RETO 4:

OpenLDAP

**Patricia Bastida Merino**

**Javier Díaz Expósito**

**INDICE**

1. **ENUNCIADO DEL RETO……………………………………...…2**

**2 CONFIGURACIÓN DEL SERVIDOR……………………………3**

**3­ CONFIGURACION DE MAQUINAS CLIENTE……………….14**

1. **ENUNCIADO DEL RETO**

En el mismo servidor en el que hemos instalado el router y el servidor SSH queremos instalar y configurar un ***servidor OpenLdap*** sobre el dominio ***xxxx.olimpo.god***, siendo *xxxx* el nombre correspondiente al dios de vuestro espacio de trabajo.

Los nombres de los dioses serán los siguientes: **Zeus | Atenea | Hera | Poseidón | Afrodita**

Por lo tanto, los dominios serán:

(GRUPO 1) 🡪 zeus.olimpo.god

(GRUPO 2) 🡪 atenea.olimpo.god

(GRUPO 3) 🡪 hera.olimpo.god

(GRUPO 4) 🡪 poseidon.olimpo.god

**Máquinas conocidas:**

* ***router:*** esta máquina es la que nos da salida al exterior
* ***dns:*** esta máquina es la misma que el router, pero nos ofrece resolución de nombres
* ***ninfa:*** es la máquina cliente dentro de vuestra red.
* ***Oráculo:*** máquina que tiene instalado el servicio FTP y donde instalaremos Apache.
* ***Bastis:*** Maquina donde instalaremos el Tomcat.

**Teniendo en cuenta todo lo anterior, se te pide lo siguiente:**

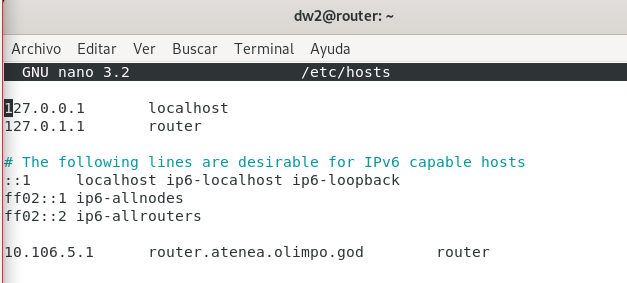
1. **CONFIGURACIÓN DEL SERVIDOR**

Instala y configuraun servidor OpenLdap en Debian 10**.** El dominio será atenea.olimpo.god:

*sudo nano /etc/hosts*

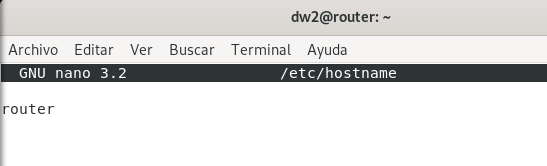
Añadimos los siguientes datos:

|  |
| --- |
| 127.0.0.1 localhost  127.0.1.1 router  10.106.5.1 router.atenea.olimpo.god router |
|  |
|  |



