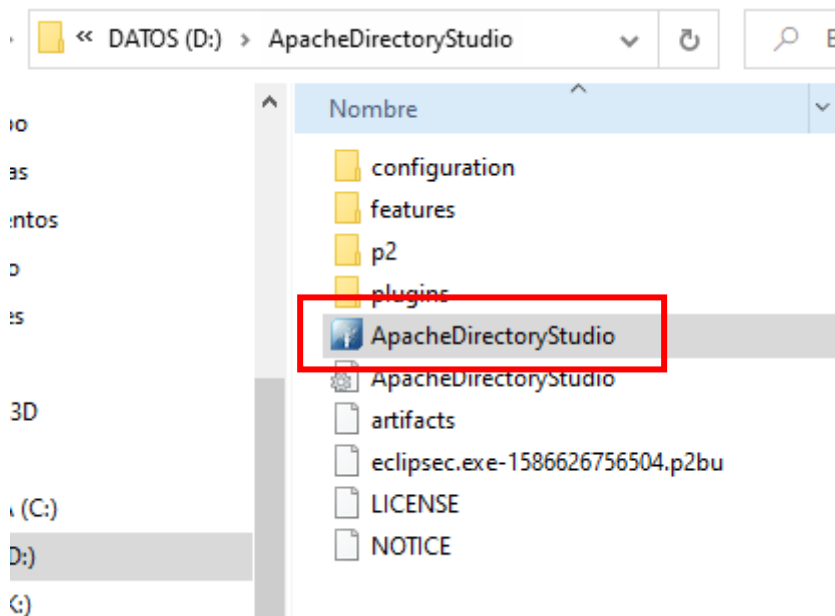
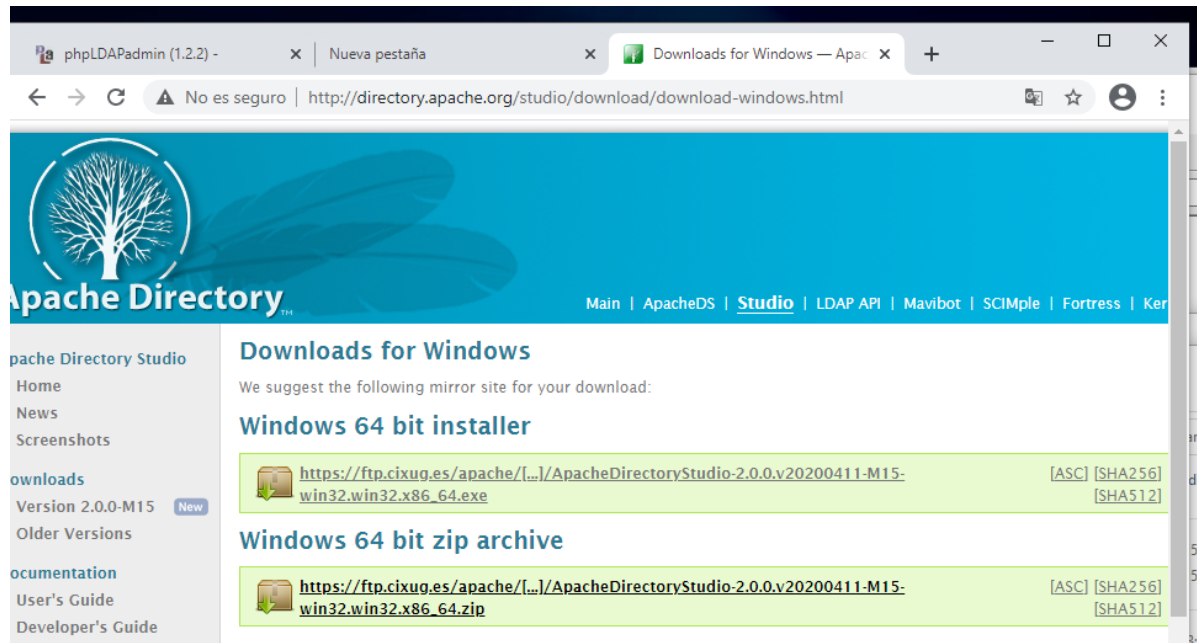


# APACHE DIRECTORY

Instalaremos otra forma de crear tanto usuarios como grupos. Encontraremos los archivos necesarios en <http://directory.apache.org/studio/downloads.html>.

Descargamos para Windows 64 bit el archivo .zip.

Posteriormente descomprimos la carpeta y ya estaría listo para usar.



Doble clic y se abrirá.



En la segunda ventana daremos los datos para el login.

New LDAP Connection

Please select an authentication method and input authentication data.

Authentication Method: Simple Authentication

Authentication Parameter: Bind DN or user: cn=admin,dc=nereaa,dc=local

Authorization ID (SASL): SASL PLAIN only

Bind password: \*\*\*\*

☒ Save password

Check Authentication

Navigation: < Back, Next >, Finish (highlighted), Cancel

Clic derecho el grupos > NEW > NEW ENTRY

The screenshot displays two overlapping NetBeans IDE windows from the "New Entry" wizard.

