



Universidad de Murcia  
Facultad de Informática

---

---

# Computación Científica en Clusters

Sesión 3: OpenLdap y NX

Boletines de prácticas

2010

---

---

Departamento de Ingeniería y Tecnología de Computadores

Área de Arquitectura y Tecnología de Computadores



## Índice general

<b>I. Boletines de prácticas</b>	<b>2</b>
B3.1. Boletín 1: Probando el servicio LDAP dado por la Universidad de Murcia . . . . .	4
B3.2. Boletín 2: OpenLdap . . . . .	5
B3.2.1. Objetivos . . . . .	5
B3.2.2. Plan de trabajo . . . . .	5
B3.2.3. Configuración de un servidor OpenLdap . . . . .	5
B3.2.4. Configuración de un cliente OpenLdap . . . . .	8
B3.2.5. Añadiendo nuevos usuarios al servicio OpenLdap . . . . .	9
B3.3. NX . . . . .	10
B3.3.1. Objetivos . . . . .	10
B3.3.2. Plan de trabajo . . . . .	10
B3.3.3. Configuración del servidor . . . . .	10
B3.3.4. Configuración del equipo desde el que nos conectaremos al servidor . . . . .	11

## Boletines de prácticas

### Consideraciones iniciales

#### Máquinas virtuales

**IMPORTANTE:** No inicies ninguna máquina virtual hasta que no se te indique que lo hagas.

En el ordenador real, y no en la máquina virtual, con el usuario **root**, cambia los permisos a los ficheros del directorio donde está la imagen de la máquina virtual:

```
# su -l //la contraseña de root es practicas
# chmod 644 /home/software/CCC-MV/*
```

Cada ordenador ya tiene instalada la aplicación VirtualBox a la cual podemos acceder a través de Aplicaciones → Herramientas del sistema → VirtualBox. Al ejecutar la aplicación, debemos encontrar una máquina virtual ya creada llamada “Fedora 11 - Server” que contiene todo lo necesario para realizar la configuración del servidor. Esta máquina virtual tiene configuradas dos interfaces de red: `eth1` y `eth2`. La primera se utilizará para comunicarse con el cliente a través de una red interna virtual creada por VirtualBox; esta interfaz tiene asignada la IP estática `10.0.1.15`. La segunda interfaz se utilizará para acceder a Internet a través de NAT; esta interfaz tiene la IP dinámica `10.0.2.15` asignada por VirtualBox.

En la máquina virtual ya existen dos cuentas de usuario: una para el superusuario (`root`) y otra para un usuario que hemos llamado “Usuario del curso CCC”, que tiene por login `ccc`. Para ambas cuentas, la contraseña es `cluster`.

Un primer paso es cambiarle el nombre a la máquina virtual ya creada, usando para ello la opción Configuración. Simplemente cámbiaselo a “Servidor”. Es de cara a poder distinguir claramente entre las máquinas. No arranques aún esta máquina.

A continuación desde Virtual Box importa una nueva máquina virtual mediante la opción Importar servicio virtualizado del menú Archivo. Esta máquina hará de cliente. El directorio donde está la máquina virtual a importar es `/home/software/CCC-MV`. Realiza después los siguientes pasos, modificando la “Configuración” de la misma:

1. Cámbiale el nombre, haz que se llame “cliente”.
2. Asegúrate que tiene 2 adaptadores de red activos. El primero que usa NAT mientras que el segundo tiene que estar conectado a una red interna.

La nueva máquina virtual, al ser importada de la que hay preparada para hacer de servidor, también tendrá el usuario `ccc` creado.

A continuación pon en marcha esta máquina virtual y usando la herramienta `system-config-network` asigna a la red interna los siguientes valores:

- IP: `10.0.1.16`
- Máscara de red: `255.255.255.0`
- Puerta de enlace: `10.0.2.2`

En la prueba que yo hice en el laboratorio, el interfaz de red que hay que cambiar es el `eth4`, pero esto puede cambiar. Para saberlo puedes usar la orden `/sbin/ifconfig`. De las 2 interfaces `eth` una de ellas tendrá asignada la dirección `10.0.2.15`, pues el otro interfaz es la red interna.

