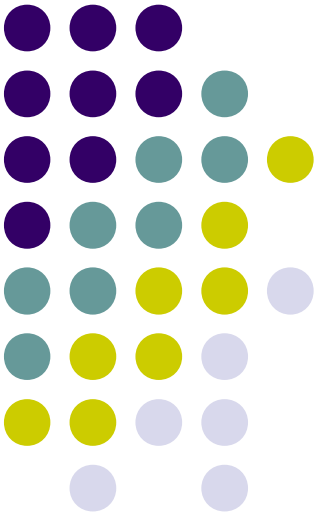
Curso de Computación Científica en Clusters

Administración de Plataformas Paralelas.

Sesiones 3: ***OpenLdap, NX***

Pilar González Férez

Universidad de Murcia



Concepto de directorio

- Un directorio es una base de datos de objetos especificados por los atributos que en cada caso procedan
- Un *servicio de directorio* es un lugar donde se centraliza información sobre los recursos de una organización
- Un *directorio* es una base de datos optimizada para lectura, navegación y búsqueda
- Los *servicios de directorio* son almacenes de información acerca de entidades de red (aplicaciones, archivos, impresoras y usuarios)
- OpenLdap es un servicio de Directorio que cumple con el protocolo LDAP

Concepto de directorio

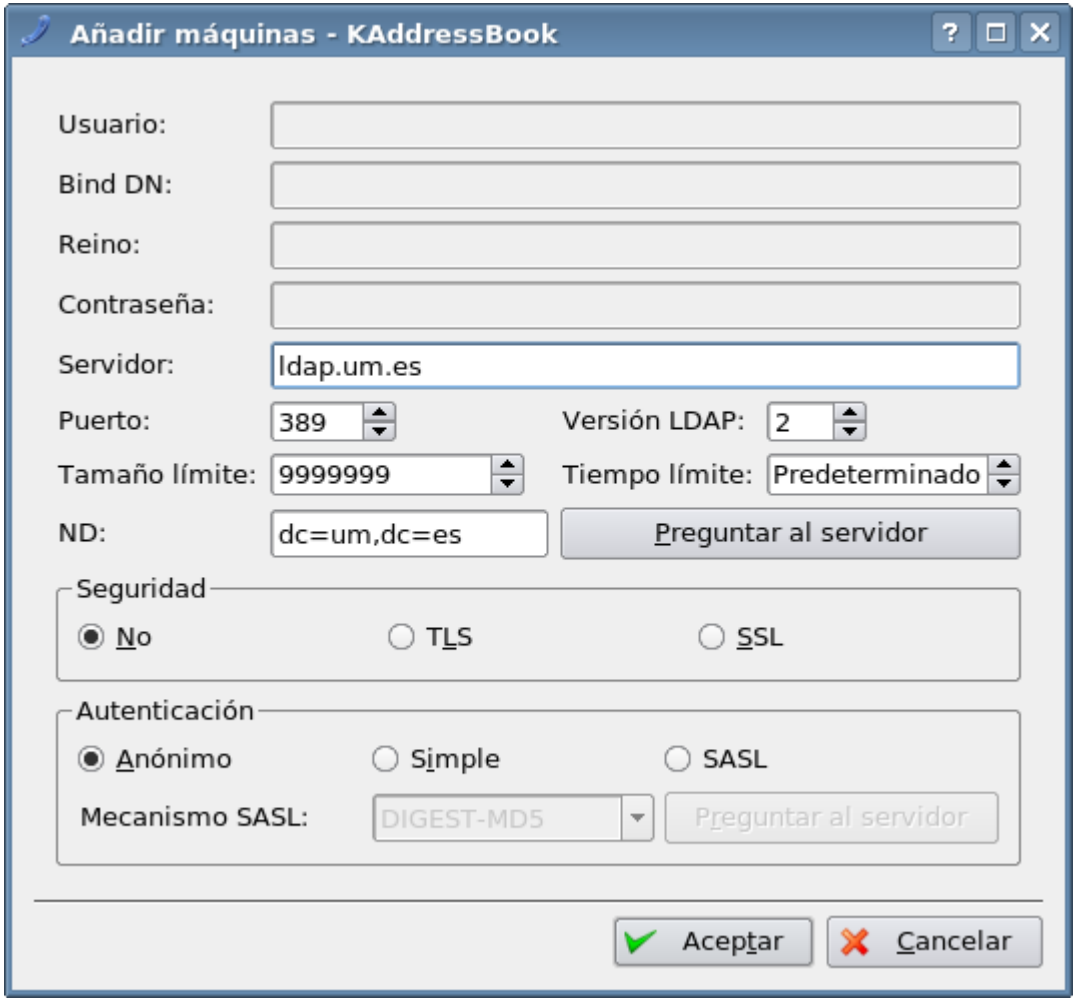
- A los objetos del directorio se les llama “entradas” y para cada tipo de entrada tenemos su *objectClass*
- La objectClass determina los atributos que se espera que tengan los objetos
- Los atributos pueden ser obligatorios (*required*) u optativos (*allowed*)
- Los obligatorios deben estar presentes en todas las entradas del respectivo objectClass en el directorio
- El ***esquema*** es el conjunto de reglas que describen qué clase de información se puede almacenar, ayudando a mantener la consistencia y la calidad de los datos
- El ***esquema*** define los objetos que se pueden almacenar en el directorio

