



GRUPO 1

Eneko González,
Xabier Parra y
David Lobo.

índice

1.	configuración Inicial:	3
2.	instalación Gestor de base de datos (MariaDB):	4
2.1.	creación usuario Administrador de BDD:	5
2.2.	Configurar acceso remoto a MariaDB:	5
3.	instalación WordPress, Apache y phpMyAdmin:	6
4.	activar https en Apache y WordPress:	9
4.1.	Activar puertos vm	12
5.	instalación LDAP revisión	13
5.1.	Instalación cliente Debian Desktop y unión al dominio	21
5.2.	Administración LDAP WEB	24
	Acceso a phpLDAPadmin en el navegador	24
5.3.	plugin LDAP inicio de sesión	25
5.4.	Instalación LDAPs SECURE	26
5.5.	Cambiar OpenLDAP Default BaseDN	27
5.6.	Crear un DN base para usuarios y grupos	29
5.7.	Crear cuentas de usuario LDAP	30
5.8.	Agregar usuarios a la base de datos SLAPD	31
5.9.	Configurar OpenLDAP con SSL/TLS	33
	Generar certificados SSL/TLS	33
	Actualizar certificados TLS de OpenLDAP Server	37
5.10.	Comprobar la conectividad TLS para LDAP	39
5.11.	Deshabilitar el acceso anónimo a OpenLDAP	39
6.	Instalación Tomcat	41
6.1.	Test Tomcat installation	43
7.	Secure Tomcat	44
8.	CAS Installation Tomcat	50
9.	Conclusión	53

1. configuración Inicial:

Para cambiar el nombre a la máquina Ubuntu, el nombre será **Debian Web**

Ubicación: **nano /etc/hostname**

Debian Web

dhclient → Para dirección automática de Ip del servidor DHCP

Para **actualizar** la maquina Ubuntu:

apt update

apt upgrade

Para que resuelva el **nombre de dominio** de la página, añadir la siguiente línea:

Primero la dirección IP de la máquina donde esté el sitio web, y luego el nombre de dominio

Ubicación: **nano /etc/hosts**

127.0.1.1 www.cibergrupo1.com

192.168.1.141 www.cibergrupo1.com

```
GNU nano 3.2 /etc/hosts
127.0.0.1    localhost
127.0.1.1    2asir
192.168.1.141 www.cibergrupo1.com
# The following lines are desirable for IPv6 capable hosts
::1          localhost ip6-localhost ip6-loopback
ff02::1      ip6-allnodes
ff02::2      ip6-allrouters
```

SSH login:

Ubicación: **nano /etc/ssh/sshd_config**

PermitRootLogin yes

systemctl restart ssh

2. instalación Gestor de base de datos (MariaDB):

Instalar **MariaDB**. El paquete que necesitamos es **mariadb-server**, así que lo instalamos mediante apt:

```
apt install mariadb-server
```

Comprobar mediante el comando **systemctl status mariadb**, que se ha instalado correctamente el servidor mariadb.

```
systemctl status mariadb
```

Configuración **modo seguro mysql**: `mysql_secure_installation`

Tendremos que **cambiar** la contraseña al usuario root y posteriormente darle a todo que sí (y).

Password del usuario **root**: 1

```
root@grupo2VM: /home/liher# mysql_secure_installation
NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB
SERVERS IN PRODUCTION USE! PLEASE READ EACH STEP CAREFULLY!

In order to log into MariaDB to secure it, we'll need the current
password for the root user. If you've just installed MariaDB, and
you haven't set the root password yet, the password will be blank,
so you should just press enter here.

Enter current password for root (enter for none):
OK, successfully used password, moving on...

Setting the root password ensures that nobody can log into the MariaDB
root user without the proper authorisation.

Set root password? [Y/n] y
New password:
Re-enter new password:
Password updated successfully!
Reloading privilege tables..
... Success!

By default, a MariaDB installation has an anonymous user, allowing anyone
to log into MariaDB without having to have a user account created for
them. This is intended only for testing, and to make the installation
go a bit smoother. You should remove them before moving into a
production environment.

Remove anonymous users? [Y/n] y
... Success!

Normally, root should only be allowed to connect from 'localhost'. This
ensures that someone cannot guess at the root password from the network.

Disallow root login remotely? [Y/n] y
... Success!

By default, MariaDB comes with a database named 'test' that anyone can
access. This is also intended only for testing, and should be removed
before moving into a production environment.

Remove test database and access to it? [Y/n] y
- Dropping test database...
... Success!
- Removing privileges on test database...
... Success!

Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.

Reload privilege tables now? [Y/n] y
... Success!

Cleaning up...

All done! If you've completed all of the above steps, your MariaDB
installation should now be secure.

Thanks for using MariaDB!
```

2.1. creación usuario Administrador de BDD:

Creación **Usuario Administrador** de la base de datos:

Ahora, crearemos un nuevo usuario con privilegios de root y acceso basado en contraseña.

```
mysql -u root
```

Creación de **AdminBdd** con permisos root:

```
GRANT ALL PRIVILEGES ON *.* TO 'adminServer'@'%' IDENTIFIED BY '1' WITH GRANT OPTION;
```

```
flush privileges;
```

2.2. Configurar acceso remoto a MariaDB:

Permitir acceso remoto al servicio MariaDB. Editar el archivo `/etc/mysql/mariadb.conf.d/50-server.cnf`:

Cambiar la directiva tiene el mismo efecto que cambiar su valor por 0.0.0.0, que es permitir las conexiones desde cualquier otra máquina externa, incluyendo conexiones desde Internet.

```
GNU nano 4.8 /etc/mysql/mariadb.conf.d/50-server.cnf
[server]

# this is only for the mysqld standalone daemon
[mysqld]

#
# * Basic Settings
#
user                = mysql
pid-file            = /run/mysqld/mysqld.pid
socket              = /run/mysqld/mysqld.sock
#port               = 3306
basedir             = /usr
datadir             = /var/lib/mysql
tmpdir              = /tmp
lc-messages-dir     = /usr/share/mysql
#skip-external-locking

# Instead of skip-networking the default is now to listen only on
# localhost which is more compatible and is not less secure.
bind-address        = 0.0.0.0
```

```
bind-address = 0.0.0.0
```

Para que los cambios tomen efecto, hay que **reiniciar el servicio mariadb**:

```
systemctl restart mariadb
```

3. instalación WordPress, Apache y phpMyAdmin:

PASO 1 (Descomprimir el archivo phpMyAdmin)

apt install wget

wget https://files.phpmyadmin.net/phpMyAdmin/5.1.3/phpMyAdmin-5.1.3-all-languages.tar.gz

ls → para ver el archivo comprimido de phpMyAdmin
tar xvf phpMyAdmin-5.1.3-all-languages.tar.gz → para descomprimir el archivo

apt update → Actualizar en busca de paquetes de sistema
apt install apache2 mariadb-server php7.4-mysql libapache2-mod-php php7.4-mbstring php-ldap

PASO 3 (Creación de Site para phpMyAdmin)

mv /root/phpMyAdmin-5.0.4-all-languages/ /var/www/html/phpmyadmin → Mover el fichero

phpMyAdmin y le cambiamos el nombre a phpmyadmin

cd /var/www/html/ → Nos dirigimos a la carpeta que hemos movido phpmyadmin

cd phpmyadmin

cp config.sample.inc.php config.inc.php → Crearemos una copia con el nombre correcto

nano config.inc.php → Editamos el fichero de configuración

escribir entre las comillas \$cfg['blowfish_secret'] = 'wedbrvfreaahuvjrvbrvbrvirfrggsedghb'

escribir lo siguiente \$cfg['TempDir'] = 'tmp';

mkdir /var/www/html/phpmyadmin/tmp

chmod 664 config.inc.php → Cambiar permiso a el fichero de configuración config

chown -R wordpress:www-data /var/www/html/phpmyadmin

chmod 777 tmp → Cambiar permiso a el fichero tmp

PASO 5 (Creación de BDD, el usuario y acceder phpMyAdmin WEB)

mysql -uroot -pgrp2/C1b → Acceder a mysql

create database wordpress;

create user 'user_grupo1@localhost';

grant all privileges on wordpress.* to 'user_grupo1@localhost' identified by

'qazwsxedc123' with grant option;

flush privileges;

SELECT user,host FROM mysql.user; → Para ver los usuarios mysql

```
MariaDB [(none)]> select user,host from mysql.user;
+-----+-----+
| User           | Host           |
+-----+-----+
| adminServer    | %              |
| mariadb.sys    | localhost      |
| mysql          | localhost      |
| root           | localhost      |
| user_wordpress | localhost      |
+-----+-----+
5 rows in set (0.001 sec)
```

PASO 6 (Creación de site para wordpress y habilitar el sitio)

Crearemos un site nuevo para wordpress para acceder con la dirección IP.

```
cd /etc/apache2/sites-available/      → Acceder a sitios disponibles de apache2
cp 000-default.conf wordpress.conf    → Crear un nuevo sitio para wordpress
nano wordpress.conf
    ServerName www.cibergrupo1.com     → El dominio del cliente, el que pida
    DocumentRoot /var/www/wordpress   → Donde se despliega el wordpress en la web
EXIT
```

```
a2ensite wordpress      → Habilitar sitio de wordpress
systemctl reload apache2 → Reiniciar el apache2
```

ls -l /etc/apache2/sites-enabled/ → Veremos que se ha creado un enlace simbólico hacia nuestro wordpress

PASO 7 (Instalación de Wordpress)

```
apt-get install wget      → Paquete que deja instalar desde la url
wget https://wordpress.org/latest.zip → Paquete Wordpress
```

```
apt install unzip      → Paquete para descomprimir el zip
unzip latest.zip        → Descomprimir paquete de wordpress
mv wordpress/ /var/www/ → Mover el fichero wordpress
cd /var/www/wordpress   → Verificar el directorio con sus ficheros
```

PASO 8 (Instalación de FTP (proftpd))

```
apt-cache search proftpd → Buscar programa proftpd-basic si no te acuerdas
apt-get install proftpd-basic → Instalar el FTP
```

adduser wordftp → **Crear un usuario con permisos a ftp y quitar login via ssh.**
 nano /etc/passwd → Acceder a la carpeta de los Usuarios

Cambiar la carpeta y el visor para que no pueda acceder con ssh
:/var/www/html/wordpress:/bin/false

Para no dejar **salir al usuario** de su **home** lo encajaremos:

nano /etc/proftpd/proftpd.conf → **Editar el archivo proftpd.conf**
 DefaultRoot ~ → **Descomentar**
 RequireValidShell off → **Descomentar para que pueda conectarse a FTP**
EXIT

systemctl restart proftpd → **Reiniciar el servicio FTP**

PASO 9 (Permisos wordpress)

cd /var/www → **Acceder a la carpeta donde se ubica wordpress**
 /var/www ## ls -l → **Ver permisos que tienen al directorio**

Cambiamos permiso al usuario FTP wordpress que es el que editará los ficheros

chown -R ftpadmin:www-data wordpress/
 chmod -R 775 wordpress/ → **Todos los permisos, excepto para los cliente rx (lectura y ejecución)**

192.168.1.141 www.cibergrupo1.com → **Editar el archivo hosts de Windows 10**

PASO 10 (Instalación wordpress)

Ir al navegador www.cibergrupo1.com

Configuración:

Database Name → **wordpress**
 Username → **user_grupo1**
 Password → **qazwsxedc123**
 Database Host → **localhost**
 Table prefix → **wp_**

Configuración cuenta wordpress:

- user=admin
- pass=1

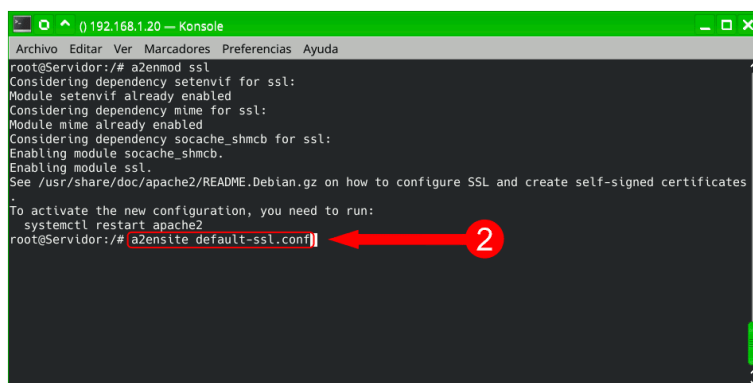
4. activar https en Apache y WordPress:

Activar módulo seguro (https) a2enmod SSL: -->

a2enmod ssl

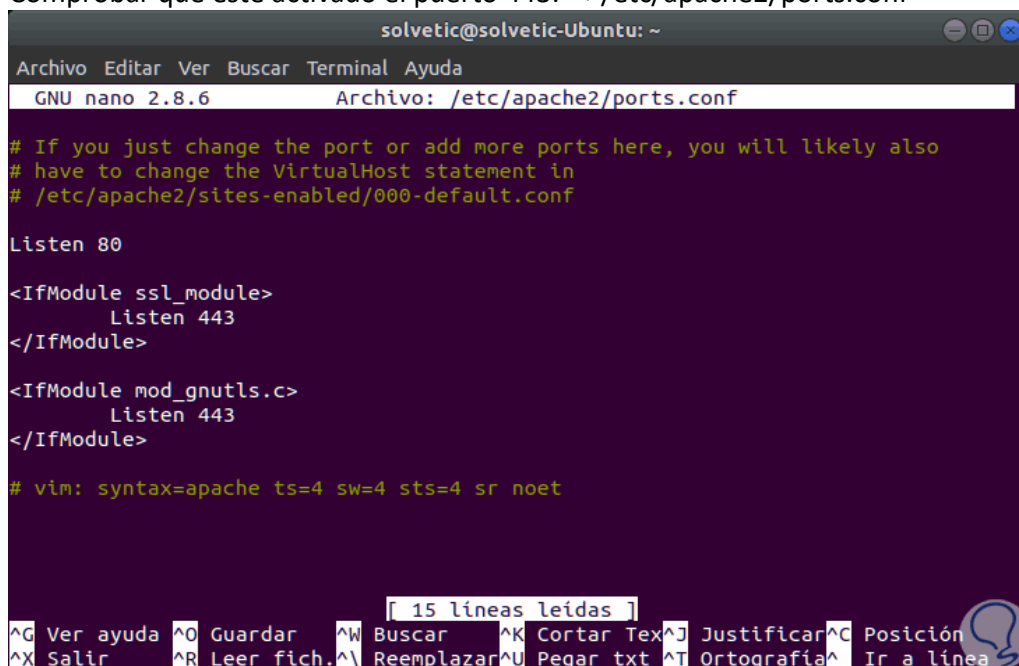
a2enmod rewrite

systemctl restart apache2



```
root@Servidor:~# a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create self-signed certificates
To activate the new configuration, you need to run:
systemctl restart apache2
root@Servidor:~# a2ensite default-ssl.conf
```

Comprobar que esté activado el puerto 443: -->/etc/apache2/ports.conf



```
solvetic@solvetic-Ubuntu: ~
GNU nano 2.8.6 Archivo: /etc/apache2/ports.conf

# If you just change the port or add more ports here, you will likely also
# have to change the VirtualHost statement in
# /etc/apache2/sites-enabled/000-default.conf

Listen 80

<IfModule ssl_module>
    Listen 443
</IfModule>

<IfModule mod_gnutls.c>
    Listen 443
</IfModule>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet

[ 15 líneas leídas ]
^G Ver ayuda ^O Guardar ^W Buscar ^K Cortar Text ^J Justificar ^C Posición
^X Salir ^R Leer fich. ^\ Reemplazar ^U Pegar txt ^T Ortografía ^_ Ir a línea
```

Creamos el directorio donde se guardan los certificados ssl: --> /etc/apache2/ssl
 Crearemos una subcarpeta con las clave pública y privada del certificado --> mkdir /etc/apache2/ssl/cibergrupo1/

```
root@debianWeb:~# mkdir /etc/apache2/ssl
root@debianWeb:~# mkdir /etc/apache2/ssl/cibergrupo2
```

Creación del certificado auto firmado y las claves públicas y privadas: →

```
openssl req -newkey rsa:2048 -x509 -nodes -days 365 -out
/etc/apache2/ssl/cibergrupo1/cibergrupo1.crt -
keyout /etc/apache2/ssl/cibergrupo1/cibergrupo1.key
```

```
root@debianWeb:~# openssl req -newkey rsa:2048 -x509 -nodes -days 365 -out /etc/apache2/ssl/cibergru
po2/cibergrupo2.crt -keyout /etc/apache2/ssl/cibergrupo2/cibergrupo2.key
Generating a RSA private key
.....+++++
.....+++++
writing new private key to '/etc/apache2/ssl/cibergrupo2/cibergrupo2.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ES
State or Province Name (full name) [Some-State]:Vizcaya
Locality Name (eg, city) []:Durango
Organization Name (eg, company) [Internet Widgits Pty Ltd]:cibergrupo2
Organizational Unit Name (eg, section) []:automon
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:
root@debianWeb:~# _
```

Editar el archivo /etc/apache2/sites-enabled/wordpress.conf

```
<VirtualHost *:80>
# RewriteEngine On
# RewriteCond %{HTTPS} !=on
# RewriteRule ^/?(.*) https://%{www.cibergrupo1.com}/$1 [R=301,L]
```

```
ServerName www.cibergrupo1.com
Redirect permanent / https://www.cibergrupo1.com/
ServerAdmin webmaster@localhost
DocumentRoot /var/www/wordpress
ErrorLog ${APACHE_LOG_DIR}/error.log
CustomLog ${APACHE_LOG_DIR}/access.log combined
</Virtualhost>
```

```
<VirtualHost *:443>
    ServerName www.cibergrupo1.com
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/wordpress
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
    SSLEngine on
    SSLCertificateFile /etc/apache2/ssl/cibergrupo1/cibergrupo1.crt
    SSLCertificateKeyFile /etc/apache2/ssl/cibergrupo1/cibergrupo1.key
</VirtualHost>
```

```
GNU nano 3.2 /etc/apache2/sites-available/wordpress.conf
VirtualHost *:80>
# The ServerName directive sets the request scheme, hostname and port that
# the server uses to identify itself. This is used when creating
# redirection URLs. In the context of virtual hosts, the ServerName
# specifies what hostname must appear in the request's Host: header to
# match this virtual host. For the default virtual host (this file) this
# value is not decisive as it is used as a last resort host regardless.
# However, you must set it for any further virtual host explicitly.
ServerName www.cibergrupol.com
ServerAdmin webmaster@localhost
DocumentRoot /var/www/wordpress
Redirect permanent / https://www.cibergrupol.com/
# Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
# error, crit, alert, emerg.
# It is also possible to configure the loglevel for particular
# modules, e.g.
#LogLevel info ssl:warn

ErrorLog ${APACHE_LOG_DIR}/error.log
CustomLog ${APACHE_LOG_DIR}/access.log combined

# For most configuration files from conf-available/, which are
# enabled or disabled at a global level, it is possible to
# include a line for only one particular virtual host. For example the
# following line enables the CGI configuration for this host only
# after it has been globally disabled with "a2disconf".
#Include conf-available/serve-cgi-bin.conf
</VirtualHost>
<VirtualHost *:443>
    ServerName www.cibergrupol.com
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/wordpress
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
    SSLEngine on
    SSLCertificateFile /etc/apache2/ssl/cibergrupol/cibergrupol.crt
    SSLCertificateKeyFile /etc/apache2/ssl/cibergrupol/cibergrupol.key
</VirtualHost>
# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

Reiniciar apache2

systemctl restart apache2

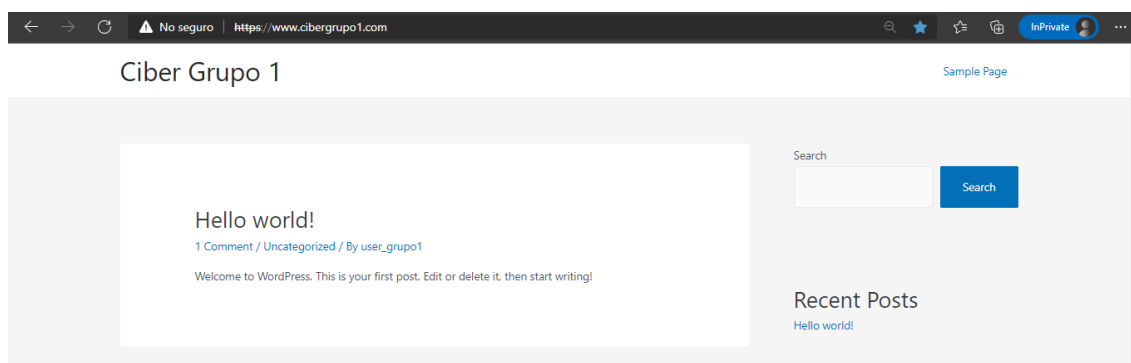
Comprobar que funcione la redirección de http a https

apt install curl

```
root@2asir:~# curl -I http://www.cibergrupo1.com
HTTP/1.1 301 Moved Permanently
Date: Fri, 25 Feb 2022 09:52:13 GMT
Server: Apache/2.4.38 (Debian)
Location: https://www.cibergrupo1.com/
Content-Type: text/html; charset=iso-8859-1

root@2asir:~#
```

Comprobacion www.cibergrupo1.com → <https://www.cibergrupo1.com>



4.1. Activar puertos vm

ssh → ufw allow 22/tcp

ssh → ufw allow OpenSSH

http → ufw allow 80/tcp

https → ufw allow 443/tcp

LDAP → ufw allow 389/tcp

LDAP Secure → ufw allow 636/tcp

mysql → ufw allow 3306/tcp

Tomcat → ufw allow 8080/tcp

Tomcat Secure → ufw allow 8443/tcp

ufw reload

ufw enable

5. instalación LDAP revisión

```
apt install slapd ldap-utils -y
```

En el siguiente paso nos pedirá poner la contraseña para la entrada del administrador LDAP.(qazwsxedc123)

Configuring slapd

Please enter the password for the admin entry in your LDAP directory.

Administrator password:

<Ok>

```
dpkg-reconfigure slapd
```

Configuring slapd

If you enable this option, no initial configuration or database will be created for you.

Omit OpenLDAP server configuration?

<Yes> <No>

En el siguiente paso nos pedirá poner el dominio creado para el directorio activo(cibergrupo1.com).

Configuring slapd

The DNS domain name is used to construct the base DN of the LDAP directory. For example, 'foo.example.org' will create the directory with 'dc=foo, dc=example, dc=org' as base DN.

DNS domain name:

pandora.ldap

<Ok>

Añadir el nombre de la organización (cibergrupo1). y después la contraseña del administrador LDAP (qazwsxedc123)

Configuring slapd

Please enter the name of the organization to use in the base DN of your LDAP directory.

Organization name:

pandora

<Ok>

No borrar la base de datos cuando se purgue

Configuring slapd

Do you want the database to be removed when slapd is purged?

<Yes> <No>

por último nos pregunta si queremos mover los datos de alguna antigua base de datos de directorio LDAP a la nueva que estamos configurando.

Configuring slapd

There are still files in /var/lib/ldap which will probably break the configuration process. If you enable this option, the maintainer scripts will move the old database files out of the way before creating a new database.

Move old database?

<Yes> <No>

Ir al directorio de configuración LDAP /etc/ldap/ldap.conf
nano /etc/ldap/ldap.conf

Buscar la dirección ip del servidor y ponerlo en la parte ldap://IP:389

```
valid_lft forever preferred_lft forever
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
group default qlen 1000
    link/ether 00:0c:29:2f:a6:0e brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.141/24 brd 192.168.1.255 scope global ens160
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe2f:a60e/64 scope link
        valid_lft forever preferred_lft forever
```

BASE dc=cibergrupo1,dc=com
URI ldap://192.168.1.141:389

```
GNU nano 3.2 /etc/ldap/ldap.conf
#
# LDAP Defaults
#
# See ldap.conf(5) for details
# This file should be world readable but not world writable.
BASE dc=cibergrupo1,dc=com
URI ldap://192.168.1.141:389
#SIZELIMIT 12
#TIMELIMIT 15
#DEREF never
# TLS certificates (needed for GnuTLS)
TLS_CACERT /etc/ssl/certs/ca-certificates.crt
```

Ir al directorio de configuración nsswitch /etc/nsswitch.conf
nano /etc/nsswitch.conf

passwd: files ldap
group: files ldap
shadow: files ldap

