

191_traballo_LDAP

Emilio Cabo Gomis

Indice

CONCEPTOS GENERALES SERVIDOR DE DOMINIO Y SERVICIO DE DIRECTORIO.....	3
¿Qué es y qué permite hacer el protocolo LDAP?.....	3
Funciones de LDAP.....	3
Elementos o atributos de LDAP.....	3
Ldap ESTRUCTURA (arquitectura). Especifica Numero y nombres de BD'S-LDAP.....	3
¿Qué es PAM ,Y NIS?.....	4
NIS:.....	4
PAM:.....	4
Name Service Switch (NSS).....	4
Protocolo DHCP.....	5
DHCPv4.....	6
DHCPv6.....	6
Protocolo DNS.....	6
¿Qué es SAMBA?.....	7
¿Qué es CIFS?.....	7
Bibliografía.....	8

CONCEPTOS GENERALES SERVIDOR DE DOMINIO Y SERVICIO DE DIRECTORIO

¿Qué es y qué permite hacer el protocolo LDAP?

Denominado **protocolo ligero de acceso a directorios**, permite el acceso a un servicio de directorio. Parecido al concepto de una agenda telefónica.

Basado en la tecnología de resolución de nombres basada en dominios nos permite acceder a información como nombres de usuario, contraseñas, direcciones de correo electrónico, entre otros datos. El protocolo de red empleado para acceder a esta información es el protocolo TCP/IP.

Funciones de LDAP

- Permite a usuarios conectarse y desconectarse de una red.
- Crear entradas en la base de datos donde se almacenan la información de directorio.
- Editar las entradas de la base de datos donde se almacenan la información de directorio.
- Gestión de autenticación y autorización de los usuarios.

Elementos o atributos de LDAP

Estos son los atributos o elementos del protocolo LDAP.**DC**= Componente de dominio

OU= Unidad organizativa

CN= Nombre común.

DN= Nombre distinguido (Distinguished name)

RDN= Nombre distinguido relativo (Relative distinguished name)

Dn= Nombre distinguido (Distinguished name)

Cn= Nombre común (Common name)

Gn= Nombre de pila (Given name)

S= Apellido (Surname)

UserPassword= Contraseña de usuario

Uid = Identificador de usuario (User identifier)

Gid= Identificador de grupo (Group identifier)

DisplayName= Nombre para mostrar

Ou = Unidad organizativa (OrganizationalUnit)

UidNumber = Número de usuario (User number)

GidNumber = Número de grupo (Group number)

También tenemos objectClass, se emplean para especificar que tipo de atributos deberían encontrarse en la entrada de base de datos en función del *objectClass* con el que trabajemos:

Account

PosixAccount

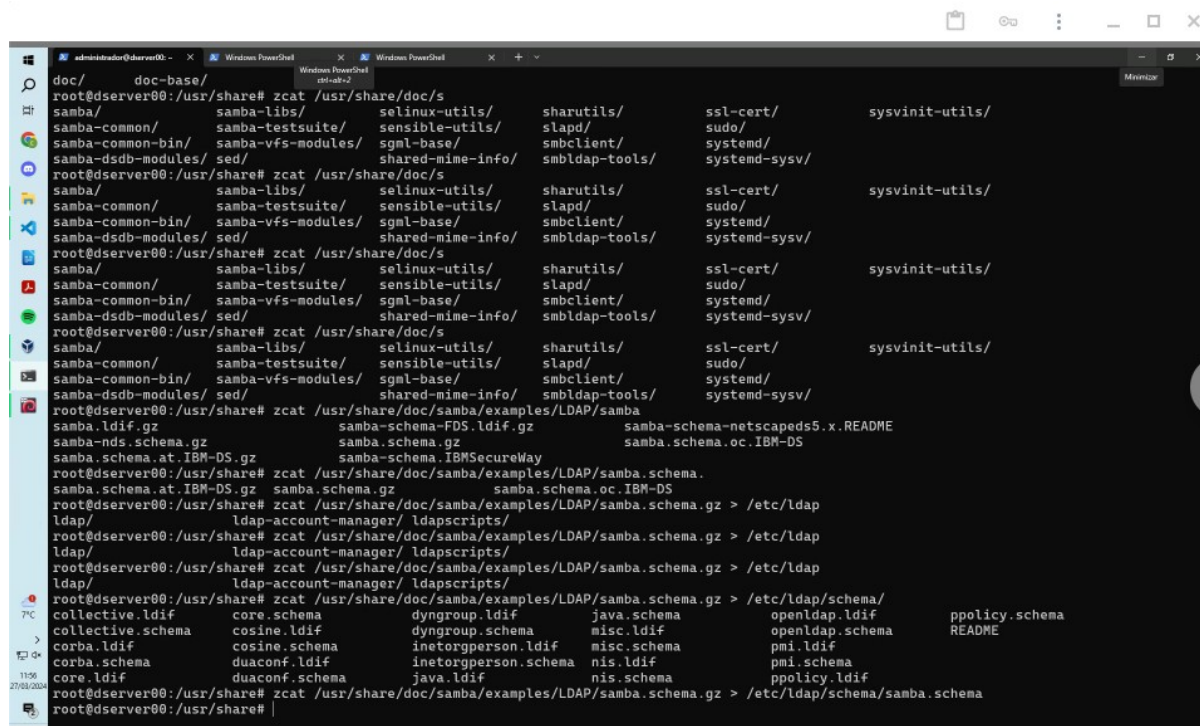
OrganizationalUnit

InetOrgPerson

Ldap ESTRUCTURA (arquitectura). Especifica Numero y nombres de BD'S-LDAP

Una vez instalado LDAP tendremos que emitir el siguiente comando para ver la arquitectura del sistema LDAP. `ls /etc/ldap/schema/`

Esta es una captura de pantalla que muestra la arquitectura de LDAP a través de una conexión SSH.



```
doc/ doc-base/
root@dserver00:/usr/share# zcat /usr/share/doc/s
samba/ samba-libs/ selinux-utils/ sharutils/ ssl-cert/ sysvinit-utils/
samba-common/ samba-testsuite/ sensible-utils/
samba-common-bin/ samba-vfs-modules/ sgml-base/ smbclient/ sudo/
samba-dsdb-modules/ sed/ shared-mime-info/ smbdap-tools/ systemd/
root@dserver00:/usr/share# zcat /usr/share/doc/s
samba/ samba-libs/ selinux-utils/ sharutils/ ssl-cert/ sysvinit-utils/
samba-common/ samba-testsuite/ sensible-utils/
samba-common-bin/ samba-vfs-modules/ sgml-base/ smbclient/ sudo/
samba-dsdb-modules/ sed/ shared-mime-info/ smbdap-tools/ systemd/
root@dserver00:/usr/share# zcat /usr/share/doc/s
samba/ samba-libs/ selinux-utils/ sharutils/ ssl-cert/ sysvinit-utils/
samba-common/ samba-testsuite/ sensible-utils/
samba-common-bin/ samba-vfs-modules/ sgml-base/ smbclient/ sudo/
samba-dsdb-modules/ sed/ shared-mime-info/ smbdap-tools/ systemd/
root@dserver00:/usr/share# zcat /usr/share/doc/samba/examples/LDAP/samba
samba.ldif.gz samba-schema-FDS.ldif.gz samba-schema-netscaped5.x.README
samba-nds.schema.gz samba.schema.gz samba.schema.oc.IBM-DS
samba.schema.at.IBM-DS.gz samba.schema.IBMSecureWay
root@dserver00:/usr/share# zcat /usr/share/doc/samba/examples/LDAP/samba.schema.
samba.schema.at.IBM-DS.gz samba.schema.gz samba.schema.oc.IBM-DS
root@dserver00:/usr/share# zcat /usr/share/doc/samba/examples/LDAP/samba.schema.gz > /etc/ldap
ldap/ ldap-account-manager/ ldapscripts/
root@dserver00:/usr/share# zcat /usr/share/doc/samba/examples/LDAP/samba.schema.gz > /etc/ldap
ldap/ ldap-account-manager/ ldapscripts/
root@dserver00:/usr/share# zcat /usr/share/doc/samba/examples/LDAP/samba.schema.gz > /etc/ldap
ldap/ ldap-account-manager/ ldapscripts/
root@dserver00:/usr/share# zcat /usr/share/doc/samba/examples/LDAP/samba.schema.gz > /etc/ldap/schema/
collective.ldif core.schema dyngroup.ldif java.schema openldap.ldif ppolicy.schema
collective.schema cosine.ldif inetorgperson.schema misc.ldif openldap.schema README
corba.ldif cosine.schema inetorgperson.ldif misc.schema pmi.ldif
corba.schema duacnf.ldif inetorgperson.schema nis.ldif pmi.schema
core.ldif duacnf.schema java.ldif nis.schema ppolicy.ldif
root@dserver00:/usr/share# zcat /usr/share/doc/samba/examples/LDAP/samba.schema.gz > /etc/ldap/schema/samba.schema
root@dserver00:/usr/share#
```

Imagen sacada de platega I – V del trabajo de Emilio Cabo Gomis.