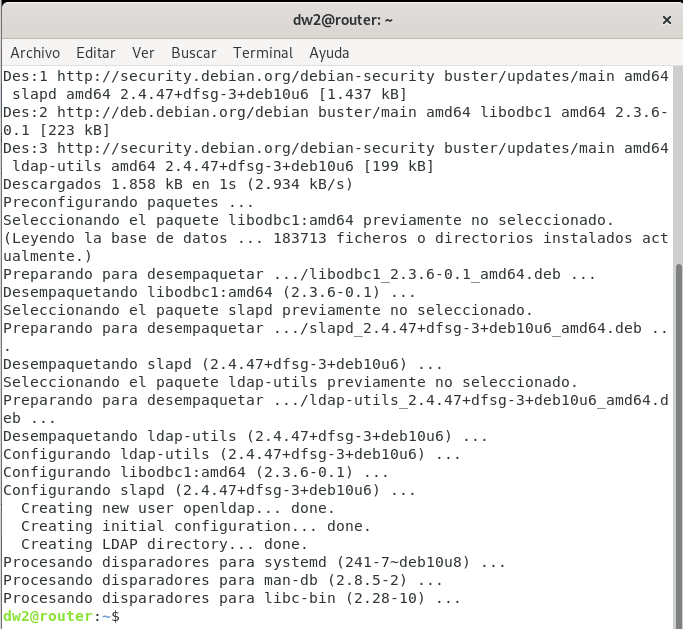
*sudo nano /etc/hostname*

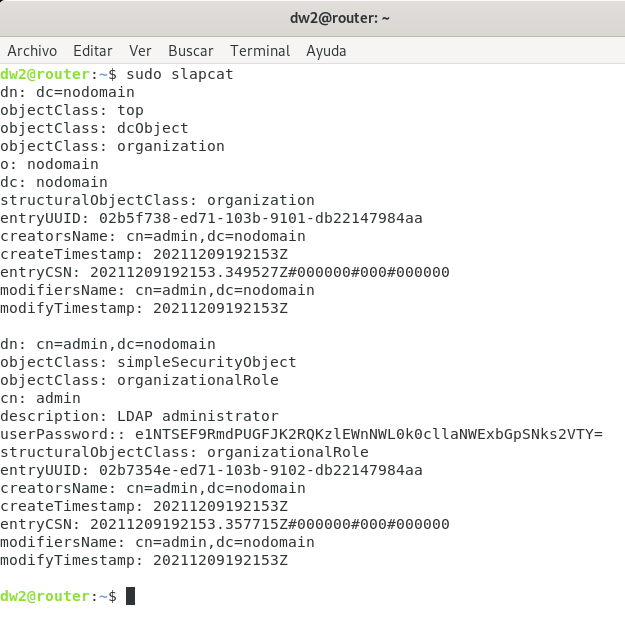
Añadimos en este archivo la palabra *router*. Es lo único que debe contener el archivo.

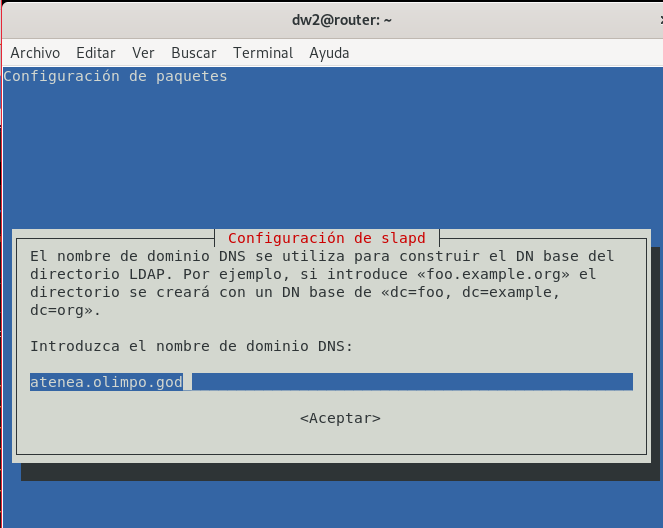


Ahora tenemos que instalar OpenLdap:

sudo apt-get install slapd idap-utils -y



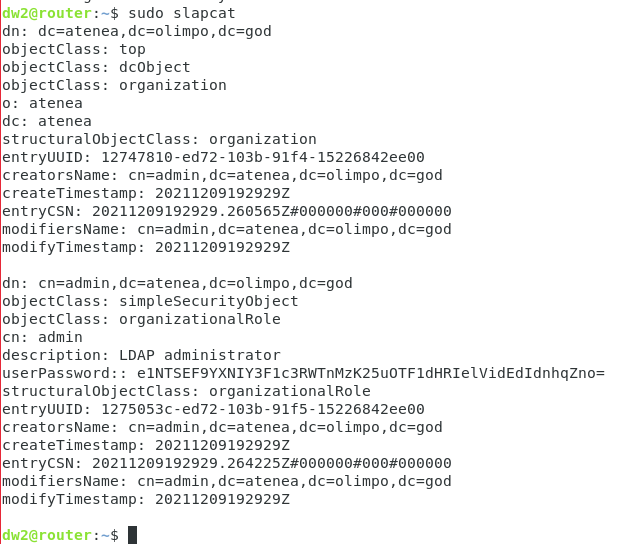






Mostrar que se ha creado correctamente el dominio.

