Gestión de LDAP en Debian

Índice de contenido

| Gestión de LDAP en Debian | 1 |
|---|----|
| 1. LDAP | 3 |
| 2. Instalación de un servidor LDAP | 6 |
| 2.1 Instalación del servicio LDAP | 6 |
| 2.2 Configuración del servicio LDAP | 9 |
| 2.3 Creación del directorio LDAP | 19 |
| Instalar Jxplorer | 19 |
| Conectar al servidor LDAP | 21 |
| Creación de las unidades organizativas | 23 |
| Creación de usuarios y grupos | 25 |
| Instalación de phpldapadmin | 39 |
| 3. Instalación de un cliente LDAP | 41 |
| 3.1 Instalar y configurar la librería libpam-ldap | 41 |
| 3.2 Instalar y configurar la librería libres-ldap | 47 |
| 3.3 Configurar nsswitch.conf | 53 |
| 4. Probar la autentificación | 54 |
| 5. Crear home del usuario al vuelo | 54 |
| | |

Realizado por: Sagrario Pedraza Labrador Módulo: Implantación de Sistemas Operativos (ISO) Curso: 2011/2012

1. LDAP

LDAP (*Lightweight Directory Access Protocol*) es un servicio de directorio optimizado para la realización rápida de operaciones de lectura y búsqueda de información.

LDAP se usa principalmente como servidor de autentificación para controlar el acceso de los usuarios a un sistema, aunque por lo que me han comentado, la tendencia hoy en día es que todos los servicios de una organización usen los datos almacenados en el servidor ldap.

Los institutos de Extremadura almacenan en LDAP además de la información de usuarios y grupos, toda la información de dns y dhcp. El control de acceso inalámbrico del IES Valle del Jerte se hace mediante un servidor que obtiene los datos de usuarios y grupos de un servidor ldap.

LDAP se puede usar también para controlar el acceso de usuarios a aplicaciones web, a servidores ftp, servidores de correo, servidores de mensajería, etc...

La ventaja de tener un servidor LDAP es que podemos tener centralizada toda la información en un único lugar. Además, un servidor LDAP se puede replicar de forma que tengamos un servidor de reserva por si el servidor principal cae.

En el sistema de autentificación con LDAP un usuario que quiere acceder al sistema envía su usuario y su contraseña al servidor y éste le concede o deniega el acceso.

Para realizar el trabajo he instalado:

- Un servidor LDAP en una máquina virtual con Debian Squeeze.
- Un cliente LDAP en una máquina virtual con Debian Squeeze.



2. Instalación de un servidor LDAP.

2.1 Instalación del servicio LDAP.

Instalar el servidor LDAP en Debian es muy sencillo. Tan sólo tenemos que instalar el paquete **slapd**. Además instalaremos también el paquete **ldap-utils** que nos va a proporcionar utilidades adicionales para realizar consultas y modificaciones del servidor ldap desde la línea de comandos.

apt-get install slapd ldap-utils



Nos pide confirmación. Pulsamos Enter para confirmar que queremos realizar la instalación. A continuación nos pedirá que introduzcamos una contraseña para el administrador de ldap:

| ~ | servidor-Idap [Corriendo] - Oracle VM VirtualBox 📃 🗆 🗴 |
|------------|---|
| <u>M</u> á | iquina <u>V</u> er <u>D</u> ispositivos Ay <u>u</u> da |
| Cor | nfiguración de paquetes |
| | |
| | |
| | v V |
| | Configuración de slapd |
| | Por favor introduzca la contraseña para la entrada de administrador de su directorio LDAP. |
| | Contraseña del administrador: |
| | ***** |
| | < <u>Aceptar></u> |
| | |
| | |
| | |
| | |
| | |
| | 😫 🕢 🗗 🛄 😥 Ctrl Derecho |

Nos pedirá que volvamos a introducir la contraseña para asegurar que la introducimos bien:

| • | servidor-Idap [Corriendo] - Oracle VM VirtualBox | – – × |
|----------------------------------|---|--------|
| <u>M</u> áquina <u>V</u> er | r <u>D</u> ispositivos Ay <u>u</u> da | |
| Configurac. | ión de paquetes | |
| Por favo su direo Verifica | or, introduzca de nuevo la misma contraseña de administrador pa ctorio LDAP para verificar que la introdujo correctamente. ación de contraseña: | ra |
| ****** | * <mark>(Aceptar></mark> | |
| | | |
| | 😂 🕢 🖬 💭 🖉 Ctrl Do | erecho |

Una vez introducida, comenzará el proceso de instalación y configuración:

| • | | servidor-Idap [Corriendo] Oracle VM VirtualBox | _ 🗆 X |
|----------------------|--------------|---|------------------------|
| <u>M</u> áquina | <u>V</u> er | Dispositivos Ayuda | |
| Configur Configur | ando | o libgcrypt11 (1.4.5–2) o libtasp1–3 (2.7–1+squeeze+1) | |
| Configur | ando | o libgnutls26 (2.8.6–1+squeeze2) | |
| Configur | ando | o libsasl2–2 (2.1.23.dfsg1–7) | |
| Configur | ando | o libldap–2.4–2 (2.4.23–7.2) | |
| Configur | ando | o libltdl7 (2.2.6b–2) | |
| Configur | ando | o libper15.10 (5.10.1–17squeeze3) | |
| Configur | ando | o libslp1 (1.2.1–7.8) | |
| Configur | ando | o psmisc (22.11-1) | |
| Configur | ando | o libdb4.7 (4.7.25-9) | |
| Configur | ando | o ldap-utils (2.4.23-7.2) | |
| Configur | ando | o libsasi2-modules (2.1.23.dfsg1-7) | |
| Configur Configur | ando | o peri-modules (5.10.1–1/squeeze3) | |
| Configur | ando | 0 000Clnst (2.2.14pz-1) | |
| updata a | anuu 1+or | υ μεγι (5.10.1-1/Squeezes) protives: utilizando (νερ/bip/propamo popo prov | oon (uen/hin/noname (n |
| upuale-a onomo) o | n me | nnatives, utilizanuo zusnzbinzprename para prov odo automático | eer /usi/pin/rename (r |
| Configur | ando | o odheinstidehian2 (2 2 14n2–1) | |
| Configur | andr | o unixodha (2 2 14n2-1) | |
| Configur | andr | o sland (2.4.23-7.2) | |
| Creati | ngr | new user openidap done. | |
| Creati | ng i | initial configuration done. | |
| Creati | ng L | LDAP directory done. | |
| Starting | Öpe | enLDAP: slapd. | |
| <u>root@ser</u> | vido | or-ldap:~# _ | |
| | | 9 🕑 🗗 | 🔲 🔘 🥝 🛃 Ctrl Derecho |

2.2 Configuración del servicio LDAP.

Bien, pues ahora que ya tenemos instalado el servidor LDAP, ahora vamos a configurarlo:



Pulsamos **enter** y se iniciará un asistente que nos irá pidiendo los datos para configurar el servicio LDAP. Lo primero que nos pregunta es si deseamos omitir la configuración de LDAP:



Sagrario Pedraza Labrador

Le respondemos "No" porque precisamente lo que queremos es configurarlo.

