

1 Ferramentas para administración do LDAP.vello

Neste apartado imos facer unha breve reseña sobre algunhas ferramentas que podemos utilizar para administrar o servidor LDAP de forma xenérica, para introducir, buscar e extraer información, mantelo en óptimo funcionamento, etc.

1.1 Sumario

- 1 Ferramentas de `ldap-utils`
 - ◆ 1.1 Exemplos de uso
- 2 Ferramentas incluídas co servidor LDAP
- 3 JXplorer

1.2 Ferramentas de `ldap-utils`

O paquera `ldap-utils` contén varios comandos útiles para manexar a información almacenada no directorio LDAP. Algúns dos máis destacables son:

- **ldapadd, ldapmodify:** Os dous comandos enlazan con mesmo executable, polo que realmente fan a mesma función de engadir ou modificar entradas no LDAP (`ldapadd` equivale a `ldapmodify -a`). Os parámetros máis importantes son:
 - ◆ **-x:** usar autenticación simple.
 - ◆ **-D dn:** dn para conectarse ao LDAP.
 - ◆ **-w contrasinal:** Contrasinal para conectarse ao LDAP.
 - ◆ **-W:** Pide o contrasinal para conectarse ao LDAP en lugar de recibilo como parámetro.
 - ◆ **-f ficheiro:** Toma a información que se debe engadir, modificar ou borrar do `ficheiro` en lugar da entrada estándar (Na páxina do manual do comando explica o formato deste ficheiro para engadir, modificar e borrar entradas).
- **ldapdelete:** De sintaxe similar ao comando anterior, recibe como entrada (ou ben pola entrada estándar ou ben dun ficheiro) unha lista de dn's para eliminalas do LDAP.
- **ldapsearch:** Permite buscar información no directorio, devolvendo o resultado da busca en formato LDIF. Para facer a busca, poderemos indicarlle o filtro polo que queremos buscar; por exemplo "(uid=xyz)" buscará as entradas que teñan un atributo `uid` co valor `xyz`. Tamén lle podemos indicar despois os atributos que queremos ver de cada entrada atopada no resultado da busca. Parámetros máis importantes:
 - ◆ **-x:** usar autenticación simple.
 - ◆ **-D dn:** dn para conectarse ao LDAP.
 - ◆ **-w contrasinal:** Contrasinal para conectarse ao LDAP.
 - ◆ **-H ldapuri:** Dirección ou direccións do servidor ou servidores LDAP a consultar.
 - ◆ **-b searchbase:** Rama do directorio na que comezar a busca.

1.2.1 Exemplos de uso

- **Exemplo 1:** Queremos crear no directorio a ou `maquinas`, para o que introducimos no ficheiro `maquinas.ldif` a seguinte información:

```
dn: ou=maquinas,dc=iescalquera,dc=local
objectClass: organizationalUnit
ou: maquinas
```

e executamos o comando:

```
sudo ldapadd -x -D cn=admin,dc=iescalquera,dc=local -W -f maquinas.ldif
Enter LDAP Password:
adding new entry "ou=maquinas,dc=iescalquera,dc=local"
```

- **Exemplo 2:** Queremos modificar o `cn` do usuario `alfredo` e agregarlle un `mail`. Creamos o ficheiro `alberto.ldif` co seguinte contido:

```
dn: uid=alfredo,ou=usuarios,dc=iescalquera,dc=local
changetype: modify
```

```
replace: cn
cn: prof - Alfredo Perez
-
add: mail
mail: alfredo@edu.xunta.es
```

e executamos o comando:

```
sudo ldapadd -x -D cn=admin,dc=iescalquera,dc=local -W -f alberto.ldif
Enter LDAP Password:
modifying entry "uid=alfredo,ou=usuarios,dc=iescalquera,dc=local"
```

- **Exemplo 3:** Buscamos no directorio a información do usuario *alfredo*:

```
ldapsearch -x -H ldap://localhost -b dc=iescalquera,dc=local "(uid=alfredo)"
```

- **Exemplo 4:** Borrarnos a ou *maquinas*:

```
sudo ldapdelete -x -D cn=admin,dc=iescalquera,dc=local -W "ou=maquinas,dc=iescalquera,dc=local"
```

1.3 Ferramentas incluídas co servidor LDAP

- **slapindex:** Este comando pode ser moi útil en caso de apagados accidentais do servidor LDAP, xa que é posible que os índices usados para acceder á información do directorio se corrompan, o que pode producir erros na busca ou inserción de información no directorio ou incluso que o servidor LDAP non poida arrancar. A función do comando é rexenerar os índices a partir da información almacenada no directorio, creando así de novo as estruturas necesarias para que o servizo LDAP funcione correctamente.