*sudo slapcat*



Crear un fichero “unidades\_organizativas.ldif”. Habrá dos unidades organizativas: “profesores” y “alumnos”.

*sudo nano unidades\_organizativas.ldif*

|  |
| --- |
| *dn: ou=profesores,dc=atenea,dc=olimpo,dc=god*  *objectClass: organizationalUnit*  *ou: profesores*  *dn: ou=alumnos,dc=atenea,dc=olimpo,dc=god*  *objectClass: organizationalUnit*  *ou: alumnos* |

*sudo ldapadd -x -D cn=admin,dc=atenea,dc=olimpo,dc=god -W -f unidades\_organizativas.ldif*

Crear un fichero “usuarios.ldif”. Mediante este fichero vamos a crear el usuario “profe1” en la unidad organizativa “profesores”, y los usuarios “usu1” y “usu2” en la unidad organizativa “alumnos”. Añade todos los objectClass y atributos que consideres necesarios.

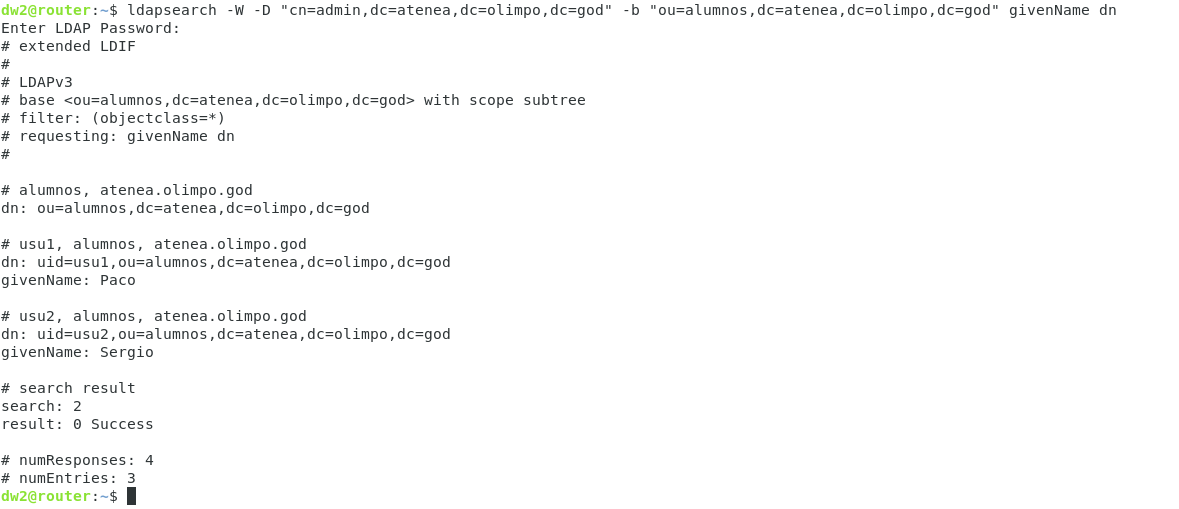
*sudo nano usuarios.ldif*

|  |
| --- |
| *dn: uid=profe1,ou=profesores,dc=atenea,dc=olimpo,dc=god*  *objectClass: inetOrgPerson*  *objectClass: posixAccount*  *objectClass: shadowAccount*  *uid: profe1*  *sn: Lopez*  *givenName: Juan*  *cn: Juan Lopez*  *uidNumber: 2000*  *gidNumber: 10000*  *userPassword: dw2*  *homeDirectory: /home/profe1*  *dn: uid=usu1,ou=alumnos,dc=atenea,dc=olimpo,dc=god*  *objectClass: inetOrgPerson*  *objectClass: posixAccount*  *objectClass: shadowAccount*  *uid: usu1*  *sn: Gomez*  *givenName: Paco*  *cn: Paco Gomez*  *uidNumber: 2001*  *gidNumber: 20001*  *userPassword: dw2*  *homeDirectory: /home/usu1*  *dn: uid=usu2,ou=alumnos,dc=atenea,dc=olimpo,dc=god*  *objectClass: inetOrgPerson*  *objectClass: posixAccount*  *objectClass: shadowAccount*  *uid: usu2*  *sn: Garcia*  *givenName: Sergio*  *cn: Sergio Garcia*  *uidNumber: 2002*  *gidNumber: 20001*  *userPassword: dw2*  *homeDirectory: /home/usu2* |