```
GNU nano 5.4 /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 ldap
group:       files ldap
shadow:      files ldap
gshadow:     files

hosts:       files dns
networks:    files

protocols:   db files
services:    db files
ethers:      db files
rpc:         db files

netgroup:    nis
```

En el siguiente paso instalaremos el administrador LDAP:

```
wget http://ftp.de.debian.org/debian/pool/main/p/phpldapadmin/phpldapadmin_1.2.6.3-0.2_all.deb
```

```
root@debianWeb:/home/userweb# wget http://ftp.de.debian.org/debian/pool/main/p/p
hpldapadmin/phpldapadmin_1.2.6.3-0.2_all.deb
--2022-02-16 09:11:30-- http://ftp.de.debian.org/debian/pool/main/p/phpldapadmin/phpldapadmin_1.2.6.3-0.2_all.deb
Resolviendo ftp.de.debian.org (ftp.de.debian.org)... 141.76.2.4
Conectando con ftp.de.debian.org (ftp.de.debian.org) [141.76.2.4]:80... conectado
.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 706228 (690K) [application/x-debian-package]
Grabando a: «phpldapadmin_1.2.6.3-0.2_all.deb»

phpldapadmin_1.2.6. 100%[=====>] 689,68K 242KB/s en 2,9s
2022-02-16 09:11:33 (242 KB/s) - «phpldapadmin_1.2.6.3-0.2_all.deb» guardado [706228/706228]
```

Siguiente, instalar el paquete phpLDAPAdmin, siguiendo el command below;

```
apt install ./phpldapadmin_1.2.6.3-0.2_all.deb
```

```
root@debianWeb:/home/userweb# apt install ./phpldapadmin_1.2.6.3-0.2_all.deb
```


Configuración de phpLDAPAdmin en Debian 10

El archivo de configuración predeterminado para phpLDAPAdmin es `/etc/phpldapadmin/config.php`. Este es el archivo que vamos a editar para realizar nuestros cambios de configuración según la configuración del servidor LDAP.

`nano /etc/phpldapadmin/config.php`

```
root@debianWeb:/home/userweb# nano /etc/phpldapadmin/config.php
```

El archivo de configuración está muy comentado. Solo vamos a hacer algunos cambios en esta demostración, suficientes para acceder y ejecutar phpLDAPAdmin para administrar el servidor LDAP.

Establezca un nombre adecuado para su servidor LDAP. Este es el nombre que aparecerá en la interfaz web de phpLDAPAdmin.

```

/*****
 * Define your LDAP servers in this section *
 *****/
...
/* A convenient name that will appear in the tree viewer and throughout
phpLDAPAdmin to identify this LDAP server to users. */
$servers->setValue('server','name','Cibergroupo1 LDAP Server');
...

```

Defina la dirección IP o el nombre de host resoluble de su servidor OpenLDAP;

```
$servers->setValue('server','host','debianWeb.cibergroupo1.com');
```

Defina el puerto en el que el servidor OpenLDAP está escuchando. En nuestra demostración, nuestro OpenLDAP está configurado con StartTLS (puerto 389).

```
/* The port your LDAP server listens on (no quotes). 389 is standard. */
$servers->setValue('server','port',389);
```

```
/* A convenient name that will appear in the tree viewer and throughout
   phpLDAPadmin to identify this LDAP server to users. */
$servers->setValue('server','name','Cibergrupol LDAP Server');

/* Examples:
   'ldap.example.com',
   'ldaps://ldap.example.com/',
   'ldapi://%2fusr%2flocal%2fvar%2frun%2fldapi'
   (Unix socket at /usr/local/var/run/ldap) */
$servers->setValue('server','host','192.168.1.141');

/* The port your LDAP server listens on (no quotes). 389 is standard. */
$servers->setValue('server','port',389);

/* Array of base DN's of your LDAP server. Leave this blank to have phpLDAPadmin
   auto-detect it for you. */
$servers->setValue('server','base',array('dc=cibergrupol,dc=com'));

/* Five options for auth_type:
   1. 'cookie': you will login via a web form, and a client-side cookie will
      store your login dn and password.
   2. 'session': same as cookie but your login dn and password are stored on the
      web server in a persistent session variable.
```

Establezca el DN base de OpenLDAP. En nuestra configuración, openLDAP base DN se establece en dc=cibergrupol,dc=com.

```
/* Array of base DN's of your LDAP server. Leave this blank to have phpLDAPadmin
   auto-detect it for you. */
$servers->setValue('server','base',array('dc=cibergrupol,dc=com'));
```

Defina su tipo de autenticación phpLDAPadmin. En esta demostración, elegimos el tipo de autenticación predeterminado, .session

```
$servers->setValue('login','auth_type','session'); Aquí Nada por defecto.
```

Definir el DN de enlace del usuario administrativo para iniciar sesión en phpLDAPadmin;

```
$servers->setValue('login','bind_id','cn=admin,dc=ldapmaster,dc=kifarunix-demo,dc=com');
```

Opcionalmente, puede especificar un atributo para usar al iniciar sesión. En nuestro caso, queremos usar DN completo como, cn=admin,dc=kifarunix-demo,dc=com, para iniciar sesión.

```
$servers->setValue('login','attr','dn');
```

Configure el incremento automático del ID de usuario al crear usuarios desde la interfaz web phpLDAPadmin. Esto garantiza que no vuelva a utilizar los ID de usuario y grupo ya asignados. En esta configuración, elegimos el ID de 10000.

```
/* The minimum number to use when searching for the next available number
(only when 'search' is used for auto_number. */
$servers->setValue('auto_number','min',array('uidNumber'=>10000,'gidNumber'=>10000));
```

```
/* The minimum number to use when searching for the next available number
(only when 'search' is used for auto_number. */
$servers->setValue('auto_number','min',array('uidNumber'=>10000,'gidNumber'=>10000));
```

Configurar Apache para phpLDAPadmin

Cree la configuración de phpLDAPadmin Apache, de la siguiente manera./etc/apache2/conf-available/phpldapadmin.conf

```
cat > /etc/apache2/conf-available/phpldapadmin.conf << 'EOL'
Alias /phpldapadmin /usr/share/phpldapadmin/htdocs
```

```
<Directory /usr/share/phpldapadmin/htdocs>
<IfModule mod_authz_core.c>
    Require all granted
</IfModule>
</Directory>
EOL
```

Establezca la propiedad del archivo en .www-data
chown -R www-data: /usr/share/phpldapadmin/

Habilitar SSL;

```
cat > /etc/apache2/sites-available/phpldapadmin.conf << 'EOL'
<VirtualHost *:443>
    ServerName www.cibergrupo1.com

    SSLEngine on
    SSLCertificateFile /etc/ssl/certs/server.crt
    SSLCertificateKeyFile /etc/ssl/private/server.key
</VirtualHost>
```

EOL

Configurar la redirección HTTP/HTTPS;

```
cat >> /etc/apache2/apache2.conf << 'EOL'
RewriteEngine On
RewriteCond %{HTTPS} off
RewriteRule ^(.*)$ https://www.cibergrupo1.com/$1 [L,R=301]
```

EOL

Deshabilitar el sitio predeterminado de Apache (con página de bienvenida)

a2dissite 000-default.conf

```
root@debianWeb:~# a2dissite 000-default.conf
Site 000-default disabled.
To activate the new configuration, you need to run:
    systemctl reload apache2
root@debianWeb:~# systemctl reload apache2
root@debianWeb:~# _
```

Habilite SSL y reescriba módulos;

a2enmod rewrite ssl

Abra Apache en el firewall para permitir el acceso externo.

ufw allow "WWW Full"

Compruebe la sintaxis de Apache;

apachectl -t

Syntax OK

Reinicie Apache;

systemctl restart apache2

```
root@debianWeb:~# apachectl -t
Syntax OK
root@debianWeb:~# systemctl restart apache2
root@debianWeb:~#
```

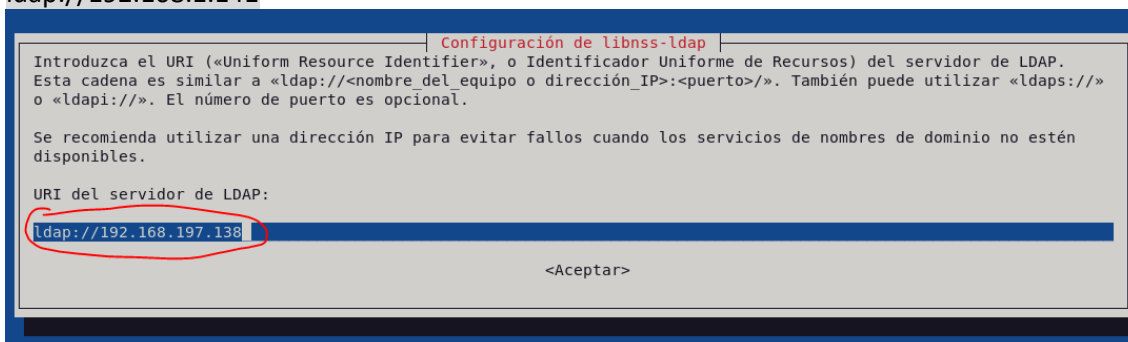
5.1. Instalación cliente Debian Desktop y unión al dominio

Instalar el paquete para el cliente LDAP:

```
apt install libpam-ldap libnss-ldap nss-updatedb nscd ldap-utils -y
```

Añadir la ip del servidor (192.168.1.141)

```
ldap://192.168.1.141
```



Configuración de libnss-ldap

Introduzca el URI («Uniform Resource Identifier», o Identificador Uniforme de Recursos) del servidor de LDAP. Esta cadena es similar a «ldap://<nombre_del_equipo_o_dirección_IP>:<puerto>/». También puede utilizar «ldaps://» o «ldapi://». El número de puerto es opcional.

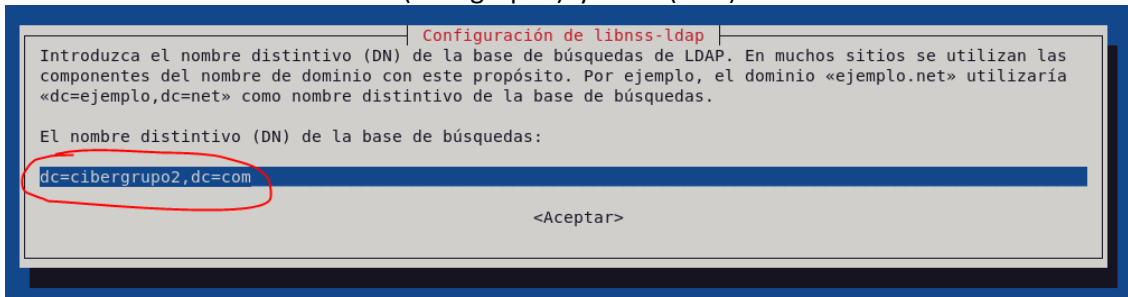
Se recomienda utilizar una dirección IP para evitar fallos cuando los servicios de nombres de dominio no estén disponibles.

URI del servidor de LDAP:

ldap://192.168.197.138

<Aceptar>

Introducir el nombre del dominio(cibergrupo1) y la raíz(com)



Configuración de libnss-ldap

Introduzca el nombre distintivo (DN) de la base de búsquedas de LDAP. En muchos sitios se utilizan las componentes del nombre de dominio con este propósito. Por ejemplo, el dominio «ejemplo.net» utilizaría «dc=ejemplo,dc=net» como nombre distintivo de la base de búsquedas.

El nombre distintivo (DN) de la base de búsquedas:

dc=cibergrupo2,dc=com

<Aceptar>

Siguientes pasos:

Versión LDAP: 3
Nombre del dispositivo: cn=admin,dc=cibergrupo1,dc=com
Contraseña admin LDAP: qazwsxedc123
Nombre del dispositivo: cn=admin,dc=cibergrupo1,dc=com

Instalar el paquete slapd:

```
apt install slapd
```

Poner la contraseña admin LDAP: qazwsxedc123

Reconfigurar la SLAPD:

```
dpkg-reconfigure slapd
```

- Omitir servidor OPENLDAP: no
- Dominio: cibergrupo1.com
- Organización: cibergrupo1
- Contraseña admin LDAP: qazwsxedc123
- Borrar bdd: no
- Mover bdd old: yes

Configuración /etc/ldap/ldap.conf

```
nano /etc/ldap/ldap.conf
```

```
GNU nano 4.8 /etc/ldap/ldap.conf
#
# LDAP Defaults
#
# See ldap.conf(5) for details
# This file should be world readable but not world writable.