Edita el fichero `/etc/sysconfig/network` y cámbiale el nombre al equipo, asignado **ccc-cliente**. Es la variable `HOSTNAME`.

Reinicia esta máquina virtual.

Pon en marcha la máquina virtual que hace de servidor, la que estaba creada inicialmente.

Entra como usuario normal en las dos máquinas virtuales, abre una terminal y conviértete en super-usuario para realizar los siguientes boletines.

Para ambos equipos, y de cara a resolver los ejercicios, es conveniente tener desactivado el cortafuegos:

```
# /etc/init.d/iptables stop
# chkconfig iptables off
```

Es importante, antes de empezar a resolver los ejercicios, comprobar que la red interna que usarían ambas máquinas para comunicarse funciona perfectamente. Puedes usar para ello la orden `ping`, así por ejemplo, desde el equipo servidor ejecutaríamos:

```
# ping 10.0.1.16
```

Tanto en el equipo servidor como en el cliente, añade al fichero `/etc/hosts` estas dos líneas, correspondiendo cada una de ellas a los nombre asignados a las dos máquinas:

```
10.0.1.15 ccc-server
10.0.1.16 ccc-cliente
```

## Activación de NFS

Un paso previo es configurar el equipo servidor como servidor NFS, y el cliente como cliente NFS.

### ■ Configuración en el servidor.

#### 1. Instalación de los paquetes:

```
# yum install nfs-utils nfs-utils-lib
```

#### 2. Modificación del fichero `/etc/exports`

```
/home 10.0.1.0/255.255.255.0(rw,no_root_squash)
```

#### 3. Demonios:

```
# /etc/init.d/nfs start
# /etc/init.d/nfslock start
```

```
# chkconfig rpcbind on
# chkconfig nfs on
# chkconfig nfslock on
```

#### 4. Comprobación:

```
# exportfs -v
```

### ■ Configuración en el cliente.

#### 1. En el fichero `/etc/fstab` añadimos la línea:

```
10.0.1.15:/home /home nfs defaults,rw,hard,intr,bg 0 0
```

#### 2. Realizamos el montaje manualmente, para que no sea necesario reiniciar el sistema.

```
# mount -t nfs -o rw,hard,intr,bg 10.0.1.15:/home /home
```

## Creación de usuarios

Para poder comprobar inicialmente el funcionamiento de OpenLdap, es conveniente que haya al menos otro usuario en el sistema, y no sólo **ccc**. Esto es debido a que **ccc** está definido tanto en el cliente como en el servidor, y no podremos realizar la autenticación mediante OpenLdap.

Usando `useradd` crea un nuevo usuario, asígnale una contraseña, y con la orden `chfn` asígnale información en su campo GECOS. Este último dato es importante de cara a obtener información más completa en las búsquedas realizadas.

### B3.1. Boletín 1: Probando el servicio LDAP dado por la Universidad de Murcia

Desde el equipo servidor realiza consultas al LDAP de la Universidad de Murcia:

1. Instalamos el paquete «`openldap-clients`»

Primero comprobaremos si está instalado: `rpm`:

```
# rpm -q openldap-clients
```

En caso de que no, procedemos a instalarlo mediante la orden `yum install`

```
# yum install openldap-clients
```

2. Entra en el directorio `/usr/share/migrationtools` que es donde se instalan las herramientas para migrar los datos ya existentes a OpenLdap
3. Para buscar usuarios que se llamen FEREZ de apellido sería:

```
# ldapsearch -h ldap.um.es -x -b "dc=um,dc=es" -LLL "(cn=*FEREZ*)"
```

4. Si consultamos sólo el nombre común:

```
# ldapsearch -h ldap.um.es -x -b "dc=um,dc=es" -LLL "(cn=*FEREZ*)" cn
```

5. Para ver su número de teléfono sería:

```
# ldapsearch -h ldap.um.es -x -b "dc=um,dc=es" -LLL "(cn=*FEREZ*)" telephoneNumber
```