Nos preguntará qué nombre de dominio queremos darle a la base de nuestro directorio LDAP. Esta base es el elemento raiz del que cuelgan todos los demás. En LDAP se almacenan los datos de forma jerárquica en forma de árbol. Para la práctica, como nombre de dominio he elegido:



A continuación nos pedirá que introduzcamos el nombre de nuestra organización:



Sagrario Pedraza Labrador

Una vez especificado, nos pedirá que introduzcamos la contraseña del administrador LDAP. La introducimos y pulsamos **<Aceptar>**:



Nos pedirá que volvamos a introducirla de nuevo para confirmar:

| • | servidor-Idap [Corriendo] - Oracle VM VirtualBox | _ 🗆 × |
|---------------|--|--------|
| <u>M</u> áqui | ina <u>V</u> er <u>D</u> ispositivos Ay <u>u</u> da | |
| Confi | guración de paquetes | |
| | | |
| | | |
| | | |
| | Configuración de slapd | |
| PO SU | ⊓ favor, introduzca de nuevo la misma contrasena de administrador pa ∣ directorio LDAP para verificar que la introdujo correctamente. | ra |
| | alfination de contraceños | |
| ve Ve | rificación de contrasena: | |
| ** | жжжжж | |
| | <a>Aceptar> | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | aracha |
| | | recho |

A continuación nos pedirá que elijamos qué motor de almacenamiento de datos queremos usar. El motor HDB es más nuevo. Lo seleccionamos:

| × | servidor-Idap [Corriendo] - Oracle VM VirtualBox | _ 🗆 × |
|--|---|--------|
| <u>M</u> áquina <u>V</u> er | <u>D</u> ispositivos Ay <u>u</u> da | |
| Configurac: | ión de paquetes | |
| | | |
| Se recor almacena de subár configur | Configuración de slapd nienda el motor HDB. Los motores BB y BDB utilizan formatos de amiento semejantes, pero HDB permite realizar cambios de nombre boles («subtree renames»). Ambos tienen las mismas opciones c pación. | le |
| En cualo Vea en (| quier caso, debe revisar la configuración de la base de datos. //usr/share/doc/slapd/README.DB_CONFIG.gz» para más detalles. | |
| Motor de | e base de datos a utilizar: | |
| | BDB HDB | |
| | < <u>Aceptar></u> | |
| | | |
| | | |
| | 🤪 🕑 🗗 🛄 💟 🖉 Ctrl D | erecho |

Nos preguntará si queremos que se elimine la base de datos cuando elijamos desinstalar ldap y borrar sus archivos de configuración. Le respondemos que no:

| • | servidor-Idap [Corriendo] - Oracle VM VirtualBox 📃 🗆 🕽 | × |
|------------|--|---|
| <u>M</u> á | iquina <u>V</u> er <u>D</u> ispositivos Ay <u>u</u> da | |
| Con | ∩figuración de paquetes ┣ | |
| | Configuración de slapd | |
| | ¿Desea que se borre la base de datos cuando se purgue el paquete slapd? <sí> ᠺᢈ</sí> | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | Service State Stat | |

Si hemos configurado anteriormente el servicio LDAP, tendremos los ficheros de la base de datos almacenados en el directorio /var/lib/ldap. Nos pregunta si queremos moverlos a un directorio de backup (concretamente a /var/backups) por si fuera necesario recuperarlos. Le decimos que si:

| ~ | sen | vidor-Idap [Corrie | endo] - Oracle VM VirtualBox | _ 🗆 × |
|----------------------------|---|--|--|-----------------------------------|
| <u>M</u> áquina <u>N</u> | <u>/</u> er <u>D</u> ispositivos | Ay <u>u</u> da | | |
| Configura | ción de paqu | etes | | |
| | | | | |
| | | | | |
| | | Configu | ración de slapd | |
| Existe proces de las | n ficheros e o de configu bases de da | n ≪∕var∕lib∕ld ración. Si act tos antiguas a | ap» que probablemente interrum iva esta opción, se moverá los ntes de crear una nueva base c | npan el ⊱ficheros de datos. |
| ل کلوده | mover la ba | se de datos an | tigua? | |
| | | <s1></s1> | <no></no> | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | 🔊 💟 Curi Derecho |

A continuación nos preguntará si queremos permitir usar el protocolo LDAPv2. Por lo que he leído actualmente se usa el protocolo LDAPv3. Tan sólo tendríamos que permitir usar LDAPv2 si tuviéramos programas antiguos que no utilizan LDAPv3.Una vez hecho ésto ya tendremos configurado el servicio LDAP.

Gestión de LDAP en Debian

| | servidor-Idap [Corriendo] - Oracle VM VirtualBox |
|----|--|
| N | Iáquina <u>V</u> er <u>D</u> ispositivos Ay <u>u</u> da |
| | |
| | Configuración de slapd |
| | El protocolo obsoleto LDAPv2 se ha desactivado de manera predeterminada en slapd. Los programas y los usuarios deberían actualizarse a LDAPv3. Debe seleccionar esta opción si aún tiene programas antiguos que no utilicen LDAPv3. Si lo hace, se añadirá la opción «allow bind_v2» al fichero de configuración «slapd.conf». |
| | ¿Desea permitir el protocolo LDAPv2? |
| | <sí></sí> |
| | |
| | |
| St | Moving old database directory to /var/backups: – directory unknown done. Creating initial configuration done. Creating LDAP directory done. arting OpenLDAP: slapd. pot@servidor_ldap:~# |
| | 😫 🕢 🗗 🛄 🖉 Ctrl Derecho |

2.3 Creación del directorio LDAP

Una vez instalado y configurado el servicio LDAP nuestra siguiente tarea será crear la estructura de nuestra base de datos LDAP e introducir los datos.

Como elegí como nombre de dominio **iesvalledeljerte.juntaextremadura.es**, la base de mi directorio es: **dc=iesvalledeljerte**, **dc=juntaextremadura**, **dc=es**. De esta base colgarán las diferentes unidades organizativas (**ou**).

Como en esta práctica sólo vamos a usar LDAP como servidor de autentificación para sistemas Linux, crearemos dos unidades organizativas:

- users: donde almacenaremos los datos de nuestros usuarios.
- groups: donde almacenaremos los datos de los grupos.

Puesto que al principio instalamos un paquete de herramientas (ldap-utils) podemos acceder al directorio LDAP mediante la línea de comandos, pero para facilitarnos la tarea de administración del mismo, recomendamos instalar dos herramientas en el equipo del administrador:

- **Phpldapadmin**: Es una aplicación web que se usa en los IES de Extremadura.
- JXplorer: Una aplicación java para admnistrar el directorio LDAP.

Como el el servidor LDAP no tiene entorno gráfico, administraremos LDAP desde nuestro equipo de administrador, instalando estas herramientas.

A continuación vamos a crear la estructura de nuestro directorio con Jxplorer, por lo tanto lo primero que haremos será instalarlo.

Instalar Jxplorer.

