Implementación y configuración de OpenLDAP

Instalación de OpenLDAP

Para instalar el paquete que contiene LDAP introducimos el siguente comando:

apt install slapd ldap-utils

```
root@servidor-planetas:/home/admin-servidor# apt install slapd ldap-utils
```

Generación de la contraseña de administrador

Durante el proceso de instalación estableceremos la contraseña de administrador del dominio, la cual será la siguiente:

·ldap-planetas-sa

```
Please enter the password for the admin entry in your LDAP directory.

Administrator password:

Please enter the admin password for your LDAP directory again to verify that
you have typed it correctly.

Confirm password:
```

Reconfiguración de OpenLDAP

Ya tenemos el dominio creado, pero con la configuración por defecto, asi que vamos a reconfigurarlo a nuestro gusto con el comando:

·dpkg-reconfigure slapd

```
root@servidor-planetas:/home/admin-servidor# dpkg-reconfigure slapd
debconf: unable to initialize frontend: Dialog
debconf: (No usable dialog-like program is installed, so the dialog based frontend cannot be used. at /usr/share/perl5/Debconf/FrontEnd/Dialog.pm line 79.)
debconf: falling back to frontend: Readline
Configuring slapd
-----------------

If you enable this option, no initial configuration or database will be created for you.

Omit OpenLDAP server configuration? [yes/no] no

The DNS domain name is used to construct the base DN of the LDAP directory. For example, 'foo.example.org' will create the directory with 'dc=foo, dc=example, dc=org' as base DN.

DNS domain name: planetas.sa

Please enter the name of the organization to use in the base DN of your LDAP directory.

Organization name: Planetas S.A.

Please enter the password for the admin entry in your LDAP directory.

Administrator password:

Please enter the admin password for your LDAP directory again to verify that you have typed it correctly.

Confirm password:

Do you want the database to be removed when slapd is purged? [yes/no] yes

There are still files in /var/lib/ldap which will probably break the configuration process. If you enable this option, the maintainer scripts will move the old database files out of the way before creating a new database.

Move old database? [yes/no] yes

  Backing up /etc/ldap/slapd.d in /var/backups/slapd-2.6.7+dfsg-1~exp1ubuntu8.2... done.
  Moving old database directory to /var/backups:
  - directory unknown... done.
  Creating initial configuration... done.
  Creating LDAP directory... done.
```

Una vez reconfigurado introducimos el comando “slapcat” para comprobar que se ha creado correctamente

```
[root@servidor-planetas:/home/admin-servidor# slapcat
dn: dc=planetas,dc=sa
objectClass: top
objectClass: dcObject
objectClass: organization
o: Planetas S.A.
dc: planetas
structuralObjectClass: organization
entryUUID: 298ecc20-a1ca-103f-931e-55ff67a54a74
creatorsName: cn=admin,dc=planetas,dc=sa
createTimestamp: 20250330154826Z
entryCSN: 20250330154826.046072Z#000000#000#000000
modifiersName: cn=admin,dc=planetas,dc=sa
modifyTimestamp: 20250330154826Z
```

Dominio creado

Estructura elaborada para usuarios, grupos y unidades organizativas

Para la correcta implementación de OpenLDAP voy a desarrollar una estructura clara y sencilla pero que a su vez sea plenamente lógica y funcional:

Voy a crear dos unidades organizativas las cuales serán:

·Usuarios

·Departamentos

Voy a crear los grupos correspondientes a cada departamento de la organización dentro de la unidad organizativa “Departamentos”, los cuales serán:

·Dirección gidNumber:1001

·Recursos Humanos gidNumber:1002

·IT gidNumber:1003

·Finanzas gidNumber:1004

·Marketing gidNumber:1005

·Producción gidNumber:1006

·Logistica gidNumber:1007

·Calidad gidNumber:1008

Para la estructura de usuarios voy a crear dos usuarios por cada departamento:

Dirección gidNumber:1001

- ·Guillermo Menor - Director General contraseña: guillermo
- ·Maria Acedo - Asistente de Dirección contraseña: maria

