SERVIDORES Y DOMINIOS UBUNTU

Andrea Díaz Maeso
2º CFGS ASIR

ÍNDICE

1) Promocionar a controlador de dominio un servidor Ubuntu.

Primero, configuramos la IP del servidor:

```
  GNU nano 4.8                  /etc/netplan/00-installer-config.yaml
# This is the network config written by 'subiquity'
network:
  ethernets:
    enp0s3:
      dhcp4: false
      addresses:
      - 192.168.1.1/24
      gateway4: 192.168.1.1
      nameservers:
       addresses: [192.168.1.1]
  version: 2
```

Cambiamos el nombre del equipo:

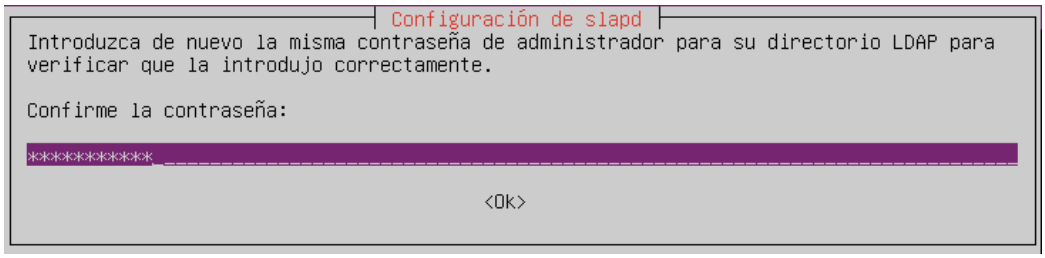
```
  GNU nano 4.8                                          /etc/hostname
UbuntuServer
```

Modificamos el fichero “/etc/hosts” para indicar el nombre de dominio:

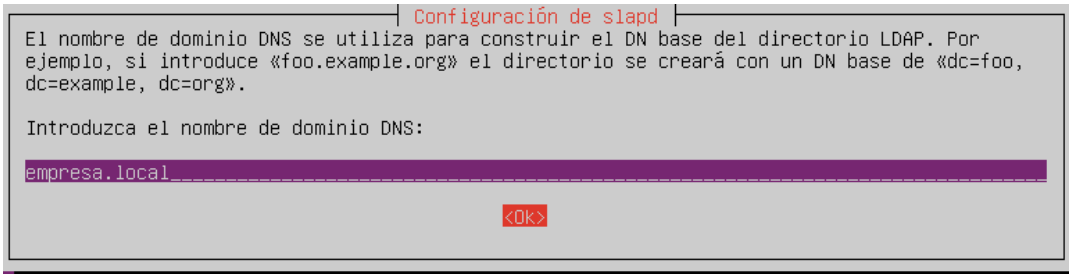
```
  GNU nano 4.8                                              /etc/hosts
127.0.0.1 localhost
127.0.1.1 ubuntuserver
192.168.1.1 UbuntuServer.empresa.local UbuntuServer
```

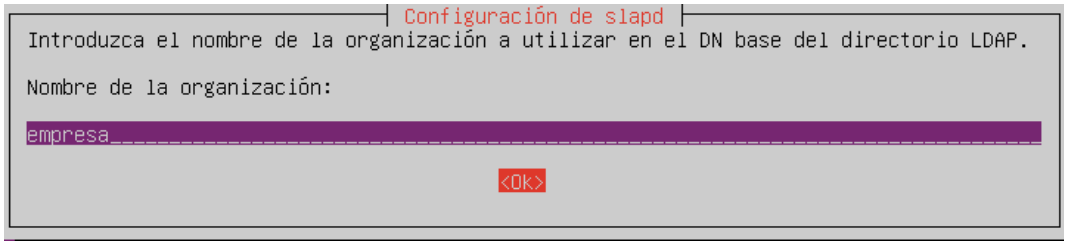
Ahora, instalamos LDAP en el servidor:

```
andrea@ubuntuserver:~$ sudo apt install slapd ldap-utils -y
```




```
andrea@UbuntuServer:~$ sudo dpkg-reconfigure slapd
```





Modificamos los ficheros “/etc/ldap/ldap.conf” y “/etc/nsswitch.conf”:

```
  GNU nano 4.8                          /etc/ldap/ldap.conf
#
# LDAP Defaults
#

# See ldap.conf(5) for details
# This file should be world readable but not world writable.

#BASE   dc=example,dc=com
#URI    ldap://ldap.example.com ldap://ldap-master.example.com:666

BASE    dc=empresa,dc=local
URI     ldap://192.168.1.1:389
```

```
  GNU nano 4.8                                /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 ldap
group:          files ldap
shadow:         files ldap
gshadow:        files
```

