

LDAP

(Lightweight Directory Access Protocol)

(Lightweight Directory Access Protocol)

DNS

(Domain Name System)



+ Alice



+ Alice



+ Alice



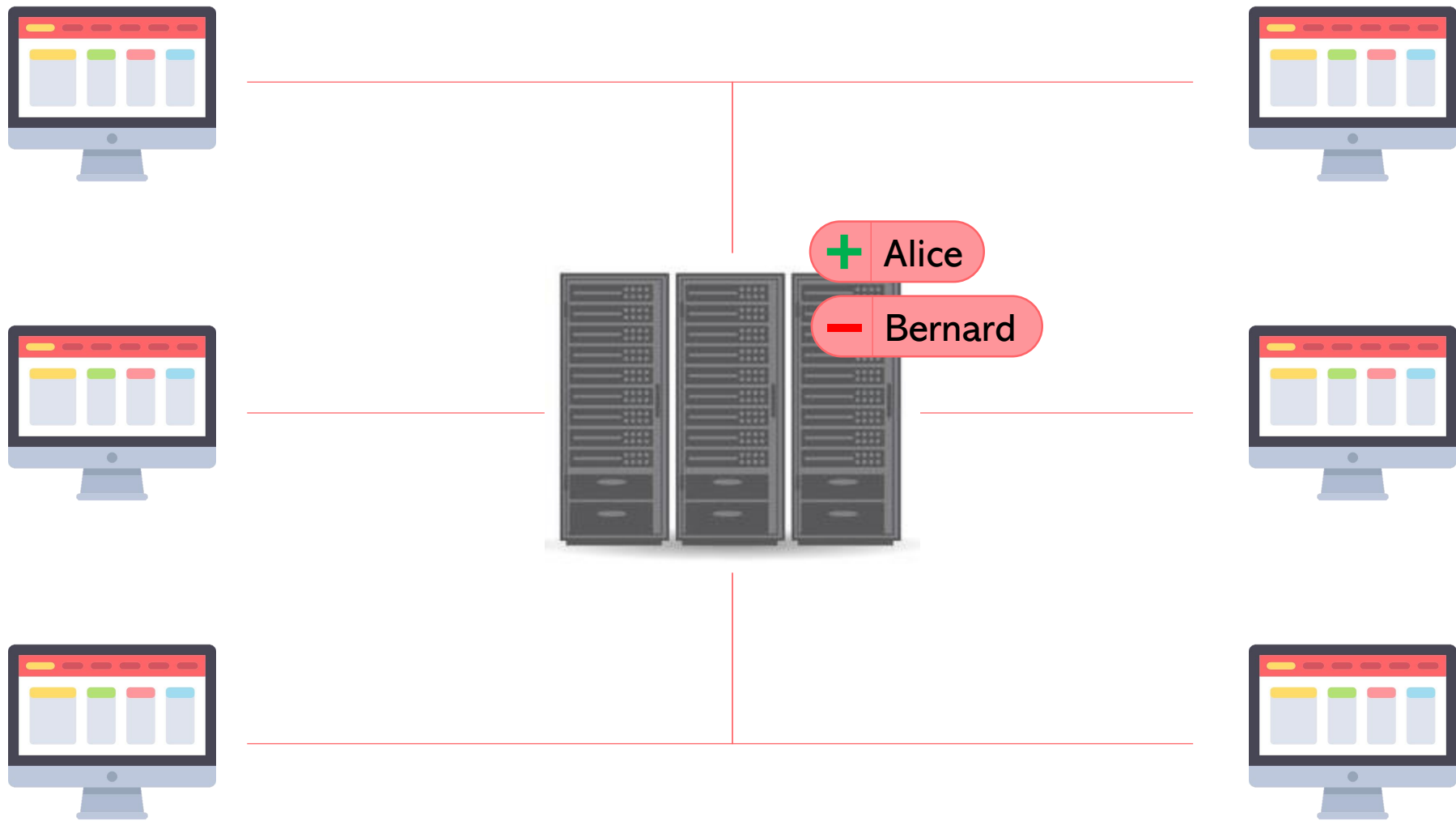
+ Alice



+ Alice



+ Alice



Autenticación