O comando debe executarse co mesmo usuario que executa o servidor LDAP (no caso de Ubuntu o usuario *openldap*), xa que os ficheiros de índices que este comando crea só poderán ser modificados polo usuario que executa o comando e executalo con outro usuario podería dar problemas de permisos ao arrancar o servidor LDAP.

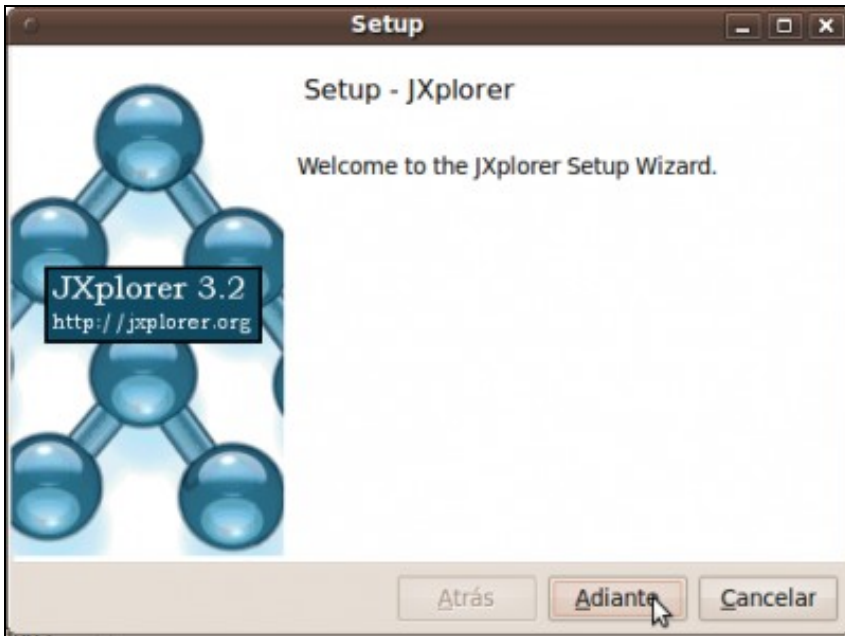
1.4 JXplorer

Existen moitas ferramentas gráficas para conectarse a un servidor LDAP e manexar a información almacenada nel, e **JXplorer** é un dos máis usados. Está implementado en Java, polo que pode usado tanto dende unha máquina Windows como Linux.

No noso caso ímolo instalar no cliente Ubuntu Desktop, e teremos que ter instalada no equipo a máquina virtual de java. A implementación que ven instalada por defecto en Ubuntu é a do paquete *openjdk-6-jre*, pero con esta implementación a conexión co servidor LDAP non funciona correctamente, polo que instalaremos a implementación de Sun (agora Oracle) da máquina virtual de Java. O paquete para instalar esta implementación está no repositorio de socios de canónica, así que podemos facer a instalación co Synaptic activando este repositorio, ou cos seguintes comandos:

```
sudo add-apt-repository "deb http://archive.canonical.com/ maverick partner"
sudo apt-get update
sudo apt-get install sun-java6-bin
```

Descargamos JXplorer da páxina de descargas (<http://sourceforge.net/projects/jxplorer>) o instalador para Linux, e executamos este instalador co usuario *root*. Desta forma comezará o asistente de instalación:



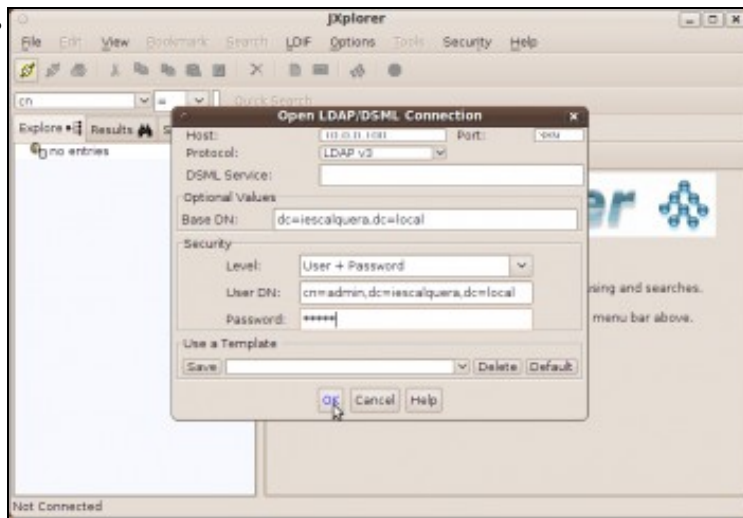
Unha vez instalado o programa, podemos executalo cos seguinte comandos:

```
cd /opt/jxplorer-3.2.1  
sh jxplorer.sh
```