Como es una aplicación java, primero instalamos java en el equipo del administrador:



A continuación instalamos Jxplorer:

Una vez que termine el proceso de instalación, ya podemos abrir Jxplorer desde el menú o desde un terminal. Veremos la pantalla principal:

Conectar al servidor LDAP

Accederemos al servidor LDAP como administrador para crear la estructura de nuestro directorio. Para lograrlo, tendremos que pulsar el botón de conectar que aparece en la barra de herramientas de Jxplorer:

Se nos abrirá un cuadro de diálogo donde introduciremos los datos de acceso:

| ✓ Ор | en LDAP/DSML Conne | ction | × | |
|--------------------|--|-------------|-----|--|
| Host: | 172.19.144.84 | Port: | 389 | |
| Protocol: | LDAP v3 | | | |
| DSML Service: | | | | |
| Coptional Values | | | | |
| Base DN: dc=iesval | Base DN: dc=iesvalledeljerte,dc=juntaextremadura,dc=es | | | |
| Security | Security | | | |
| Level: | User + Password | ~ | | |
| User DN: | deljerte,dc=juntaextrem | adura,dc=es | | |
| Password: | *otototototok | | | |
| Use a Template | | | | |
| Save Idap | | | | |
| OK Cancel Help | | | | |

Resumiendo:

- Dirección IP del servidor de LDAP En mi práctica: 172.19.144.84.
- Protocolo del servidor: El que elegimos al instalarlo: LDAPv3.
- Base del directorio: iesvalledeljerte.juntaextremadura.es
- Nombre usuario administrador: cn=admin,dc=iesvalledeljerte,dc=juntaextremadura,dc=es
- Contraseña: La del usuario administrador.

Pulsamos el botón OK. JXplorer conectará con el servidor LDAP y nos mostrará el directorio:

| × | JXplorer | – – × |
|---|---|-------|
| <u>F</u> ile <u>E</u> dit <u>V</u> iew <u>B</u> ookmark <u>S</u> earch <u>L</u> DIF | [:] <u>O</u> ptions <u>T</u> ools Secur <u>i</u> ty <u>H</u> elp | |
| 💋 🖉 🎒 👗 🖻 🛍 🛍 🛛 🗙 | | |
| cn 💙 = 💙 🛛 Quick | Search | |
| Explore 📲 Results 🚧 Schema 🗣 | HTML View 🗈 Table Editor 🗈 | |
| ▼ 🚱 World | organization/Main.html | |
| ✓ ● juntaextremadura ✓ ● juntaextremadura ✓ ● jesvalledeljerte ▷ 彎n admin | ခ်ိန်ခြံ JXplorer ခ်ိန်ခြံ | |
| | Main Address Other | |
| | organization | |
| | Organization: iesvalledeljerte | |
| | Description: | |
| | User Password: | |
| | Telephone Number: | |
| | Facsimile Number: | |
| | Locality Name: | |
| | Submit Restablecer | |
| | | |
| | | |
| | | |
| Connected To 'ldap://172.19.144.84:389' | | |

Como podemos ver en la imagen anterior, tan sólo tenemos creado el directorio base del que cuelga el usuario administrador: **admin**.

Creación de las unidades organizativas

Primero crearemos la unidad organizativa **users**, para lo que haremos clic con el botón derecho del ratón sobre **iesvalledeljerte**. Se nos abre un menú de contexto donde elegimos "**New**":

| * | JXplorer | _ 🗆 🗙 |
|--|---|-------|
| <u>F</u> ile <u>E</u> dit <u>V</u> iew <u>B</u> ookmark <u>S</u> earch <u>L</u> DIF | [:] <u>O</u> ptions <u>T</u> ools Secur <u>i</u> ty <u>H</u> elp | |
| x x 🖨 🗼 🖻 🛍 🔳 🗙 🗎 | | |
| cn | Search | |
| Explore 📲 Results 🏘 Schema 🗣 | HTML View 🗈 Table Editor 🗈 | |
| V 🚱 World | organization/Main.html | |
| ✓ ● es ✓ ● juntaextremadura ✓ ● juntaextremadura | and IXplorer | |
| D Besvaller D Badmir ■ Add to Bookmar | ks Ctrl+B Heir Address Other | |
| 🕅 Search | Ctrl+F Main Address Other | |
| 🗋 New | _{Ctrl+N} organization | |
| E Copy DN | organization: iesvalledeljerte | |
| 👗 Cut Branch | Ctrl+U Description: | |
| 🖺 Copy Branch | Ctrl+O User Password: | |
| 🖷 Paste Branch | Ctrl+P elephone Number: | |
| Paste Alias | Facsimile Number: | |
| × Delete | Ctrl+D Locality Name: | |
| Rename | Ctd+M | |
| at Refresh | Ctri+R Submit Restablecer | |
| Connected To 'ldap://172.19.144.84:389' | | |

Introducimos los datos para crear la unidad organizativa users:

| * | JXplorer | | |
|---|--|--|--|
| <u>F</u> ile <u>E</u> dit <u>V</u> iew <u>B</u> ookmark <u>S</u> earch <u>L</u> D | DIF <u>O</u> ptions <u>T</u> ools Secur <u>i</u> ty <u>H</u> elp | | |
| S S 😂 L 🖻 🖻 💼 🔳 🗙 | D == 🚸 🖷 | | |
| cn | sk Search | | |
| Explore 📲 Results 🏟 Schema 🖓 | HTML View 🗈 Table Editor 🗈 | | |
| ▼ 🚱 World | organization/Main.html | | |
| ✓ ● juntaextremadura | Set Entry Object Classes × | | |
| D [®] admin | ✓ Suggest Classes? | | |
| | Parent DN: dc=iesvalledeljerte,dc=juntaextremadura,dc=es | | |
| | Enter RDN: ou=users | | |
| | Available Classes: Selected Classes: | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | V V | | |
| | Add Remove | | |
| | OK Cancel Help | | |
| | | | |
| | | | |
| | L | | |
| Connected To 'ldap://172.19.144.84:389' | | | |

En el cuadro de texto RDN introducimos: **ou=users**. Como lo que estamos creando es una unidad organizacional (**organizationalUnit**), en "Available Classes" seleccionamos "organizationalUnit" y pulsamos el botón "Add". Las otras dos clases que aparecen por defecto (organizationalRole y simpleSecurityObject) las quitamos seleccionándolas y pulsando el botón "Remove" porque no las necesitamos.