BASE    dc=cibergrupo1,dc=com
URI      ldap://192.168.1.141:389

#SIZELIMIT      12
#TIMELIMIT      15
#DEREF          never

# TLS certificates (needed for GnuTLS)
TLS_CACERT      /etc/ssl/certs/ca-certificates.crt
```

Ir al directorio de configuración nsswitch `/etc/nsswitch.conf`
`nano /etc/nsswitch.conf`

```
passwd:      files ldap
group:       files ldap
shadow:      files ldap
```

```
GNU nano 5.4 /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 ldap
group:       files ldap
shadow:      files ldap
gshadow:     files

hosts:       files dns
networks:    files

protocols:   db files
services:    db files
ethers:      db files
rpc:         db files

netgroup:    nis
```

Actualizar base de datos LDAP:
`nss_updatedb ldap`

Editar el siguiente fichero `/usr/share/pam-configs/mkhomedir`
`nano /usr/share/pam-configs/mkhomedir`



5.2. Administración LDAP WEB

Acceso a phpLDAPAdmin en el navegador

Puede acceder a phpLDAPAdmin utilizando la dirección,
<https://www.cibergrupo1.com/phpldapadmin>

The screenshot shows the phpLDAPAdmin web interface. On the left, there is a sidebar with the phpLDAPAdmin logo and a link to 'Cibergrupo1 LDAP Server' with a 'conectar' button. The main area has a dark blue header that says 'Autenticar al servidor Cibergrupo1 LDAP Server'. Below this, there is a login form with the following fields and options:

- Login:** A text input field containing 'cn=admin,dc=cibergrupo1,dc=com'.
- Contraseña:** A password input field with masked characters (dots).
- Anónimo:** A checkbox that is currently unchecked.
- Identificarse:** A button to submit the login information.

Haga clic en **iniciar** sesión para iniciar sesión en la interfaz de usuario web phpLDAPAdmin. Como ya definimos el DN de enlace de administrador, simplemente ingrese la contraseña e inicie sesión;

2 Unidades Organizativas (groups, users)

groups:

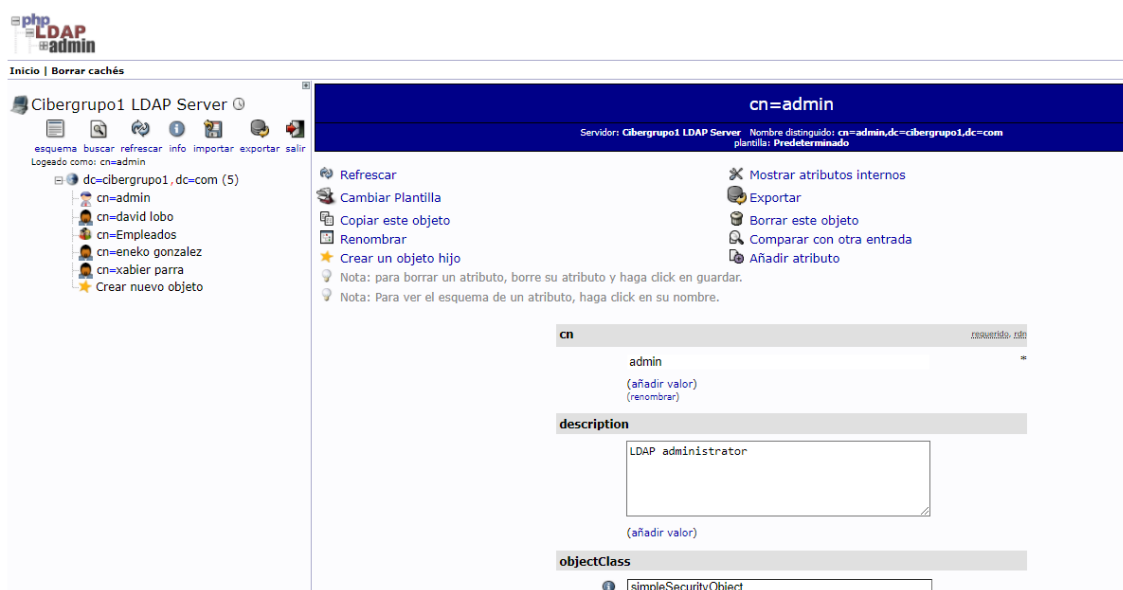
Empleados

users:

Eneko

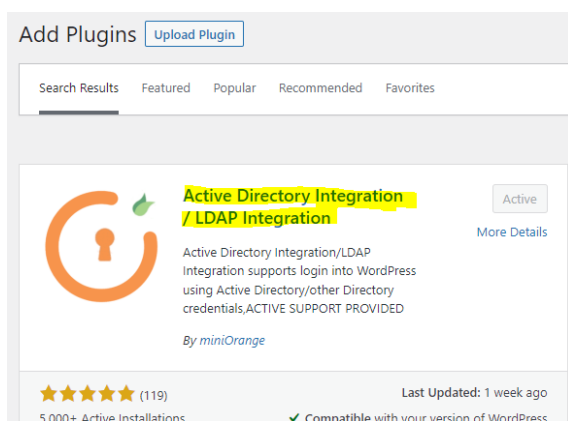
David

Xabier



5.3. plugin LDAP inicio de sesión

Instalar el plugin Active Directory Integration/ LDAP Integration



Conexión LDAP

Check our Premium features and find out how to get the configuration done through the videos and guides below.

[LDAP/AD Plugin Setup](#) [Premium Plugin Features](#) [Setup LDAP/AD plugin](#) [Setup LDAPS connection](#)

NOTE: You need to find out the values for the below given fields from your LDAP Administrator.

*Select Your Directory Server:

*LDAP Server: ☒ 192.168.1.141

Select ldap or ldaps from the above dropdown list. Specify the host name for the LDAP server in the above text field. Edit the port number if you have custom port number.

*Username: ☒ cn=admin,dc=cibergrupo1,dc=com

You can specify the Username of the LDAP server in the either way as follows
Username@domainname or Distinguished Name(DN) format

*Password: ☒

The above username and password will be used to establish the connection to your LDAP server.

[Test Connection & Save](#) [Troubleshooting](#)

5.4. Instalación LDAPs SECURE

Instalar paquetes LDAP

```
apt -y install slapd ldap-utils ldapscripts
```

poner contraseña admin = qazwsxedc123

```
root@debianWeb:~# slapcat
dn: dc=cibergrupo2,dc=com
objectClass: top
objectClass: dcObject
objectClass: organization
o: cibergrupo2.com
dc: cibergrupo2
structuralObjectClass: organization
entryUUID: b6276252-2935-103c-92c2-29de30e8d943
creatorsName: cn=admin,dc=cibergrupo2,dc=com
createTimestamp: 20220223204834Z
entryCSN: 20220223204834.367890Z#000000#000#000000
modifiersName: cn=admin,dc=cibergrupo2,dc=com
modifyTimestamp: 20220223204834Z
```

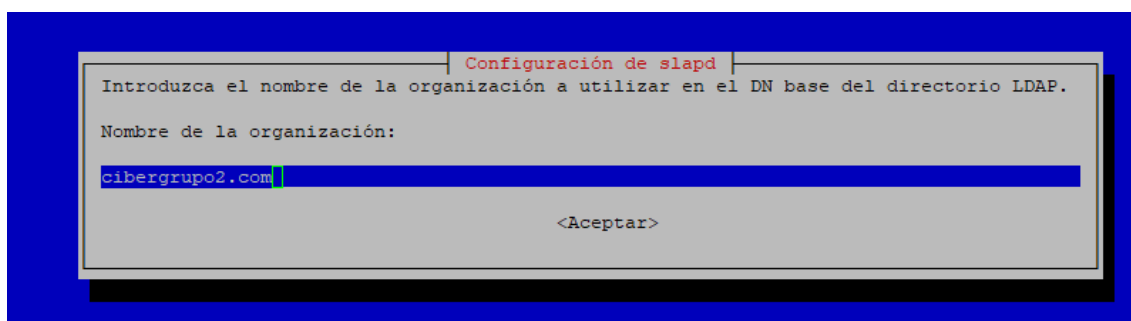
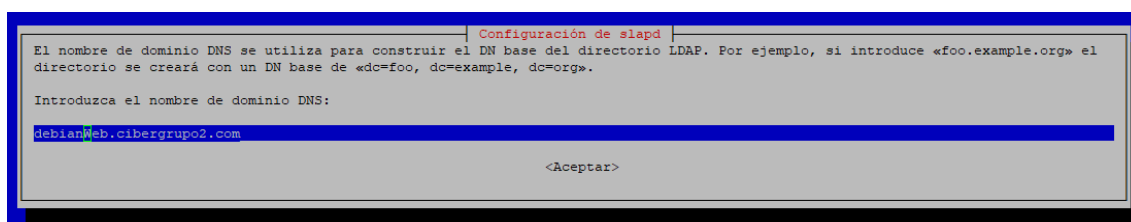
Ver la configuración de la base de datos LDAP `slapcat`



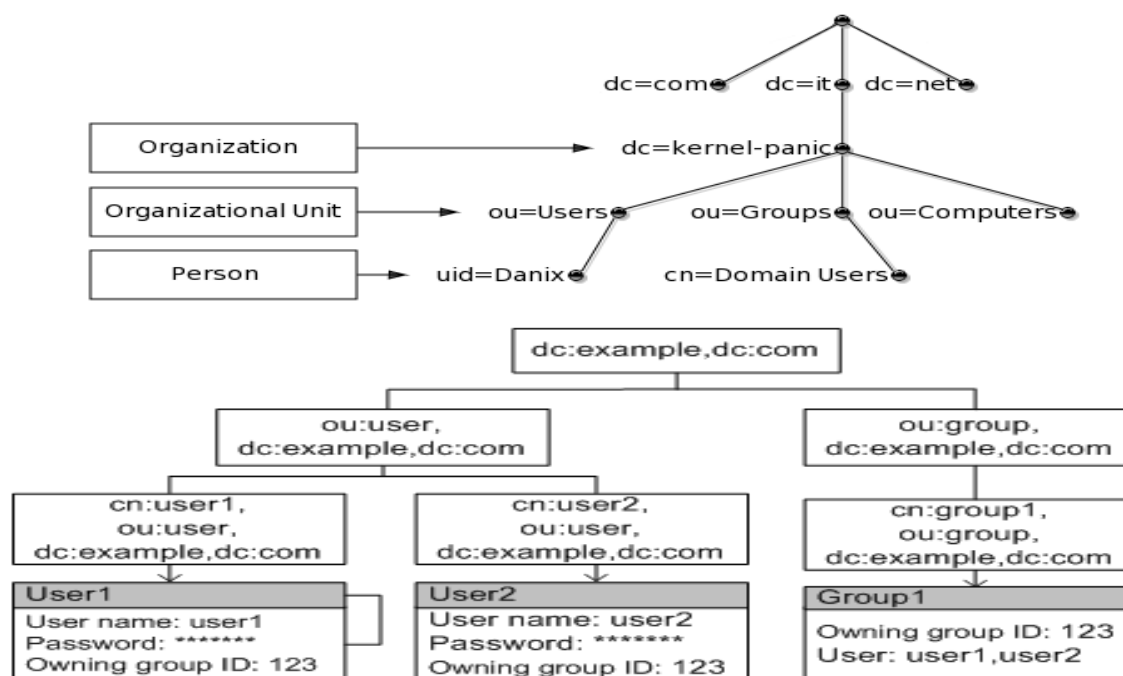
5.5. Cambiar OpenLDAP Default BaseDN

Sin embargo, si necesita el DN base predeterminado de OpenLDAP, debe volver a configurar el paquete slapd como se muestra a continuación y seguir las indicaciones. `dpkg-reconfigure slapd`

Cuando se ejecuta el comando, se le preguntará si debe omitir la configuración del servidor OpenLDAP. Seleccione **No** para crear la configuración automáticamente.



ESQUEMA:



5.6. Crear un DN base para usuarios y grupos

A partir de la salida de configuración de la base de datos SLAPD anterior, se ha creado el DN base para el administrador de OpenLDAP. Sin embargo, dado que vamos a administrar otros usuarios aparte del administrador LDAP, debe crear un DN base para usuarios y grupos.

Por lo tanto, cree un archivo de formato de intercambio LDAP () con el siguiente contenido y utilícelo para crear el DN base de usuario/grupo. Asegúrese de reemplazar el nombre de dominio en consecuencia. `ldif`

`nano user_group_base.ldif`