Autorización

Consulta: búsquedas y lecturas

Actualización: escrituras

Start TLS

Bind

Search

Compare

Add

Delete

Modify

Modify Distinguished Name

Abandon

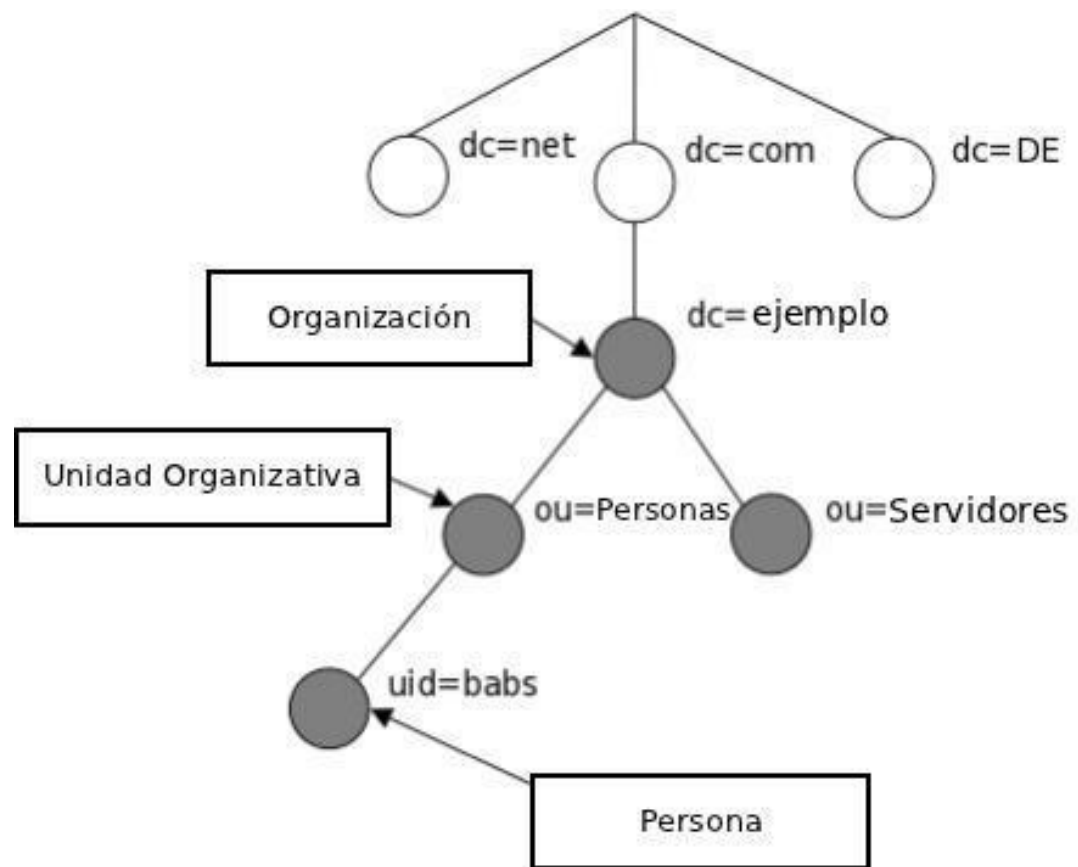
Extended Operation

Unbind



TCP (P 389)