*sudo* ldapadd -x -D cn=admin,dc=atenea,dc=olimpo,dc=god -W -f usuarios.ldif

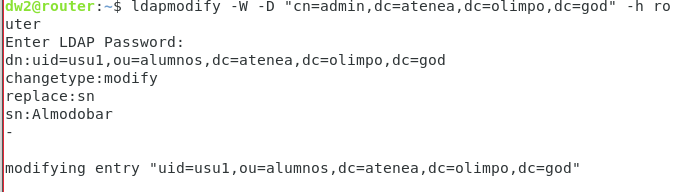
Utilizando un comando “ldap” para mostrar todos los elementos del directorio que pertenecen a la unidad organizativa “alumnos”.

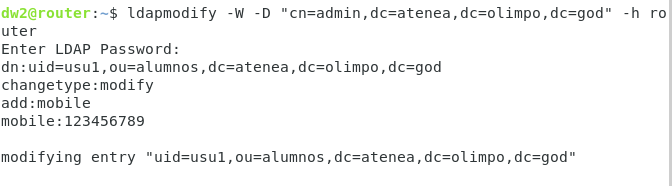
*ldapsearch -W -D “cn=admin,dc=atenea,dc=olimpo,dc=god” -b “ou=alumnos, dc=atenea,dc=olimpo,dc=god” givenName dn*



Investigar cómo utilizar el comando “ldapmodify” y cambia el apellido al usuario “usu1” de la unidad organizativa “alumnos” y añádele el número de teléfono.

*sudo nano modificar.ldif -W -D “cn=admin,dc=atenea,dc=olimpo,dc=god” -h router*





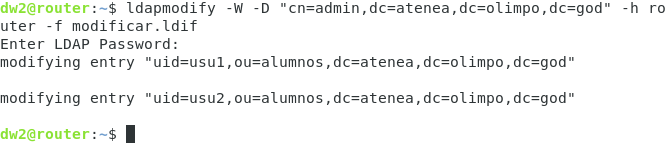
Busca información sobre los atributos que pueden tener entradas con los siguientes objectClass: organizationalUnit, inetOrgPerson, posixAccount y organizationalRole.

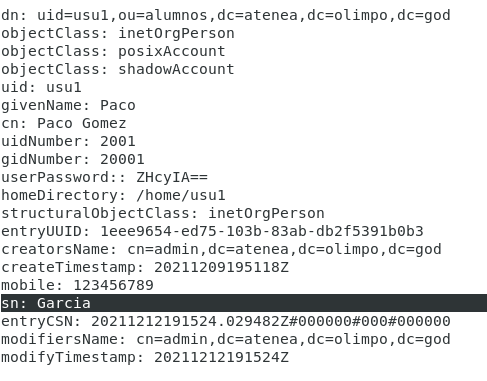
Señala los atributos que debe tener la entrada obligatoriamente para cada uno de ellos.

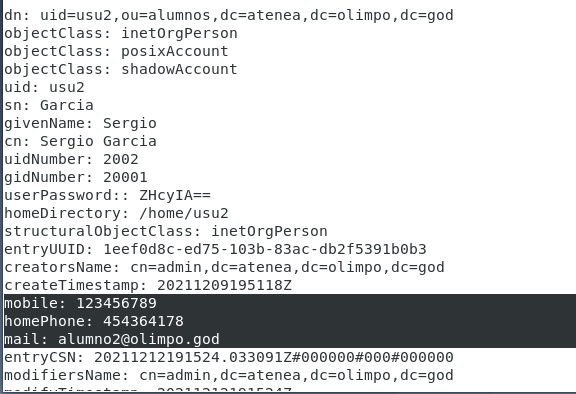
Crear un fichero “modificar.ldif”. Mediante este fichero modificarás un atributo del alumno “usu1” (cualquira) y añadiras tres atributos que no tenía a la entrada de “usu2”.