Una vez hecho ésto, pulsamos el botón OK y veremos que la unidad organizacional users se ha creado:

Del mismo modo, creamos la unidad organizacional groups:

| Y | JXplorer _ |
|--|--|
| <u>F</u> ile <u>E</u> dit <u>V</u> iew <u>B</u> ookmark <u>S</u> ear | arch LDIF <u>O</u> ptions <u>T</u> ools Secur <u>i</u> ty <u>H</u> elp |
| øø 🚑 🗼 🖻 🛍 🔳 | 1 X D = 🔅 🔹 |
| cn 💙 = 💙 | Quick Search |
| Explore 📲 Results 🏘 Schema | a 🚱 HTML View 🗈 Table Editor 🗎 |
| Vorld | ✓ Set Entry Object Classes × |
| v ● es v ● juntaextremadura | ✓ Suggest Classes? nalUnit |
| O jesvalledeljerte Pa | arent DN: dc=iesvalledeljerte,dc=juntaextremadura,dc=es |
| P ≝admin D ‱ users En | nter RDN: ou=groups |
| AV | vailable Classes: Selected Classes: |
| 0 | organization organizationalUnit |
| 0 | prganizationalPerson |
| 0 | organizationalRole |
| P | person v |
| | |
| | Add Remove |
| | OK Cancel Help |
| - | seeAlso |
| | st |
| | street telephoneNumber |
| | Submit Reset Change Class Properties |
| " Connected To 'ldap://172.19.144.8 | 84:389' |

Comprobamos que se ha creado:

| ~ | JXplorer | _ 🗆 X |
|--|--|------------------------|
| <u>F</u> ile <u>E</u> dit <u>V</u> iew <u>B</u> ookmark <u>S</u> earch <u>L</u> DI | F <u>O</u> ptions <u>T</u> ools Secur <u>i</u> ty <u>H</u> elp | |
| øø 🖉 🚔 % Pa Pa 💼 🔳 🗙 D 🔤 🚸 💿 | | |
| cn 💙 = 💙 🛛 Quick | < Search | |
| Explore 📲 Results 🏘 Schema 🗣 | HTML View 🖻 Table Editor 🖺 | |
| 🗢 🚱 World | attribute type | value |
| ✓ ● es ✓ ● iuntooxtromoduro | objectClass | organizationalUnit |
| | objectClass | top |
| Þ ® _∃ admin | ou | groups |
| 🕨 🥁 groups | businessCategory | |
| ▷ iiii users | description | |
| | destinationIndicator | |
| | facsimileTelephoneNumber | |
| | internationaliSDNNumber | [=] |
| | | |
| | physicalDeliveryOfficeName | |
| | postalAddress | |
| | postalCode | |
| | postoniceBox | |
| | registeredAddress | |
| | searchGuide | |
| | seeAlso | |
| | et | |
| | street | |
| | telephoneNumber | |
| Connected To !/don://172 10 144 04:2001 | Submit Reset C | nange Class Properties |
| connected to hdap://172.19.144.84:389 | | |

Creación de usuarios y grupos

A continuación vamos a crear los usuarios, los grupos y asignamos los usuarios a sus grupos.

| Primero creamos los grupos: | Después creamos los usuarios: |
|-----------------------------|-------------------------------|
| • alumnos (gid=1001). | • sagrario (uid=1001) |
| • Profesores (gid=1002) | • adrian (uid=1002) |
| | • natalia (uid=1003) |
| | • esteban (uid=1004) |

Pulsamos con el botón derecho del ratón sobre la entrada groups y en la casilla **RDN** escribimos "**cn=alumnos**" para crear el grupo de alumnos. Seleccionamos sólo la clase **posixGroup** en "Available Classes" y pulsamos el botón "Add" para añadirla. A continuación pulsamos el botón **OK**.

Pulsamos el botón "Submit" y comprobamos que el grupo se ha creado.

| → JXplorer _ □ × | | | |
|---|--|-----------------------|--|
| <u>F</u> ile <u>E</u> dit ⊻iew <u>B</u> ookmark <u>S</u> earch <u>L</u> D | F <u>O</u> ptions <u>T</u> ools Secur <u>i</u> ty <u>H</u> elp | | |
| øø 🖉 🚑 🗼 🖻 🛍 🖻 🗙 D 🔤 🚸 💿 | | | |
| cn 💙 = 💙 🛛 Quic | < Search | | |
| Explore 📲 Results 🏘 Schema 🔩 | HTML View 🗈 Table Editor 🗈 | ~ | |
| 🗢 🚱 World | attribute type | value | |
| | cn | alumnos | |
| Juntaextremadura iesvalledelierte | gidNumber | 1001 | |
| ▶ [®] admin | objectClass | posixGroup | |
| 🔰 🗼 groups | objectClass | top | |
| iii users | description | | |
| | memberUid | | |
| | userPassword | | |
| | | | |
| | Submit Reset Cha | ange Class Properties | |
| Connected To 'ldap://172.19.144.84:389' | | | |

Del mismo modo, creamos el grupo de profesores:

| File Edit View Bookmark Search I DI | JXplorer | _ 🗆 × |
|--|----------------------------|-----------------------|
| Sie For Sten For Search For Obrous Tools Security Help | | |
| cn | Search | |
| Explore 📲 Results 🏘 Schema 🗣 | HTML View 🗈 Table Editor 🗎 | |
| 🗢 🚱 World | attribute type | value |
| ✓ es ✓ es | cn | profesores |
| ✓ • jesvalledelierte | gidNumber | 1002 |
| ▷ [®] □ admin | objectClass | posixGroup |
| 🚽 🧟 groups | objectClass | top |
| Balumnos Balumnos Secondaria Secondaria Secondaria Secondaria Se | description | |
| P ≝ profesores | memberUid | |
| | Submit Reset Cha | ange Class Properties |
| Connected To 'ldap://172.19.144.84:389' | | |

Una vez creados los grupos, pasamos a crear los usuarios. Para ello, hacemos clic con el botón derecho sobre la unidad organizativa **users** e igual que antes, hacemos clic en "New". En "Available Classes" seleccionamos los tipos "posixAccount", "person" e "inetOrgPerson" para disponer de los campos de datos que nos ofrece cada uno de los tipos:

| ▼ | JXplorer | _ — × | |
|---|--|------------------------|--|
| <u>F</u> ile <u>E</u> dit <u>V</u> iew <u>B</u> ookmark <u>S</u> earch <u>L</u> DI | F <u>O</u> ptions <u>T</u> ools Secur <u>i</u> ty <u>H</u> elp | | |
| øøe k 🖻 🛍 🔳 🗙 | øø 👙 🗼 🖻 🛍 💼 🛛 🗙 🗅 🥅 🚸 🛑 | | |
| cn 💙 = 💙 🛛 Quick | < Search | | |
| Explore 📲 Results 🚧 Schema 🗣 | HTML View 💽 Table Editor 🗈 | | |
| 🗢 😝 World | attribute type | [value] | |
| ✓ es ✓ iuptaextremadura | cn | Sagrario | |
| | gidNumber | 1001 | |
| ▶ In admin | homeDirectory | /home/sagrario | |
| ∽ 🚟 groups | objectClass | inetOrgPerson | |
| Image: Second | objectClass | organizationalPerson | |
| D E profesores | objectClass | person | |
| 🗾 🔁 users | objectClass | posixAccount | |
| | objectClass | top | |
| | sn | Pedraza Labrador | |
| | uid | sagrario | |
| | uidNumber | 1001 | |
| | audio | | |
| | businessCategory | | |
| | carLicense | | |
| | departmentNumber | | |
| | description | | |
| | destinationIndicator | | |
| | displayName | | |
| | employeeNumber | | |
| | empioyeeiype | | |
| | | | |
| | Submit Reset C | hange Class Properties | |
| Connected To 'ldap://172.19.144.84:389' | | | |

Al seleccionar el tipo "person" disponemos de campos como el nombre, apellidos, etc...

Al seleccionar el tipo "inetOrgPerson" dispondremos de campos como el e-mail, etc...