Usos de un directorio

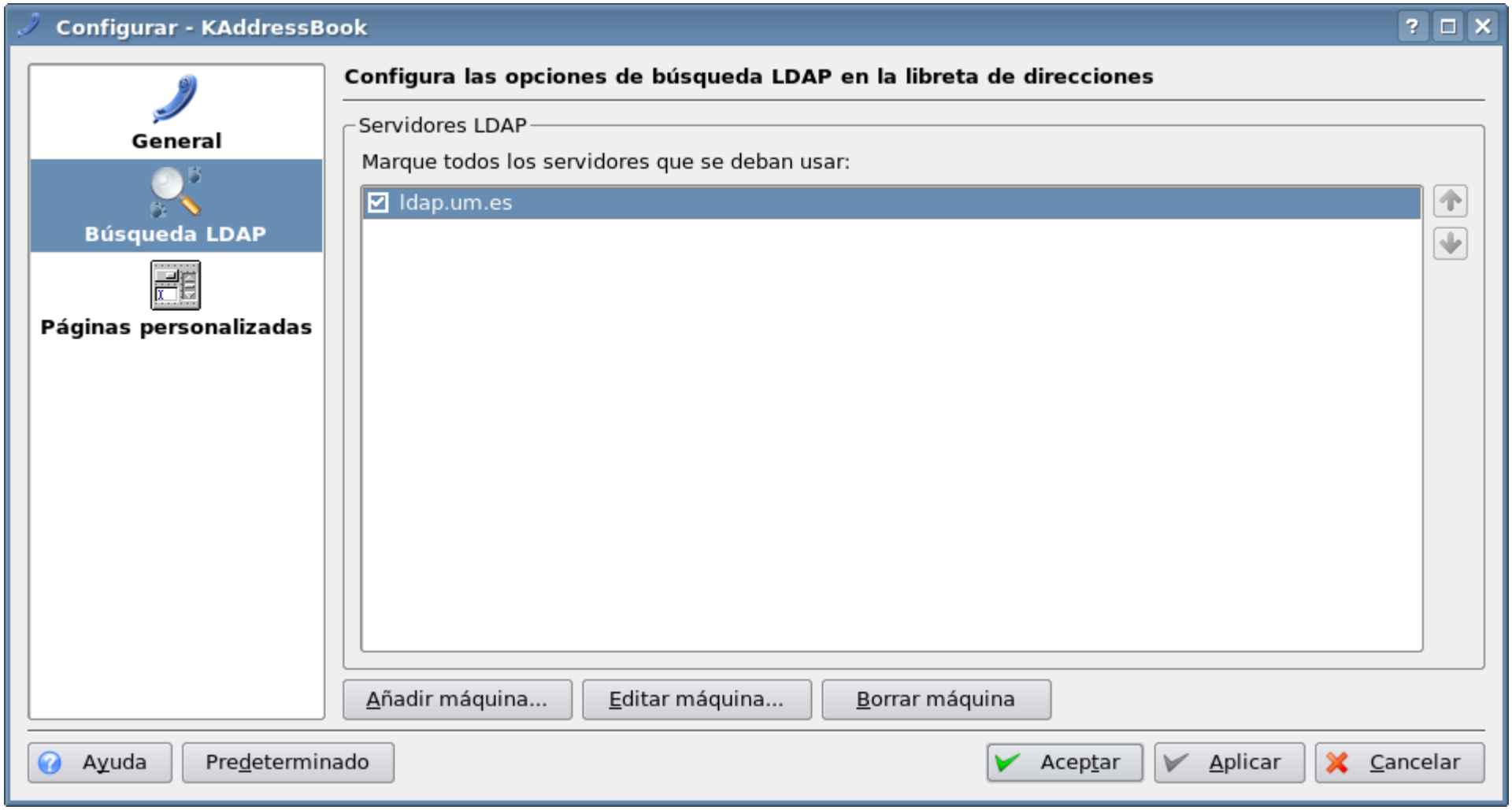
- 3 usos principales:
  - Directorio de red:
    - Gestión de cuentas de usuario
  - Directorio de empresa:
    - Servidor de datos global para la información compartida
    - Detalles acerca de las personas, organizaciones, dispositivos, ...
  - Directorio de negocios:
    - Detalles acerca de socios comerciales, clientes, proveedores, ...
- En general, un directorio sirve para almacenar todo tipo de objetos