Recursos Humanos gidNumber:1002

·Romeo Menor - Secretario Ejecutivo

·Nerea Mulero - Técnico de Nóminas

IT gidNumber:1003

·Jose Prieto - Administrador de Sistemas

·David Mulero - Desarrollador Web

Finanzas gidNumber:1004

·Santiago Martin - Contable

·Estela Alvarez - Analista Financiero

Marketing gidNumber:1005

·Javier Torre - Responsable de Marketing Digital

·Justo Mulero - Diseñador Gráfico

Producción gidNumber:1006

·Orujo Prieto - Jefe de Producción

·Julia Muñoz - Operaria de Línea

Logística gidNumber:1007

·Carolina Castillo - Responsable de Almacén

·Roberto Mendoza - Supervisor de Transporte

Calidad gidNumber:1008

·Elena Navarro - Inspectora de Control de Calidad

·Alberto Ríos - Auditor de Procesos

Implementación en el domino de la estructura elaborada

Para implementar la estructura elaborada en primer lugar crearé tres archivos dentro de la ruta:

·/etc/ldap/archivos_base

En la que se incluirán los archivos:

·ou.ldif

·grupos.ldif

·usuarios.ldif

Que contendrán parámetros base de configuración para cada uno de los objetos, los cuales habrá que personalizar para cada creación de objeto en el dominio.

Unidades organizativas

Voy a comenzar por las unidades organizativas:

·Ruta del archivo ldif para la creación de unidades organizativas:

·/etc/ldap/archivos_base/ou.ldif

```
dn: ou=usuarios,dc=planetas,dc=sa
objectClass: top
objectClass: organizationalUnit
ou: usuarios

dn: ou=departamentos,dc=planetas,dc=sa
objectClass: top
objectClass: organizationalUnit
ou: departamentos
```

Las creamos mediante el comando:

·ldapadd -x -D "cn=admin,dc=planetas,dc=sa" -w "ldap-planetas-sa" -f ou.ldif

```
root@servidor-planetas:/etc/ldap/archivos_base# ldapadd -x -D "cn=admin,dc=planetas,dc=sa" -w "ldap-planetas-sa" -f ou.ldif
adding new entry "ou=usuarios,dc=planetas,dc=sa"

adding new entry "ou=departamentos,dc=planetas,dc=sa"
```

Unidades organizativas creadas

Grupos

A continuación voy a crear los grupos por cada departamento:

·Ruta del archivo ldif para la creación de grupos:

·/etc/ldap/archivos_base/grupos.ldif

```
dn: cn=Dirección,ou=departamentos,dc=planetas,dc=sa
objectClass: top
objectClass: posixGroup
cn: Dirección
gidNumber: 1001

dn: cn=Recursos Humanos,ou=departamentos,dc=planetas,dc=sa
objectClass: top
objectClass: posixGroup
cn: Recursos Humanos
gidNumber: 1002

dn: cn=IT,ou=departamentos,dc=planetas,dc=sa
objectClass: top
objectClass: posixGroup
cn: IT
gidNumber: 1003

dn: cn=Finanzas,ou=departamentos,dc=planetas,dc=sa
objectClass: top
objectClass: posixGroup
cn: Finanzas
gidNumber: 1004

dn: cn=Marketing,ou=departamentos,dc=planetas,dc=sa
objectClass: top
objectClass: posixGroup
cn: Marketing
gidNumber: 1005

dn: cn=Producción,ou=departamentos,dc=planetas,dc=sa
objectClass: top
objectClass: posixGroup
cn: Producción
gidNumber: 1006

dn: cn=Logística,ou=departamentos,dc=planetas,dc=sa
objectClass: top
objectClass: posixGroup
cn: Logística
gidNumber: 1007

dn: cn=Calidad,ou=departamentos,dc=planetas,dc=sa
objectClass: top
objectClass: posixGroup
cn: Calidad
gidNumber: 1008
```

Lo añadimos con el comando:

·ldapadd -x -D "cn=admin,dc=planetas,dc=sa" -w "ldap-planetas-sa" -f grupos.ldif

```
root@servidor-planetas:/etc/ldap/archivos_base# ldapadd -x -D "cn=admin,dc=planetas,dc=sa" -w "ldap-planetas-sa" -f grupos.ldif
adding new entry "cn=Dirección,ou=departamentos,dc=planetas,dc=sa"

adding new entry "cn=Recursos Humanos,ou=departamentos,dc=planetas,dc=sa"

adding new entry "cn=IT,ou=departamentos,dc=planetas,dc=sa"

adding new entry "cn=Finanzas,ou=departamentos,dc=planetas,dc=sa"

adding new entry "cn=Marketing,ou=departamentos,dc=planetas,dc=sa"

adding new entry "cn=Producción,ou=departamentos,dc=planetas,dc=sa"

adding new entry "cn=Logística,ou=departamentos,dc=planetas,dc=sa"

adding new entry "cn=Calidad,ou=departamentos,dc=planetas,dc=sa"
```