¿Qué es PAM ,Y NIS?

NIS:

El NIS o "Network Information Service" es un servicio de red que sirve para organizar estaciones de trabajo, usuarios... A diferencia del protocolo LDAP no emplea una estructura de dominio para realizar la organización de los elementos. A pesar de esto, emplea una estructura cliente-servidor.

Antiguamente este protocolo era conocido como Yellow Pages pero el nombre no propietario ha sido cambiado a NIS. Es posible que algunos comandos sigan apareciendo como `yp<command>`.

PAM:

Es un módulo de autenticación de LDAP de LINUX. Permite cambiar las contraseñas en el servicio de directorio y cifrar las conexiones mediante el SSL/TSL.

Es un servicio muy modular dado que permite gestionar las políticas de seguridad dependiendo del usuario que se conecte. Elimina la necesidad de tener cuentas locales en el equipo.

En platega lo usabamos para el montaje de las carpetas en función del usuario que iniciase

sesión.

Name Service Switch (NSS)

Desarrollado por Sun Microsystems, permite configurar y acceder a las bases de datos de cuentas de usuarios y claves. Algunos ejemplos que nosotros hemos configurado en PLATEGA I – V son: `"/etc/passwd"`, `"/etc/groups"`, `"/etc/hosts"`.

El siguiente archivo es un archivo de configuración de NSS a modo de ejemplo.

```
#!/bin/bash
```

```
#cabgomemi // Cabo Gomis, Emilio
```

```
#Necesarios permisos de super usuario para ejecutar
```

```
#Configuración de dns client side máquina uclient01
```

```
#Configuración de dns client side máquina uclient02
```

```
cat << EOL >/etc/resolv.conf
```

```
nameserver 172.16.5.10
```

```
search lpyme10.net
```

```
EOL
```

```
cat <<EOL > /etc/nsswitch.conf
```

```
# /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:    files systemd
```

```
group:     files systemd
```

```
shadow:    files
```

```
gshadow:   files
```

```
#hosts:     files mdns4_minimal [NOTFOUND=return] dns
```

```
hosts:      files dns
```

```
networks:   files
```

```
protocols:  db files
```

```
services:   db files
```

```
ethers:     db files
```

```
rpc:        db files
```

```
netgroup:   nis
```

```
EOL
```

```
systemctl restart networking
```

La comprobación del funcionamiento del NSS es realizar el comando `"getent passwd"`.

1. El protocolo NFS que función tiene:

2. Objetos que administra un dominio:

Protocolo DHCP

Asigna dinámicamente direcciones IP y otra información en función de lo que le pidamos al protocolo. Pero esa es la función principal del protocolo.

Existen dos tipos de protocolos DHCP.

DHCPv4

DHCPv6

DHCPv4

Asigna dinámicamente direcciones IP.

El servidor y el cliente DHCPv4 envían entre sí los siguientes mensajes periódicamente.

- Detección de DHCP (DHCPDISCOVER) -> Inicia el procedimiento de descubrimiento de servidor es dhcp.
- Oferta de DHCP (DHCPOFFER) -> El server ofrece una dirección IP al cliente.
- Solicitud de DHCP (DHCPREQUEST) -> Renovación de la dirección IP por parte del cliente.
- Acuse de recibo de DHCP (DHCPACK) -> Acuse de recibo por parte del servidor al cliente.

DHCPv6.

Modos de oprecación.

DHCPv6 Statefull: Que el cliente obtenga toda la configuración de red del servidor DHCPv6.