Consultas con KaddressBook en Linux

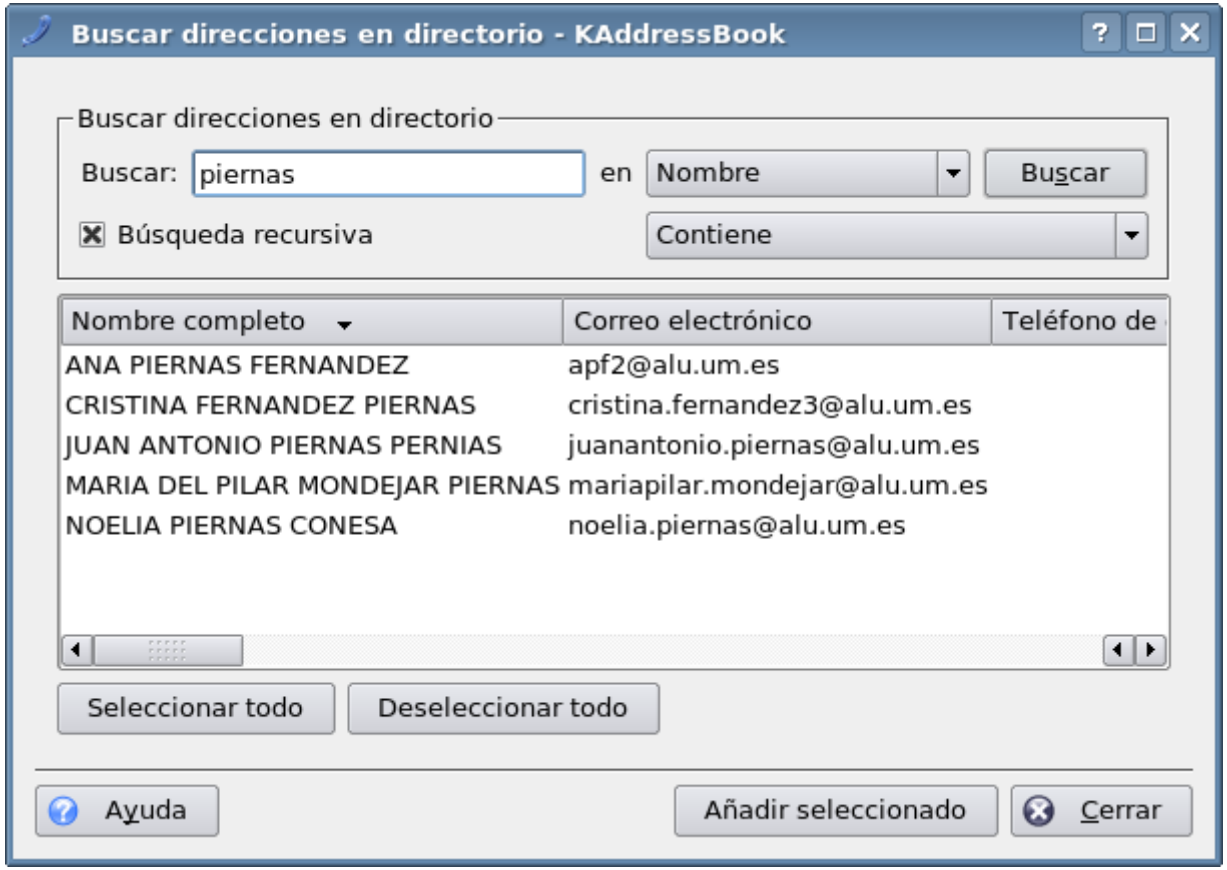
- Utilizamos el directorio de la UMU (basado en LDAP)