**Top Window: Object Classes**

- Title Bar:** New Entry
- Message:** Please select object classes of the entry. Select at least one structural object class.
- Available object classes:** A scrollable list containing: account, alias, applicationEntity, applicationProcess, bootableDevice, certificationAuthority, certificationAuthority-V2, country, cRLDistributionPoint, dcObject, deltaCRL, device, dmd.
- Add / Remove Buttons:** Two buttons located between the lists.
- Selected object classes:** A list containing: posixGroup, top.

**Bottom Window: Attributes**

- Title Bar:** New Entry
- Message:** Please enter the attributes for the entry. Enter at least the MUST attributes.
- DN:** cn=jefes,ou=groups,dc=nereaa,dc=local
- Attribute Table:**

Attribute	Description	Value
objectClass		posixGroup ( <i>structural</i> )
objectClass		top ( <i>abstract</i> )
cn		jefes
gidNumber		2000
- Navigation Buttons:** Located at the bottom of the window are "< Back", "Next >", "Finish", and "Cancel".

Nosotros necesitamos crear un grupo ya enlazado a la conexión y específico para este caso.

**New Entry**

**Entry Creation Method**

Please select the entry creation method.

☐ Create entry from scratch

☒ Use existing entry as template

ou=groups,dc=nereaa,dc=local

Buttons: < Back, Next >, Finish, Cancel

**New Entry**

**Object Classes**

Please select object classes of the entry. Select at least one structural object class.

Available object classes: account, alias, applicationEntity, applicationProcess, bootableDevice, certificationAuthority, certificationAuthority-V2, country, cRLDistributionPoint, dcObject, deltaCRL, device, dmd

Selected object classes: groupOfUniqueNames, organizationalUnit, top

Buttons: < Back, Next >, Finish, Cancel

**New Entry**

**Distinguished Name**

Please select the parent of the new entry and enter the RDN.

Parent: ou=groups,dc=nereaa,dc=local

RDN: cn=jefes

DN Preview: cn=jefes,ou=groups,dc=nereaa,dc=local

Buttons: < Back, Next >, Finish, Cancel

**New Entry**

**Attributes**

Please enter the attributes for the entry. Enter at least the MUST attributes.

DN: cn=jefes,ou=groups,dc=nereaa,dc=local

Attribute Description	Value
objectClass	groupOfUniqueNames (structural)
objectClass	top (abstract)
cn	jefes
uniqueMember	uid=zipi,ou=people,dc=nereaa,dc=local

Buttons: < Back, Next >, Finish, Cancel

**LDAP - cn=jefes,ou=groups,dc=nereaa,dc=local - ldap - Apache Directory Studio**

File Edit Navigate Search LDAP Window Help

LDAP Browser

- Root DSE (2)
- dc=nereaa,dc=local (3)
  - cn=admin
  - ou=groups (2+)
    - cn=gemeleos
    - cn=jefes
  - ou=people (2)
    - uid=zape
    - uid=zipi

Attributes

Attribute Description	Value
objectClass	groupOfUniqueNames (structural)
objectClass	top (abstract)
cn	jefes
uniqueMember	uid=zipi,ou=people,dc=nereaa,dc=local

Outline

- cn=jefes,ou=groups,dc=nereaa,dc=local
  - objectClass (2)
  - uniqueMember (1)
  - cn (1)

Comprobamos que podemos entrar con zipi, antes tendremos que modificar el fichero .htaccess.

```

1 AuthType Basic
2 AuthBasicProvider ldap
3
4 AuthName "Usuario y contraseña"
5
6 # Generar el filtro de búsqueda
7
8 AuthLDAPURL "ldap://192.168.3.112/dc=nereaa,dc=local?uid?sub?objectClass=*"
9
10
11
12
13 # DN opcional para enlazar con la fase de búsqueda
14
15 AuthLDAPBindDN "cn=admin,dc=nereaa,dc=local"
16
17 # Contraseña opcional para enlazar la fase de búsqueda
18
19 AuthLDAPBindPassword paso
20
21 Require ldap-group cn=jefes,ou=groups,dc=nereaa,dc=local
22
23
    
```

192.168.3.212/ldap

Iniciar sesión

http://192.168.3.212

Tu conexión con este sitio web no es privada

Nombre de usuario: zipi

Contraseña: \*\*\*\*

Buttons: Iniciar sesión, Cancelar

operadonweb

No es seguro https://192.168.3.212/ldap/

Nerea Álvarez Justel - nerea.alvjus@educa.jcyl.es

Ahora realizamos un ejemplo práctico, con php LDAP admin.