Del mismo modo añadimos más usuarios:

| | JXplorer | _ 🗆 X | | |
|---|--|------------------------|--|--|
| <u>F</u> ile <u>E</u> dit <u>V</u> iew <u>B</u> ookmark <u>S</u> earch <u>L</u> DI | F <u>O</u> ptions <u>T</u> ools Secur <u>i</u> ty <u>H</u> elp | | | |
| øøe 🛦 🖻 🛍 🔳 🗙 | ØØ# 1% Pa Pa Ca X D = 1% ● | | | |
| cn 💙 = 💙 🛛 Quick | k Search | | | |
| Explore 📲 Results 🏘 Schema 🖓 | HTML View 🗈 Table Editor 🖺 | ~ | | |
| ▼ 🚱 World | attribute type | value | | |
| ✓ es ✓ es | cn | Adrian | | |
| ✓ ● jesvalledelierte | gidNumber | 1001 | | |
| ▶ [®] admin | homeDirectory | /home/adrian 🗧 | | |
| ∽ 🚟 groups | objectClass | inetOrgPerson | | |
| Image: Second | objectClass | organizationalPerson | | |
| | objectClass | person | | |
| v ﷺ users | objectClass | posixAccount | | |
| D Sagrario | objectClass | top | | |
| | sn · · | Navas Pedraza | | |
| | uid | loop | | |
| | audia | 1002 | | |
| | husinessCategory | | | |
| | carlicense | | | |
| | departmentNumber | | | |
| | description | | | |
| | destinationIndicator | | | |
| | displayName | | | |
| | employeeNumber | | | |
| | employeeType | ~ | | |
| Connected To 'ldap://172.19.144.84/389' | Submit Reset Cl | nange Class Properties | | |
| | | | | |

| ~ | JXplorer | × | |
|--|---|-----------------------|--|
| <u>F</u> ile <u>E</u> diit ⊻iew <u>B</u> ookmark <u>S</u> earch LDIF | ⁼ <u>O</u> ptions <u>T</u> ools Secur <u>i</u> ty <u>H</u> elp | | |
| 8 🔊 🍜 1 ங 🛍 🗰 🗶 🗙 🗅 📼 🚸 🜑 | | | |
| cn | Search | | |
| Explore 📲 Results 🏟 Schema 🔩 | HTML View 💽 Table Editor 🖺 | | |
| vorld ₩ | attribute type | value | |
| | cn | Natalia | |
| ✓ • juntaextremadura | gidNumber | 1002 | |
| ▶ Isstanciacijence | homeDirectory | /home/natalia | |
| Þ ﷺ groups | objectClass | inetOrgPerson | |
| ⊽ .‱users | objectClass | organizationalPerson | |
| D C Adrian | objectClass | person | |
| Natalia | objectClass | posixAccount | |
| V 😋 Sagrario | objectClass | top | |
| | sn | Navas Pedraza | |
| | uid | natalia | |
| | uidNumber | 1003 | |
| | Submit Reset Cha | ange Class Properties | |
| Opening Connection To Idap://172.19.144.84:389 | | | |

| ✓ JXplorer _ □ X | | | |
|---|--|-----------------------|--|
| <u> </u> | F <u>O</u> ptions <u>T</u> ools Secur <u>i</u> ty <u>H</u> elp | | |
| Ø Ø 5 1 = 6 6 Z X | S S 5 4 Pr | | |
| cn 💙 = 💙 🛛 Quict | < Search | | |
| Explore 📲 Results 🏘 Schema 🗣 | HTML View 🗈 Table Editor 🗎 | | |
| ▼ 🚱 World | attribute type | value | |
| ✓ es ✓ es | cn | Esteban | |
| | gidNumber | 1002 | |
| | homeDirectory | /home/esteban | |
| ▷ 👹 groups | objectClass | inetOrgPerson | |
| ⊽ users | objectClass | organizationalPerson | |
| P 🖉 Adrian | objectClass | person | |
| Ba Netelie | objectClass | posixAccount | |
| V Sagrario | objectClass | top | |
| P - B Sagrano | sn | Navas Martin | |
| | uid | esteban | |
| | uidNumber | 1004 | |
| Opening Connection To Iden///172-10-144 | Submit Reset Ch | ange Class Properties | |
| Opening Connection To Idap://172.19.144 | Opening Connection To Idap://172.19.144.84:389 | | |

A continuación asignamos los usuarios Adrian y Sagrario al grupo de alumnos editando la unidad organizacional "alumnos" y en la pestaña "Table Editor" especificando sus nombres de usuario en "memberUid". Habrá un campo "memberUid" por cada usuario del grupo:

| ~ | JXplorer | _ 🗆 X | |
|--|---|-----------------------|--|
| <u>F</u> ile <u>E</u> dit <u>V</u> iew <u>B</u> ookmark <u>S</u> earch <u>L</u> DI | ⁼ <u>O</u> ptions <u>T</u> ools Secur <u>i</u> ty <u>H</u> elp | | |
| x x 😂 1 🖻 🖻 🖷 🗙 | øøø 😹 🖡 🖻 🛍 🖻 i 🗙 i 🗅 📼 i 🚸 i 💿 | | |
| cn | Search | | |
| Explore 📲 Results 🏘 Schema 🗣 | HTML View 🗈 Table Editor 🗈 | | |
| 🗢 🚱 World | attribute type | value | |
| ✓ • es | cn | alumnos | |
| | gidNumber | 1001 | |
| | objectClass | posixGroup | |
| ⊽ 🚆 groups | objectClass | top | |
| 📃 🔰 alumnos | memberUid | Adrian | |
| D_E profesores | memberUid | Sagrario | |
| V ﷺ users | description | | |
| D Stepan | userPassword | | |
| ≥ Stepan | | | |
| Sagrario | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | Submit Reset Cha | ange Class Properties | |
| Connected To 'ldap://172.19.144.84:389' | | | |

| ✓ J×plorer _ □ × Eile Edit View Bookmark Search LDIF Options Tools Security Help | | |
|--|----------------------------|----------------------|
| ØØ ● % Pa Pa Ca × D ca 🚸 ● | | |
| cn 💙 = 💙 🛛 Quick | Search | |
| Explore 📲 Results 🏟 Schema 🚱 | HTML View 🗈 Table Editor 🗈 | |
| 🗢 🚱 World | attribute type | value |
| ♥ • es | cn | profesores |
| ✓ ■ juntaextremadura | gidNumber | 1002 |
| | objectClass | posixGroup |
| ⊽ ä groups | objectClass | top |
| ▷ [®] alumnos | memberUid | Esteban |
| <mark>™</mark> ∎ profesores | memberUid | Natalia |
| V ‱ users | description | |
| V ℃ Adrian | userPassword | |
| | | |
| ▷ 📴 Sagrario | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | Submit Reset Cha | nge Class Properties |
| | | |
| Connected To 'ldap://172.19.144.84:389' | | |

Del mismo modo, asignamos los usuarios Natalia y Esteban al grupo profesores:

Sagrario Pedraza Labrador

Instalación de phpldapadmin

Hemos visto cómo modificar el directorio ldap con Jxplorer. Si quisiéramos usar phpldapadmin, tan sólo tendríamos que instalarlo:

| • | | | ser | /idor-ld | ap [Co | orriendo] | - Oracle | VM Vi | rtualBo | x | | (| - 1 | □ × □ |
|---|---|--|---|---|--|--|--|--|-------------------------------------|--------------------------------|--------------------------------------|----------------------------------|-------------|-------|
| <u>M</u> áquina | Ver | Dispos | itivos | Ay <u>u</u> da | | | | | | | | | | |
| | R) | X byte | es:0 | (0.0 B |) TX | bytes: | 0 (0.0 | B) | | | | | | |
| root@sen Leyendo Creando Leyendo Se insta apach file libapn libxm | rvid lis árbo la alará e2 ap libap ruti 12 m. | or–lda ta de ol de inforr án los pache2 pache2 l1–lda ime–su | p:~# paqu depe ació sig -mpm -mod p li | apt–g etes ndenci n de e uiente –prefo –php5 bcap2 t open | et in . Hec as stado s paq rk ap libap libex ssl p | stall p ho uetes e ache2–u r1 liba pat1 li hp5–cli | hpldapa ho xtras: tils ap prutil1 bmagic1 php5-c | dmin ache2 liba libo ommon | .2–bin prutil nig2 l php5– | apac 1–dbd ibpcr ldap | ne2.2– -sqlit 23 lib 2hp5–s | common e3 qdbm14 uhosin | ח 4 ח | |
| sgml- | base | ssl-0 | ert | xml-co | re re | npo cii | phpo c | 011111011 | pripo | raap | 511po o | anosti | | |
| raquete: www-bi ca-cei | s su: rows0 rtif | geriad er apa icates | is: iche2 ; sgm | -doc a 1-base | pache –doc | 2–suexe openssl | c apach –blackl | e2–su ist d | exec-c ebhelp | ustom | php-p | ear | | |
| Se insta apacho file libapo libxm phplda | alara e2 ap libap ruti 12 m apado | án los pache2 pache2 l1–lda ime–su min s§ | ; sig ?-mpm ?-mod ?p li ?ppor (ml-b | uiente –prefo –php5 bcap2 t open ase ss | s paq rk ap libap libex ssl p l–cer | uetes N ache2–u r1 liba pat1 li hp5–cli t xml–c | UEVOS: tils ap prutil1 bmagic1 php5–c ore | ache2 liba libo ommon | .2-bin prutil nig2 l php5- | apac 1–dbd ibpcr ldap | ne2.2– –sqlit e3 lib ohp5–s | common e3 qdbm14 uhosin | า 1 า | |
| 0 actua. Necesity | liza(| dos, 2 | 8 se | insta | larán do op | , O par | a elimi | nar y | 28 no | actu | alizad | os. | | |
| Se util ¿Desea (| izara cont | án 38. inuar | 4 MB [S/n | ,o mb de es]? _ | ue ar pacio | de dis | co adic | ional | despu | iés de | esta | opera | ció | n. |
| | | | | | | | | | 90 | 7 🔟 🗹 | 🖉 🕲 | Ctrl De | re | ho |

El archivo de configuración de ldap es /etc/phpldapadmin.conf.

Ésta es la pantalla de acceso de phpldapadmin:

| • | phpLDAPadmin (1.2.0.5) Iceweasel | _ 🗆 × |
|---|---|------------------------|
| <u>A</u> rchivo <u>E</u> ditar <u>V</u> er Hi <u>s</u> to | orial <u>M</u> arcadores Herramien <u>t</u> as Ay <u>u</u> da | |
| phpLDAPadmin (1.2.0.5) | | |
| 💠 🚹 172.19.144.84/php | pldapadmin/ 🗘 🗸 🔘 🚼 🗸 Go | ogle 🔺 🏤 |
| | | |
| LDAP | | |
| | | ý 🥫 🏘 🚳 |
| Inicio Borrar cachés Ver cach | | |
| 🚚 My LDAP Server | Autentificar al servidor My LDAP Server | |
| 👮 conectar | | |
| | Advertencia: Esta conexión web no está encriptada. | |
| | | |
| | cogni: | |
| | | |
| | Contraseña: | |
| | | |
| | | |
| | | |
| | | |
| | | 1205 |
| | | 1.2.0.5 Sourceforge |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

Para entrar tendremos que introducir el usuario administrador y su contraseña:

Login: cn=admin,dc=iesvalledeljerte,dc=juntaextremadura,dc=es

Una vez dentro, veremos la estructura de nuestro directorio ldap del mismo modo que la veíamos con JXplorer:

3. Instalación de un cliente LDAP.

En un sistema Linux, los usuarios se autentifican con los datos almacenados en los ficheros:

- /etc/passwd
- /etc/group
- /etc/shadow

Si queremos que los usuarios de un equipo cliente puedan acceder con los datos almacenados en un servidor ldap, básicamente habrá que hacer lo siguiente:

- Instalar y configurar la librería libpam-ldap.
- Instalar y configurar la librería libnss-ldap.
- Configurar nsswitch.conf.

3.1 Instalar y configurar la librería libpam-ldap

En Debian es sencillo instalar esta librería:

Pulsamos Enter para que comience la instalación. Una vez instalado, se inicia automáticamente un asistente de configuración que nos irá haciendo preguntas para configurarla.

En cualquier momento podemos reconfigurar libpam-ldap con tan sólo ejecutar: dpkg-reconfigure libpam-ldap.

Lo primero que nos preguntará es el URI del servidor ldap. Introduciremos la IP de nuestro servidor ldap de la siguiente manera: **ldap://172.19.144.84**:

| • | cliente-Idap [Corriendo] - Oracle VM VirtualBox | – 🗆 × |
|------------|---|--------|
| <u>M</u> á | iquina <u>V</u> er <u>D</u> ispositivos Ay <u>u</u> da | |
| Cor | nfiguración de paquetes | |
| | | |
| | | |
| | Introduzca el URI («Uniform Resource Identifier», o Identificador | |
| | Uniforme de Recursos) del servidor de LDAP. Esta cadena es similar a | |
| | utilizar «ldaps://» o «ldapi://». El número de puerto es opcional. | |
| | Se recomienda utilizar una dirección IP para evitar fallos cuando los | |
| | servicios de nombres de dominio no estén disponibles. | |
| | URI del servidor de LDAP: | |
| | ldap://172.19.144.84 | |
| | (Aconton) | |
| | | |
| | | |
| | | |
| | | |
| | | racha |
| | | erecno |

A continuación nos pedirá que introduzcamos el nombre de nuestro dominio base. Introducimos el nombre que elegimos cuando instalamos el servidor ldap:

| × | cliente-Idap [Corriendo] - Oracle VM VirtualBox | _ 🗆 🗙 |
|--|--|-----------|
| <u>M</u> áquina <u>V</u> er <u>D</u> is | positivos Ay <u>u</u> da | |
| Configuración (| de paquetes | |
| Introduzca e muchos sitio propósito. f «dc=ejemplo El nombre d | Configuración de libpam-ldap el nombre distintivo (DN) de la base de búsquedas de LDAP. os se utilizan las componentes del nombre de dominio con es Por ejemplo, el dominio «ejemplo.net» utilizaría ,dc=net» como nombre distintivo de la base de búsquedas. istintivo (DN) de la base de búsquedas: | En ste |
| dc=iesvalle | deljerte3,dc=juntaextremadura,dc=es | |
| | <aceptar></aceptar> | |
| | | |
| | | |
| | | |
| | | |
| | 😂 🕢 🗗 🛄 💟 🖉 Ctrl D | erecho |