6. Las búsquedas anteriores usando el campo teléfono como referente de búsqueda quedarían:

```
# ldapsearch -h ldap.um.es -x -b "dc=um,dc=es" -LLL "(telephoneNumber=*765*)"
# ldapsearch -h ldap.um.es -x -b "dc=um,dc=es" -LLL "(telephoneNumber=*765*)" cn
# ldapsearch -h ldap.um.es -x -b "dc=um,dc=es" -LLL "(telephoneNumber=*765*)" telephoneNumber
```

7. Búsquedas similares se pueden hacer desde la Web de la Universidad de Murcia, desde la dirección <http://www.um.es/atika/directorio/>. Realiza una búsqueda para comprobarlo.

## B3.2. Boletín 2: OpenLdap

### B3.2.1. Objetivos

El objetivo de este primer boletín es configurar un servidor de **OpenLdap** así como un equipo cliente del mismo. El servidor nos permitirá no sólo buscar objetos en la base de datos definida, sino también la autenticación de los usuarios desde los equipos cliente. Para ello, tendremos que pasar toda la información relevante al directorio, es decir, la información referente a las cuentas de usuario tienen que formar parte de la base de datos, en otro caso no sería posible la autenticación.

### B3.2.2. Plan de trabajo

El plan de trabajo para este boletín será el siguiente:

1. Configuración de un servidor OpenLdap
2. Configuración de un cliente OpenLdap
3. Añadiendo nuevos usuarios al servicio OpenLdap

### B3.2.3. Configuración de un servidor OpenLdap

Los pasos son los siguientes:

1. Antes de empezar este ejercicio, y también los siguientes, hay que desactivar el cortafuegos, si no se ha desactivado antes. Para ello ejecutaremos estas dos órdenes:

```
# /etc/init.d/iptables stop
# chkconfig iptables off
```

2. Instalamos los paquetes «openldap», «openldap-servers», «openldap-clients», «nss\_ldap» y «migrationtools».

Primero comprobaremos si los paquetes están instalados usando la orden rpm:

```
# rpm -q openldap openldap-clients openldap-servers nss_ldap migrationtools
```

En caso de que no estén instalados, procedemos a instalarlos mediante la orden yum install

```
# yum install openldap openldap-clients openldap-servers nss_ldap migrationtools
```

3. Entra en el directorio `/usr/share/migrationtools` que es donde se instalan las herramientas para migrar los datos ya existentes a OpenLdap
4. Editamos el fichero `/etc/openldap/ldap.conf` y establecemos cuál va a ser el nombre de nuestro directorio. En nuestro caso decidimos que se va a llamar “dc=ccc-ldap,dc=com”. Por tanto, en dicho fichero sustituimos la línea:

```
BASE dc=example,dc=com
```

Por:

```
BASE dc=ccc-ldap,dc=com
```

5. Procedemos de la misma manera con `/etc/openldap/slapd.conf`. En este caso tenemos que sustituir `my-domain` por `ccc-ldap` en tres líneas:

```
suffix          "dc=my-domain,dc=com"
....
rootdn          "cn=Manager,dc=my-domain,dc=com"
...
by dn.exact="cn=Manager,dc=my-domain,dc=com" read
```

Quedarían como:

```
suffix          "dc=ccc-ldap,dc=com"
....
rootdn          "cn=Manager,dc=ccc-ldap,dc=com"
...
by dn.exact="cn=Manager,dc=ccc-ldap,dc=com" read
```

6. Copiamos el fichero `/usr/share/doc/openldap-servers-2.4.15/DB_CONFIG.example` al directorio `/var/lib/ldap/`. Ten en cuenta que el fichero destino se tiene que llamar `DB_CONFIG`. De la misma manera, la ruta indicada depende de la versión de `openldap-servers` instalada. Puedes usar la orden

```
# rpm -ql openldap-servers | grep DB_CONFIG.example
```

para averiguar el nombre exacto del fichero.

Para copiar el fichero:

```
# cp /usr/share/doc/openldap-servers-2.4.15/DB_CONFIG.example /var/lib/ldap/DB_CONFIG
```

7. Edita el fichero `migrate_common.ph` y modifica la siguientes líneas para establecer el nombre del directorio LDAP.

```
# Default DNS domain
$DEFAULT_MAIL_DOMAIN = "padl.com";

# Default base
$DEFAULT_BASE = "dc=padl,dc=com";
```

Como ya hemos dicho, en este ejemplo, le vamos a llamar `ccc-ldap.com`. Las líneas quedarían como:

```
# Default DNS domain
$DEFAULT_MAIL_DOMAIN = "ccc-ldap.com";

# Default base
$DEFAULT_BASE = "dc=ccc-ldap,dc=com";
```

8. A continuación migramos los datos que queremos que formen parte del directorio. En el paquete `migrationtools` hay un conjunto de ficheros, escritos en Perl, que permiten la migración de usuarios, grupos, alias, host, etc., del sistema “normal” a LDAP.

Con `migrate_base.pl` se establecen los tipos de entradas que van a haber en la BD del openldap.

```
# ./migrage_base.pl > /tmp/base.ldif
```

Con `migrate_passwd.pl` se migran los ficheros `/etc/passwd` y `/etc/shadow`, mientras que con `migrate_group.pl` se migra `/etc/group`.

```
# ./migrage_passwd.pl /etc/passwd > /tmp/passwd.ldif
# ./migrage_group.pl /etc/group > /tmp/group.ldif
```

9. A continuación añadimos los ficheros migrados a la base de datos. Estos van a ser los primeros elementos que se incluyan en la misma.

```
# slapadd -l /tmp/base.ldif
# slapadd -l /tmp/passwd.ldif
# slapadd -l /tmp/group.ldif
```

10. El siguiente paso es cambiar el propietario y el grupo propietario de los ficheros de las bases de datos. Tienen que pertenecer al usuario **ldap** y al grupo **ldap**. Estos ficheros residen en `/var/lib/ldap/`

```
# cd /var/lib/ldap
# chown ldap.ldap *
```

11. Lanzamos el demonio y lo configuramos para que se lance de forma automática en cada arranque. Si ha habido algún problema de configuración el demonio se “quejará”, en caso contrario, pondrá en funcionamiento el servicio OpenLdap.

```
# /etc/init.d/ldap start
# chkconfig ldap on
```

12. Si queremos hacer uso de OpenLdap para realizar la autenticación de usuarios tenemos que indicarlo mediante la herramienta `system-config-authentication`. En este caso, habrá que activar la opción en dos de las fichas. La primera es “Información de usuario” mientras que la segunda es “Autenticación”. En ambos casos seleccionamos la opción “Habilitar el soporte LDAP”. El primero es para obtener la información del usuario, lo que sería su nombre, su identificador de usuario, grupos a los que pertenece, etc. Mientras que el segundo es para realizar la autenticación del usuario mediante su contraseña.

Comprobamos que el nombre es el correcto mediante la opción “Configurar LDAP”, asegurándonos que es “`dc=ccc-ldap,dc=com`”.

13. Es el momento de probar si está funcionando el servicio:

La orden `slapcat` va a mostrar todos los datos almacenados en el directorio.

```
# slapcat
```

Por su parte, `slaptest` comprueba si el fichero `slapd.conf` es correcto.

```
# slaptest
```

Finalmente podemos realizar búsquedas en el directorio:

```
# ldapsearch -h 10.0.1.15 -x -b "dc=ccc-ldap,dc=com" -LLL "(cn=*CCC*)" cn
```

### B3.2.4. Configuración de un cliente OpenLdap

Terminada la configuración del servidor, procedemos a realizar la configuración del equipo cliente.

1. Los paquetes «`openldap`», «`openldap-clients`», «`nss_ldap`» tienen que estar instalados en los equipos cliente. Comprobamos si están instalados, y si no lo están procedemos a instalarlos.

```
# rpm -q openldap openldap-clients nss_ldap
```

Para instalarlos

```
# yum install openldap openldap-clients nss_ldap
```

2. A continuación usamos la herramienta `system-config-authentication` para activar la autenticación y la obtención de información del usuario mediante OpenLdap. Para ello en las dos de las fichas, Información de usuario y Autenticación, seleccionamos la opción “Habilitar el soporte LDAP”.