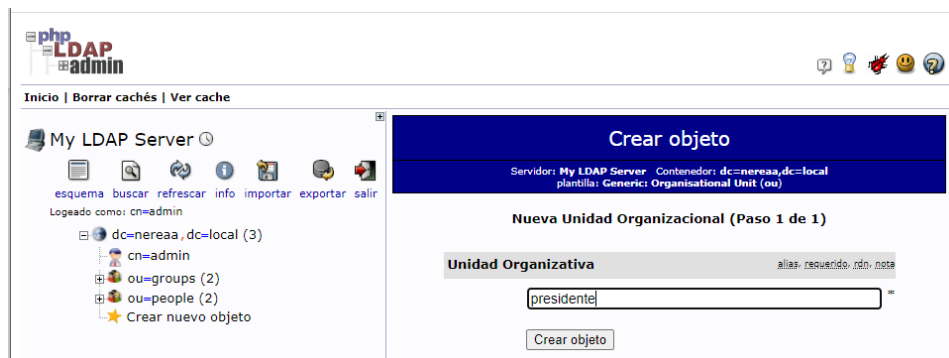
Se pide crear la unidad organizativa presidentes, en el grupo América, añadir los usuarios Clinton (Bill Clinton) y Trump (Donald Trump).

Primeramente, iniciamos sesión.



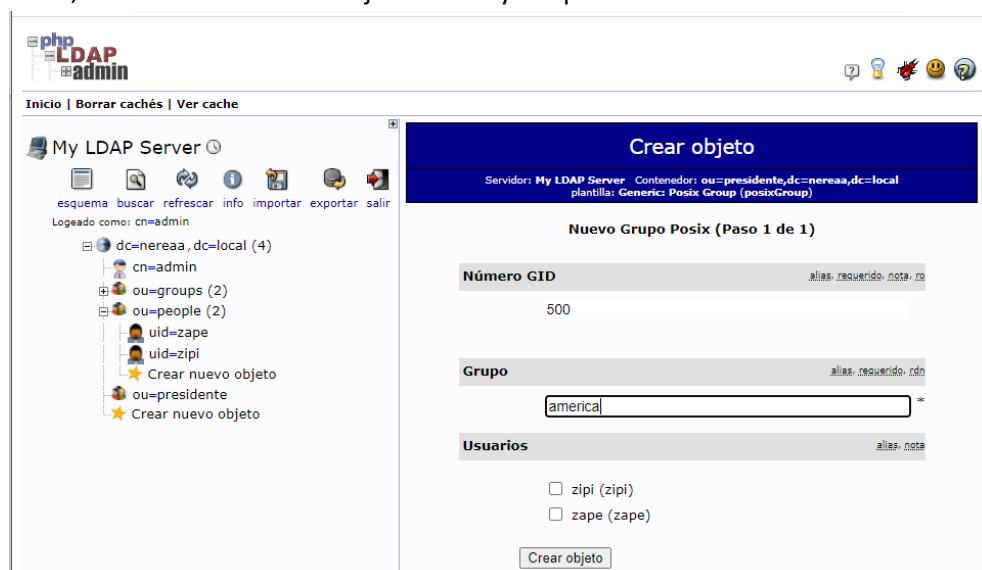
The screenshot shows the phpLDAPadmin web interface. At the top, there's a navigation bar with 'Inicio | Borrar cachés | Ver cache'. Below it, a sidebar on the left shows 'My LDAP Server' with a 'conectar' button. The main content area has a blue header 'Autenticar al servidor My LDAP Server'. Below this, a red warning message states: 'Advertencia: Esta conexión web no está encriptada.' The login form includes fields for 'Login:' (containing 'cn=admin,dc=nereaa,dc=local') and 'Contraseña:' (masked with dots). There's an 'Anónimo' checkbox and an 'Identificarse' button.

Crearemos la unidad organizativa, hacemos clic en el general, seleccionamos crear objeto nuevo y Unidad Organizacional.



The screenshot shows the 'Crear objeto' (Create object) page. The sidebar on the left shows the LDAP tree structure: 'dc=nereaa,dc=local (3)' containing 'cn=admin', 'ou=groups (2)', and 'ou=people (2)'. The main content area has a blue header 'Crear objeto' with server details. Below, it says 'Nueva Unidad Organizacional (Paso 1 de 1)'. The form has a label 'Unidad Organizativa' and a text input field containing 'presidente'. A 'Crear objeto' button is at the bottom.

Ahora crearemos el grupo dentro de esta unidad organizativa “presidente”. Clic en presidentes, seleccionamos crear objeto nuevo y Grupo Posix.



The screenshot shows the 'Crear objeto' page for creating a new Posix group. The sidebar on the left shows the LDAP tree structure, now including 'ou=presidente' under 'ou=people (2)'. The main content area has a blue header 'Crear objeto' with server details. Below, it says 'Nuevo Grupo Posix (Paso 1 de 1)'. The form has three fields: 'Número GID' (500), 'Grupo' (america), and 'Usuarios' (checkboxes for 'zipi (zipi)' and 'zape (zape)'). A 'Crear objeto' button is at the bottom.

Tras crear el grupo, crearemos los usuarios, pero desde otro ya creado. Una vez copiado el usuario cambias los valores a el usuario nuevo. Se crean los dos usuarios.