Ahora nos preguntará qué versión de LDAP vamos a utilizar. Recordemos que elegimos usar LDAPv3 en el servidor:

| ~ | cliente-Idap [Corriendo] - Oracle VM VirtualBox | _ 🗆 🗙 |
|--------------------------------------|--|--------|
| <u>M</u> áquina <u>V</u> er <u>[</u> | <u>D</u> ispositivos Ay <u>u</u> da | |
| Configuración | n de paquetes | |
| | | |
| | | |
| | | |
| Introduzes | Configuración de libpam-ldap | |
| recomienda | a utilizar el número de versión más alto 💭e esté disponible. | |
| Versión de | e LDAP a utilizar: | |
| | | |
| | 2 | |
| | | |
| | < <u>Aceptar></u> | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | 😂 🕢 🗗 🛄 💟 🖉 Ctrl D | erecho |

En el siguiente paso nos pregunta si necesitamos permitimos que la cuenta del admnistrador de LDAP se comporte como el administrador local. Le decimos que sí.

| ~ | cliente-Idap [Corriendo] - Oracle VM | VirtualBox | _ 🗆 × |
|--|--|--------------------------------------|--------|
| <u>M</u> áquina <u>V</u> er <u>D</u> isposit | tivos Ay <u>u</u> da | | |
| Configuración de p | paquetes | | |
| | | | |
| | | | |
| | Configuración de libpam- | ldap | |
| Esta opción per PAM cambien las | rmite que las herramientas de la s contraseñas locales. | s contraseñas que utilic | en |
| La contraseña d archivo separad | de la cuenta del adminnstrador d do que sólo podrá leer el admini | e LDAP se guardará en un strador. | |
| Esta opción se | debería desactivar, si se monta | «/etc» mediante NFS. | |
| ሪDesea permitir el administrado | r que la cuenta del administrado pr local? | r de LDAP se comporte co | mo |
| | KS1> | <no></no> | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | 😂 🕢 🗗 🛄 💟 🖉 Ctrl De | erecho |

En la siguiente ventana respondemos que no se necesita usuario para acceder a la base de datos de ldap.

Nos pedirá que introduzcamos la cuenta del administrador de ldap. Introduciremos la que creamos en el servidor de ldap: **cn=admin,dc=iesvalledeljerte,dc=instituto,dc=extremadura,dc=es**

| ~ | cliente-Idap [Corriendo] - Oracle VM VirtualBox | _ 🗆 × |
|-----|--|--------|
| Má | quina <u>V</u> er <u>D</u> ispositivos Ay <u>u</u> da | |
| Con | figuración de paquetes | |
| | | |
| | | |
| _ | | |
| | Configuración de libpam-ldap Introduzca el nombre de la cuenta del administrador de LDAP. | |
| | Esta cuenta se usará automáticamente para la gestión de la base de datos, por lo que debe tener los privilegios administrativos apropiado | is. |
| | Cuenta del administrador de LDAP: | |
| | cn=admin,dc=iesvalledeljerte,dc=juntaextremadura,dc=es | |
| | <aceptar></aceptar> | |
| | | |
| | | |
| | | |
| | | |
| | | erecho |
| | | creeno |

Nos pedirá que introduzcamos la contraseña del administrador de ldap. La introducimos:

En la siguiente ventana nos informa de los posibles modos para cifrar la contraseña:

Elegimos crypt:

| • | cliente-Idap [Corriendo] - Oracle VM VirtualBox | _ 🗆 🗙 |
|--------------------------|---|--------|
| <u>M</u> áquina <u>V</u> | er <u>D</u> ispositivos Ay <u>u</u> da | |
| Configura | ción de paquetes Configuración de libpam-ldap Algoritmo de cifrado local a utilizar en las contraseñas. en claro | |
| | <mark>crypt</mark> nds ad exop md5 | |
| | <aceptar></aceptar> | |
| | | |
| | 😂 😳 🗗 🛄 🔘 🖉 Ctrl De | erecho |

Los módulos PAM nos permiten configurar cómo se va a realizar la autentificación en el sistema. Como queremos permitir tanto la autentificación de los usuarios almacenados localmente en el equipo, como por ejemplo root, como la autentificación de los usuarios almacenados en ldap, marcaremos ambas opciones:

- Unix Authentication.
- LDAP Auhentication.

De este modo, se configurará automáticamente PAM para permitir ambos sistemas de autentificación. Pulsamos "Aceptar" y habremos terminado de configurar libpam-ldap.

3.2 Instalar y configurar la librería libnss-ldap

Instalar libnss-ldap es sencillo:

Pulsamos Enter para que comience la instalación. Se inicia automáticamente un asistente de configuración que nos irá haciendo preguntas para configurarla.

Una vez instalado, en cualquier momento podemos configurar libnss-ldap con tan sólo ejecutar: dpkg-reconfigure libnss-ldap.

Lo primero que nos pedirá el asistente será el URI del servidor ldap. Introduciremos: la IP del servidor ldap de la siguiente manera: http://172.19.144.84:

| Cliente-Idap [Corriendo] - Oracle VM VirtualBox |
|--|
| Maquina Ver Dispositivos Ayuda |
| Configuración de paquetes |
| |
| Configuración de libnss-ldap Introduzca el URI («Uniform Resource Identifier», o identificador uniforme de recursos) para el servidor LDAP que utiliza. Esta cadena es similar a ldap:// <nombre de="" dirección="" equipo="" ip="" o="">:<puerto>/. También puede utilizar ldaps:// o ldapi://. El número de puerto es opcional.</puerto></nombre> |
| NOTA: Es siempre una buena idea especificar una dirección IP en vez de un nombre, ya que reduce el riesgo de fallos en caso de que el servicio de nombres no esté disponible. |
| Identificador de recursos para el servidor LDAP: |
| ldap://172.19.144.84 |
| <aceptar></aceptar> |
| |
| |
| 😂 🕢 🗗 💭 🕼 Ctrl Derecho |

A continuación nos preguntará el nombre del administrador ldap:

cn=admin,dc=iesvalledeljerte,dc=juntaextremadura,dc=es

| | cliente-Idap [Corriendo] - Oracle VM VirtualBox | . 🗆 🗙 |
|----|---|-------|
| M | áquina <u>V</u> er <u>D</u> ispositivos Ay <u>u</u> da | |
| Со | nfiguración de paquetes | |
| | | |
| | | |
| | Configuración de libnss-ldap Escoja que cuenta se utilizará para las consultas nss con privilegios de root. | ; |
| | Nota: Para que funcione esta opción la cuenta necesita permisos para poder acceder a los atributos LDAP que están asociados con las entradas «shadow» de los usuarios así como a las contraseñas de los usuarios y grupos. | |
| | Cuenta LDAP para root: | |
| | cn=admin,dc=iesvalledeljerte,dc=juntaextremadura,dc=es | |
| | <pre>KAceptar></pre> | |
| L | | |
| | | |
| | | |
| | | |
| | 😂 🕢 🗗 🛄 💟 🖉 Ctrl Dere | cho |