Consultas con KaddressBook en Linux



Consultas con KaddressBook en Linux



Consultas desde la línea de órdenes en Linux

- El paquete openldap-clients para Linux permite lanzar consultas ldap, modificar passwords, etc…
- Ejemplo:

```
$ ldapsearch -h ldap.um.es -x -b "dc=um,dc=es" -LLL "(cn=JU*PIERNAS*C*)" cn sn1
mail telephoneNumber
dn: uid=piernas.PDI,dc=usuarios,dc=um,dc=es
mail: piernas@um.es
cn: JUAN PIERNAS CANOVAS
sn1: PIERNAS CANOVAS
telephoneNumber: +34 968367657
```

Protocolo LDAP

- Permite varias modalidades de conexión siendo la habitual 389/TCP:

```
# grep ldap /etc/services
ldap            389/tcp
ldap            389/udp
ldaps           636/tcp                         # LDAP over SSL
ldaps           636/udp                         # LDAP over SSL
```

- Es asíncrono:
  - Pueden haber varias peticiones en curso
  - El directorio las resuelve y contesta cuando puede

LDIF (LDAP Data Interchange Format)

- Formato de exportación e importación de datos entre servidores LDAP
- Cada servidor LDAP tiene libertad para disponer los datos físicamente en el disco cómo crea conveniente
- LDIF unifica el tratamiento de los datos y su migración de un servidor otro
- Es un fichero de texto ASCII donde se relacionan las entradas del directorio,
- Puede contener 1 o varias entradas del directorio (hasta todas) separadas cada una de ellas por una línea en blanco
- El número y tipo de atributos puede ser diferente en cada caso dependiendo del tipo de la entrada

LDIF

- Permite:
  - Sincronizar directorios
  - Volcar los datos de usuarios de una base de datos a LDIF para importarlo en el directorio LDAP
  - Realizar pequeños cambios manuales editando un fichero de este tipo para importar los cambios sobre el directorio, ...
- Ejemplo:

```
cn: JUAN PIERNAS CANOVAS
cnn: JUAN
sn: PIERNAS CANOVAS
dni: 12345678
telephoneNumber: 7657
rfc822Mailbox: piernas@ditec.um.es
postalAddress: Facultad de Informatica
organizationalUnitName: Facultad de Informatic
...
```

OpenLDAP

- Soporta el protocolo LDAP (*LightWeight Directory Access Protocol,* protocolo ligero para acceder a directorios de información)
- Para realizar la autenticación con LDAP, tenemos que pasar toda la información relevante del sistema al directorio
- En el servidor los paquetes se necesitan los paquetes: openldap, openldap-clients, openldap-servers, nss_ldap y migrationtools
- En el paquete ***migrationtools*** vienen utilidades para la migración que, desde los formatos propios de cada fichero, generan un LDIF.
  - Utilidades en `/usr/share/migrationtools/`
  - `/usr/share/doc/migrationtools-47/migration-tools.txt` Este fichero explica las herramientas
  - Este paso no es obligatorio pero facilita el inicio

Migración con OpenLDAP

```
$ migrate_passwd.pl /etc/passwd
dn: uid=root,ou=People,dc=padl,dc=com
uid: root
cn: root
objectClass: account
objectClass: posixAccount
objectClass: top
userPassword: {crypt}x
loginShell: /bin/bash
uidNumber: 0
gidNumber: 0
homeDirectory: /root
gecos: root

[ ... ]
```

Migramos y añadimos los usuarios definidos en el sistema al directorio

```
# migrate_passwd.pl /etc/passwd > /tmp/passwd.ldif
# slapadd -l /tmp/passwd.ldif
```