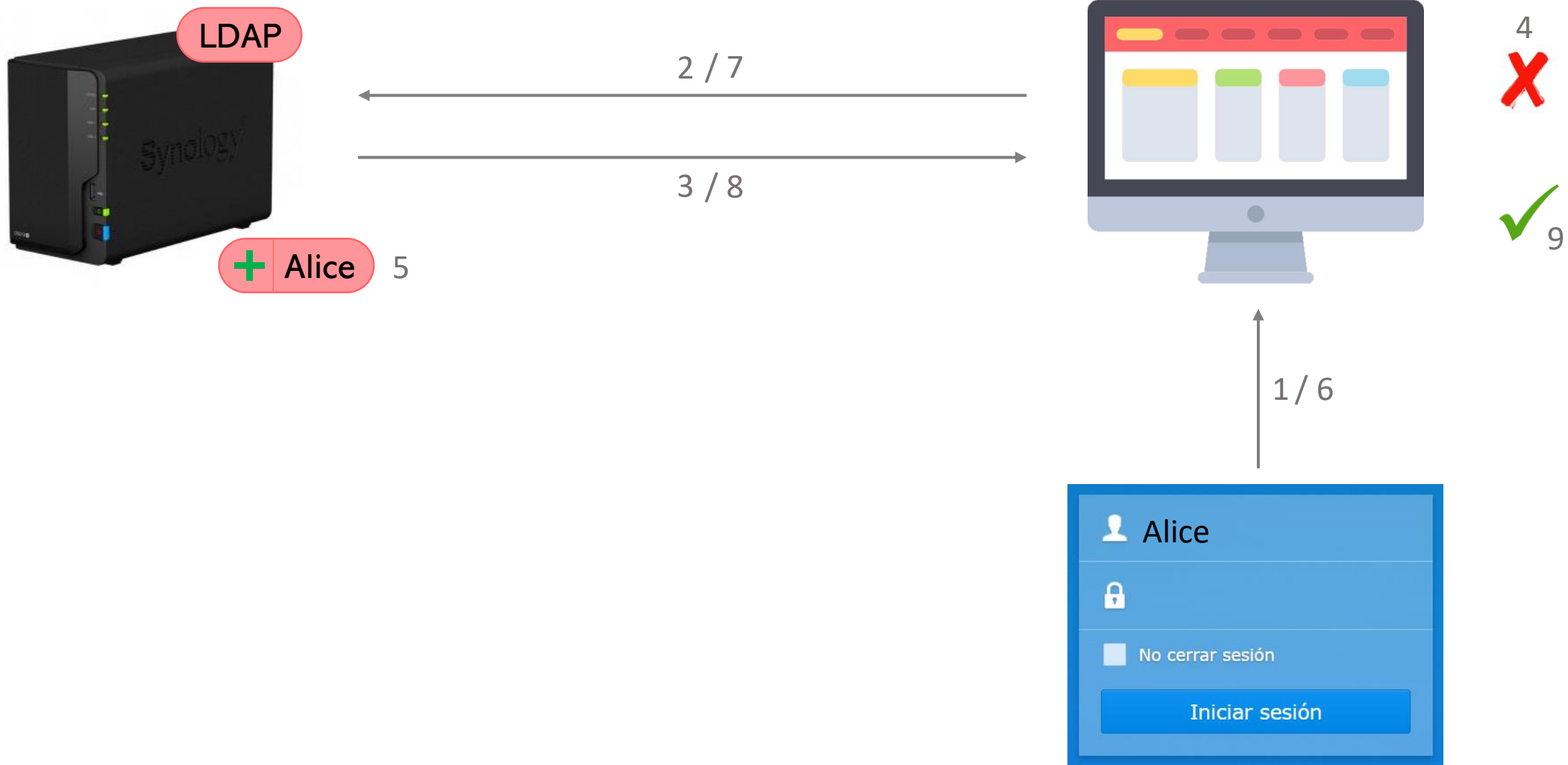
RFC 4511 (LDAPv3)



dn: cn=John Doe,dc=example,dc=com
cn: John Doe
givenName: John
sn: Doe
telephoneNumber: +1 888 555 6789
telephoneNumber: +1 888 555 1232
mail: john@example.com
manager: cn=Barbara Doe,dc=example,dc=com
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: top

LDAP

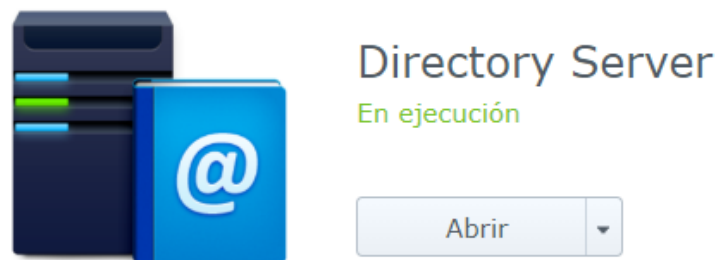
¿Qué vamos a hacer?