Nos preguntará la versión de LDAP. Elegimos LDAPv3:

| ~ | cliente-Idap [Corriendo] - Oracle VM VirtualBox 📃 🛛 |) × |
|-----|---|-----|
| Má | áquina <u>V</u> er <u>D</u> ispositivos Ay <u>u</u> da | |
| Cor | nfiguración de paquetes | |
| | | |
| | | |
| | Configuración de libnss-ldap | 1 |
| | Introduzca la versión del protocolo LDAP que debería usar idapos. | |
| | que esté disponible. | |
| | Versión de LDAP a utilizar. | |
| | | |
| | 3 | |
| | | |
| | (Arentar) | |
| | | |
| | | 1 |
| | | |
| | | |
| | | |
| | Se 🗗 🗐 🕐 🛃 Ctrl Derech | 10 |

Nos preguntará si hace falta un usuario para acceder a la base de datos LDAP. Le decimos que no:

Nos preguntará si queremos dar privilegios especiales de LDAP para root. Le decimos que sí:

| ~ | cliente-Idap [Corriendo] - Oracle VM VirtualBox | _ 🗆 × |
|----|---|--------|
| Ma | áquina <u>V</u> er <u>D</u> ispositivos Ay <u>u</u> da | |
| Co | nfiguración de paquetes | |
| | | |
| | | |
| Г | Configuración de libnss-ldap | |
| | Esta opción permite que las herramientas que realizan consultas al sistema nss a través del motor libnss-ldap proporcionen más informació si se llaman como usuario root. | in |
| | Debería deshabilitar esta opción si está utilizando un directorio ∕etc montado por NFS o cualquier otra configuración a medida. | : |
| | ¿Dar privilegios especiales de LDAP para root? | |
| | <s1> <no></no></s1> | |
| | | |
| | N | |
| | | |
| | | |
| | | |
| | Section De 🕑 🕞 🗐 🛞 🖉 Ctri De | erecho |

Nos pedirá que indiquemos una cuenta para las consultas nss con privilegios de root. Indicamos la del administrador:

| * | cliente-Idap [Corriendo] - Oracle VM VirtualBox 🛛 🗕 | - x | | |
|---|---|------------|--|--|
| <u>M</u> áquina <u>V</u> er <u>D</u> ispositivos Ay <u>u</u> da | | | | |
| Configuración de paquetes | | | | |
| | | | | |
| | | | | |
| | Escoja que cuenta se utilizará para las consultas nss con privilegios de root. | ; | | |
| | Nota: Para que funcione esta opción la cuenta necesita permisos para poder acceder a los atributos LDAP que están asociados con las entradas «shadow» de los usuarios así como a las contraseñas de los usuarios y grupos. | | | |
| | Cuenta LDAP para root: | | | |
| | cn=admin,dc=iesvalledeljerte,dc=juntaextremadura,dc=es | | | |
| | <aceptar></aceptar> | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | 😫 🕢 🗗 🖾 💟 🖉 Ctrl Dere | cho | | |

Nos preguntará por la contraseña del usuario root. La introducimos:

| • | cliente-Idap [Corriendo] - Oracle VM VirtualBox 📃 🗆 🗙 | | | |
|---|--|--|--|--|
| <u>M</u> áquina <u>V</u> er <u>D</u> ispositivos Ay <u>u</u> da | | | | |
| Configuración de paquetes | | | | |
| | | | | |
| | | | | |
| | Introduzca la contraseña se utilizará cuando Lonss-Idap intente autenticarse al directorio LDAP con la cuenta LDAP de root. | | | |
| | La contraseña se guardará en un fichero independiente («/etc/libnss-ldap.secret») al que sólo podrá acceder root. | | | |
| | Si introduce una contraseña vacía se reutilizará la antigua contraseña. | | | |
| | Contraseña para la cuenta LDAP de root: | | | |
| | ****** | | | |
| | <mark><aceptar></aceptar></mark> | | | |
| | | | | |
| | | | | |
| | | | | |
| | Service and the service of the servi | | | |

Nos informa de que **nsswitch.conf** no se gestiona automáticamente. Esto quiere decir que tendremos que modificar el fichero /etc/nsswitch.conf para que nuestro sistema se autentifique con ldap:

El asistente terminará y con ello habremos configurado casi todo.

Para terminar la configuración de libnss-ldap vamos a modificar el fichero /etc/libnss-ldap.conf anñadiendo las líneas que le indican en qué unidades organizativas se encuentran los usuarios y los grupos:

nss_base_passwd ou=users,dc=iesvalledeljerte,dc=juntaextremadura,dc=es nss_base_group ou=group,dc=iesvalledeljerte,dc=juntaextremadura,dc=es

3.3 Configurar nsswitch.conf

Por último, editamos el fichero /etc/nsswitch.conf y añadimos la palabra ldap detrás de la palabra compat en las líneas passwd, group y shadow. De este modo, estamos indicando que se utilice LDAP como alternativa para autentificar los usuarios:

| # /etc/nsswitch.conf # # Example configuration of GNU Name Service Switch functionality. # If you have the `glibc-doc-reference' and `info' packages installed, try: # `info libc "Name Service Switch"' for information about this file. | | | | | |
|---|-------------|--|--|--|--|
| passwd: | compat Idap | | | | |
| group: | compat Idap | | | | |
| shadow: | compat Idap | | | | |
| hosts: | files dns | | | | |
| networks: | files | | | | |
| protocols: | db files | | | | |
| services: | db files | | | | |
| ethers: | db files | | | | |
| rpc: | db files | | | | |
| netgroup: | nis | | | | |

4. Probar la autentificación

Para comprobar si funciona la autentificación arranco la máquina virtual servidora de ldap y la máquina virtual cliente de ldap.

A continuación, inicio sesión en la máquina cliente, y ejecuto el comando:

getent passwd

Este comando me muestra todos los usuarios que hay en el sistema, tanto los locales como los que están almacenados en ldap. Si no se mostraran los de ldap es porque habría algún error en la configuración.

Para asegurarnos de que se realiza la autentificación, instalamos el paquete libpam-dotfile:

apt-get install libpam-dotfile

Una vez instalado, ejecutamos el comando pamtest passwd usuariodeldap. Por ejemplo:

pamtest passwd sagrario

Nos pedirá la contraseña. Si todo está bien configurado, veremos un mensaje que dice:

Authentication successful.

También podríamos ejecutar el comando **su** (switch user) desde una consola de root a un usuario almacenado en ldap. Si nos permite cambiar de usuario y no nos pide contraseña es porque la autentificación con ldap está funcionando correctamente.

5. Crear home del usuario al vuelo

Tal y como está configurado el sistema, tenemos nuestros usuarios creados en el servidor ldap y éste nos va a permitir autentificarnos en un cliente con ellos, pero si no tenemos un directorio home creado en la máquina cliente nos advertirá de ello.

Podemos hacer que se cree el directorio home de un usuario al vuelo cuando éste inicie sesión por primera vez añadiendo la siguiente línea al fichero de configuración /etc/pam.d/common-session:

session required pam_mkhomedir.so skel=/etc/skel umask=0022