Grupos creados

Usuarios

Finalmente creamos los usuarios:

·Ruta del archivo ldif para la creación de grupos:

·/etc/ldap/archivos_base/usuarios.ldif

De momento voy a crear solo dos usuarios para las pruebas, crearé todos los usuarios cuando implemente el servidor NFS

```
dn: uid=guillermo,ou=usuarios,dc=planetas,dc=sa
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: Guillermo Menor
sn: Menor
uid: guillermo
uidNumber: 2001
gidNumber: 1001
homeDirectory: /home/guillermo
loginShell: /bin/bash
userPassword: {SSHA}uyU7/Xjk73K86hue137oH60ilTWjkt0x

dn: uid=maria,ou=usuarios,dc=planetas,dc=sa
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: Maria Acedo
sn: Acedo
uid: maria
uidNumber: 2002
gidNumber: 1001
homeDirectory: /home/maria
loginShell: /bin/bash
userPassword: {SSHA}3LTu73NISkV+442NrxuHRkFf+T/13uCn
```

Lo añadimos con el comando:

·ldapadd -x -D "cn=admin,dc=planetas,dc=sa" -w "ldap-planetas-sa" -f usuarios.ldif

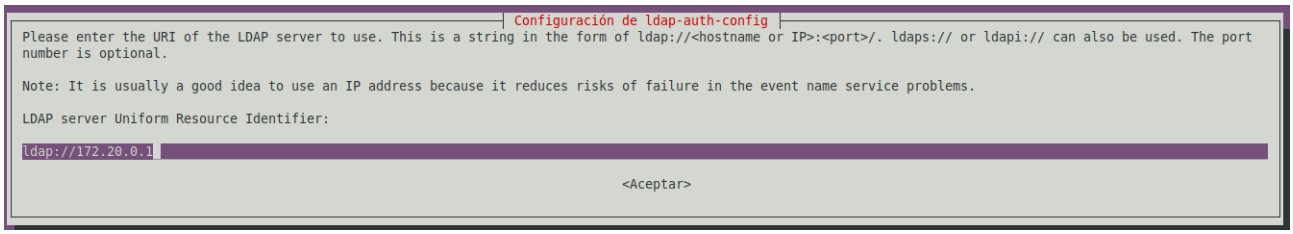
```
root@servidor-planetas:/etc/ldap/archivos_base# ldapadd -x -D "cn=admin,dc=planetas,dc=sa" -w "ldap-planetas-sa" -f usuarios.ldif
adding new entry "uid=guillermo,ou=usuarios,dc=planetas,dc=sa"

adding new entry "uid=maria,ou=usuarios,dc=planetas,dc=sa"
```