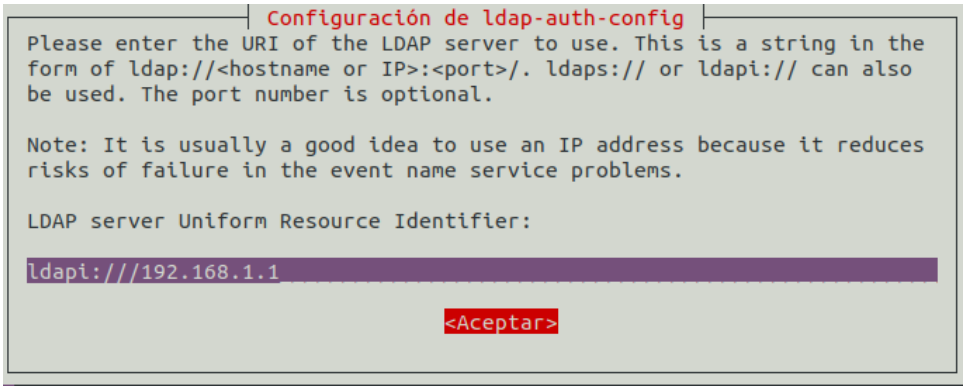
Comprobamos que el dominio se ha creado correctamente:

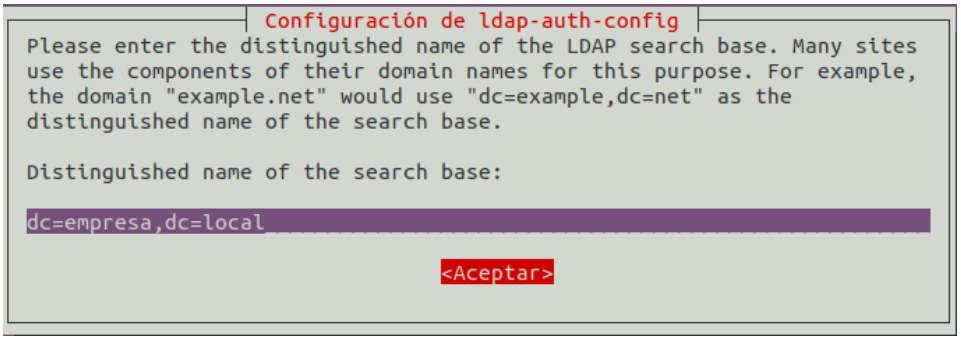
```
andrea@UbuntuServer:~$ sudo slapcat
dn: dc=empresa,dc=local
objectClass: top
objectClass: dcObject
objectClass: organization
o: empresa
dc: empresa
structuralObjectClass: organization
entryUUID: 9a84dd72-77a9-103d-929a-77d1e402b344
creatorsName: cn=admin,dc=empresa,dc=local
createTimestamp: 20230425113937Z
entryCSN: 20230425113937.992651Z#000000#000#000000
modifiersName: cn=admin,dc=empresa,dc=local
modifyTimestamp: 20230425113937Z

dn: cn=admin,dc=empresa,dc=local
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator
userPassword:: e1NTSEF9VDJlMjBPWnUzYnZpRkR1Qml5TERWU1dCd3ZHdG5FT2o=
structuralObjectClass: organizationalRole
entryUUID: 9a860256-77a9-103d-929b-77d1e402b344
creatorsName: cn=admin,dc=empresa,dc=local
createTimestamp: 20230425113937Z
entryCSN: 20230425113938.000202Z#000000#000#000000
modifiersName: cn=admin,dc=empresa,dc=local
modifyTimestamp: 20230425113937Z
```

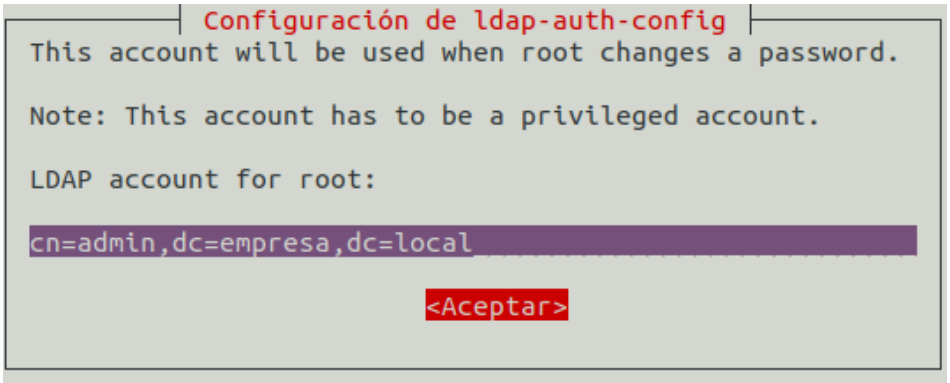
2) Añadir un cliente Windows y otro Ubuntu al dominio.