*sudo nano modificar.ldif*

|  |
| --- |
| dn:uid=usu1,ou=alumnos,dc=atenea,dc=olimpo,dc=god  changetype:modify  replace:sn  sn:Garcia  dn:uid=usu2,ou=alumnos,dc=atenea,dc=olimpo,dc=god  changetype:modify  add:mobile  mobile: 123456789  -  add:homePhone  homePhone: 454364178  -  add: mail  mail: [alumno2@olimpo.god](mailto:alumno2@olimpo.god) |







Crear un archivo ldif para añadir un nuevo profesor “profe2” y un alumno más a los existentes “usu3”.

*sudo nano usuarios2.ldif*

|  |
| --- |
| dn: uid=profe2,ou=profesores,dc=atenea,dc=olimpo,dc=god  objectClass: inetOrgPerson  objectClass: posixAccount  objectClass: shadowAccount  uid: profe2  sn: Gomez  givenName: Alfredo  cn: Alfredo Gomez  uidNumber: 2004  gidNumber: 10000  userPassword: dw2  homeDirectory: /home/profe2  dn: uid=usu3,ou=alumnos,dc=atenea,dc=olimpo,dc=god  objectClass: inetOrgPerson  objectClass: posixAccount  objectClass: shadowAccount  uid: usu3  sn: Sanchez  givenName: Pedro  cn: Pedro Sanchez  uidNumber: 2003  gidNumber: 20001  userPassword: dw2  homeDirectory: /home/usu3 |

*sudo ldapadd -x -D cn=admin,dc=atenea,dc=olimpo,dc=god -W -f usuarios2.ldif*

Muestra de nuevo todos los elementos del directorio que pertenecen a la unidad organizativa “profesores” y “alumnos”.