LDAP

¿Cómo hacerlo?

Instalación Servidor



Instalación Servidor

Configuración

Copia de seguridad y restaurar

Administrar usuarios

Administrar grupos

Inicio de sesión único (SSO) de G Suite

Directory Server

?

—

□

×

Servidor

☒ Activar servidor LDAP

☒ Como el servidor proveedor

FQDN:

Contraseña:

Confirmar contraseña:

☐ Como el servidor Consumer de Synology Directory Server

Proveedor dirección:

Cifrado:

Base DN:

Nombre de usuario:

Contraseña:

Estado de la conexión: --

Configuración de la conexión

Información de autenticación

Base DN:

Bind DN:

Aplicar

Restablecer

Instalación Servidor

Información del usuario

Rellenar los siguientes campos

Nombre *:	<input type="text" value="Usuario Redes 2"/>
Descripción:	<input type="text" value="Usuario para la prueba de rede"/>
Correo electrónico *:	<input type="text" value="redes@redes.com"/>
Contraseña *:	<input type="password" value="....."/>
Confirmar contraseña *:	<input type="password" value="....."/>

☐ No permitir que el usuario cambie la contraseña de la cuenta

☐ Deshabilitar esta cuenta

☒ Inmediatamente

☐ Después de:

* Este campo es obligatorio.

Unir grupos

Seleccione grupos:

Nombre	Descripción	<input type="checkbox"/> Agregar
users	Directory default group	<input checked="" type="checkbox"/>
Directory Operators	Directory default admin group	<input type="checkbox"/>
Directory Clients	Directory default client group	<input type="checkbox"/>
Directory Consumers	Directory default consumer group	<input type="checkbox"/>
administrators	System default admin group	<input type="checkbox"/>

Más atributos

Editar atributos adicionales del usuario

Número de empleado:	<input type="text"/>
Departamento:	<input type="text"/>
Tipo de empleado:	<input type="text"/>
Título:	<input type="text"/>
Teléfono del trabajo:	<input type="text"/>
Teléfono de casa:	<input type="text"/>
Teléfono móvil:	<input type="text"/>
Dirección:	<input type="text"/>
Fecha de nacimiento	<input type="text"/>

Probar el funcionamiento del servidor LDAP

```
ldapsearch -H "ldap://<URI>" -b "<Base DN>"
```

