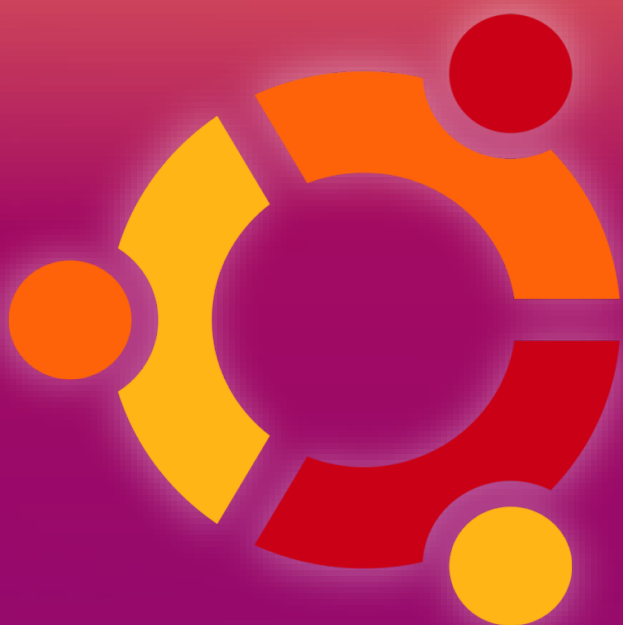


UBUNTU SERVER: LDAP



IMPLANTACIÓN DE SISTEMAS
JUAN CARLOS NAVIDAD GARCÍA

TEORÍA DE LDAP:

1. ¿Qué es un servicio de directorio, en qué modelo se basa y tipos de servicio de directorio?

Un servicio de directorio es un sistema que almacena y organiza información sobre usuarios, recursos y servicios de una red. Se utiliza para localizar y acceder a información y recursos de manera eficiente y segura.

Los servicios de directorio suelen implementarse siguiendo el modelo cliente-servidor, de modo que una aplicación que desea acceder al directorio no accede directamente a la base de datos, sino que llama a una función de la API (Application Programming Interface), que envía un mensaje a un proceso en el servidor. Dicho proceso accede al directorio y devuelve el resultado de la operación.

Por ejemplo, AD DS, Active Directory, LDAP son tipos de servicio de directorio.

2. Ejemplos de uso del servicio de directorio

Por ejemplo, para uso empresarial, se puede utilizar para autenticación de usuarios, libreta de direcciones, representaciones organizativas, etc.

3. Define:

a. LDAP

LDAP significa "Protocolo de acceso ligero a directorios" (Lightweight Directory Access Protocol, en inglés). Es un protocolo utilizado para acceder y administrar información almacenada en un servicio de directorio.

b. OpenLDAP

OpenLDAP es una implementación de software libre y de código abierto del protocolo LDAP (Protocolo de Acceso Ligero a Directorios). OpenLDAP es un servidor de directorio que proporciona un sistema de almacenamiento y recuperación de información de directorio basado en LDAP.

c. LAM

Es una interfaz web para administrar OpenLDAP.

4. ¿Dónde se encuentran los Archivos de configuración de OpenLDAP?

/etc/ldap.conf

5. ¿Cómo se llaman las estructuras de datos que almacenan y organizan la información del directorio?

Hacemos referencia a una entrada del DIT mediante su Nombre Distinguido o Distinguished Name, (DN). Los DNs son secuencias de Relative Distinguished Names (RDNs) y cada RDN se corresponde con una rama del DIT partiendo de la raíz hacia la entrada dentro del directorio.

6. ¿Qué formato tiene la estructura de directorio?

Tiene un formato de estructura jerárquica en forma de árbol invertido.

7. ¿Qué tipo de información almacena el directorio LDAP y cuál es su unidad básica de información?

El directorio LDAP almacena una amplia variedad de tipos de información, incluyendo información de usuario, información de grupo, información de recursos y servicios, información de dispositivos.

La unidad básica de información en un directorio LDAP se llama entrada (entry) o también objeto (object).

8. Diferencia entre DN, RDN y CN

El DN es un identificador único que se asigna a cada entrada en un directorio LDAP. Por ejemplo: uid=Alejandro, ou=usuarios, dc:síntesis, dc:com

Por otro lado, un RDN es una parte del DN que identifica de manera única una entrada, como por ejemplo, uid=Alejandro.

CN en cambio es un atributo y se usa para establecer los nombres comunes.

9. ¿Qué es un atributo?

Un atributo es una propiedad o característica que describe una entrada u objeto.

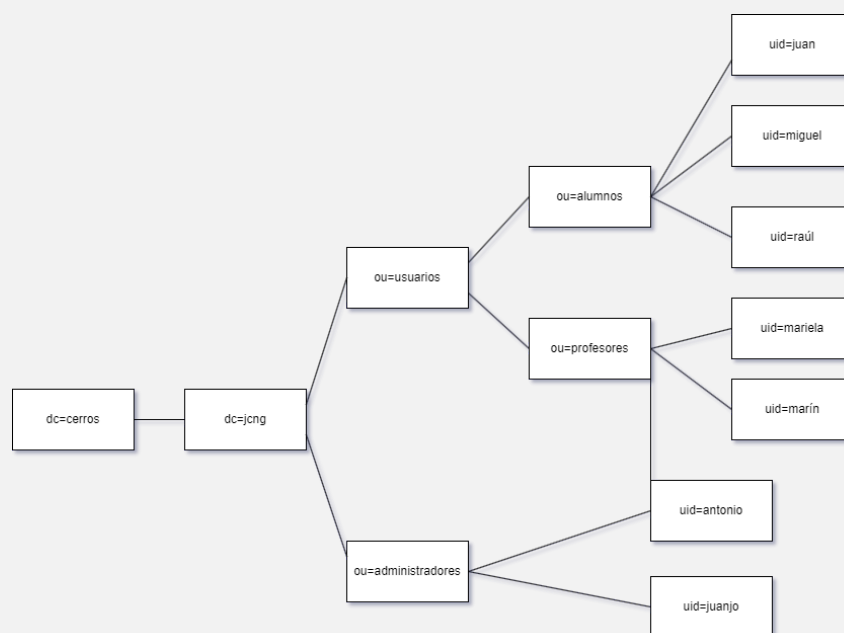
10. ¿Cómo se representan las entradas del directorio en el servidor?

Las entradas del directorio en un servidor de directorio se representan como objetos que contienen una colección de atributos que describen los objetos o entradas que se almacenan en el directorio.

11. Partes de una entrada

Una entrada se compone de DN, esta se compone de RDN que a su vez pueden contener atributos, clases, valores o relaciones.

12. Invéntate un ejemplo de estructura de servicio de directorio LDAP. Inspírate en el ejemplo de la teoría.



INSTALACIÓN DE LDAP:

1. Instala openLDAP en el servidor.

- Verifica ip, nombre del equipo

```
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.10.251 netmask 255.255.255.0 broadcast 192.168.10.255
    inet6 fe80::a00:27ff:fe20:d5a5 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:20:d5:a5 txqueuelen 1000 (Ethernet)
    RX packets 5512 bytes 8223999 (8.2 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1465 bytes 95349 (95.3 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
clienteu-jcng@clienteu-jcng:~$ hostname
clienteu-jcng
```

- Actualiza

```
clienteu-jcng@clienteu-jcng:~$ sudo apt-get update
Obj:1 http://es.archive.ubuntu.com/ubuntu focal InRelease
Obj:2 http://es.archive.ubuntu.com/ubuntu focal-updates InRelease
Obj:3 http://es.archive.ubuntu.com/ubuntu focal-backports InRelease
Obj:4 http://es.archive.ubuntu.com/ubuntu focal-security InRelease
Ign:5 http://download.webmin.com/download/repository sarge InRelease
Obj:6 http://download.webmin.com/download/repository sarge Release
Leyendo lista de paquetes... Hecho
```

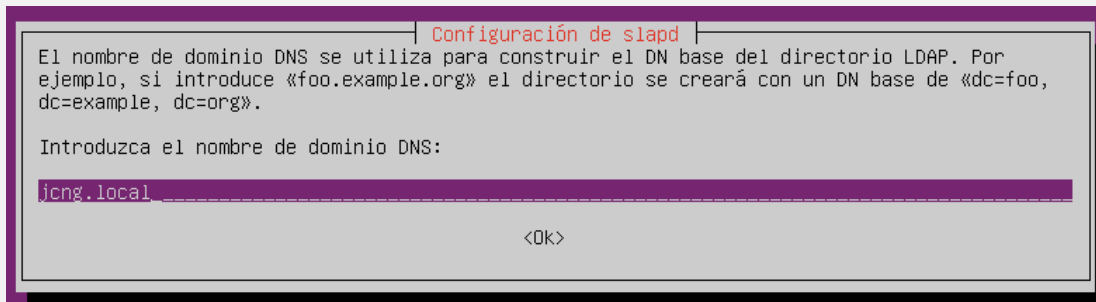
- Instala software necesario

```
clienteu-jcng@clienteu-jcng:~$ sudo apt-get install slapd ldap-utils
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  libodbc1
```

```
clienteu-jcng@clienteu-jcng:~$ sudo service slapd status
• slapd.service - LSB: OpenLDAP standalone server (Lightweight Directory Access Protocol)
   Loaded: loaded (/etc/init.d/slapd; generated)
   Drop-In: /usr/lib/systemd/system/slapd.service.d
            └─slapd-remain-after-exit.conf
   Active: active (running) since Wed 2023-03-15 07:24:53 UTC; 1s ago
     Docs: man:systemd-sysv-generator(8)
  Process: 3962 ExecStart=/etc/init.d/slapd start (code=exited, status=0/SUCCESS)
    Tasks: 3 (limit: 2271)
   Memory: 3.4M
    CGroup: /system.slice/slapd.service
```

2. Configura openLDAP:

- Dominio: tunombreiniciales.local



Configuración de slapd

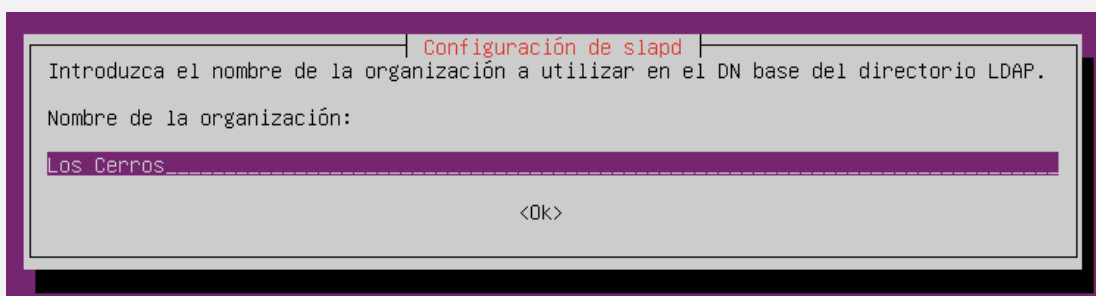
El nombre de dominio DNS se utiliza para construir el DN base del directorio LDAP. Por ejemplo, si introduce «foo.example.org» el directorio se creará con un DN base de «dc=foo, dc=example, dc=org».

Introduzca el nombre de dominio DNS:

jcng.local

<Ok>

- Empresa: los cerros



Configuración de slapd

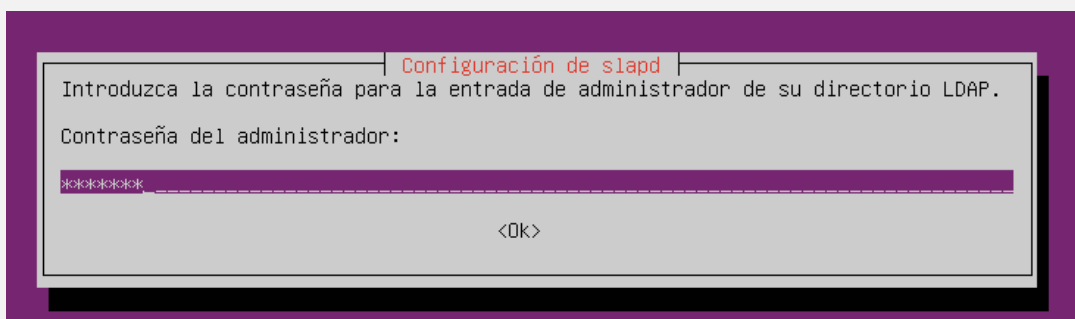
Introduzca el nombre de la organización a utilizar en el DN base del directorio LDAP.

Nombre de la organización:

Los Cerros

<Ok>

- Contraseña Rootroot



Configuración de slapd

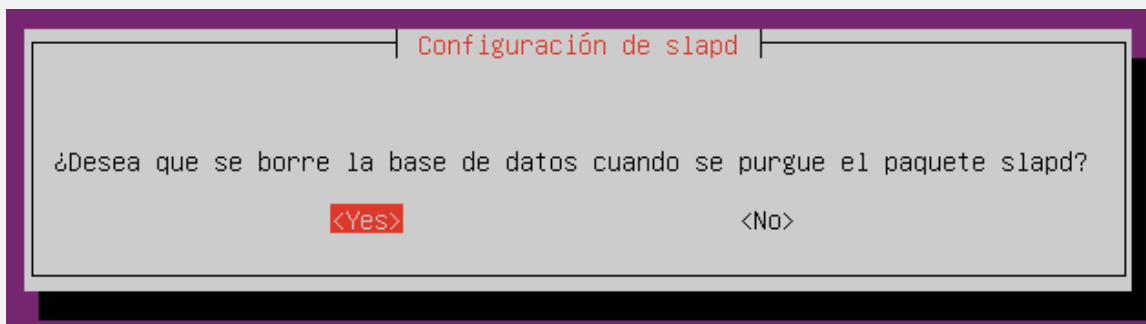
Introduzca la contraseña para la entrada de administrador de su directorio LDAP.

Contraseña del administrador:

xxxxxxxxxx

<Ok>

- Borrar las bd anteriores

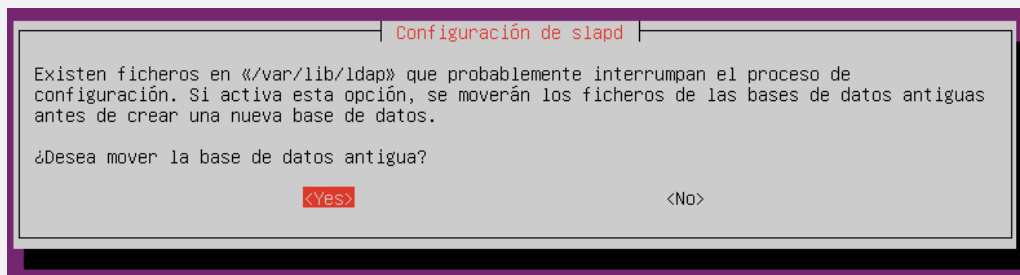


Configuración de slapd

¿Desea que se borre la base de datos cuando se purgue el paquete slapd?

<Yes> <No>

- Mover la bd antigua: si



3. Comprueba que se ha iniciado el servicio

```
clienteu-jcng@clienteu-jcng:~$ sudo service slapd status
• slapd.service - LSB: OpenLDAP standalone server (Lightweight Directory Access Protocol)
   Loaded: loaded (/etc/init.d/slapd; generated)
   Drop-In: /usr/lib/systemd/system/slapd.service.d
            └─slapd-remain-after-exit.conf
   Active: active (running) since Wed 2023-03-15 07:24:53 UTC; 13min ago
```

4. Verifica la configuración con el comando slapcat

Mostrara

- DN del dominio
- Información sobre el usuario administrador admin

```
clienteu-jcng@clienteu-jcng:~$ sudo slapcat
dn: dc=jcng,dc=local
objectClass: top
objectClass: dcObject
objectClass: organization
o: Los Cerros
dc: jcng
structuralObjectClass: organization
entryUUID: 1fb54e16-5750-103d-8b34-6f51513a7ed9
creatorsName: cn=admin,dc=jcng,dc=local
createTimestamp: 20230315073829Z
entryCSN: 20230315073829.532534Z#000000#000#000000
modifiersName: cn=admin,dc=jcng,dc=local
modifyTimestamp: 20230315073829Z

dn: cn=admin,dc=jcng,dc=local
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator
userPassword:: e1NTSEF9WT1LNfJzWkNkTE9FUfFMN1ZwS0c0SXhML2hYeG00RTk=
structuralObjectClass: organizationalRole
entryUUID: 1fb66db4-5750-103d-8b35-6f51513a7ed9
creatorsName: cn=admin,dc=jcng,dc=local
createTimestamp: 20230315073829Z
entryCSN: 20230315073829.539877Z#000000#000#000000
modifiersName: cn=admin,dc=jcng,dc=local
modifyTimestamp: 20230315073829Z
```


5. Añadir información al directorio (bd) mediante archivos .ldif para crear el siguiente DIT

- Unidades organizativas
 - i. Pcs del aula
 - ii. Los grupos
 - iii. Los alumnos

```
GNU nano 4.8 unidades_organizativas.ldif
dn: ou=pc_aula, dc=jcng, dc=local
objectClass: top
objectClass: organizationalUnit
ou: pc_aula

dn: ou=grupos, dc=jcng, dc=local
objectClass: top
objectClass: organizationalUnit
ou: grupos

dn: ou=alumnos, dc=jcng, dc=local
objectClass: top
objectClass: organizationalUnit
ou: alumnos
```

- 4 alumnos de forma que
 - i. el UID sea el primer apellido para el primer alumno, el segundo apellido para el segundo alumno, tu nombre para el tercer alumno y las iniciales para el cuarto
 - ii. la contraseña será el nombre del usuario seguido de 987

```
dn: cn=jcng, ou=alumnos, dc=jcng, dc=local
objectClass: posixAccount
objectClass: inetOrgPerson
uid: jcng
uidNumber: 1113
gidNumber: 1113
cn: Juan
sn: Navidad
homeDirectory: /home/jcng
loginShell: /bin/bash
userPassword: jcng987
```

```
dn: cn=navidad, ou=alumnos, dc=jcng, dc=local
objectClass: posixAccount
objectClass: inetOrgPerson
uid: navidad
uidNumber: 1110
gidNumber: 1110
cn: Juan Carlos
sn: Navidad
homeDirectory: /home/navidad
loginShell: /bin/bash
userPassword: navidad987

dn: cn=garcia, ou=alumnos, dc=jcng, dc=local
objectClass: posixAccount
objectClass: inetOrgPerson
uid: garcia
uidNumber: 1111
gidNumber: 1111
cn: Juan Carlos
sn: Garcia
homeDirectory: /home/garcia
loginShell: /bin/bash
userPassword: garcia987

dn: cn=juan, ou=alumnos, dc=jcng, dc=local
objectClass: posixAccount
objectClass: inetOrgPerson
uid: juan
uidNumber: 1112
gidNumber: 1112
cn: Juan
sn: Carlos
homeDirectory: /home/juan
loginShell: /bin/bash
userPassword: juan987
```

- dos grupos
 - i. SMR1
 - 1. Dos usuarios
 - ii. SMR2
 - 1. Los otros dos usuarios

```
dn: cn=SMR1,ou=grupos,dc=jcng,dc=local
objectClass: top
objectClass: groupOfNames
cn: SMR1
member: uid=navidad,ou=alumnos,dc=jcng,dc=local
member: uid=garcia,ou=alumnos,dc=jcng,dc=local

dn: cn=SMR2,ou=grupos,dc=jcng,dc=local
objectClass: top
objectClass: groupOfNames
cn: SMR2
member: uid=juan,ou=alumnos,dc=jcng,dc=local
member: uid=jcng,ou=alumnos,dc=jcng,dc=local_
```

- Modifica el segundo usuario añadiéndole una descripción y para que el uidNumber sea 1100

```
dn: cn=garcia,ou=alumnos,dc=jcng,dc=local
changetype: modify
replace: description
description: El segundo apellido es el usuario 2
-
replace: uidNumber
uidNumber: 1100
```

```
clienteu-jcng@clienteu-jcng:~$ ldapmodify -x -D cn=admin,dc=jcng,dc=local -W -f modifica.ldif
Enter LDAP Password:
modifying entry "cn=garcia,ou=alumnos,dc=jcng,dc=local"
```

- Buscando en el directorio verifica que se ha realizado el cambio

```
clienteu-jcng@clienteu-jcng:~$ ldapsearch -x -b "ou=alumnos,dc=jcng,dc=local" "(objectClass=posixAccount)" uidNumber cn description_
```

```
# garcia, alumnos, jcng.local
dn: cn=garcia,ou=alumnos,dc=jcng,dc=local
cn: Juan Carlos
cn: garcia
description: El segundo apellido es el usuario 2
uidNumber: 1100
```

- Vuelve a modificarlo para quitar la descripción y verifícalo

```
dn: cn=garcia,ou=alumnos,dc=jcng,dc=local
changetype: modify
delete: description
```

```
clienteu-jcng@clienteu-jcng:~$ ldapmodify -x -D cn=admin,dc=jcng,dc=local -W -f modifica.ldif
Enter LDAP Password:
modifying entry "cn=garcia,ou=alumnos,dc=jcng,dc=local"
```

```
# garcia, alumnos, jcng.local
dn: cn=garcia,ou=alumnos,dc=jcng,dc=local
cn: Juan Carlos
cn: garcia
uidNumber: 1100
```

- Añade el teléfono al tercer usuario y cambia la contraseña por 123456

```
dn: cn=juan,ou=alumnos,dc=jcng,dc=local
changetype: modify
replace: userPassword
userPassword: 123456
-
replace: telephoneNumber
telephoneNumber: 643342953
```

```
clienteu-jcng@clienteu-jcng:~$ ldapmodify -x -D cn=admin,dc=jcng,dc=local -W -f modifica.ldif
Enter LDAP Password:
modifying entry "cn=juan,ou=alumnos,dc=jcng,dc=local"
```

```
# juan, alumnos, jcng.local
dn: cn=juan,ou=alumnos,dc=jcng,dc=local
cn: Juan
telephoneNumber: 643342953
```

- Busca información del

i. grupo smr1

```
clienteu-jcng@clienteu-jcng:~$ ldapsearch -x -b "ou=grupos,dc=jcng,dc=local" "(cn=SMR1)"
# extended LDIF
#
# LDAPv3
# base <ou=grupos,dc=jcng,dc=local> with scope subtree
# filter: (cn=SMR1)
# requesting: ALL
#
# SMR1, grupos, jcng.local
dn: cn=SMR1,ou=grupos,dc=jcng,dc=local
objectClass: top
objectClass: groupOfNames
cn: SMR1
member: cn=navidad,ou=alumnos,dc=jcng,dc=local
member: cn=garcia,ou=alumnos,dc=jcng,dc=local
```

ii. todos los usuarios

```
clienteu-jcng@clienteu-jcng:~$ ldapsearch -x -b "ou=alumnos,dc=jcng,dc=local" _
```

```
# garcia, alumnos, jcng.local
dn: cn=garcia,ou=alumnos,dc=jcng,dc=local
objectClass: posixAccount
objectClass: inetOrgPerson
gidNumber: 1111
cn: Juan Carlos
cn: garcia
sn: Garcia
homeDirectory: /home/garcia
loginShell: /bin/bash
uid: 1100
uidNumber: 1100

# navidad, alumnos, jcng.local
dn: cn=navidad,ou=alumnos,dc=jcng,dc=local
objectClass: posixAccount
objectClass: inetOrgPerson
uid: navidad
uidNumber: 1110
gidNumber: 1110
cn: Juan Carlos
cn: navidad
sn: Navidad
homeDirectory: /home/navidad
loginShell: /bin/bash
```

6. Herramienta LAM

- Instálala en el servidor

```
clienteu-jcng@clienteu-jcng:~$ sudo apt install ldap-account-manager
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
```

- Configúrala

```
GNU nano 4.8 /etc/apache2/conf-enabled/ldap-account-manager.conf
Alias /lam /usr/share/ldap-account-manager

<Directory /usr/share/ldap-account-manager>
    Options +FollowSymLinks
    AllowOverride All
    # Require all granted
    Require ip 127.0.0.1 192.168.10.0/24
    DirectoryIndex index.html
</Directory>

<Directory /var/lib/ldap-account-manager/tmp>
```

← → ↻ 🏠 192.168.10.251/lam/templates/login.php ☆ 🔒

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

LAM - 6.7 ¿Desea más funciones? ¡Obtenga LAM Pro! Configuración de LAM

Nombre del usuario

Contraseña

Idioma

Configuración general Tipos de cuentas Módulos Preferencias del módulo

Preferencias del servidor

Dirección del servidor * ?

Activar TLS ?

Sufijo del arbol ?

Límite de búsqueda LDAP ?

Opciones Avanzadas

Configuración del idioma

Idioma por defecto ?

Zona horaria ?

Tipos de cuentas activos

Usuarios

Cuentas de usuario (p.ej. UNIX,Samba y Kolab) ⬇️ ✖️

Sufijo LDAP ?

Atributos del listado ?

Etiqueta personalizada ?

Filtro LDAP adicional ?

Oculto ☐ ?

Grupos

Cuentas del grupo (p.ej. Unix y Samba) ⬆️ ✖️

Sufijo LDAP ?

Atributos del listado ?

Etiqueta personalizada ?

Filtro LDAP adicional ?

Oculto ☐ ?

7. Usando la herramienta gráfica LDAP account manager LAM

- Elimina el usuario con tus iniciales

¿Realmente desea quitar las cuentas especificadas?

Nombre de la cuenta: jcng
DN: cn=jcng,ou=alumnos,dc=jcng,dc=local

Eliminar Cancelar

- Cambia al primer usuario UID a 1111 y el directorio home /home/Apellido1

homeDirectory requerido
/home/navidad

loginShell
/bin/bash

objectClass
posixAccount
inetOrgPerson (estructural)
(añadir valor)

sn requerido
Navidad
(añadir valor)

uid requerido
navidad
(añadir valor)

uidNumber requerido
1111

- Crea un grupo de administradores y mete dentro al usuario de tu nombre

Guardar Establecer contraseña default Cargar perfil ?

administradores
Sufijogrupos > jcng > local ? Identificador RDNcn ?

Unix

Nombre del grupo * administradores ?
Número GID 11010 ?
Descripción ?
Miembros del grupo Editar miembros ?
juan (Juan)

- Crea un nuevo usuario con UID iniciales y tres dígitos, debe permanecer al grupo administradores

Atributos del destinatario

cn requerido

jcng *

uid

jcng123

ou

administradores

- Añade al usuario anterior una dirección de e-mail y teléfono

Nombre jcng

Apellido * jcng

Datos de contacto

Número de teléfono 643342943 +

Dirección de correo electrónico navidadgarcia.juancarlos@loscerros.org +