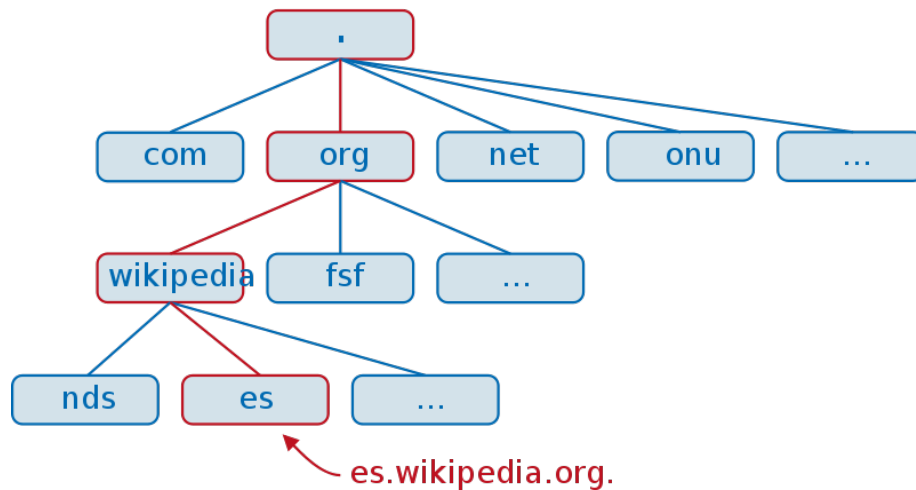
DHCPv6 Stateless: Que el cliente obtenga el prefijo de la red y luego genere el GUA. Pero hay información a mayores como (dirección de DNS, Dominio...). esperando a ser enviada por un servicio DHCPv6 stateless.

SLAAC (Sin configuración de DHCPv6): Solo obtendrá el prefijo de red del router con IPv6 habilitado.

Protocolo DNS

El Sistema de Nombres de Dominio (DNS) es un sistema de nombres **jerárquico** que nos permite identificar cualquier recurso existente en una red; relacionando la dirección IP con un nombre. Un nombre de dominio completo (FQDN).

La siguiente imagen es una imagen ilustrativa de FQDN.



Se dice que es un sistema jerarquizado debido a que en una determinada zona hay un servidor DNS que es el encargado de resolver las peticiones DNS en una determinada zona.

Los nombres de dominio completos de los DNS autorizados de una zona están listados en los registros NS.

En caso de que la dirección IP de la consulta no esté en los registros, el servidor DNS consultará al siguiente en la jerarquía y así sucesivamente hasta encontrar la respuesta a la petición de resolución de nombres.

¿Qué es SAMBA?

Es una implantación del protocolo de compartición de ficheros e impresoras de Windows, previamente conocido como SMB.

Su función principal es la de permitir el compartición de ficheros e impresoras desde LINUX a Windows y viceversa.

Mediante el modelo cliente servidor permite a un cliente windows conectarse a un server samba (LINUX) . Y así poder emplear un dominio LINUX como si de un dominio windows se tratara.

¿Qué es CIFS?

Principalmente provee de acceso a gestionar los archivos de una manera remota.

Es un protocolo que nosotros implementamos en Platega.

Debian9 ldap+smb3

Ldap-tools
smbatools

CentOS7 smb4-comoAD

Samba-tools
ldb
ldifde(client/serv)
csvde
pws/vbs/ds

heterogeneo(ws03-19/CentOS

perl
ldb/ldifde
pws/smba-tools

windows server AD

pws
ldifde
csvde
vbscript
perl

Bibliografía

IBM

<https://www.ibm.com/docs/en/aix/7.1?topic=guide-network-information-service#endr0911001>

ORACLE

https://docs.oracle.com/cd/E37929_01/html/E36688/nis2ldap-35.html

IES San Clemente.

https://manuais.iessanclemente.net/index.php?title=Acceso_dende_os_clientes_Linux_%C3%A1s_carpetas_compartidas_por_Samba3:_pam_mount#Montaxe_de_recursos_en_funci.C3.B3n_do_usuario_que_inicie_a_sesi.C3.B3n:_pam-mount
https://manuais.iessanclemente.net/index.php/Escenario_1.B_-_Instalaci%C3%B3n_e_configuraci%C3%B3n_do_servizo_de_DNS#Introduci.C3.B3n_ao_servizo_DNS

WIKIPEDIA

https://en.wikipedia.org/wiki/Name_Service_Switch
[https://es.wikipedia.org/wiki/Samba_\(software\)](https://es.wikipedia.org/wiki/Samba_(software))
https://en.wikipedia.org/wiki/Name_server#Authoritative_name_server
https://en.wikipedia.org/wiki/Domain_Name_System
<https://es.wikipedia.org/wiki/OpenLDAP>

CIFS

<https://cifs.com/>