Instalación Cliente

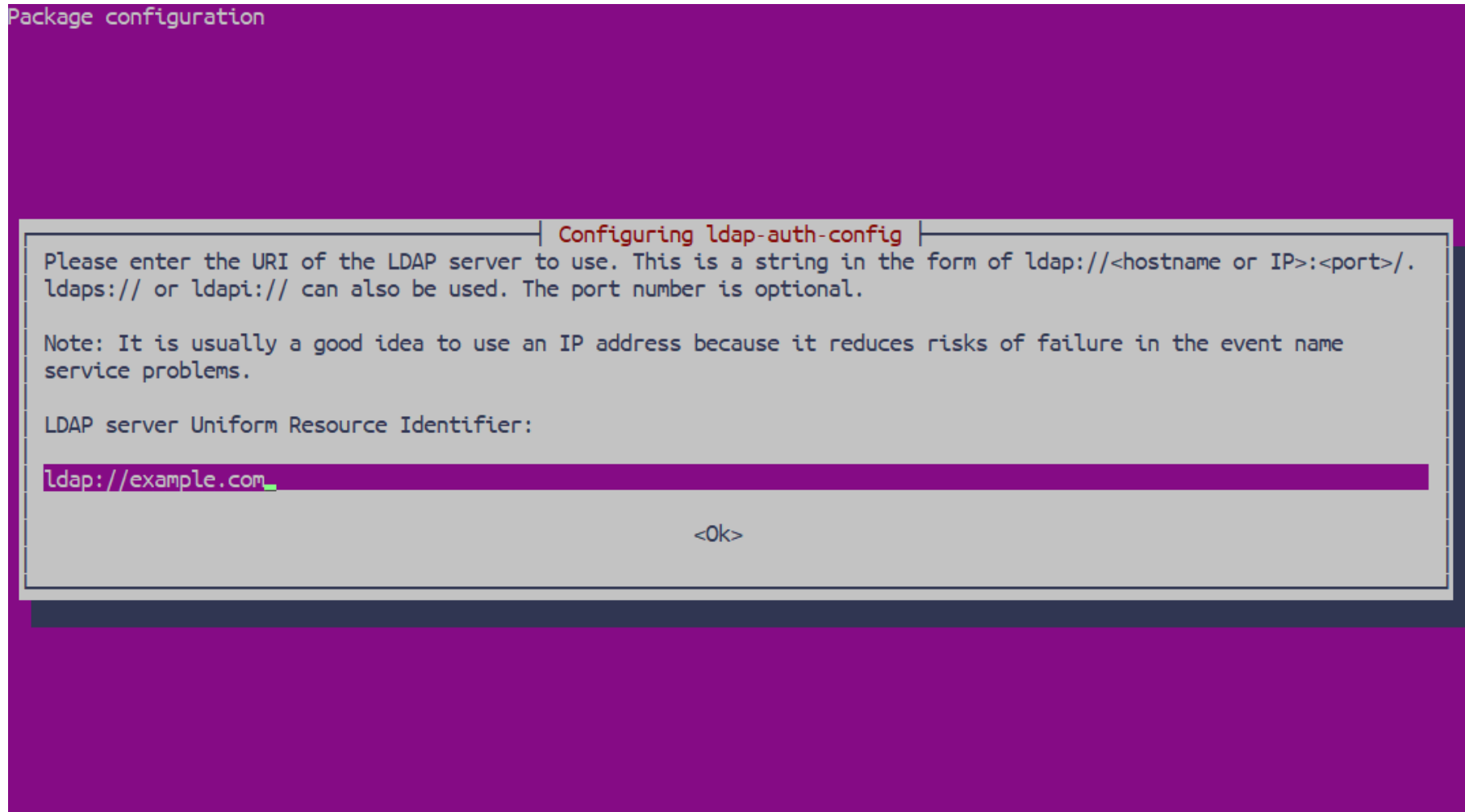
Debemos instalar los paquetes que se vayan a necesitar. *Es recomendable que antes de instalar actualicemos la librería de programas instalables.*

```
sudo apt-get update
```

```
sudo apt-get -y install libnss-ldap libpam-ldap ldap-utils nscd
```