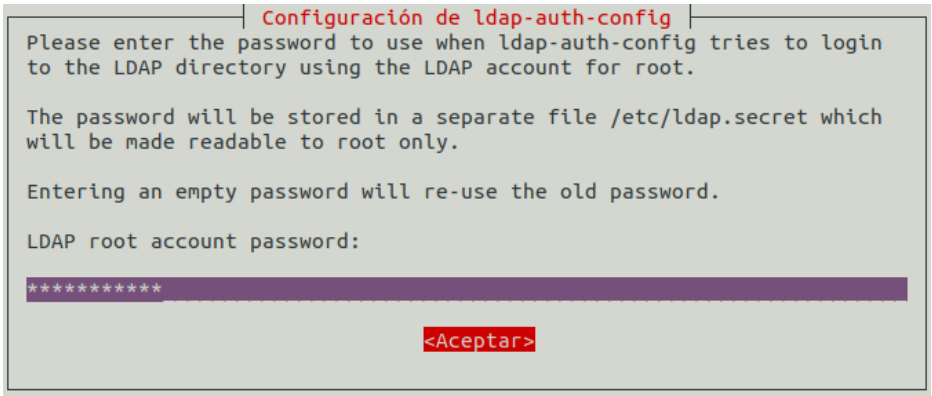
Para añadir un cliente Ubuntu, tenemos que instalar y configurar LDAP también en el cliente:

```
andrea@andrea-VirtualBox:~$ sudo apt install libnss-ldap libpam-ldap ldap-utils
 -y
```









El siguiente paso es modificar los siguientes ficheros:

```
  GNU nano 2.9.3                /etc/nsswitch.conf                Modificado

# /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:         compat ldap
group:          compat ldap
shadow:         compat ldap
gshadow:        files
```

```
  GNU nano 2.9.3            /etc/pam.d/common-password

# The "obscure" option replaces the old `OBSCURE_CHECKS_ENAB' option in
# login.defs.
#
# See the pam_unix manpage for other options.

# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules.  See
# pam-auth-update(8) for details.

# here are the per-package modules (the "Primary" block)
password        requisite                       pam_pwquality.so retry=3
password        [success=3 default=ignore]      pam_unix.so obscure use_authto$
password        sufficient                      pam_sss.so use_authtok
password        [success=1 user_unknown=ignore default=die]     pam_ldap.so us$
```

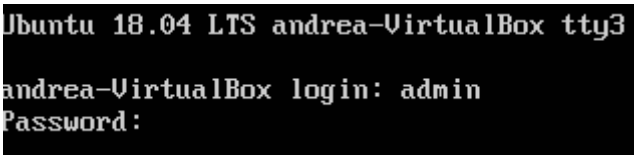
```
  GNU nano 2.9.3            /etc/pam.d/common-password            Modificado

# The "obscure" option replaces the old `OBSCURE_CHECKS_ENAB' option in
# login.defs.
#
# See the pam_unix manpage for other options.

# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules.  See
# pam-auth-update(8) for details.

# here are the per-package modules (the "Primary" block)
password        requisite                       pam_pwquality.so retry=3
password        [success=3 default=ignore]      pam_unix.so obscure use_authto$
password        [success=1 user_unknown=ignore default=die]     pam_ldap.so us$
```

```
  GNU nano 2.9.3            /etc/pam.d/common-session             Modificado

# pam-auth-update(8) for details.

# here are the per-package modules (the "Primary" block)
session [default=1]                     pam_permit.so
# here's the fallback if no module succeeds
session requisite                       pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
session required                        pam_permit.so
# The pam_umask module will set the umask according to the system default in
# /etc/login.defs and user settings, solving the problem of different
# umask settings with different shells, display managers, remote sessions etc.
# See "man pam_umask".
session optional                        pam_umask.so
# and here are more per-package modules (the "Additional" block)
session required        pam_unix.so
session optional                        pam_sss.so
session optional                        pam_ldap.so
session optional        pam_systemd.so
session optional        required pam_mkhomedir.so skel=/etc/skel/ umask=077
# end of pam-auth-update config
```

Ahora, iniciamos el servicio:

```
andrea@andrea-VirtualBox:~$ sudo systemctl start libnss-ldap
```

Reiniciamos la máquina, cerramos sesión y cuando pida nombre de usuario, pulsamos Ctrl+Alt+F3 para abrir la terminal e iniciamos sesión con un usuario de dominio:



No me deja entrar con el usuario que he configurado para LDAP.

A partir de aquí no he podido continuar porque no me funcionaban las máquinas de Windows y no ha habido forma de hacerme unas nuevas a tiempo.

3) Permitir el acceso y administración remota desde cualquier equipo cliente.

4) Crear un servidor de actualizaciones en el equipo servidor.

5) Comprobar que desde el cliente ubuntu podemos instalarnos el editor Geany.