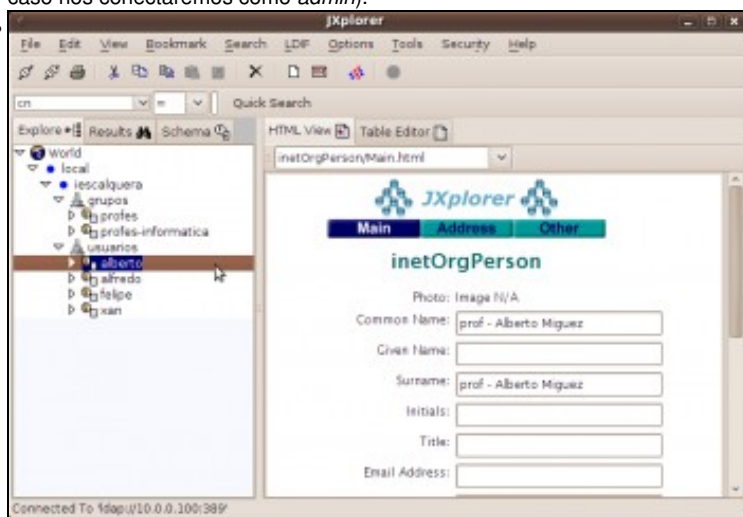
A continuación móstranse algunhas opcións do programa:



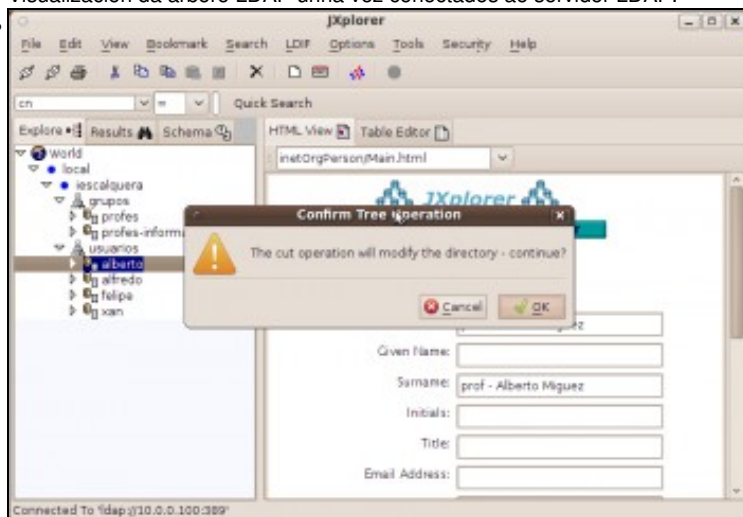
Ventá do programa antes de conectarse a ningún servidor LDAP. O primeiro botón da barra de ferramentas permítenos conectarnos a un servidor.



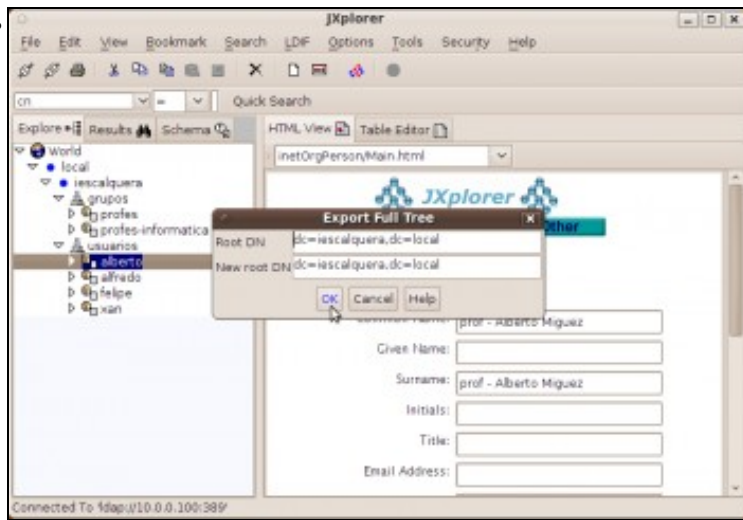
Ventá de conexión ao servidor LDAP. Teremos que indicar os datos do servidor (dirección IP, porto), a rama base do LDAP (no noso caso *dc=iescalquera,dc=local*) e as credenciais para conectarmos (podemos seleccionar anónimo, pero se queremos facer modificacións no noso caso nos conectaremos como *admin*).



Visualización da árbore LDAP unha vez conectados ao servidor LDAP.



Podemos mover elementos dun lugar a outro arrastrándoos na visualización na árbore (por exemplo, arrastrar o usuario *alfredo* sobre a ou *grupos*). Esta operación tamén se pode facer coas opcións de cortar e pegar.



O menú **LDIF** ofrece opcións como exportar todo ou unha rama do directorio a un ficheiro LDIF ou importar un ficheiro LDIF.

-- Antonio de Andrés Lema e Carlos Carrión Álvarez