Cliente: Autenticación con LDAP en Linux

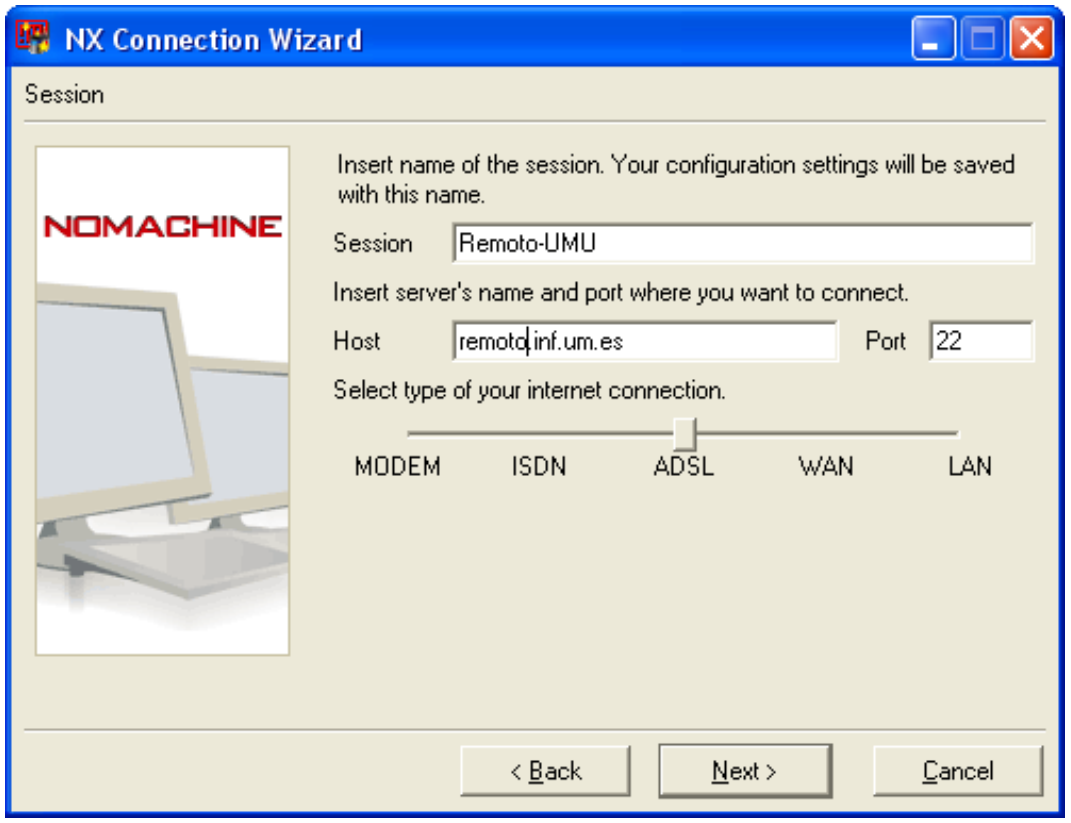
- Se necesitan los paquetes: `openldap,openldap-clients y nss_ldap`
- Hay que preparar al cliente, indicando cuál es nuestro servidor LDAP en el fichero `/etc/openldap/ldap.conf`
- Para NSS hay que modificar `/etc/nsswitch.conf` para establecer que queremos hacer uso de LDAP
- Para autenticar con LDAP, tenemos que indicar que se usen las bibliotecas de LDAP a través de PAM
- Tanto para NSS como para PAM, los cambios los podemos hacer fácilmente con `system-config-authentication`
  - Incluso nos permite indicar el servidor LDAP y el nombre del directorio, realizando la configuración del fichero `/etc/openldap/ldap.conf`

Protocolo NX

- NX permite el acceso remoto en modo gráfico
- Protocolo que “comprime” el protocolo X-Window reduciendo el tráfico de red y los *round-trips* entre clientes y servidor
- NX usa el protocolo de SSH para las transferencias de datos
- 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

Protocolo NX

- Para la configuración del servidor en Linux, basta con descargar e instalar los paquetes `nxnode`, `nxclient` y `nxserver` (La configuración por defecto ya es funcional)
- Para el acceso desde Windows, primero configuramos la conexión:



Protocolo NX

- El cliente ofrecido por NoMachine soporta los protocolos VNC, RDP y X-Windows: