# OPENLDAP

**TAREA A REALIZAR:**

Crear un Dominio en Linux con OpenLdap e integrar un cliente Linux y uno Windows. De tal forma que se pueda validar usuarios en el dominio Linux.

**¿Qué es?**

**OpenLDAP** es una implementación libre y de [código abierto](https://es.wikipedia.org/wiki/C%C3%B3digo_abierto) del protocolo Lightweight Directory Access Protocol ([LDAP](https://es.wikipedia.org/wiki/LDAP)) desarrollada por el proyecto OpenLDAP.

LDAP, es un protocolo que ofrece el acceso a un servicio de directorio implementado sobre un entorno de red, con el objeto de acceder a una determinada información. Puede ejecutarse sobre TCP/IP o sobre cualquier otro servicio de transferencia orientado a la conexión.

1-Crear máquina con Ubuntu 18 y ponerle una IP estática.

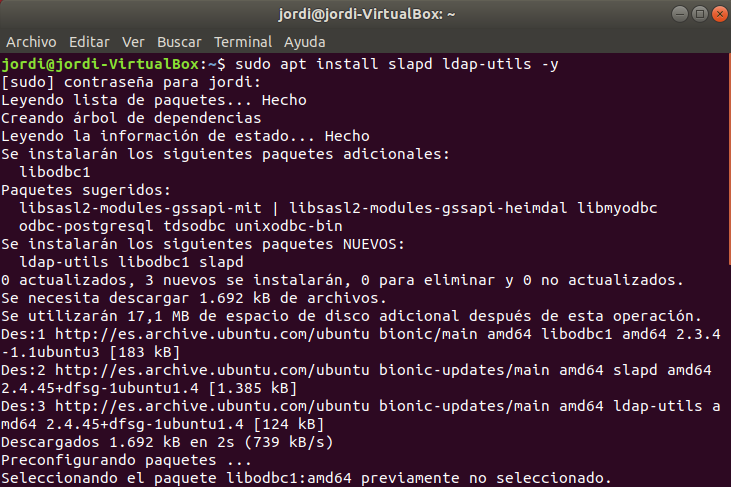
Ya sabemos como crear una máquina ubuntu y como darle una IP estática,así que lo hacemos,pongo la captura con esto ya hecho.



2-Instalar el servidor SLAPD

Con el comando siguiente haremos un paso previo a instalar y configurar el servidor:

**“sudo apt install slapd ldap-utils -y”**

****

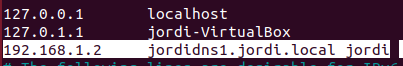
Y ahora vamos a poner la contraseña de administrador:



Después tendremos que editar el fichero **/etc/hosts** y tendremos que poner la IP del servidor y el nombre del servidor.



Añadimos esta línea:



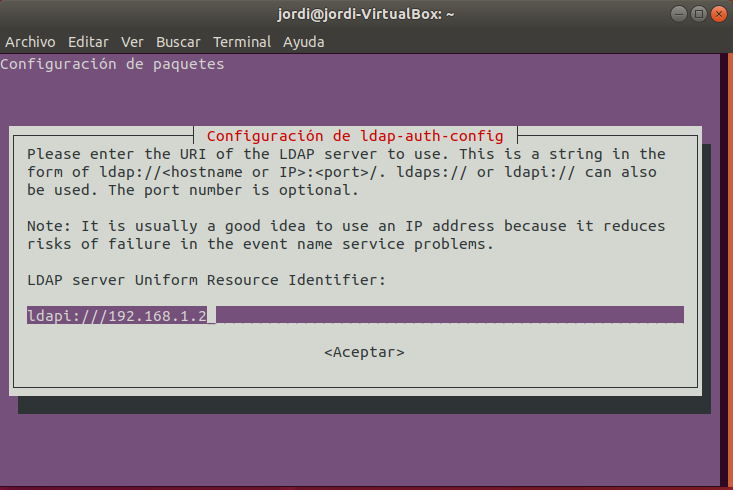
Después guardamos y salimos.

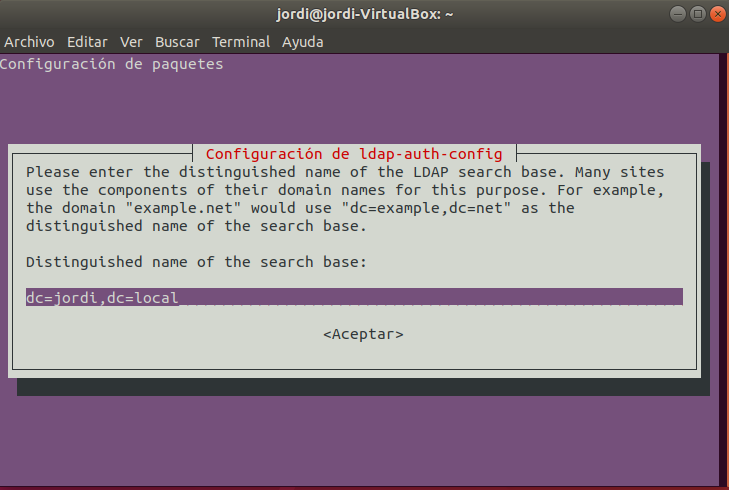
Este fichero se utiliza para obtener una relación entre un nombre de máquina y una dirección IP: en cada línea de /etc/hosts se especifica una dirección IP y los nombres de máquina que le corresponden, de forma que un usuario no tenga que recordar direcciones sino nombres de hosts. Habitualmente se suelen incluir las direcciones, nombres y aliases de todos los equipos conectados a la red local, de forma que para comunicación dentro de la red no se tenga que recurrir a DNS a la hora de resolver un nombre de máquina.

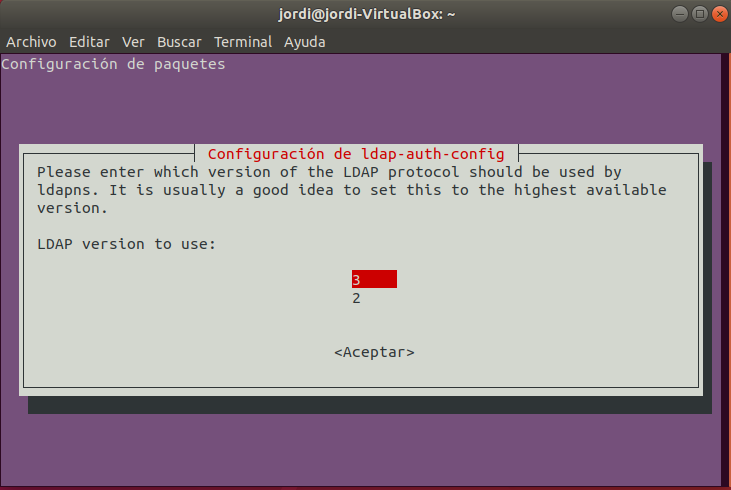
Ahora vamos a instalar el **servidor** y a configurarlo:

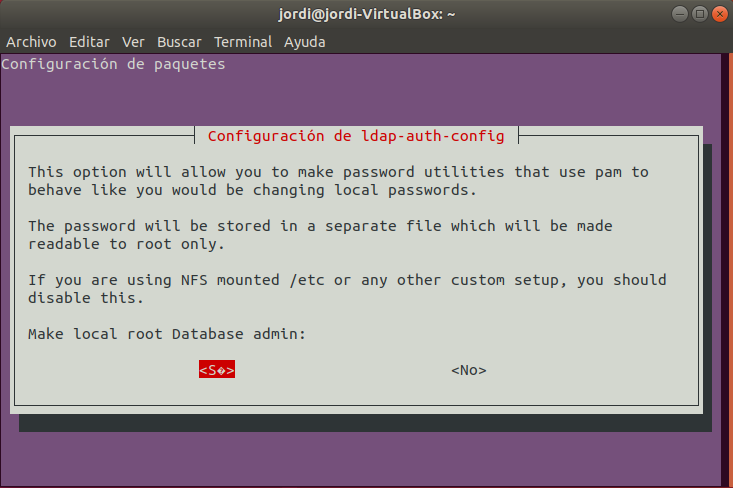
Ponemos el comando

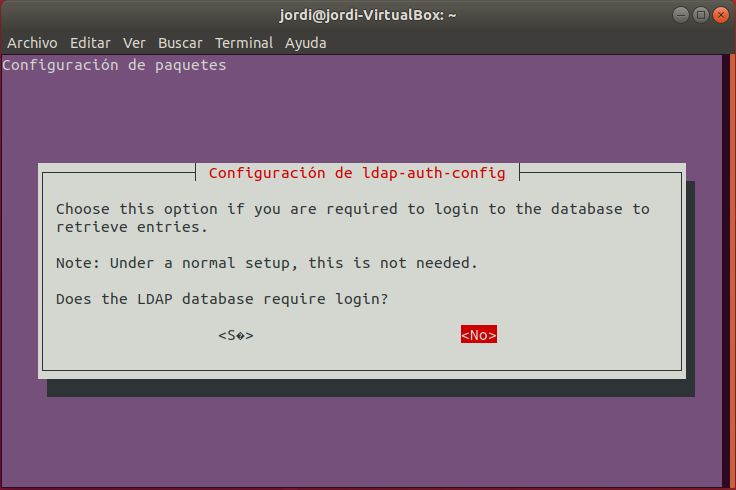
**“sudo apt install libnss-ldap -y”**

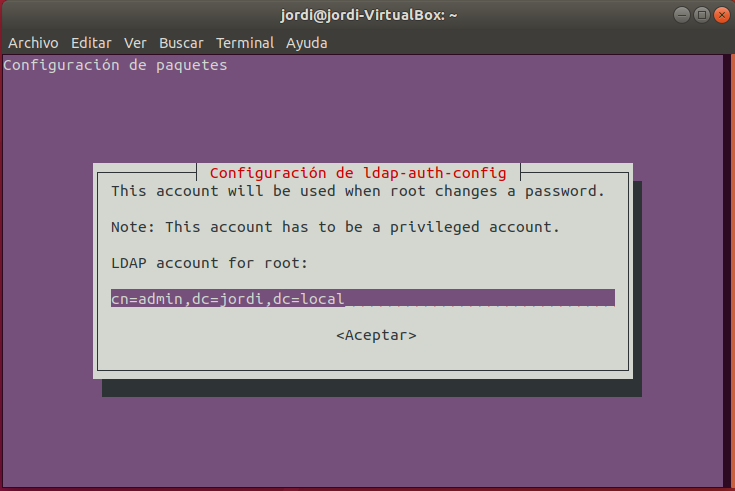
****



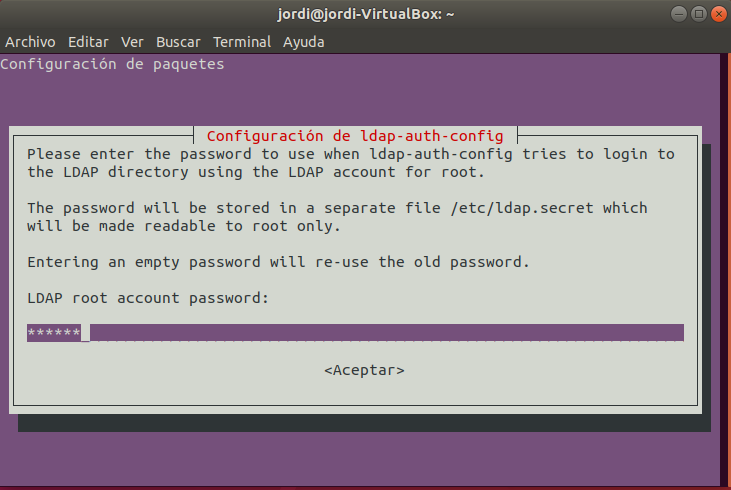








Escribimos la contraseña que hemos puesto antes:



Aceptamos y se terminará de instalar.

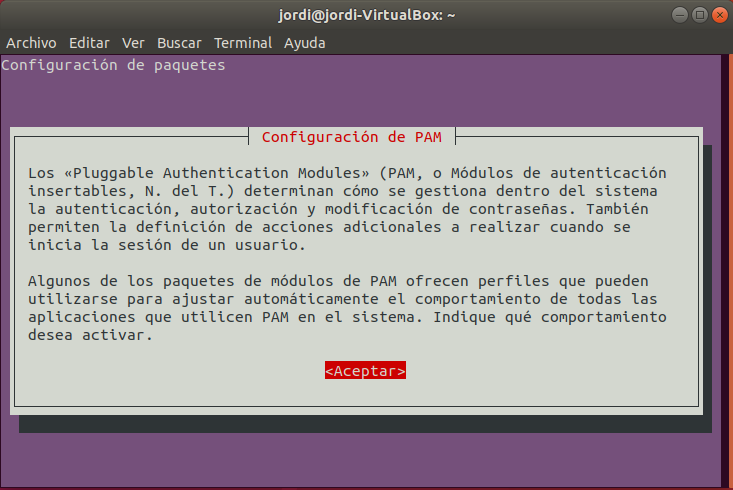
**Vamos a configurar OPENLDAP:**

Primero configuraremos la autentificación de clientes con los comandos:

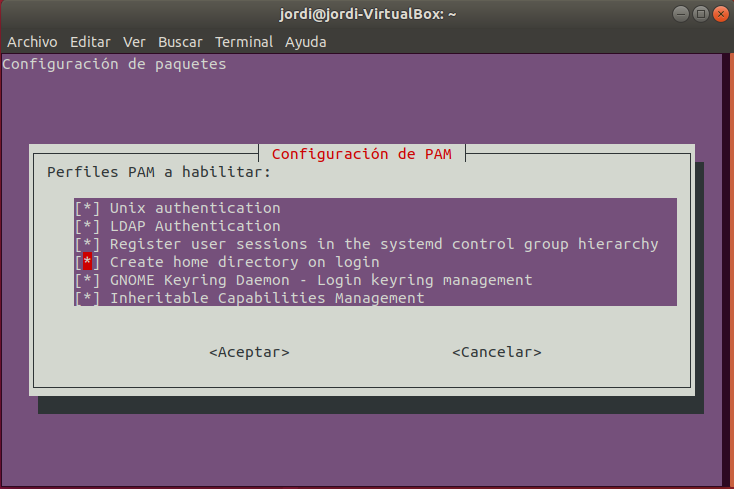




Y empieza la configuración:

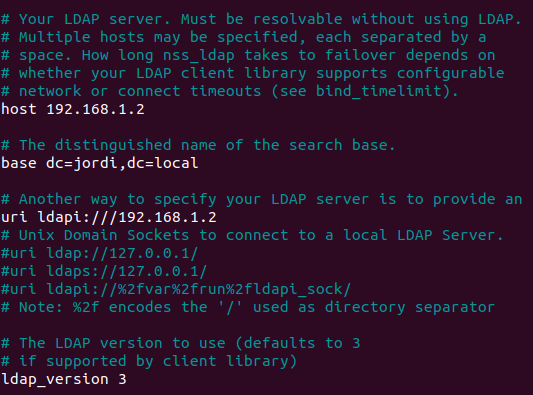


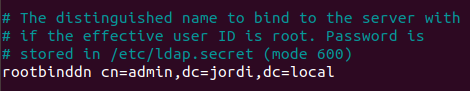
Tenemos que marcar la opción de crear un “home”:

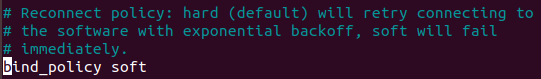
****

Ahora tenemos que entrar en el archivo ldap.conf y comprobar que está de una manera determinada,sino ya sabemos que cuando hay errores en los archivos de configuración,las cosas no suelen ir muy bien.

Hacemos **“sudo nano /etc/ldap.conf”**







Es importante que esté así,sino nos dará errores en las validaciones de usuarios.

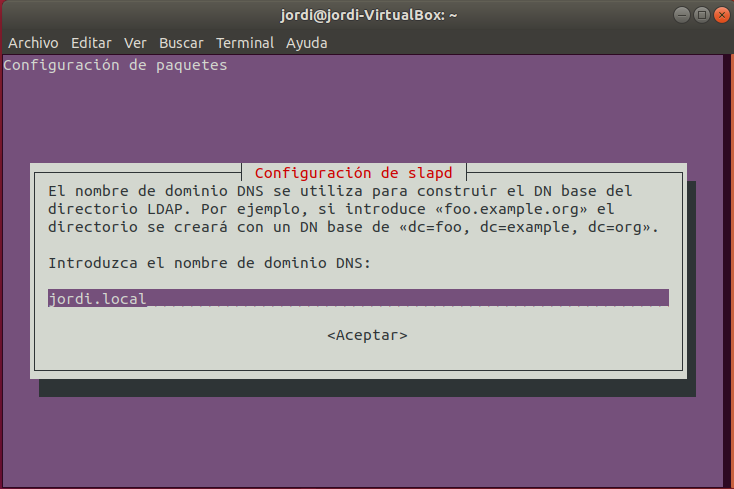
**Ahora vamos a configurar slapd**

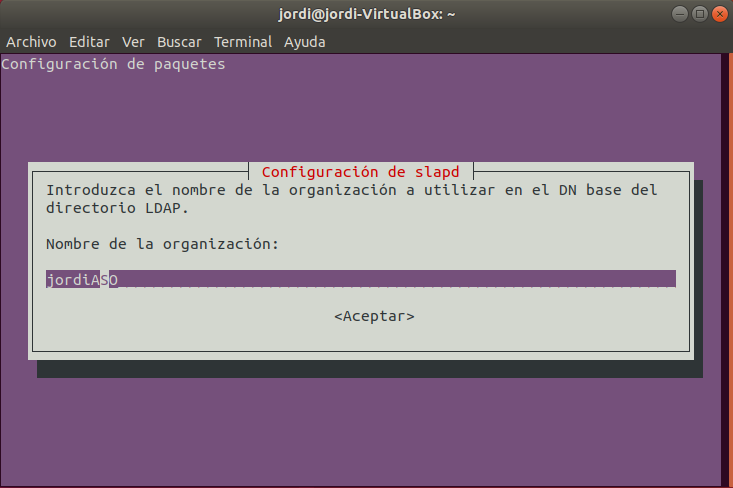
Comando:

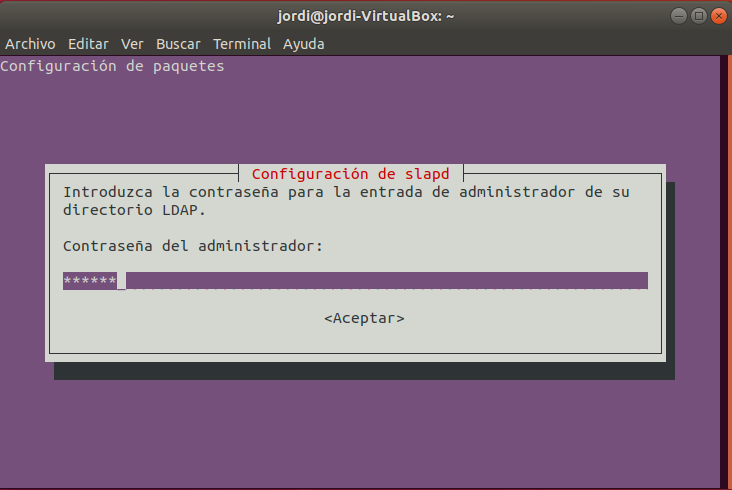
**“sudo dpkg-reconfigure slapd”**

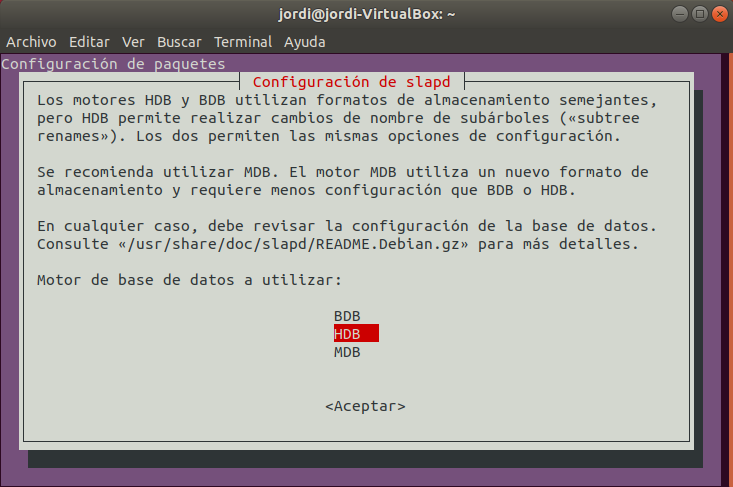
Como antes seguimos los pasos:

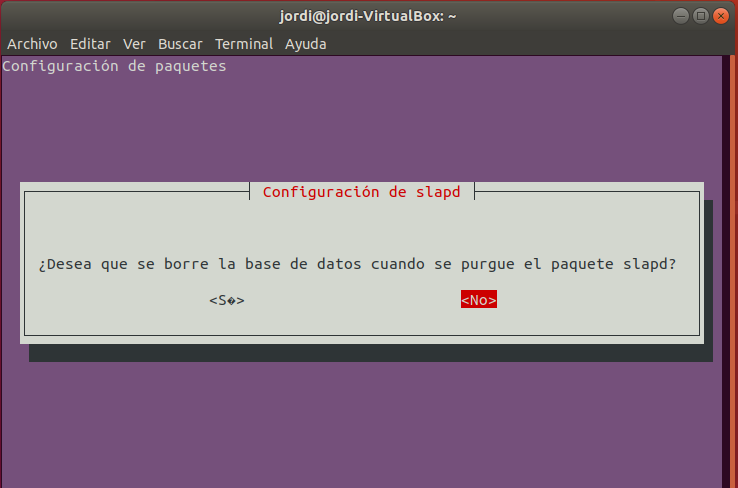




****

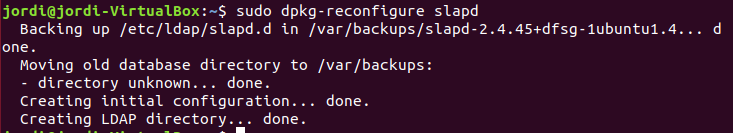








Y nos saldrá que ha hecho todo esto:

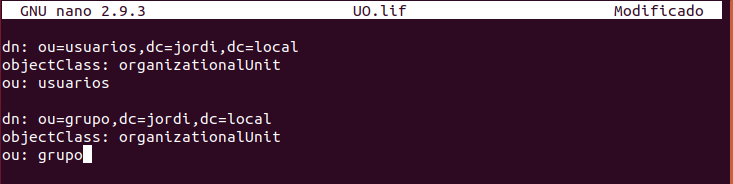


3-Crear estructura de directorio

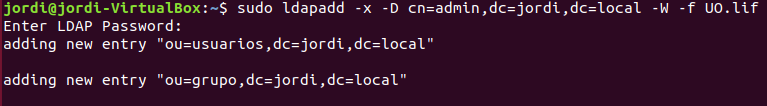
Vamos a tener que poner las UO en alguna parte,así que vamos a crear un archivo para que se agreguen ahí:

nano Uo.lif

Tiene que tener esta estructura:



Para añadir las nuevas entradas tendremos que poner el siguiente comando:



Nos pedirá la contraseña del administrador,se la ponemos y las añade.

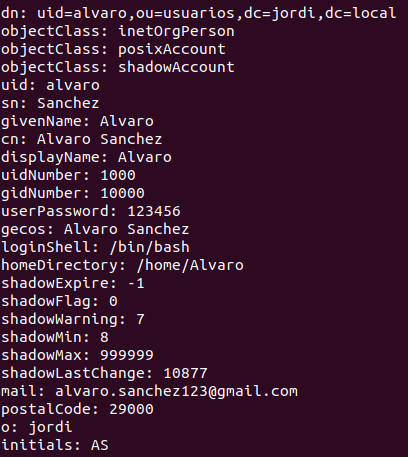
Vamos a crear un usuario,en este caso será Alvaro.Tenemos que crear otro archivo y que sea de la siguiente manera:



Como antes,tenemos que añadir la entrada a la configuración de ldap:

OJO!!

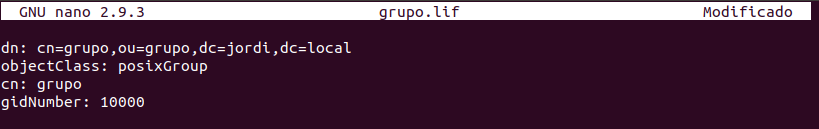
Los atributos tienen que estar sin tabular,sino nos dará error.



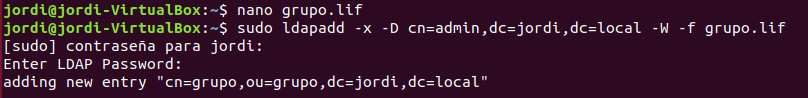


Ahora vamos a crear un grupo,que será igual que antes,creamos el archivo:

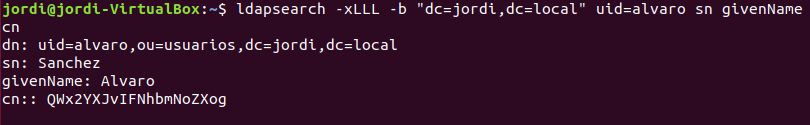




Y añadimos la entrada:



Para comprobar que todo está correcto usamos el siguiente comando:



Y vemos como está todo correctamente

También podemos volver a usar el comando **slapcat** para mostrar el contenido completo del directorio.

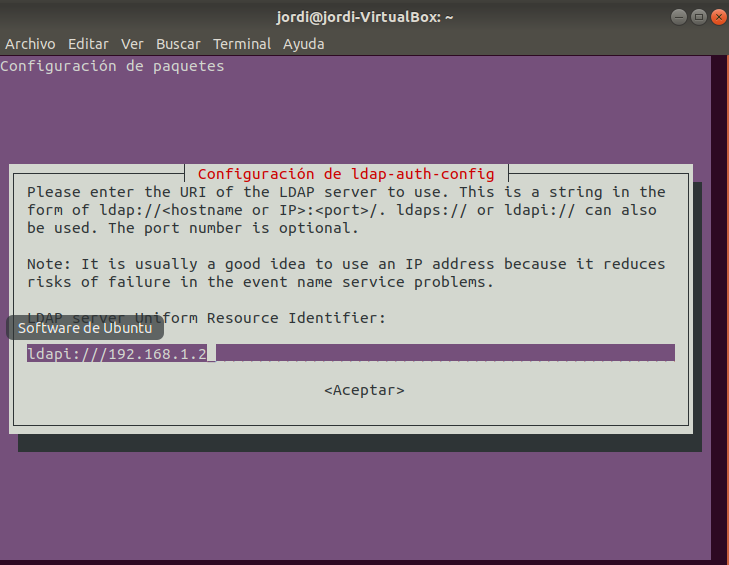
4-Añadir cliente Ubuntu

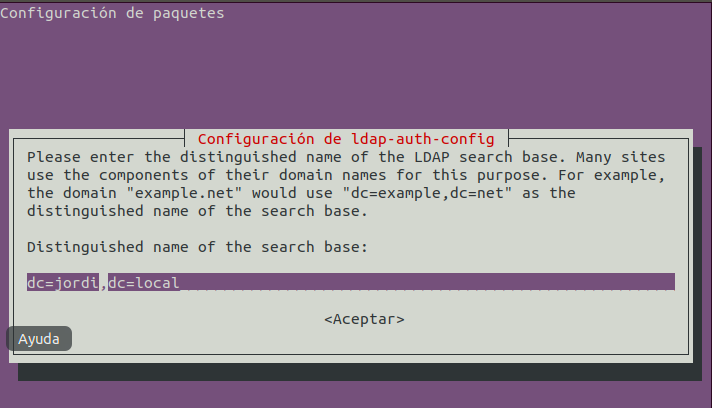
Creamos una nueva máquina virtual y le ponemos una IP estática que esté dentro de la misma red que el servidor:

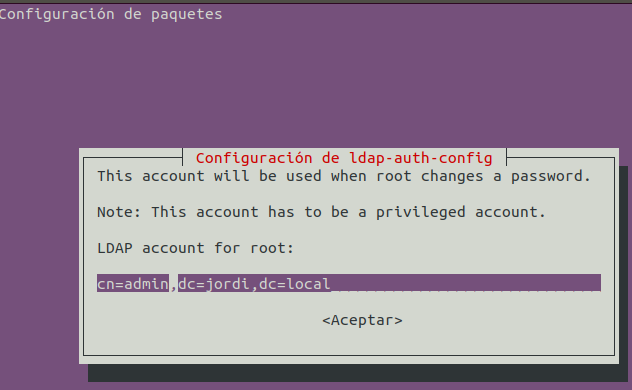
Luego tendremos que instalar el cliente con el comando:

**“sudo apt-get install libpam-ldap libnss-ldap nss-updatedb libnss-db nscd ldap-utils -y”**

Una vez se haya instalado,vamos a configurar el cliente como hemos hecho antes,la única diferencia es que tiene que tener la dirección del server como en la siguiente imagen:

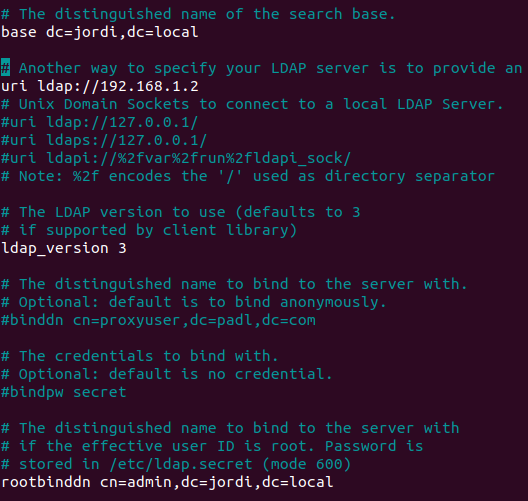


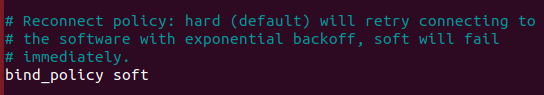


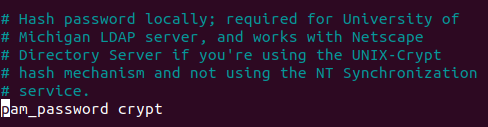


Una vez terminado este proceso,vamos a modificar el **ldap.conf** como antes:

**“sudo nano /etc/ldap.conf”**

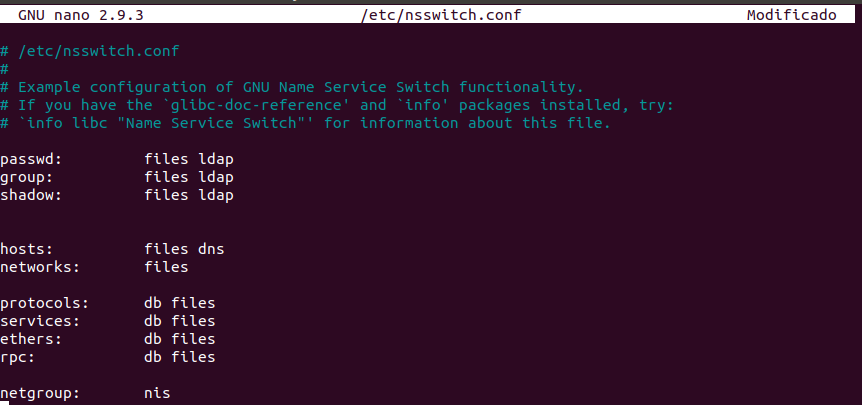
****





Ahora tendremos que modificar el archivo **nsswich.conf**,este es el fichero de configuración de las Bases de Datos del Sistema y del sistema de Conmutación de los Servicios de Nombres (Name Service Switch)

Y lo dejaremos de la siguiente manera:



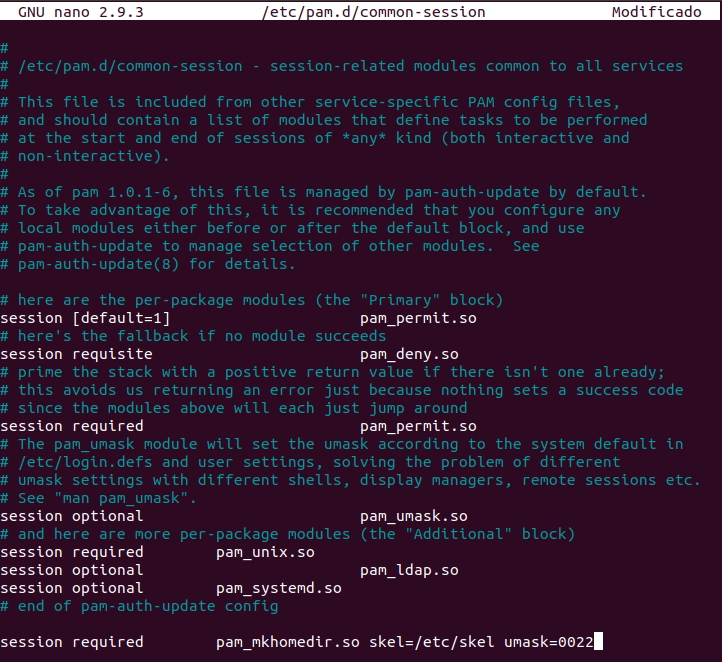
Si ejecutamos **“sudo nss\_updatedb ldap”**  nos saldrá esto:



Si sale un error seguramente sea porque no hemos configurado bien **/etc/ldap.conf**  y no encuentra el servidor,aseguraos de que está puesto exactamente como en la foto de arriba.

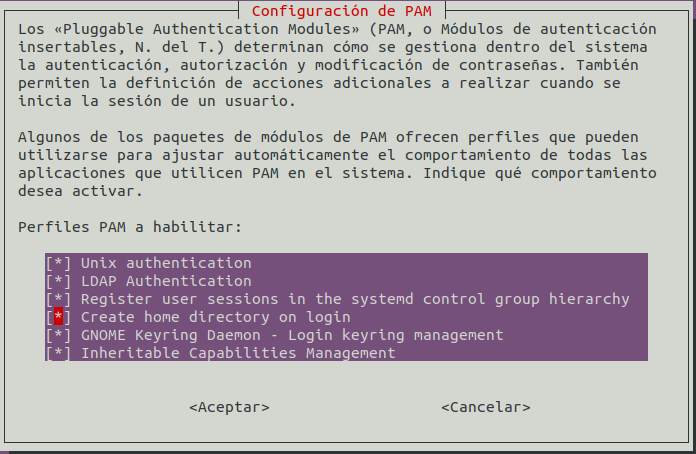
Ahora tendremos que crear el escritorio de trabajo y para ello tendremos que editar el archivo **/etc/pam.d/common-session**

**NO TENEMOS QUE TOCAR NADA**,solo añadir una líne al final del archivo:



Ahora actualizamos las políticas de autenticación con:

**“sudo pam-auth-update”**



Vamos a comprobar que el usuario ha sido creado con **sudo** **getent passwd**

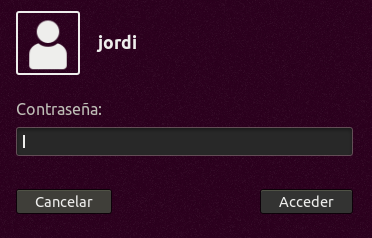


Vemos como se ha creado perfectamente.

Comprobar que funciona el inicio de sesión

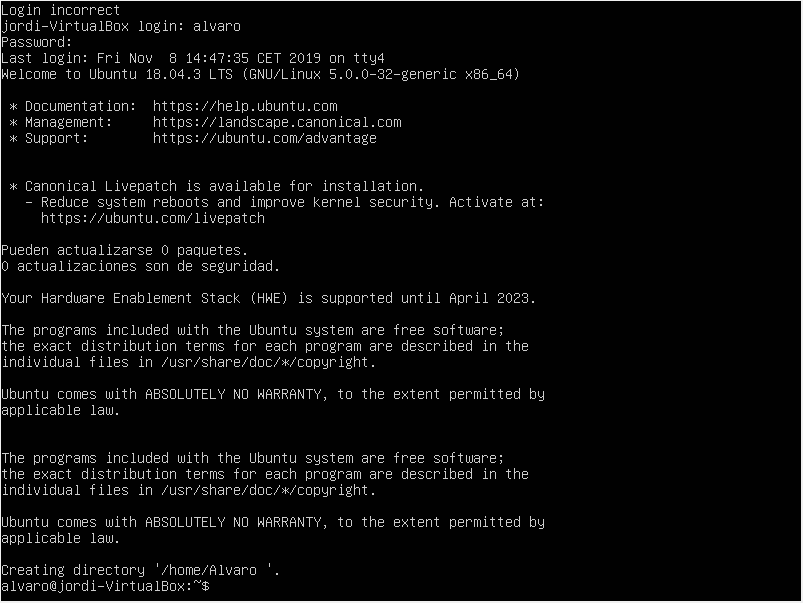
La forma más sencilla de comprobar que podemos iniciar sesión en el servidor usando LDAP consiste en arrancar el sistema en modo texto (o arrancarlo en modo gráfico y usar la combinación de teclas alt + ctrl + f3 para ir a una consola de texto) y escribir las credenciales de un usuario LDAP.

Hacenmos alt+ctrl +f3 aquí



Y entraremos en modo texto.

Nos pedirá las credenciales y metemos las del usuario que hemos creado antes:



Vemos cómo hemos iniciado con Álvaro al final de la imagen introduciendo su user y password.

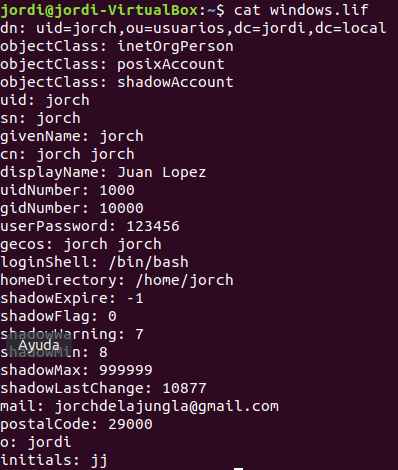
Ya lo tendríamos configurado en Ubuntu 18.Ahora vamos a por Windows.

5-Añadir cliente Windows

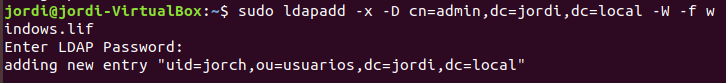
Lo primero que tendremos que hacer es crear el usuario en el **servidor**(como siempre).

Creamos el archivo de usuario **windows.lif**

**“sudo nano windows.lif”**

****

Lo añadimos a la configuración de ldap:



Ponedlo a vuestro gusto y con el usuario que queráis y comprobamos que está bien creado con **sudo slapcat**

Una vez creado el usuario vamos a crear una máquina Windows o a utilizar una que ya

tengamos,lo que queráis:

No podemos acceder al servidor ldap de ninguna manera,tendremos que utilizar **pGina**

**¿Qué es?**

pGina es un reemplazo de proveedor de credenciales de código abierto (y GINA) enchufable. Permite métodos alternativos de autenticación de usuario interactiva y gestión de acceso en máquinas que ejecutan el sistema operativo Windows.

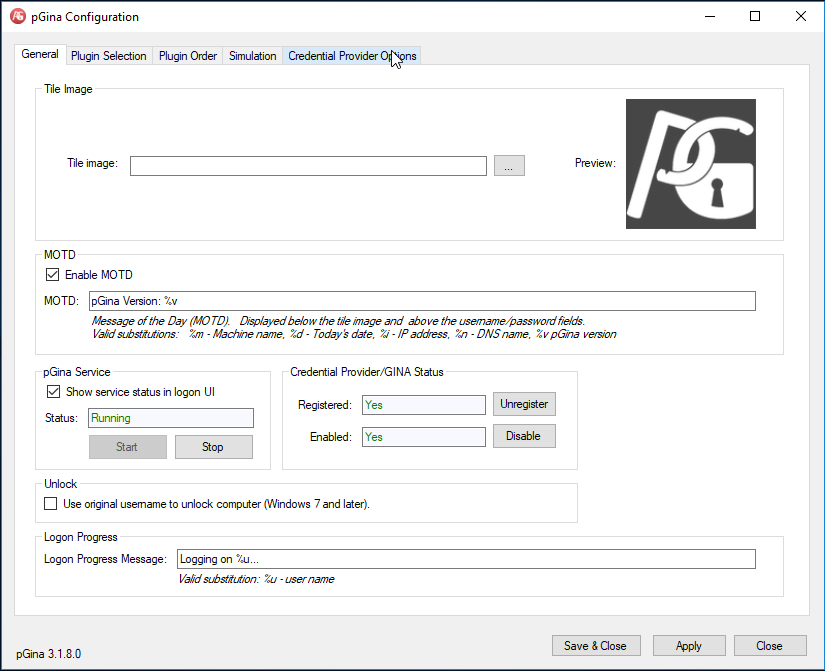
pGina es un reemplazo flexible para el proveedor de credenciales predeterminado de Windows (o GINA en XP y sistemas anteriores). Con pGina, puede integrar clientes de Windows en sistemas de gestión de identidad heterogéneos existentes. Con pGina, puede admitir clientes Windows con una sola base de datos OpenLDAP u otro backend de almacenamiento de identidad, sin la sobrecarga de una instalación completa de Active Directory.

pGina viene con muchos complementos listos para usar (MySQL, **LDAP**, Logging, Single User)

Lo primero será descargarlo de su página oficial.