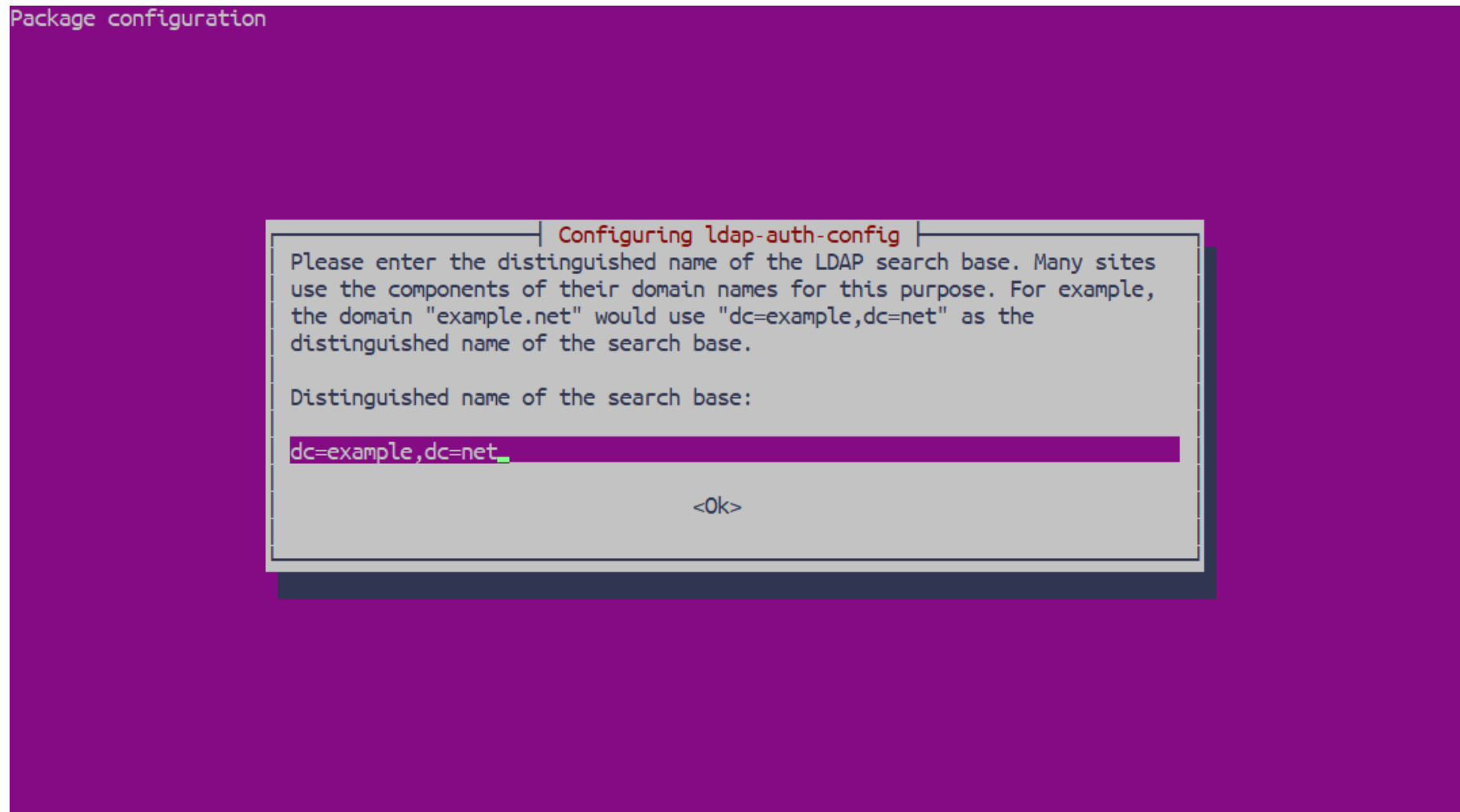
Las siguientes imágenes se corresponden con la configuración del cliente **nscd**. Sirven como guía, aunque es preferible leer para comprobar que se está configurando de la manera deseada.

Instalación Cliente



Debemos modificar el prefijo por defecto (*ldapi:///*) por (*ldap://*) tal y como se muestra en la imagen.

Instalación Cliente



Ponemos la *Base DN* del servidor LDAP.

Instalación Cliente

Package configuration

Configuring ldap-auth-config

Please enter which version of the LDAP protocol should be used by ldapns. It is usually a good idea to set this to the highest available version.

LDAP version to use:

☒ 3

☐ 2

<Ok>

Instalación Cliente

Package configuration

Configuring ldap-auth-config

This option will allow you to make password utilities that use pam to behave like you would be changing local passwords.

The password will be stored in a separate file which will be made readable to root only.

If you are using NFS mounted /etc or any other custom setup, you should disable this.

Make local root Database admin:

☒ <Yes>

☐ <No>

Instalación Cliente

Package configuration

Configuring ldap-auth-config

Choose this option if you are required to login to the database to retrieve entries.