El siguiente paso es “Configurar LDAP”, indicando:

En el campo “DN de Base de búsqueda para LDAP”:

```
dc=ccc-ldap,dc=com
```

En “Servidor LDAP”:

```
ldap://10.0.1.15
```

Con los pasos anteriores hemos configurado tanto el proceso de búsqueda como la autenticación.

3. Para comprobar que está funcionando procedemos a realizar búsquedas:

```
# ldapsearch -h 10.0.1.15 -x -b "dc=ccc-ldap,dc=com" -LLL "(cn=*CCC*)" cn
```

4. Por último, procedemos a realizar una autenticación con el usuario definido sólo en el servidor OpenLdap. Para hacer esta autenticación puedes optar por dos métodos. El primero sería simplemente usar la orden `su -l usuario`. El segundo sería cerrar de la sesión actual, y abrirla de nuevo con el otro usuario.

Observa que debido al NFS configurado previamente, los ficheros del usuario son accesibles desde el equipo cliente.

### B3.2.5. Añadiendo nuevos usuarios al servicio OpenLdap

Una opción sencilla para añadir nuevos elementos a la base de datos de OpenLdap es usar la herramienta Luma. Con ella se pueden hacer consultas, navegar por toda la base de datos, crear unos usuarios, gestionar los ya existentes, etc.

1. Instala el paquete luma con

```
# yum install luma
```

2. Para ejecutar la herramienta hay dos opciones:

- Desde el menú `Aplicaciones en Herramientas` del sistema aparece una nueva entrada llamada Luma.
- Desde una consola de texto se ejecuta la orden:

```
# luma
```

3. Para poder crear usuarios con esta herramienta es necesario asignarle una contraseña al administrador del directorio OpenLdap. En nuestro caso, el administrador es el usuario `Manager`, que queda fijado en el fichero `/etc/openldap/slapd.conf`.

Los pasos son:

Primero obtener la encriptación de la contraseña que queramos asignar. Si elegimos “cluster” usando la herramienta `slappasswd` obtenemos la cadena encriptada.

```
# slappasswd
New password:
Re-enter new password:
{SSHA}B0po5ExXvb//A8X/vP10hYVPh6AvLlCu
```

A continuación copiamos la cadena encriptada usando el ratón y la añadimos al fichero `/etc/openldap/slapd.conf` con una entrada como la siguiente:

```
rootpw {SSHA}B0po5ExXvb//A8X/vP10hYVPh6AvLlCu
```

Por último reiniciamos el demonio:

```
# /etc/init.d/ldap restart
```

4. El siguiente paso es indicar el servidor Ldap con el que queremos trabajar. Para ello en la opción de menú `Settings` seleccionamos `Edit Server List`, en el botón `Add` incluir `ccc-ldap.com`.

En `Network Options` establecemos el `Hostname` con la dirección `10.0.1.15`

En `Autenticación` fijamos los siguientes valores:

- `Anonymous bind` tiene que estar marcado.
- `Mechanism` tiene que estar a `Simple`
- `Bind as` lo fijamos a `cn=Manager, dc=ccc-ldap, dc=com`
- `Password` asignamos “cluster” o la contraseña decidida.

5. A continuación entre todas las opciones posibles destacamos las siguientes:

- `Massive User Creation` ⇒ que permite la creación de usuarios de forma masiva. Si se indica el nombre de usuario `comp` y dos números, mínimo 1 y máximo 10, creará 10 usuarios: **comp1**, ..., **comp10**. La propia herramienta asigna la contraseña, de forma aleatoria a cada usuario creado.
- `Search` ⇒ con la que podemos realizar consultas en el directorio.
- `User Managent` ⇒ gestión de usuarios, permitiendo la creación de nuevos usuarios.
- `Browser` ⇒ navegar por los distintos elementos del directorio.