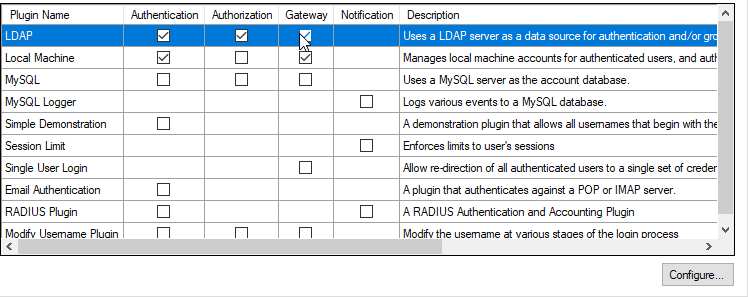
<http://pgina.org/download.html>

Una vez lo tengamos vamos a configurar LDAP para poder acceder,este es el inicio:



Le damos a **“Plugin Selection”** en la barra de arriba y activamos LDAP y seguimos los pasos:

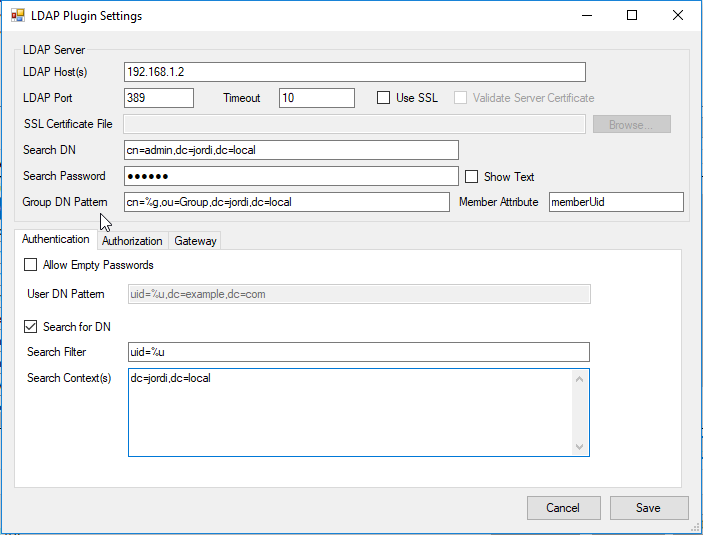
Una vez seleccionado le damos a **Configure**



Vamos a tener que configurar los parámetros siguientes.

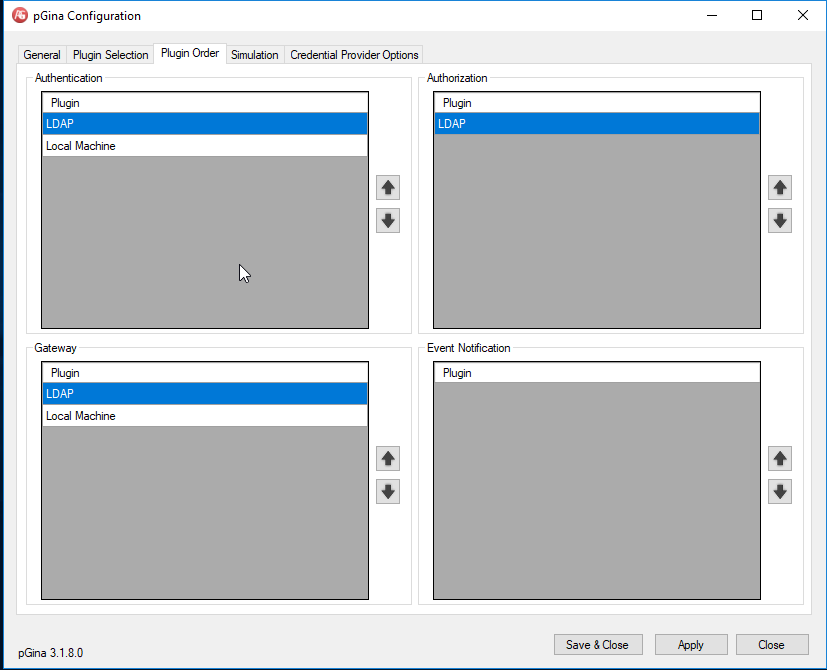
Tenéis que poner la IP del **servidor** y completar los demás campos.

Si os acordáis lo que hace %g y %u es completar el grupo y el usuario(Práctica perfil móvil).

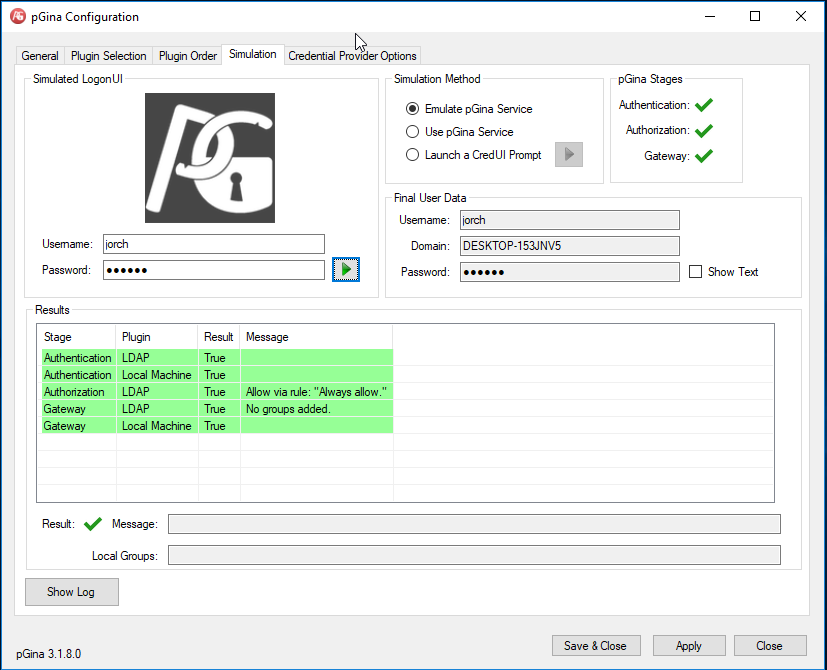


Y guardamos.

Comprobamos que los plugins están en el siguiente orden:

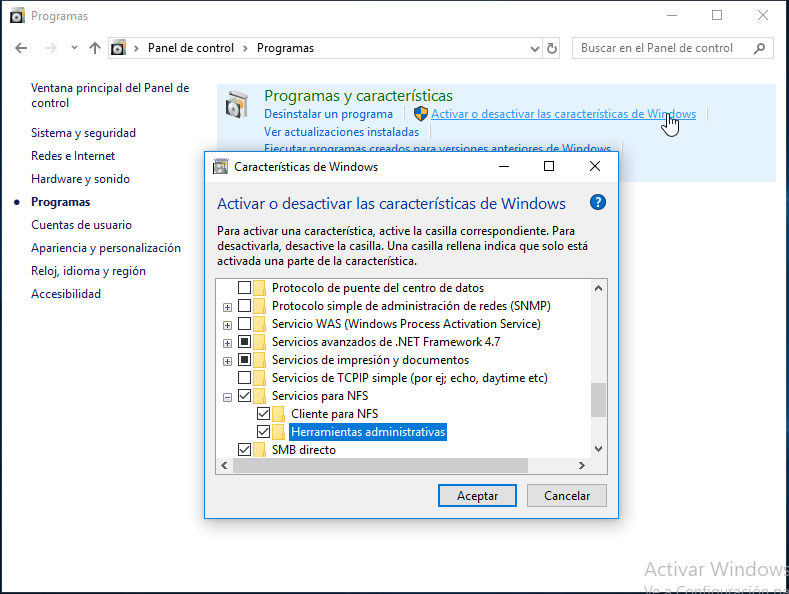


Ahora vamos al simulador para ver si todo está correctamente,ponemos credenciales y probamos:



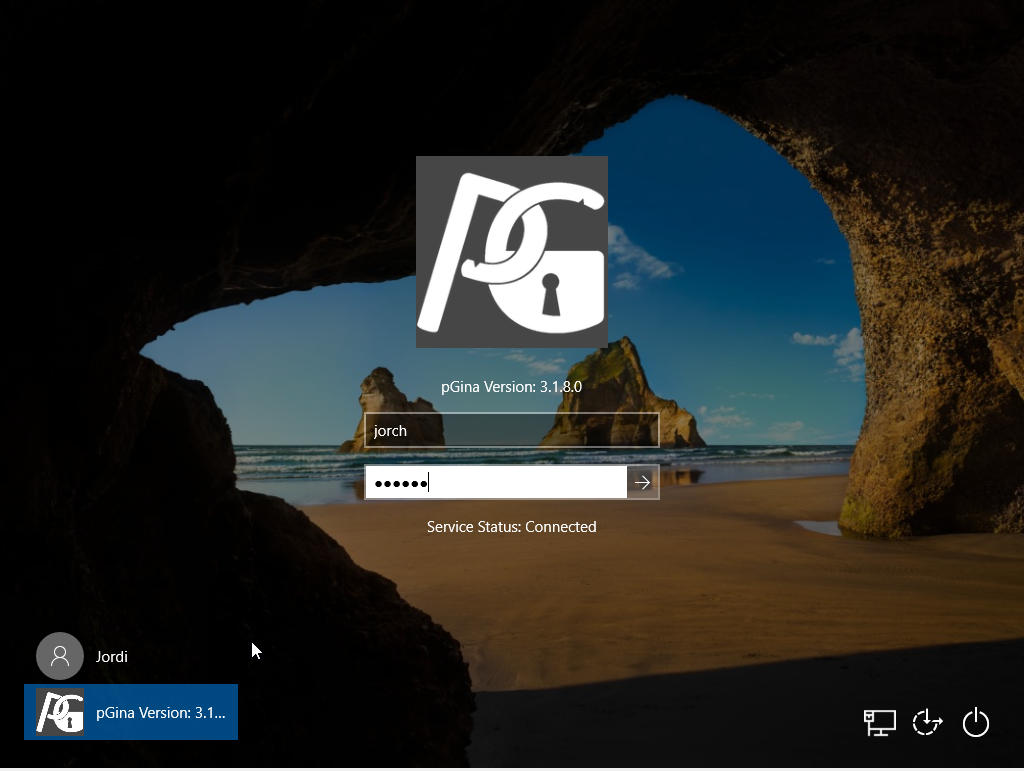
La primera vez que lo hagáis os saldrá la segunda fila en rojo,a mi me ha salido y pensaba que estaba mal y por eso no he hecho captura,es porque todavía no hemos entrado desde la propia máquina Windows,una vez iniciemos sesión con nuestro usuario creado el Linux,cuando volvamos a simular la entrada al servidor se nos pondrá en verde.

Una vez comprobado que funciona,activamos los siguientes servicios(NFS) y reiniciamos para aplicar cambios:

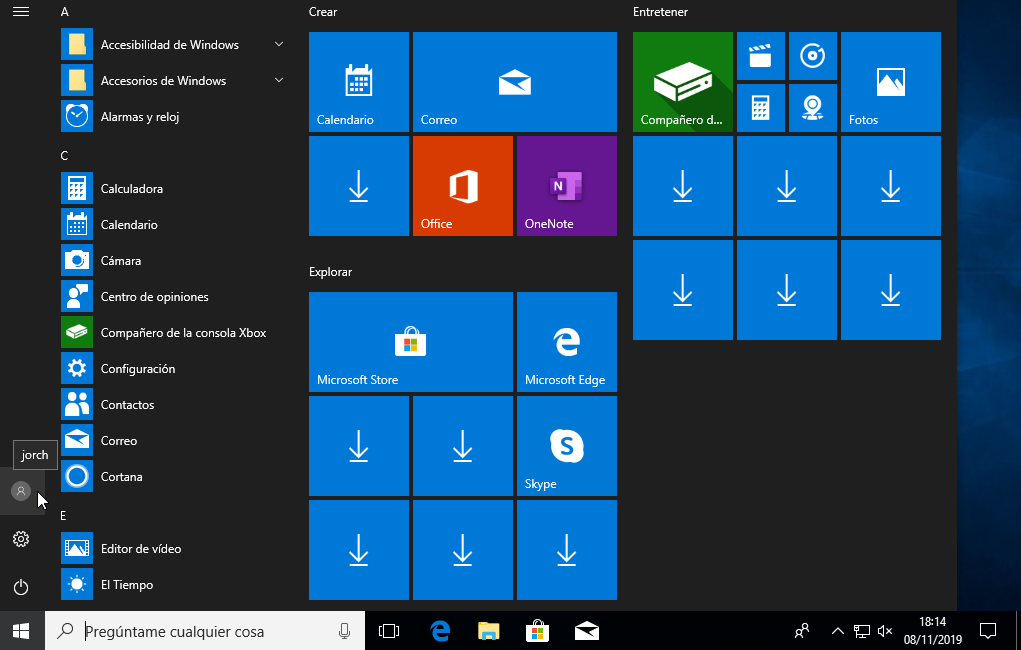


Una vez hayamos reiniciado nos saldrá la opción de loguearnos con pGina.

Metemos las credenciales del usuario creado en Linux y accedemos:



Como vemos hemos accedido en Windows sin ningun problema:



Bibliografía

<https://www.atareao.es/tutoriales/autenticar-usuarios-nss-pam-y-ldap/>

<http://somebooks.es/capitulo-11-instalar-y-configurar-openldap-en-ubuntu-14-04-lts/3/>

<http://joaalsai.com/index.php/2018/08/09/configurar-un-equipo-cliente-con-linux-mint-18-para-autenticarse-en-el-servidor-openldap/>