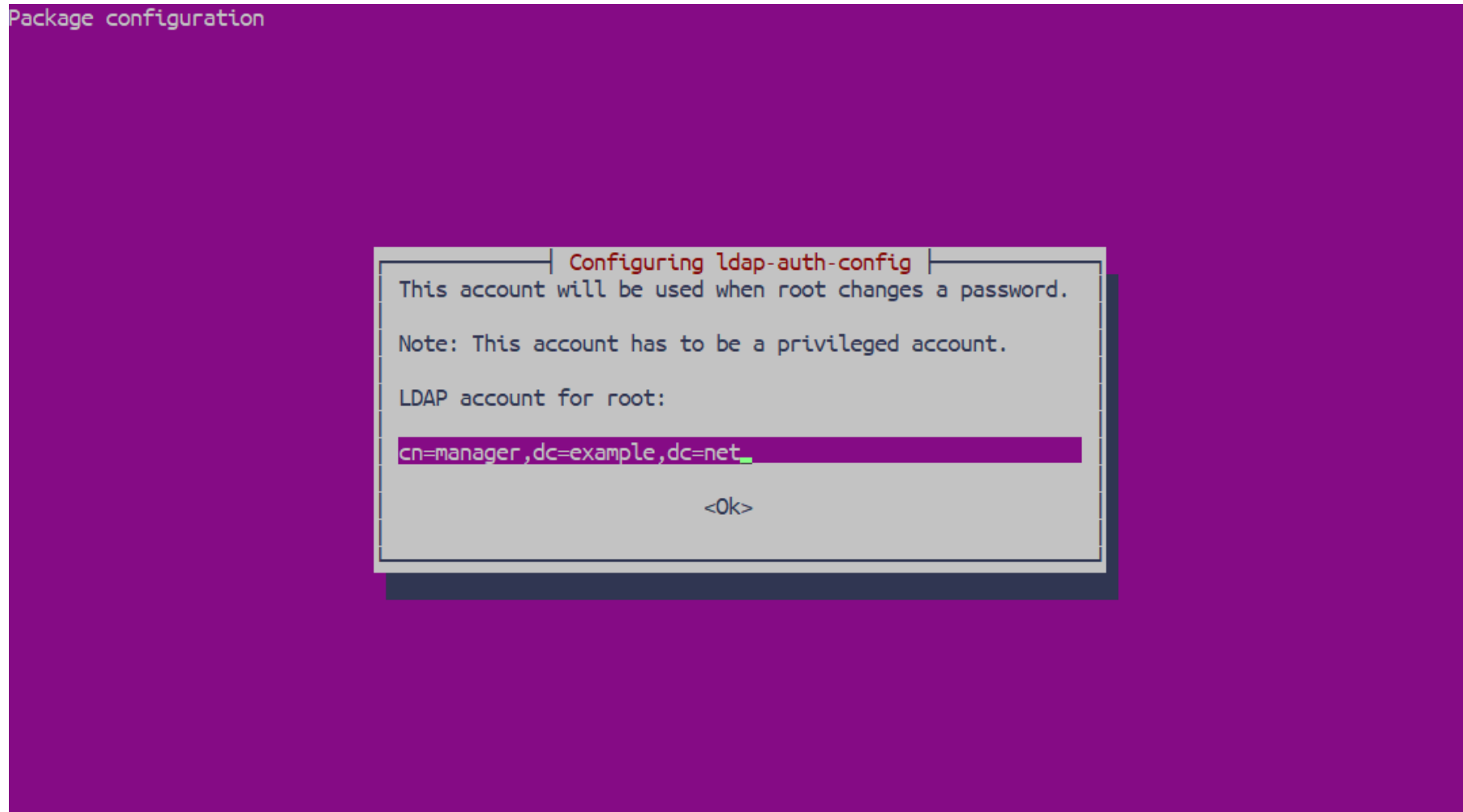
Note: Under a normal setup, this is not needed.

Does the LDAP database require login?

<Yes>

<No>

Instalación Cliente



Ponemos la *Bind DN* del servidor LDAP.

Instalación Cliente

Package configuration

Configuring ldap-auth-config

Please enter the password to use when ldap-auth-config tries to login to the LDAP directory using the LDAP account for root.