Destacar que cuando se crea un usuario con esta herramienta el problema que se tiene es que no crea el directorio de trabajo. Por tanto, a mano tendríamos que realizar la creación de dichos directorios, así como copiarles los ficheros de inicialización.

## B3.3. NX

### B3.3.1. Objetivos

En este caso vamos a trabajar con NX, una herramienta que nos permite conectarnos al equipo remoto usando un entorno gráfico. Actualmente, la tecnología la desarrolla la compañía *Nomachine* (<http://www.nomachine.com>). Aunque el núcleo de la tecnología NX es GPL, la compañía ofrece productos comerciales. Los clientes NX para Linux, Windows, etc. son gratuitos. Los servidores, para Linux/Solaris, hasta dos conexiones, también.

### B3.3.2. Plan de trabajo

Se van a realizar los siguientes ejercicios:

1. Configuración del servidor
2. Configuración del equipo desde el que nos conectaremos al servidor

### B3.3.3. Configuración del servidor

Realiza los siguientes ejercicios en el equipo servidor:

1. Abre un navegador Web y conéctate a la dirección `http://www.nomachine.com/download.php`
2. Pincha en la opción `NX Free Edition for Linux`
3. A continuación en `NX Free Edition for Linux RPM - i386`
4. Procede a hacer la descarga del `Client`, del `Node` y del `server`. Los ficheros descargados se habrán guardado en el directorio `Descargas` del usuario **ccc**.
5. Siendo el usuario **root** instala los paquetes descargados:

```
# rpm -i /home/ccc/Descargas/nx*
```

6. Copia el paquete `nxclient` al equipo cliente:

```
# scp /home/ccc/Descargas/nxclient*.rpm root@10.0.1.16:
```

Te pedirá la contraseña del usuario **root** en el equipo cliente.

7. Cierra la sesión abierta en este equipo. La podrías tener abierta, ya que no interfiere para la resolución del ejercicio.

### B3.3.4. Configuración del equipo desde el que nos conectaremos al servidor

En este caso la máquina a configurar sería un PC externo al cluster. Pero como no es posible, vamos a resolver estos apartados en el equipo cliente:

1. Como usuario **root** procede a instalar el paquete `nxclient` (Fue copiado desde el servidor)

```
# rpm -i /root/nxclient*
```

2. Ejecuta el NX que lo encuentras en el menú Aplicaciones, dentro en el menú Internet, a continuación pincha en `NX Client for Linux` y a continuación `NX Client for Linux`.

Se abre una primera ventana que nos pide la configuración de la sesión:

- **Session:** `severmv` (Nombre arbitrario para esa sesión)
- **Host:** `10.0.1.15` (Dirección del equipo servidor, al que nos conectaremos)
- **Select type of your internet connection:** Velocidad de la conexión.

En la siguiente ventana seleccionamos el tipo de sistema operativo de la máquina destino, y el sistema de ventanas usado. En este caso `Unix` y `GNOME`. También podemos seleccionar el tamaño del escritorio remoto que abrirá.

Finalizamos eligiendo si queremos que cree un icono en el Escritorio.

Terminada la configuración inicial nos abre una ventana de autenticación en la que nos pide la contraseña del usuario `ccc`. (Podríamos cambiar el usuario).

3. Se ha abierto una sesión NX en la máquina remota, en la que puedes trabajar como si estuvieras sentado en el equipo.
4. Comprueba que realmente estás en el equipo remoto, y trabaja un poco en la sesión abierta.
5. Cierra la sesión. Para cerrar sesión puede usar el menú Sistema la opción `Cerrar la sesión de ccc`.
6. Vuelve a realiza la conexión NX, y abre un navegador Web y edita un fichero.
7. Procede a cerrar la sesión pero desconectando, de forma que la próxima vez que nos conectemos la encontraremos igual que la hemos dejado. Para ello, pulsa en el X de la esquina superior derecha del NX, y aparecerá un cuadro de diálogo en el que hay que seleccionar `Disconnect`.
8. Vuelve a abrir con NX la sesión remota y comprueba que se ha abierto conforme la has dejado.