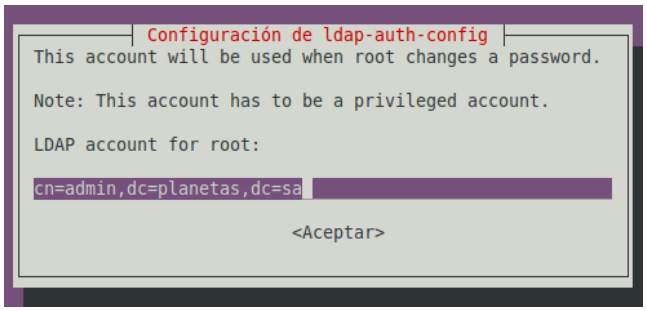
Usuarios creados

Configuración en equipo-cliente para el inicio de sesión

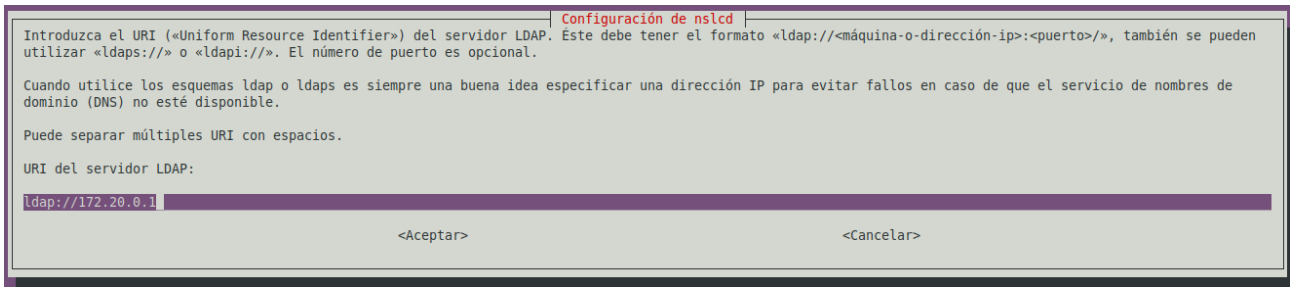
Habrá que instalar los siguientes paquetes:

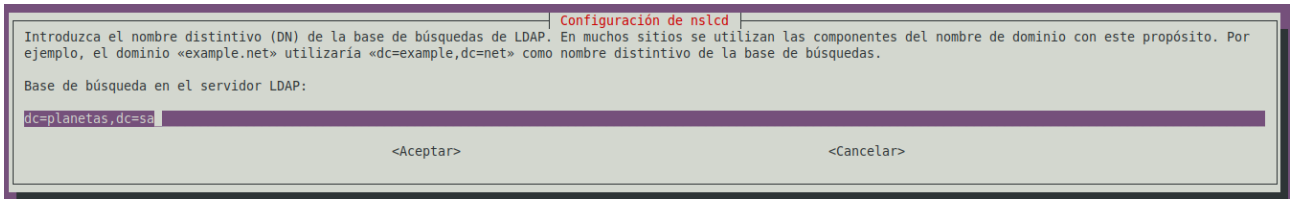
·apt install libnss-ldap libpam-ldap ldap-utils nscd -y



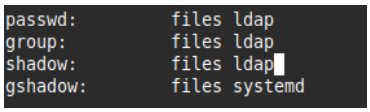


Instalo nslcd





Modifico /etc/nsswitch.conf

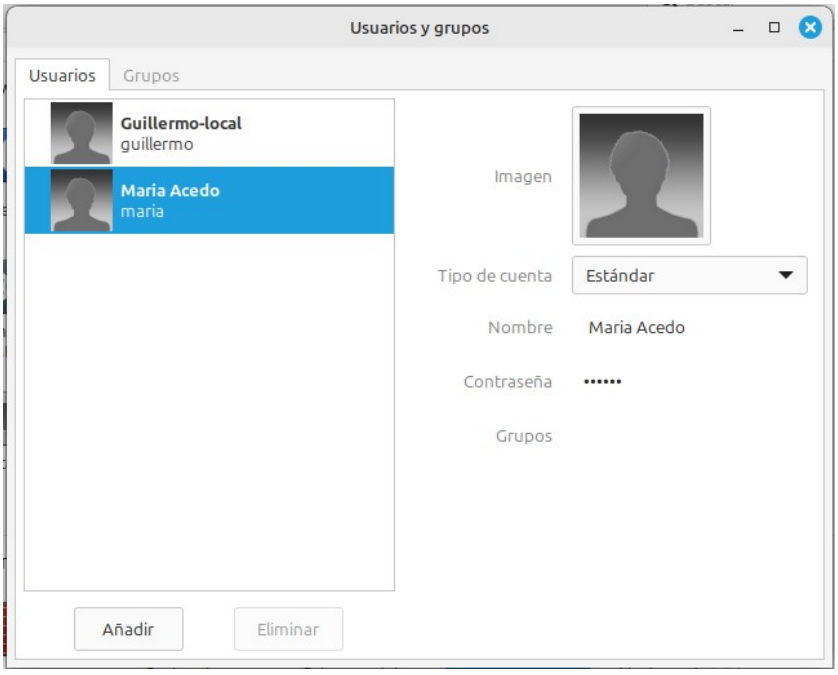


Modifico /etc/pam.d/common-session

```
session optional        pam_mkhomedir.so skel=/etc/skel umask=077
```

Pruebas de inicio de sesión en equipo-cliente

Pruebo el inicio de sesión grafico con el usuario “maria”:



Ya puedo iniciar sesión en equipo-cliente con los usuarios de OpenLDAP