The password will be stored in a separate file /etc/ldap.secret which will be made readable to root only.

Entering an empty password will re-use the old password.

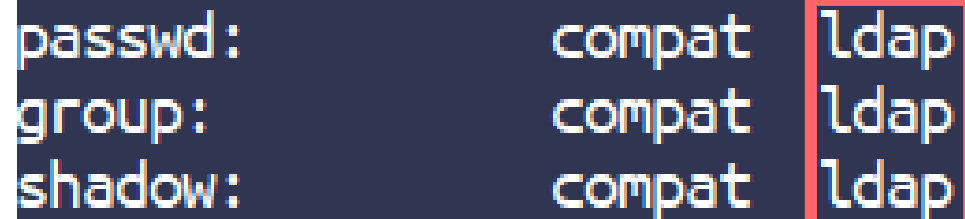
LDAP root account password:

<Ok>

Instalación Cliente

Debemos editar el siguiente archivo, e introducir **ldap** donde se especifica en la imagen:

```
sudo vim /etc/nsswitch.conf
```



```
passwd:      compat ldap
group:       compat ldap
shadow:      compat ldap
```

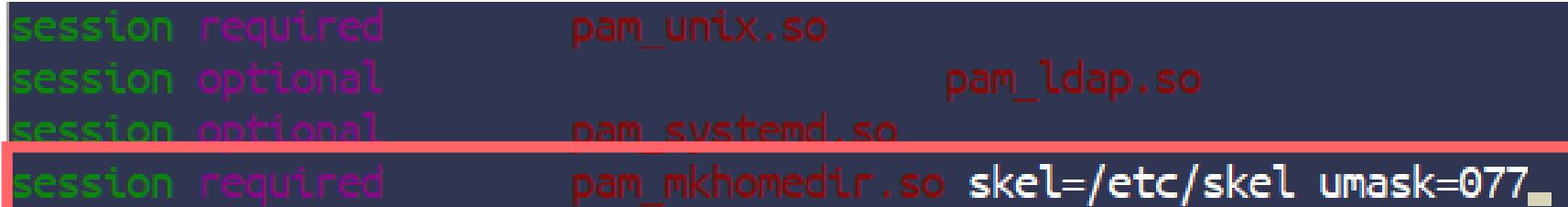

Instalación Cliente

Debemos editar el siguiente archivo, e introducir al final del mismo la línea:

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

Tal y como se especifica en la imagen:

```
sudo vim /etc/pam.d/common-session
```

A screenshot of a terminal window showing the contents of the file /etc/pam.d/common-session. The file contains four lines of PAM configuration. The first three lines are: 'session required pam_unix.so', 'session optional pam_ldap.so', and 'session optional pam_systemd.so'. The fourth line, which is highlighted with a red rectangular box, is 'session required pam_mkhomedir.so skel=/etc/skel umask=077_'. The text is color-coded: 'session' is green, 'required' is purple, 'optional' is green, and the module names and options are red. A cursor is visible at the end of the fourth line.

```
session required          pam_unix.so
session optional          pam_ldap.so
session optional          pam_systemd.so
session required          pam_mkhomedir.so skel=/etc/skel umask=077_
```

Por último, reiniciamos el cliente con el comando: `sudo service nscd restart`

Comprobamos el funcionamiento del cliente

Para comprobar que el cliente instalado funciona correctamente ejecutamos el siguiente comando, donde en *<usuario>* ponemos un usuario de pruebas del LDAP.

```
getent passwd <usuario>
```

```
jorge@Jorge:~$ getent passwd prueba  
prueba:x:1000002:1000001:prueba:/home/prueba:/bin/sh
```

Un caso real

Para entrar como otro usuario en Linux ejecutamos el siguiente comando, donde en *<usuario>* ponemos un usuario del LDAP.

su - <usuario>

```
jorge@Jorge:~$ su - prueba
Password:
Creating directory '/home/prueba'.
$ _
```



JorgeMunnozAguado