```
dn: ou=people,dc=cibergrupo1,dc=cibergrupo1,dc=com
objectClass: organizationalUnit
ou: people
```

```
dn: ou=group,dc=cibergrupo1,dc=cibergrupo1,dc=com
objectClass: organizationalUnit
```

```
ou: group
```

Agregar usuarios y grupos DN base a la base de datos SLAPD

Una vez que haya creado un archivo `ldif` para usuarios y grupos base DN, puede rellenar la base de datos `slapd` con esta información utilizando el comando como se muestra a continuación; `ldapadd`

```
ldapadd -x -D cn=admin,dc=cibergrupo1,dc=cibergrupo1,dc=com -W -f
user_group_base.ldif
```

Cuando se le solicite, introduzca la contraseña de administrador LDAP establecida anteriormente. Y se hará solo lo siguiente:

Enter LDAP Password: admin password

```
adding new entry "ou=people,dc=cibergrupo1,dc=cibergrupo1,dc=com"
```

```
adding new entry "ou=group,dc=ldapmaster,dc=kifarunix-demo,dc=com"
```

5.7. Crear cuentas de usuario LDAP

Para agregar cuentas de usuario LDAP al servidor LDAP, se debe crear un archivo LDIF que contenga la definición de atributos para los usuarios.

Para agregar un usuario con una contraseña, debe generar el hash de contraseña del usuario mediante el comando `slappasswd`

```
New password: qazwsxedc123
```

```
Re-enter new password: qazwsxedc123Y
```

```
{SSHA}m64fb1FKjSzsZ3126aAkYVHkzBdczXt6
```

También puede crear una contraseña de usuario utilizando el comando después de crear el usuario. Consulte la sección a continuación sobre Restablecimiento de contraseña de usuario. `ldappasswd`

A continuación, cree un nuevo archivo `ldif` de usuario que contenga la definición de atributos para el usuario como se muestra a continuación.

nano new_user.ldif

```
dn: uid=admin,ou=people,dc=cibergeupo1,dc=cibergrupo1,dc=com
```

```
objectClass: inetOrgPerson
```

```
objectClass: posixAccount
```

```
objectClass: shadowAccount
```

```
uid: LDAP
```

```
cn: LDAP
```

```
givenName: grupo1
```

```
sn: Ramoneda
```

```
userPassword: {SSHA}m64fb1FKjSzsZ3126aAkYVHkzBdczXt6
```

```
loginShell: /bin/bash
```

```
uidNumber: 10000
```

```
gidNumber: 10000
```

```
homeDirectory: /home/LDAP
```

```
shadowMax: 60
```

```
shadowMin: 1
```

```
shadowWarning: 7
```

```
shadowInactive: 7
```

```
shadowLastChange: 0
```

```
dn: cn=admin,ou=group,dc=cibergrupo1,dc=cibergrupo1,dc=com
```

```
objectClass: posixGroup
```

```
cn: admin
```

```
gidNumber: 10000
```

```
memberUid: admin
```

```
GNU nano 5.4 new_user.ldif
dn: uid=liherLDAP,ou=people,dc=debianWeb,dc=cibergrupo2,dc=com
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: liherLDAP
cn: liherLDAP
givenName: Liher
sn: Ramoneda
userPassword: {SSHA}m64fb1FKjSzsZ3l26aAkYVHkzBdczXt6
loginShell: /bin/bash
uidNumber: 10000
gidNumber: 10000
homeDirectory: /home/liherLDAP
shadowMax: 60
shadowMin: 1
shadowWarning: 7
shadowInactive: 7
shadowLastChange: 0

dn: cn=liherLDAP,ou=group,dc=debianWeb,dc=cibergrupo2,dc=com
objectClass: posixGroup
cn: liherLDAP
gidNumber: 10000
memberUid: liherLDAP

```

5.8. Agregar usuarios a la base de datos SLAPD

Una vez que haya creado los usuarios con sus atributos en un archivo LDIF, puede agregarlos a la base de datos mediante el comando `ldapadd`

```
ldapadd -x -D cn=admin,dc=ldapmaster,dc=kifarunix-demo,dc=com -W -f new_user.ldif
Cuando se le solicite, introduzca la contraseña de administrador de LDAP.
Enter LDAP admin Password: qazwsxedc123
adding new entry "uid=admin,ou=people,dc=cibergrupo1,dc=cibergrupo1,dc=com"
```

```
adding new entry "cn=admin,ou=group,dc=cibergrupo1,dc=cibergrupo1,dc=com"
```

```
root@debianWeb:~# ldapadd -x -D cn=admin,dc=debianWeb,dc=cibergrupo2,dc=com -W -f new_user.ldif
Enter LDAP Password:
adding new entry "uid=liherLDAP,ou=people,dc=debianWeb,dc=cibergrupo2,dc=com"
adding new entry "cn=liherLDAP,ou=group,dc=debianWeb,dc=cibergrupo2,dc=com"
```

Para enumerar todos los usuarios LDAP bajo un DN base, simplemente use el comando `ldapsearch`

```
ldapsearch -x -LLL -b "dc=ldapmaster,dc=kifarunix-demo,dc=com"
```

```
root@debianWeb:~# ldapsearch -x -LLL -b "dc=debianWeb,dc=cibergrupo2,dc=com"
dn: dc=debianWeb,dc=cibergrupo2,dc=com
objectClass: top
objectClass: dcObject
objectClass: organization
o: cibergrupo2.com
dc: debianWeb

dn: ou=people,dc=debianWeb,dc=cibergrupo2,dc=com
objectClass: organizationalUnit
ou: people

dn: ou=group,dc=debianWeb,dc=cibergrupo2,dc=com
objectClass: organizationalUnit
ou: group

dn: uid=liherLDAP,ou=people,dc=debianWeb,dc=cibergrupo2,dc=com
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: liherLDAP
cn: liherLDAP
givenName: Liher
sn: Ramoneda
loginShell: /bin/bash
uidNumber: 10000
gidNumber: 10000
homeDirectory: /home/liherLDAP
shadowMax: 60
shadowMin: 1
shadowWarning: 7
shadowInactive: 7
shadowLastChange: 0

dn: cn=liherLDAP,ou=group,dc=debianWeb,dc=cibergrupo2,dc=com
objectClass: posixGroup
cn: liherLDAP
gidNumber: 10000
memberUid: liherLDAP
```

Para enumerar atributos específicos del ,objectClass

`ldapsearch -x -LLL -b "dc=cibergrupo1,dc=cibergrupo1,dc=com" '(objectclass=*)' uid givenName sn`

```
root@debianWeb:~# ldapsearch -x -LLL -b "dc=debianWeb,dc=cibergrupo2,dc=com" '(objectclass=*)' uid givenName sn
dn: dc=debianWeb,dc=cibergrupo2,dc=com

dn: ou=people,dc=debianWeb,dc=cibergrupo2,dc=com

dn: ou=group,dc=debianWeb,dc=cibergrupo2,dc=com

dn: uid=liherLDAP,ou=people,dc=debianWeb,dc=cibergrupo2,dc=com
uid: liherLDAP
givenName: Liher
sn: Ramoneda

dn: cn=liherLDAP,ou=group,dc=debianWeb,dc=cibergrupo2,dc=com
```

Esto imprimirá la identificación de usuario, nombres y apellidos. Por supuesto, puede pasar la salida a herramientas de procesamiento de texto como grep para extraer los atributos que necesita.


```
ldapsearch -x -LLL -b "dc=cibergrupo1,dc=cibergrupo1,dc=com" '(objectclass=*)' uid
givenName sn | grep -vE 'uid=|dn:'
```

```
root@debianWeb:~# ldapsearch -x -LLL -b "dc=debianWeb,dc=cibergrupo2,dc=com" '(objectclass=*)' uid givenName sn | grep -vE 'uid=|dn:'
uid: liherLDAP
givenName: Liher
sn: Ramoneda
```

5.9. Configurar OpenLDAP con SSL/TLS

Generar certificados SSL/TLS

En esta guía, vamos a utilizar certificados autofirmados. También puede utilizar certificados SSL/TLS comerciales de su CA de confianza.

Para configurar el servidor OpenLDAP con certificado SSL/TLS, necesita un servidor y un archivo `.CA certificate certificateserver certificate key`

Cree un directorio para almacenar los certificados.

```
mkdir -p /etc/ssl/openldap/{private,certs,newcerts}
```

Una vez que haya creado los directorios anteriores, abra el archivo de configuración y establezca el directorio para almacenar certificados y claves SSL / TLS en la sección `/usr/lib/ssl/openssl.cnf` [CA_default]

```
nano /usr/lib/ssl/openssl.cnf
```

```
...
```

```
[ CA_default ]
```

```
#dir      = ./demoCA          # Where everything is kept
dir       = /etc/ssl/openldap
certs     = $dir/certs        # Where the issued certs are kept
crl_dir   = $dir/crl          # Where the issued crl are kept
database  = $dir/index.txt    # database index file.
...
```

```
GNU nano 5.4 /usr/lib/ssl/openssl.cnf
#
# OpenSSL example configuration file.
# This is mostly being used for generation of certificate requests.
#
# Note that you can include other files from the main configuration
# file using the .include directive.
#.include filename
#
# This definition stops the following lines choking if HOME isn't
# defined.
HOME            = .
#
# Extra OBJECT IDENTIFIER info:
#oid_file        = $ENV::HOME/.oid
#oid_section     = new_oids
#
# System default
openssl_conf = default_conf
#
# To use this configuration file with the "-extfile" option of the
# "openssl x509" utility, name here the section containing the
# X.509v3 extensions to use:
# extensions     =
# (Alternatively, use a configuration file that has only
# X.509v3 extensions in its main [= default] section.)
#
[ new_oids ]
#
# We can add new OIDs in here for use by 'ca', 'req' and 'ts'.
# Add a simple OID like this:
# testoid1=1.2.3.4
# Or use config file substitution like this:
# testoid2=${testoid1}.5.6
#
# Policies used by the TSA examples.
tsa_policy1 = 1.2.3.4.1
tsa_policy2 = 1.2.3.4.5.6
tsa_policy3 = 1.2.3.4.5.7
#
#####
[ ca ]
default_ca = CA_default # The default ca section
#
#####
[ CA_default ]
#
#dir          = ./demoCA # Where everything is kept
#dir          = /etc/ssl/openssl[]
#certs        = $dir/certs # Where the issued certs are kept
#crl_dir       = $dir/crl # Where the issued crl are kept
#database     = $dir/index.txt # database index file.
#unique_subject = no # Set to 'no' to allow creation of
# several certs with same subject.
```

También necesita algunos archivos para realizar un seguimiento de los certificados firmados.

```
echo "1001" > /etc/ssl/openssl/serial
```

```
touch /etc/ssl/openssl/index.txt
```

Cree un archivo de clave de CA ejecutando el siguiente comando. Cuando se le solicite, escriba la frase de contraseña. Password=12345678

```
openssl genrsa -aes256 -out /etc/ssl/openssl/private/cakey.pem 2048
```

Para quitar la frase de contraseña de la clave de CA;

```
openssl rsa -in /etc/ssl/openssl/private/cakey.pem -out
/etc/ssl/openssl/private/cakey.pem
```

Cree el certificado de CA. Asegúrese de establecer el común para que coincida con el FQDN del servidor.

```
openssl req -new -x509 -days 3650 -key /etc/ssl/openssl/private/cakey.pem -out /etc/ssl/openssl/certs/cacert.pem
```

```
root@debianWeb:~# openssl req -new -x509 -days 3650 -key /etc/ssl/openssl/private/cakey.pem -out /etc/ssl/openssl/certs/cacert.pem
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ES
State or Province Name (full name) [Some-State]:VIZCAYA
Locality Name (eg, city) []:DURANGO
Organization Name (eg, company) [Internet Widgits Pty Ltd]:cibergrupo2
Organizational Unit Name (eg, section) []:automon
Common Name (e.g. server FQDN or YOUR name) []:debianWeb.cibergrupo2.com
Email Address []:
root@debianWeb:~#
```

A continuación, genere la clave del servidor LDAP; Password=12345678

```
openssl genrsa -aes256 -out /etc/ssl/openssl/private/ldapserver-key.key 2048
```

Elimine la frase de contraseña de clave asignada. Password=qazwsxedc123

```
openssl rsa -in /etc/ssl/openssl/private/ldapserver-key.key -out /etc/ssl/openssl/private/ldapserver-key.key
```

Genere la solicitud de firma de certificado (CSR). Asegúrese de configurar los mismos detalles que al generar el archivo de certificado de CA anterior.

```
openssl req -new -key /etc/ssl/openssl/private/ldapserver-key.key -out /etc/ssl/openssl/certs/ldapserver-cert.csr
```

```
root@debianWeb:~# openssl req -new -key /etc/ssl/openssl/private/ldapserver-key.key -out /etc/ssl/openssl/certs/ldapserver-cert.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ES
State or Province Name (full name) [Some-State]:VIZCAYA
Locality Name (eg, city) []:DURANGO
Organization Name (eg, company) [Internet Widgits Pty Ltd]:cibergrupo2
Organizational Unit Name (eg, section) []:automon
Common Name (e.g. server FQDN or YOUR name) []:debianWeb.cibergrupo2.com
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:12345678
An optional company name []:
root@debianWeb:~#
```

Genere el certificado del servidor LDAP y fírmelo con la clave de CA y el certificado generado anteriormente.

```
openssl ca -keyfile /etc/ssl/openldap/private/cakey.pem -cert
/etc/ssl/openldap/certs/cacert.pem -in /etc/ssl/openldap/certs/ldapserver-cert.csr -out
/etc/ssl/openldap/certs/ldapserver-cert.crt
```

```
root@debianWeb:~# openssl ca -keyfile /etc/ssl/openldap/private/cakey.pem -cert /etc/ssl/openldap/certs/cacert.pem -in /etc/ssl/openldap/certs/
ldapserver-cert.csr -out /etc/ssl/openldap/certs/ldapserver-cert.crt
Using configuration from /usr/lib/ssl/openssl.cnf
Check that the request matches the signature
Signature ok
Certificate Details:
  Serial Number: 4097 (0x1001)
  Validity
    Not Before: Feb 23 21:50:35 2022 GMT
    Not After : Feb 23 21:50:35 2023 GMT
  Subject:
    countryName           = ES
    stateOrProvinceName   = VIZCAYA
    organizationName      = ciberggrupo2
    organizationalUnitName = automon
    commonName            = debianWeb.ciberggrupo2.com
  X509v3 extensions:
    X509v3 Basic Constraints:
      CA:FALSE
  Netscape Comment:
    OpenSSL Generated Certificate
  X509v3 Subject Key Identifier:
    A9:CE:0D:94:93:04:BB:84:11:B9:9B:60:91:4B:00:1F:59:E0:1D:07
  X509v3 Authority Key Identifier:
    keyid:CE:AD:01:8B:7F:4A:13:DF:15:88:0B:19:FB:7E:27:E2:66:0F:30:D3

Certificate is to be certified until Feb 23 21:50:35 2023 GMT (365 days)
Sign the certificate? [y/n]y

1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
root@debianWeb:~#
```

Para comprobar el servidor LDAP en contra de la CA;
openssl verify -CAfile /etc/ssl/openldap/certs/cacert.pem
/etc/ssl/openldap/certs/ldapserver-cert.crt

```
-----
```

```
/etc/ssl/openldap/certs/ldapserver-cert.crt: OK
```

Ahora, tenemos el archivo de certificado de CA, el certificado de servidor y el archivo de clave de servidor en los siguientes directorios respectivos.

```
/etc/ssl/openldap/certs/cacert.pem
/etc/ssl/openldap/certs/ldapserver-cert.crt
/etc/ssl/openldap/private/ldapserver-key.key
```

```
root@debianWeb:~# ls /etc/ssl/openldap/certs/
cacert.pem  ldapserver-cert.crt  ldapserver-cert.csr
root@debianWeb:~# ls /etc/ssl/openldap/
certs/  index.txt  index.txt.attr  index.txt.old  newcerts/  private/  serial  serial.old
root@debianWeb:~# ls /etc/ssl/openldap/private/
cakey.pem  ldapserver-key.key
root@debianWeb:~#
```

A continuación, establezca la propiedad del directorio de certificados OpenLDAP en usuario.openldap

```
chown -R openldap: /etc/ssl/openldap/
```

Actualizar certificados TLS de OpenLDAP Server

A continuación, debe actualizar los certificados TLS de OpenLDAP Server. Por lo tanto, cree un archivo LDIF para definir los atributos TLS como se muestra a continuación;

```
nano ldap-tls.ldif
```

```
dn: cn=config
changetype: modify
add: olcTLSCACertificateFile
olcTLSCACertificateFile: /etc/ssl/openldap/certs/cacert.pem
-
replace: olcTLSCertificateFile
olcTLSCertificateFile: /etc/ssl/openldap/certs/ldapserver-cert.crt
-
replace: olcTLSCertificateKeyFile
olcTLSCertificateKeyFile: /etc/ssl/openldap/private/ldapserver-key.key
```



```
192.168.197.129 - PuTTY
GNU nano 5.4 ldap-tls.ldif
dn: cn=config
changetype: modify
add: olcTLSCACertificateFile
olcTLSCACertificateFile: /etc/ssl/openldap/certs/cacert.pem
-
replace: olcTLSCertificateFile
olcTLSCertificateFile: /etc/ssl/openldap/certs/ldapserver-cert.crt
-
replace: olcTLSCertificateKeyFile
olcTLSCertificateKeyFile: /etc/ssl/openldap/private/ldapserver-key.key
[]
```

Reemplace las ubicaciones de sus certificados y archivos de claves en consecuencia. Para modificar estas entradas en la base de datos LDAP, utilice el comando como se muestra a continuación; ldapmodify

```
ldapmodify -Y EXTERNAL -H ldapi:/// -f ldap-tls.ldif
```

```
.....
```

```
SASL/EXTERNAL authentication started
```

```
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
```

```
SASL SSF: 0
```

```
modifying entry "cn=config"
```

```
.....
```

COMPROBACIONES*** Para verificar que los archivos están en su lugar;

```
slapcat -b "cn=config" | grep -E "olcTLS"
```

```
olcTLSCACertificateFile: /etc/ssl/openldap/certs/cacert.pem
```

```
olcTLSCertificateFile: /etc/ssl/openldap/certs/ldapserver-cert.crt
```

```
olcTLSCertificateKeyFile: /etc/ssl/openldap/private/ldapserver-key.key
```

Para comprobar la validez de la configuración LDAP, ejecute el siguiente comando;

```
slaptest -u
```

```
config file testing succeeded
```

```
*****
```

A continuación, abra el archivo de configuración y cambie la ubicación del certificado de CA./etc/ldap/ldap.conf

```
nano /etc/ldap/ldap.conf
```

```
...
```

```
# TLS certificates (needed for GnuTLS)
```

```
#TLS_CACERT /etc/ssl/certs/ca-certificates.crt
```

```
TLS_CACERT /etc/ssl/openldap/certs/cacert.pem
```

```
GNU nano 5.4 /etc/ldap/ldap.conf
#
# LDAP Defaults
#
# See ldap.conf(5) for details
# This file should be world readable but not world writable.
#BASE    dc=example,dc=com
#URI      ldap://ldap.example.com ldap://ldap-provider.example.com:666
#SIZELIMIT    12
#TIMELIMIT    15
#DEREF        never
# TLS certificates (needed for GnuTLS)
#TLS_CACERT    /etc/ssl/certs/ca-certificates.crt
TLS_CACERT    /etc/ssl/openldap/certs/cacert.pem
```

Reinicie el demonio OpenLDAP.

```
systemctl restart slapd
```

5.10. Comprobar la conectividad TLS para LDAP

Para verificar la conectividad TLS de OpenLDAP, ejecute el siguiente comando. Si la conexión está bien, debe obtener la salida, `.anonymous`

```
ldapwhoami -H ldap://cibergrupo2.com -x -ZZ
anonymous
```

```
-----
```

```
ldapwhoami -H ldapi:/// -x -ZZ
anonymous
```

5.11. Deshabilitar el acceso anónimo a OpenLDAP

Deshabilitar el acceso anónimo a OpenLDAP de tal manera que necesite autenticarse para poder acceder a LDAP;

```
nano disable-anon.ldif
```

```
.....
dn: cn=config
changetype: modify
add: olcDisallows
olcDisallows: bind_anon
```

```
dn: cn=config
changetype: modify
add: olcRequires
olcRequires: authc
```

```
dn: olcDatabase={-1}frontend,cn=config
changetype: modify
add: olcRequires
```

```
olcRequires: authc
```

```
GNU nano 5.4                                disable-anon.ldif *
dn: cn=config
changetype: modify
add: olcDisallows
olcDisallows: bind_anon

dn: cn=config
changetype: modify
add: olcRequires
olcRequires: authc

dn: olcDatabase={-1}frontend,cn=config
changetype: modify
add: olcRequires
olcRequires: authc
```

Actualizar la base de datos slapd;
ldapadd -Y EXTERNAL -H ldapi:/// -f disable-anon.ldif

```
root@debianWeb:~# ldapadd -Y EXTERNAL -H ldapi:/// -f disable-anon.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "cn=config"

modifying entry "cn=config"

modifying entry "olcDatabase={-1}frontend,cn=config"

root@debianWeb:~#
```

Pruebe la autenticación anónima.

ldapwhoami -H ldapi:/// -x -ZZ

```
....
ldap_bind: Inappropriate authentication (48)
    additional info: anonymous bind disallowed
....
```


Autenticación de prueba

```
ldapwhoami -H ldapi:/// -x -ZZ -D "uid=mibeyam,ou=people,dc=ldapmaster,dc=kifarunix-  
demo,dc=com" -x -W
```

Enter LDAP Password:

```
dn:uid=mibeyam,ou=people,dc=ldapmaster,dc=kifarunix-demo,dc=com
```

NO FUNCIONA

6. Instalación Tomcat

Paso 1 – Instalar Java

```
sudo apt update
```

```
sudo apt install default-jdk -y
```

Compruebe la versión actual activa de Java:

```
java -version
```

```
root@debianWeb:~# java -version  
openjdk version "11.0.14" 2022-01-18  
OpenJDK Runtime Environment (build 11.0.14+9-post-Debian-1deb11u1)  
OpenJDK 64-Bit Server VM (build 11.0.14+9-post-Debian-1deb11u1, mixed mode, sharing)  
root@debianWeb:~#
```

Paso 2 – Crear usuario Tomcat

Para crear una nueva cuenta y la carpeta tomcat, escriba:

```
mkdir /opt/tomcat
```

```
cd /opt/tomcat
```

```
useradd -r -m -U -d /opt/tomcat -s /bin/false tomcat
```

```
root@debianWeb:~# useradd -m -d /opt/tomcat -U -s /bin/false tomcat  
root@debianWeb:~# _
```

El comando anterior creará un usuario y un grupo con el nombre "" en su sistema.tomcat

Step 3 – Install Tomcat on Debian 10

wget <https://downloads.apache.org/tomcat/tomcat-9/v9.0.58/bin/apache-tomcat-9.0.58.tar.gz>

```
root@debianWeb:~# wget https://downloads.apache.org/tomcat/tomcat-10/v10.0.16/bin/apache-tomcat-10.0.16.tar.gz
--2022-02-14 12:58:35-- https://downloads.apache.org/tomcat/tomcat-10/v10.0.16/bin/apache-tomcat-10.0.16.tar.gz
Resolviendo downloads.apache.org (downloads.apache.org)... 135.181.214.104, 88.99.95.219, 2a01:4f8:10a:201a::2, ...
Conectando con downloads.apache.org (downloads.apache.org) [135.181.214.104]:443... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 11906902 (11M) [application/x-gzip]
Grabando a: «apache-tomcat-10.0.16.tar.gz»

apache-tomcat-10.0.16.ta 100%[=====] 11,35M 10,9MB/s en 1,0s
2022-02-14 12:58:37 (10,9 MB/s) - «apache-tomcat-10.0.16.tar.gz» guardado [11906902/11906902]
```

Después de descargar el archivo de archivo, extraiga el archivo en el directorio de inicio de tomcat /opt/tomcat omitiendo la carpeta principal.

tar -xvzf apache-tomcat-9.0.58.tar.gz

A continuación, establezca los permisos de archivo adecuados.

sudo chown -R tomcat:tomcat /opt/tomcat/

sudo chmod -R u+x /opt/tomcat/bin

chmod -R 777 /opt/tomcat

```
root@debianWeb:~# chown -R tomcat:tomcat /opt/tomcat/
root@debianWeb:~# chmod -R u+x /opt/tomcat/bin
root@debianWeb:~# _
```

Ahora tiene la última aplicación Tomcat en su sistema.

6. Update .bashrc file

Open .bashrc file in a text editor.

nano ~/.bashrc

Add/modify the following lines in .bashrc file.

export JAVA_HOME=/usr/lib/jvm/java-1.11.0-openjdk-amd64

export CATALINA_HOME=/opt/tomcat/apache-tomcat-9.0.58

Update JAVA_HOME with the latest one on your system. You can find the installed JVM filename with following command.

\$ ls /usr/lib/jvm/

Save and exit the file. Run the following command to apply changes.

~/.bashrc

6.1. Test Tomcat installation

Run the following command to start Tomcat server.

```
$CATALINA_HOME/bin/startup.sh
```

You will see the following output

```
Using CATALINA_BASE: /opt/tomcat
```

```
Using CATALINA_HOME: /opt/tomcat
```

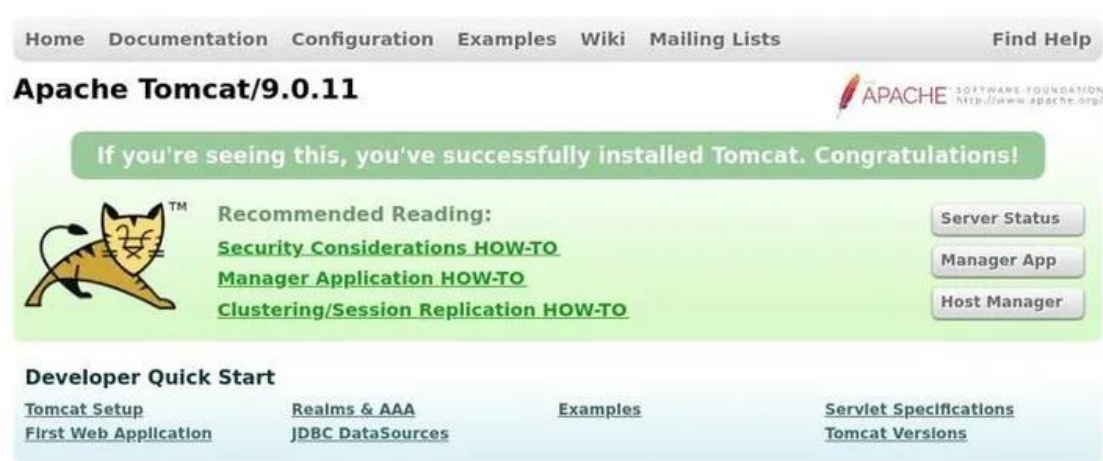
```
Using CATALINA_TMPDIR: /opt/tomcat/temp
```

```
Using JRE_HOME: /usr/lib/jvm/java-7-openjdk-amd64/
```

```
Using CLASSPATH: /opt/tomcat/bin/bootstrap.jar:/opt/tomcat/bin/tomcat-juli.jar
```

Tomcat started

Open browser and go to <http://www.cibergrupo2.com:8080> since Tomcat server runs on port 8080. You will be able to see the default tomcat page.



Please note, at this point you will be able to access tomcat only from the machine where it has been installed. If you want to be able to access this server from other systems, you need to open port 8080 in your firewall using the following command

```
$ sudo ufw allow 8080/tcp
```

```
$ sudo ufw allow 8443/tcp
```

In this article, we have shown how to install tomcat in Ubuntu. Apache tomcat is a very powerful web server for hosting Java-based applications. It is used by millions of websites all over the world.

7. Secure Tomcat

1. Crear una nueva keystore:

Debemos abrir un terminal y navegar hasta el directorio donde deseamos tener el keystore. Debemos recordar el alias que utilizaremos, ya que lo necesitaremos más tarde.

```
cd /etc/apache2/ssl /cibergrupo1/  
keytool -genkey -alias cibergrupo1 -keyalg RSA -keystore KeyStore.jks -keysize 2048
```

```
root@debianWeb:~# $JAVA_HOME/bin/keytool -genkey -alias cibergrupo2 -keyalg RSA -keystore KeyStore.jks -keysize 2048  
Introduzca la contraseña del almacén de claves:  
Volver a escribir la contraseña nueva:  
¿Cuáles son su nombre y su apellido?  
[Unknown]: cibergrupo2.com  
¿Cuál es el nombre de su unidad de organización?  
[Unknown]: automon  
¿Cuál es el nombre de su organización?  
[Unknown]: grupo2  
¿Cuál es el nombre de su ciudad o localidad?  
[Unknown]: vizcaya  
¿Cuál es el nombre de su estado o provincia?  
[Unknown]: durango  
¿Cuál es el código de país de dos letras de la unidad?  
[Unknown]: ES  
¿Es correcto CN=cibergrupo2.com, OU=automon, O=grupo2, L=vizcaya, ST=durango, C=ES?  
[no]: si  
root@debianWeb:~# _
```

2. Generar un CSR a partir de la keystore:

```
keytool -certreq -alias cibergrupo1 -keystore KeyStore.jks -file cibergrupo1.csr
```

```
root@debianWeb:~# $JAVA_HOME/bin/keytool -certreq -alias cibergrupo2 -keystore KeyStore.jks -file cibergrupo2.csr  
Introduzca la contraseña del almacén de claves:  
root@debianWeb:~#
```

5. Importamos el certificado de nuestro dominio

Debemos usar el mismo alias que utilizamos al generar la clave privada.

```
keytool -import -keystore KeyStore.jks -file cibergrupo1.crt
```

```
Válido desde: Mon Feb 21 21:05:51 CET 2022 hasta: Tue Feb 21 21:05:51 CET 2023
Huellas digitales del certificado:
    SHA1: C5:8D:21:D9:1F:96:8A:D8:0D:2A:A1:25:7B:09:1C:0E:F6:3D:4E:68
    SHA256: EB:CA:91:05:A0:0B:78:84:92:6A:F9:A1:19:79:DE:16:86:CE:8A:FA:52:43:60:84:3B:57:F2:85
:14:92:95:0E
Nombre del algoritmo de firma: SHA256withRSA
Algoritmo de clave pública de asunto: Clave RSA de 2048 bits
Versión: 3

Extensiones:

#1: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
  KeyIdentifier [
    0000: 4D 5F B4 71 BC CE F3 4C 8B DA 3F DA B3 8B CE 81 M_.q...L...?.....
    0010: 7B 4F 14 D6 .0..
  ]
]

#2: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
  CA:true
  PathLen:2147483647
]

#3: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
  KeyIdentifier [
    0000: 4D 5F B4 71 BC CE F3 4C 8B DA 3F DA B3 8B CE 81 M_.q...L...?.....
    0010: 7B 4F 14 D6 .0..
  ]
]

¿Confiar en este certificado? [no]: si
Se ha agregado el certificado al almacén de claves
root@debianWeb:~# $JAVA_HOME/bin/keytool -import -keystore KeyStore.jks -file /etc/apache2/ssl/ciber
grupo2/cibergrupo2.crt _
```

En este punto, ya tendremos nuestra keystore completa y lista para usar en su servidor Tomcat.

```
root@debianWeb:~# nano /opt/tomcat/apache-tomcat-10.0.16/conf/server.xml
```

```
nano /opt/tomcat/apache-tomcat-9.0.58/conf/server.xml
<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true" maxThreads="150"
scheme="https" secure="true"
keystoreFile="/etc/apache2/cibergrupo1/KeyStore.jks" keystorePass="qazwsxedc12
3"
clientAuth="false" sslProtocol="TLS" sslVerifyClient="optional"

sslEnabledProtocols="TLSv1.2,TLSv1.1,SSLv2Hello"/>
```

```
GNU nano 5.4 /opt/tomcat/apache-tomcat-9.0.58/conf/server.xml
Documentation at /docs/config/service.html
-->
<Service name="Catalina">

  <!--The connectors can use a shared executor, you can define one or more named thread pools-->
  <!--
  <Executor name="tomcatThreadPool" namePrefix="catalina-exec-"
    maxThreads="150" minSpareThreads="4"/>
  -->

  <!-- A "Connector" represents an endpoint by which requests are received
  and responses are returned. Documentation at :
  Java HTTP Connector: /docs/config/http.html
  Java AJP Connector: /docs/config/ajp.html
  APR (HTTP/AJP) Connector: /docs/apr.html
  Define a non-SSL/TLS HTTP/1.1 Connector on port 8080
  -->
  <Connector port="8080" protocol="HTTP/1.1"
    connectionTimeout="20000"
    redirectPort="8443" />
    <Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
      maxThreads="150" scheme="https" secure="true"
      keystoreFile="/etc/apache2/ssl/cibergrupo2/KeyStore.jks" keystorePass="1234"
      clientAuth="false" sslProtocol="TLS" sslVerifyClient="optional"
      sslEnabledProtocols="TLSv1.2,TLSv1.1,SSLv2Hello"/>

  <!-- A "Connector" using the shared thread pool-->
  <!--
  <Connector executor="tomcatThreadPool"
    port="8080" protocol="HTTP/1.1"
    connectionTimeout="20000"
    redirectPort="8443" />
  -->
```

Reiniciar servicio tomcat

```
cd /opt/tomcat/apache-tomcat-9.0.58/bin/
./shutdown.sh
./startup.sh
```

```
root@debianWeb:~# cd /opt/tomcat/apache-tomcat-9.0.58/bin/
root@debianWeb:/opt/tomcat/apache-tomcat-9.0.58/bin# ./shutdown.sh
Using CATALINA_BASE:   /opt/tomcat/apache-tomcat-9.0.58
Using CATALINA_HOME:   /opt/tomcat/apache-tomcat-9.0.58
Using CATALINA_TMPDIR: /opt/tomcat/apache-tomcat-9.0.58/temp
Using JRE_HOME:        /usr/lib/jvm/java-1.11.0-openjdk-amd64
Using CLASSPATH:       /opt/tomcat/apache-tomcat-9.0.58/bin/bootstrap.jar:/opt/tomcat/apache-tomcat-9.0.58/bin/tomcat-juli.jar
Using CATALINA_OPTS:
NOTE: Picked up JDK_JAVA_OPTIONS:  --add-opens=java.base/java.lang=ALL-UNNAMED --add-opens=java.base/java.io=ALL-UNNAMED --add-opens=java.base/java.util=ALL-UNNAMED --add-opens=java.base/java.util.concurrent=ALL-UNNAMED --add-opens=java.rmi/sun.rmi.transport=ALL-UNNAMED
root@debianWeb:/opt/tomcat/apache-tomcat-9.0.58/bin# ./startup.sh
Using CATALINA_BASE:   /opt/tomcat/apache-tomcat-9.0.58
Using CATALINA_HOME:   /opt/tomcat/apache-tomcat-9.0.58
Using CATALINA_TMPDIR: /opt/tomcat/apache-tomcat-9.0.58/temp
Using JRE_HOME:        /usr/lib/jvm/java-1.11.0-openjdk-amd64
Using CLASSPATH:       /opt/tomcat/apache-tomcat-9.0.58/bin/bootstrap.jar:/opt/tomcat/apache-tomcat-9.0.58/bin/tomcat-juli.jar
Using CATALINA_OPTS:
Tomcat started.
root@debianWeb:/opt/tomcat/apache-tomcat-9.0.58/bin# _
```

Paso 4 – Crear usuario Tomcat

Ahora, configure su tomcat con cuentas de usuario para asegurar el acceso a las páginas de administrador / administrador. Para ello, edite el archivo conf/tomcat-users.xml en su editor y pegue el siguiente código dentro de <tomcat-users> </tomcat-users> etiquetas.

Recomendamos cambiar la contraseña en la siguiente configuración con contraseña de alta seguridad.

```
sudo nano /opt/tomcat/conf/tomcat-users.xml
```

Agregue los siguientes valores. Asegúrese de cambiar la contraseña para el acceso de administrador y administrador.

```
<!-- user manager can access only manager section -->
<role rolename="manager-gui" />
<user username="cibergrupo1" password="qazwsxedc123" roles="manager-gui" />

<!-- user admin can access manager and admin section both -->
<role rolename="admin-gui" />
<user username="cibergrupo1" password="qazwsxedc123" roles="manager-gui,admin-gui" />
```

Paso 5 - Habilitar el acceso remoto a Tomcat

Las aplicaciones predeterminadas Tomcat manager y host-manager solo son accesibles para localhost. Para permitir el acceso a estas páginas desde el sistema remoto, debe modificar los siguientes archivos de configuración. Puede permitir un sistema remoto específico o permitir todo.

Edite el archivo para la aplicación de administrador y administrador de host:context.xml

```
sudo nano /opt/tomcat/webapps/manager/META-INF/context.xml
```

Comenta la sección agregada para la restricción de direcciones IP para permitir conexiones desde cualquier lugar.

```
<Context antiResourceLocking="false" privileged="true" >
  <CookieProcessor className="org.apache.tomcat.util.http.Rfc6265CookieProcessor"
    sameSiteCookies="strict" />
  <!-- <Valve className="org.apache.catalina.valves.RemoteAddrValve"
    allow="127\.\d+\.\d+\.\d+|::1|0:0:0:0:0:0:0:1" /> -->
  ...
</Context>
```

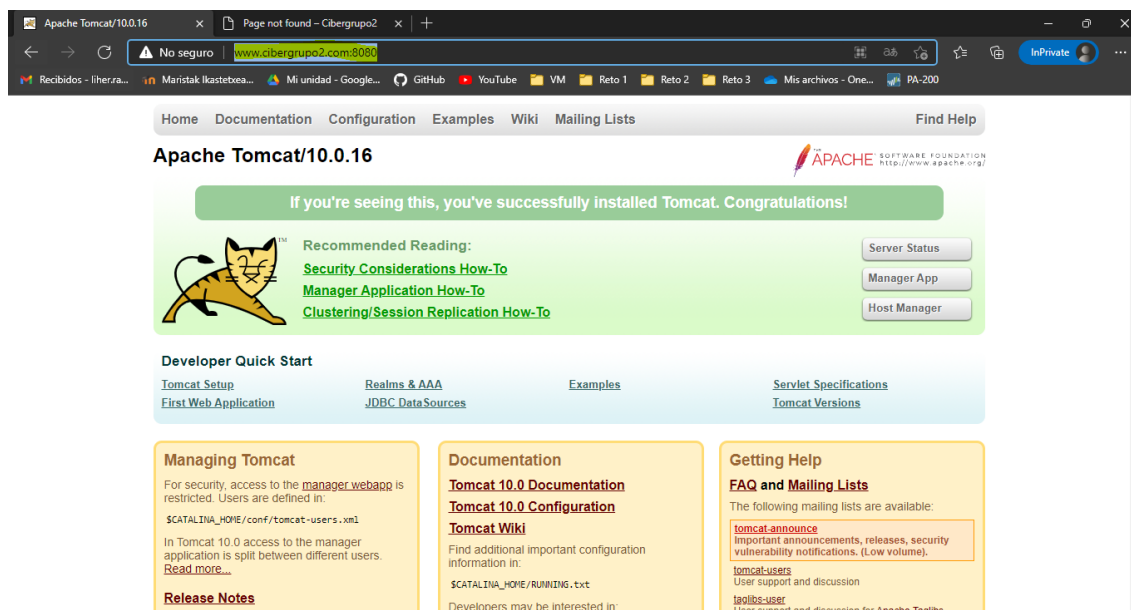
Además, edite el contexto.xml para la interfaz host-manager y comente la sección similar a la anterior.

sudo nano /opt/tomcat/apache-tomcat-9.0.58/webapps/host-manager/META-INF/context.xml

Paso 7 – Acceda a la interfaz web de Tomcat

El servidor Tomcat predeterminado se ejecuta en el puerto 8080. Cómo ha configurado Tomcat en su sistema, puede acceder a la interfaz web desde su sistema. Puede acceder a las interfaces tomcat ingresando la dirección IP de su servidor o un nombre de dominio apuntando a ese servidor, seguido del puerto 8080 en su navegador:

Cambie con la IP del servidor () o el dominio o localhost. www.cibergrupo1.com
<https://www.cibergrupo1.com:8443>



8. CAS Installation Tomcat

apt install git

git clone <https://github.com/apereo/cas-overlay-template.git>

cd cas-overlay-template

Use --refresh-dependencies to force-update SNAPSHOT versions

./gradlew clean build

cd build/

mv build/libs/cas.war /opt/tomcat/apache-tomcat-9.0.58/webapps/

```
root@debianWeb:~/cas-overlay-template# ls
build      docker-build.sh  Dockerfile  docker-run.sh  gradle      gradlew      helm      lombok.config  README.md
build.gradle  docker-compose.yml  docker-push.sh  etc           gradle.properties  gradlew.bat  LICENSE.txt  Procfile      settings.gra
root@debianWeb:~/cas-overlay-template# cd build
root@debianWeb:~/cas-overlay-template# cd build/
root@debianWeb:~/cas-overlay-template# mv build/libs/cas.war /opt/tomcat/apache-tomcat-9.0.58/webapps/
root@debianWeb:~/cas-overlay-template# mv build/libs/cas.war /opt/tomcat/apache-tomcat-9.0.58/webapps/
```

systemctl restart tomcat.service

```
root@debianWeb:~/cas-overlay-template# mv build/libs/cas.war /opt/tomcat/apache-tomcat-9.0.58/webapps/
root@debianWeb:~/cas-overlay-template# cd /opt/tomcat/apache-tomcat-9.0.58/bin/
root@debianWeb:/opt/tomcat/apache-tomcat-9.0.58/bin# ./shutdown.sh
Using CATALINA_BASE:   /opt/tomcat/apache-tomcat-9.0.58
Using CATALINA_HOME:   /opt/tomcat/apache-tomcat-9.0.58
Using CATALINA_TMPDIR: /opt/tomcat/apache-tomcat-9.0.58/temp
Using JRE_HOME:        /usr/lib/jvm/java-1.11.0-openjdk-amd64
Using CLASSPATH:       /opt/tomcat/apache-tomcat-9.0.58/bin/bootstrap.jar:/opt/tomcat/apache-tomcat-9.0.58/bin/tomcat-juli.jar
Using CATALINA_OPTS:
NOTE: Picked up JDK_JAVA_OPTIONS:  --add-opens=java.base/java.lang=ALL-UNNAMED --add-opens=java.base/java.io=ALL-UNNAMED --add-opens=java.base/java.util=ALL-UNNAMED --add-opens=java.base/java.util.concurrent=ALL-UNNAMED --add-opens=java.xml/sun.rmi.transport=ALL-UNNAMED
root@debianWeb:/opt/tomcat/apache-tomcat-9.0.58/bin# ./startup.sh
Using CATALINA_BASE:   /opt/tomcat/apache-tomcat-9.0.58
Using CATALINA_HOME:   /opt/tomcat/apache-tomcat-9.0.58
Using CATALINA_TMPDIR: /opt/tomcat/apache-tomcat-9.0.58/temp
Using JRE_HOME:        /usr/lib/jvm/java-1.11.0-openjdk-amd64
Using CLASSPATH:       /opt/tomcat/apache-tomcat-9.0.58/bin/bootstrap.jar:/opt/tomcat/apache-tomcat-9.0.58/bin/tomcat-juli.jar
Using CATALINA_OPTS:
Tomcat started.
root@debianWeb:/opt/tomcat/apache-tomcat-9.0.58/bin#
```

Ruta	Versión	Nombre a Mostrar	Ejecutándose	Sesiones	Comandos
/	Ninguno especificado	Welcome to Tomcat	true	0	Arrancar Parar Recargar Replegar Expirar sesiones sin trabajar 30 minutos
/cas	Ninguno especificado		true	0	Arrancar Parar Recargar Replegar Expirar sesiones sin trabajar 30 minutos
/docs	Ninguno especificado	Tomcat Documentation	true	0	Arrancar Parar Recargar Replegar Expirar sesiones sin trabajar 30 minutos
/examples	Ninguno especificado	Servlet and JSP Examples	true	0	Arrancar Parar Recargar Replegar Expirar sesiones sin trabajar 30 minutos
/host-manager	Ninguno especificado	Tomcat Host Manager Application	true	0	Arrancar Parar Recargar Replegar Expirar sesiones sin trabajar 30 minutos
/manager	Ninguno especificado	Tomcat Manager Application	true	2	Arrancar Parar Recargar Replegar Expirar sesiones sin trabajar 30 minutos

Editar cas-overlay-template/build.gradle

compile "org.apereo.cas:cas-server-webapp:\${project.appServer}:\${casServerVersion}"
 compile "org.apereo.cas:cas-server-support-ldap:\${project.'cas.version'}"

```

GNU nano 5.4 cas-overlay-template/build.gradle
  imageName = "${project.'containerImageOrg'}:${project.'containerImageName'}:${project.version}"
}

dependencies {
    /**
     * Do NOT modify the lines below or else you will risk breaking dependency management.
     */
    implementation enforcedPlatform("org.apereo.cas:cas-server-support-bom:${project.'cas.version'}")
    implementation platform(org.springframework.boot.gradle.plugin.SpringBootPlugin.BOM_COORDINATES)

    /**
     * CAS dependencies and modules may be listed here.
     */
    /**
     * There is no need to specify the version number for each dependency
     * since versions are all resolved and controlled by the dependency management
     * plugin via the CAS bom.
     */
    implementation "org.apereo.cas:cas-server-core-api-configuration-model"
    implementation "org.apereo.cas:cas-server-webapp-init"

    if (project.hasProperty("casModules")) {
        compile "org.apereo.cas:cas-server-webapp:${project.appServer}:${casServerVersion}"
        compile "org.apereo.cas:cas-server-support-ldap:${project.'cas.version'}"
    }

    def dependencies = project.getProperty("casModules").split(",")
    dependencies.each {
        def projectsToAdd = rootProject.subprojects.findAll {project ->
            project.name == "cas-server-core-${it}" || project.name == "cas-server-support-${it}"
        }
        projectsToAdd.each {implementation it}
    }
}
  
```

Crear el nuevo cas.war de la siguiente manera:

```
cd cas-overlay-template
```

```
ls
```

```
#cas-overlay-template/      ./gradlew clean copyCasConfiguration build
```

```
#cas-overlay-template/      mv cas.war    /opt/tomcat/****/webapss/
```

```
systemctl daemon-reload
```

```
systemctl restart tomcat
```

9. Conclusión

A la hora de montar los servicios principales como la configuración inicial de la máquina, crear tanto la base de datos con mariadb como sus usuarios y la instalación de WordPress y apache no nos ha supuesto ningún problema ya que se disponían conocimientos previos para poder hacerlos.

En cuanto a LDAP, se ha hecho una investigación para adquirir conocimientos sobre esta para poder implementarlo a nuestro servidor. No ha habido ningún tipo de problema en poder hacerlo. también hemos implementado un equipo al dominio y una interfaz web para poder gestionar todo de manera más eficiente y por último lo hemos securizado.

también se ha instalado el servicio de tomcat, el cual era necesario para implementar aplicaciones web realizadas en java. En este caso se ha implementado CAS(Central Authentication Service) como aplicación, que sirve para el SSO(Single Sign-On).

Esta aplicación a supuesto varios problemas a la hora de enlazarla con LDAP y vincularla a los usuarios de la BBDD con lo cual no se ha podido completar en su totalidad.