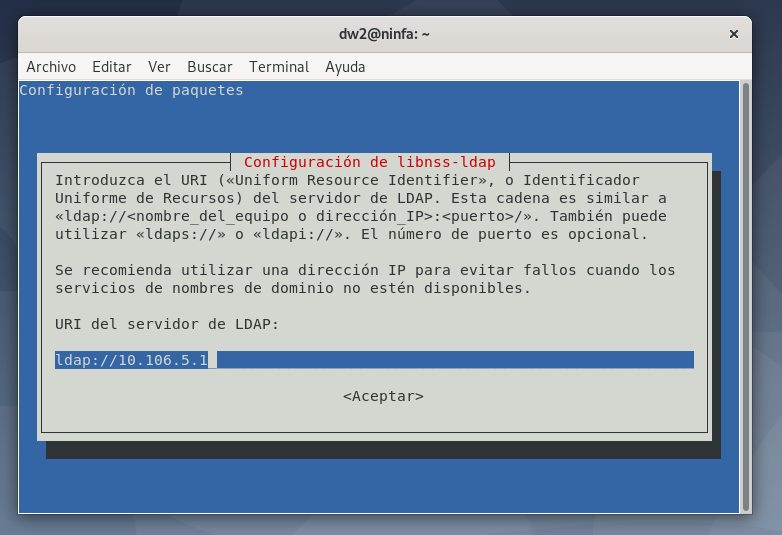


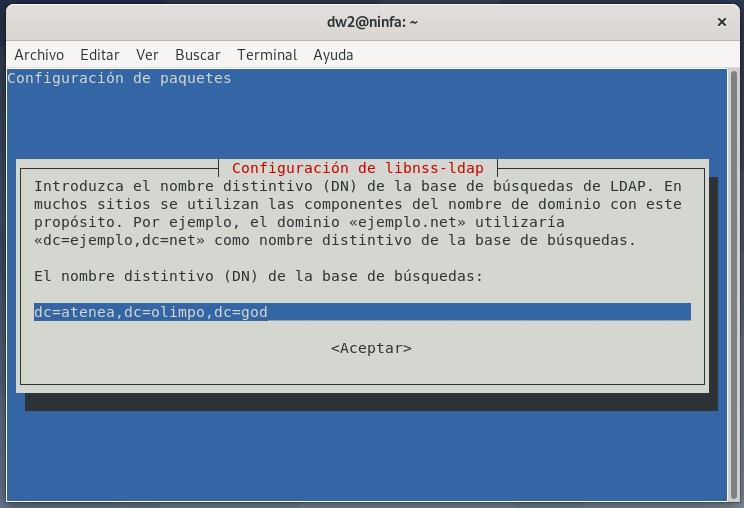
1. **CONFIGURACION DE MAQUINAS CLIENTE**

Configura los diferentes clientes/máquinas de la red para que puedan autenticarse contra el servidor OpenLdap.

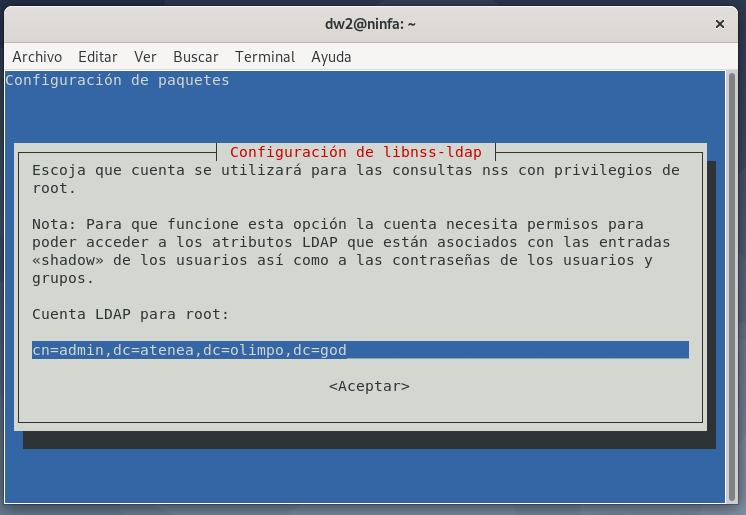
\*Instalación de paquetes necesarios:

*sudo apt-get install libnss-ldap libpam-ldap ldap-utils -y*

****

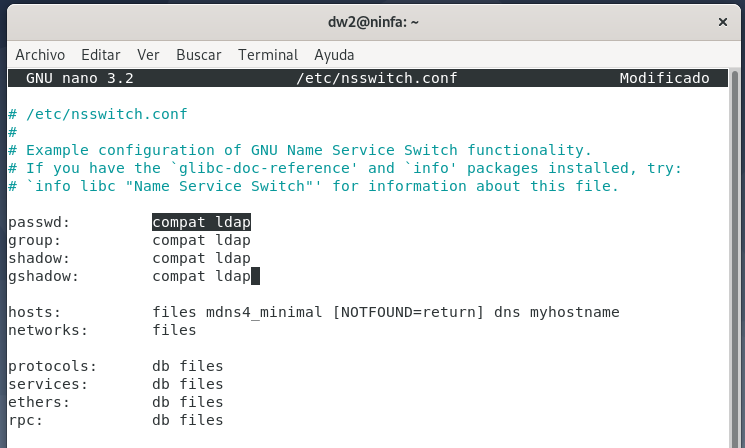
****

****

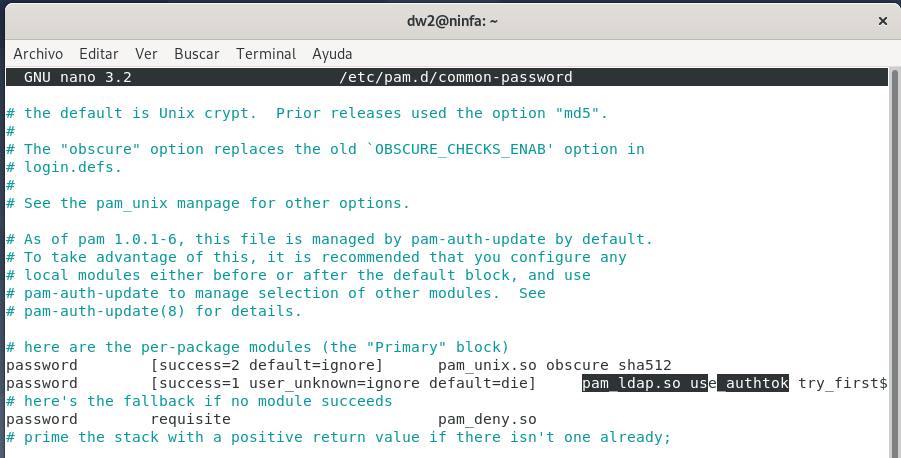
****

Introducimos el siguiente comando y cambiamos el valor de passwd, group, shadow y de gshadow por compat ldap en todas ellas.

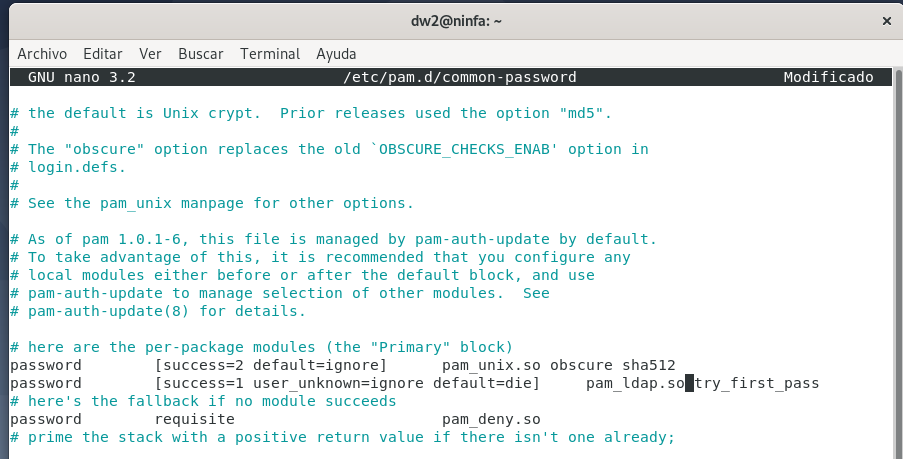
*sudo nano /etc/nsswitch.conf*

****

*sudo nano /etc/pam.d/common-password*

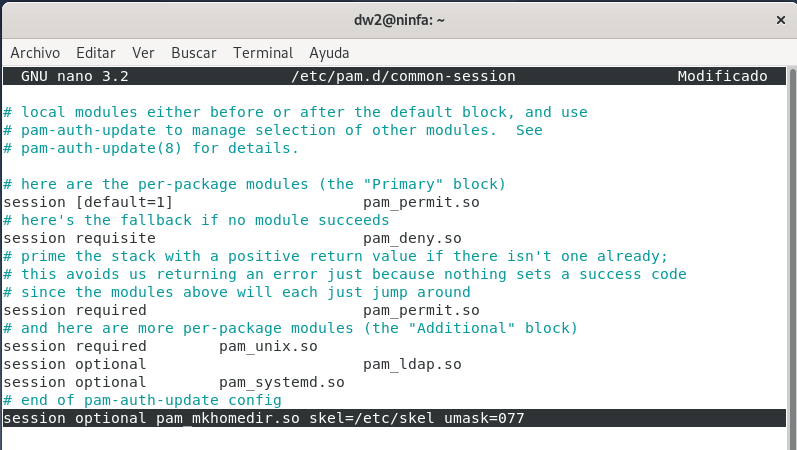
****

Hay que eliminar use\_authtok:

****

*sudo nano /etc/pam.d/common-sesion*

Añadimos en la última línea del archivo lo seleccionado en la siguiente captura:

****

Instalamos el programa sysy-rc-conf con el siguiente comando:

*sudo apt-get install sysv-rc-conf*

Y ahora lo activamos libnss-ldap con el siguiente comando:

*sudo sysv-conf libnss-ldap on*

Reiniciamos la máquina cliente y comprobamos que logea:

