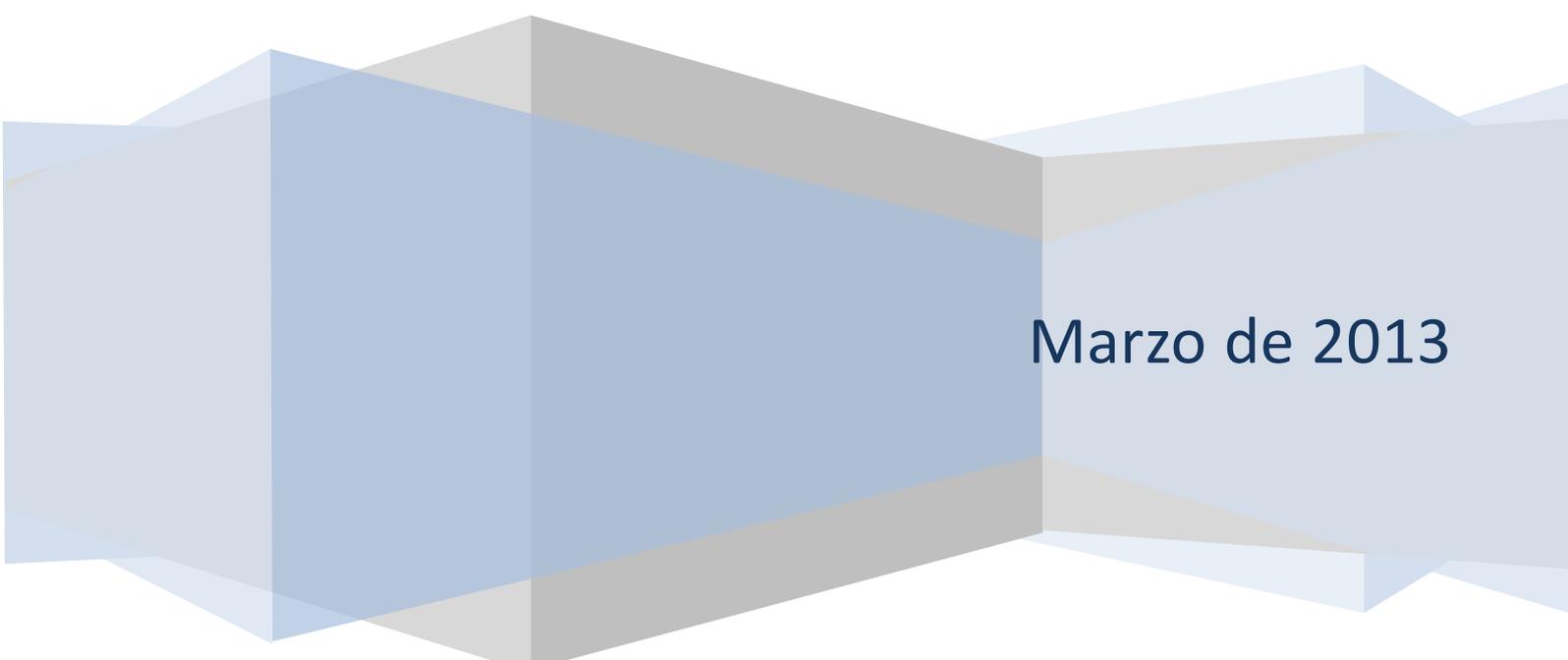


Módulo Superior de Diseño de Aplicaciones Web

# Despliegue de Aplicaciones Web

Tarea 5

José Luis Comesaña Cabeza



Marzo de 2013

Para la realización de la tarea, donde ponga **xxxxx** debes cambiarlo por tu inicial de nombre seguido por tu primer apellido. Así, en caso de llamarte Antonio López, pues deberás usar alopez.

**Para una empresa que opera con su negocio a través de Internet se pide lo siguiente.**

**1. Configura tu servidor con la IP 192.168.200.200 (o si usas otra indica cuál).**

**Instala y configura el servidor de nombres bind para que: Administre el dominio dominioempresa-xxxxx-daw05.local.**

Para conocer nuestra IP local probamos con el comando `ifconfig -a` lo cual nos da esta salida: Nos indica que la IP de nuestro servidor es la `10.0.2.15`, y será la que usaremos para la resolución de los ejercicios de esta tarea. Podríamos obligarle a utilizar otra como la `192.168.200.200` modificando el fichero `/etc/network/interfaces`

```

jose Luis@jose Luis-VirtualBox: ~
jose Luis@jose Luis-VirtualBox:~$ ifconfig -a
eth0      Link encap:Ethernet direcciónHW 08:00:27:ad:1d:f5
          Direc. inet:10.0.2.15 Difus.:10.0.2.255 Másc:255.255.255.0
          Dirección inet6: fe80::a00:27ff:fead:1df5/64 Alcance:Enlace
          ACTIVO DIFUSIÓN FUNCIONANDO MULTICAST MTU:1500 Métrica:1
          Paquetes RX:248 errores:0 perdidos:0 overruns:0 frame:0
          Paquetes TX:271 errores:0 perdidos:0 overruns:0 carrier:0
          colisiones:0 long.colaTX:1000
          Bytes RX:86087 (86.0 KB) TX bytes:48987 (48.9 KB)

lo        Link encap:Bucle local
          Direc. inet:127.0.0.1 Másc:255.0.0.0
          Dirección inet6: ::1/128 Alcance:Anfitrión
          ACTIVO BUCLE FUNCIONANDO MTU:16436 Métrica:1
          Paquetes RX:49 errores:0 perdidos:0 overruns:0 frame:0
          Paquetes TX:49 errores:0 perdidos:0 overruns:0 carrier:0
          colisiones:0 long.colaTX:0
          Bytes RX:4857 (4.8 KB) TX bytes:4857 (4.8 KB)

jose Luis@jose Luis-VirtualBox:~$

```

introduciéndole el contenido:

```

auto lo
iface lo inet loopback auto eth0
iface eth0 inet static
address 192.168.200.200
netmask 255.255.255.0
network 192.168.200.0
broadcast 192.168.200.255
gateway 192.168.200.1

```

Pero no es necesario para los ejercicios que realizamos a continuación, por lo que mantendremos la ofrecida por `ifconfig`.

Primero actualizamos los repositorios del sistema operativo con:

```
apt-get update
```

A continuación actualizamos el sistema operativo:

```
apt-get upgrade
```

Instalamos los paquetes necesarios para el funcionamiento de BIND:

```
apt-get install bind9 bind9utils
```

Verificamos que está instalado y funcionando correctamente:

```
service bind9 status
```

que nos indica que bind9 se está ejecutando

Hacemos una copia de seguridad del archivo que vamos a modificar:

```
cp /etc/bind/named.conf.local{,.original}
```

(esta orden es igual a `cp /etc/bind/named.conf.local /etc/bind/named.conf.original`)

Editamos el fichero `named.conf.local` tecleando:

```
gedit /etc/bind/named.conf.local
```

Y en su interior tecleamos:

```
zone "dominioempresa-jlcomesana-daw05.local"{
    type master;
    file "/var/lib/bind/master/db.dominioempresa-jlcomesana-daw05.local";
};
```

Como el camino indicado no existe, lo creamos con:

```
mkdir /var/lib/bind/master
```

Comprobamos la sintaxis del archivo de configuración tecleando:

```
named-checkconf /etc/bind/named.conf.local
```

Como no aparece nada significa que es correcto sintácticamente, de lo contrario nos indicaría el error producido.

**Crea el registro tipo host tienda (tienda.dominioempresa-xxxxx-daw05.local) que apunte al servidor 192.168.200.200**

Ahora, para completar el punto 1 de la tarea y realizar el punto 2, editamos el fichero que indicamos en el apartado **file** del **named.conf.local**, por lo que tecleamos:

```
gedit /var/lib/bind/master/db.dominioempresa-jlcomesana-daw05.local
```

y le incluimos:

```
$ORIGIN dominioempresa-jlcomesana-daw05.local.
$TTL 86400 ; 1 dia
@      IN      SOA      tienda      postmaster (
        1      ; serie
        6H     ; refresco (6 horas)
        1H     ; reintentos (1 hora)
        2W     ; expira (2 semanas)
        3H     ; mínimo (3 horas)
)
      NS      tienda
tienda IN      A       10.0.2.15
www    IN      A       10.0.2.15
mail   IN      A       10.0.2.16
```

Comprobamos la zona que acabamos de crear (**dominioempresa-jlcomesana-daw05.local**):

```
named-checkzone dominioempresa-jlcomesana-daw05.local /var/cache/bind/db.dominioempresa-jlcomesana-daw05.local
```

Como nos sale todo OK vamos a crear el archivo **/var/cache/bind/db.10.0.2** para la zona inversa:

```
gedit /var/lib/bind/master/db.10.0.2
```

y le introducimos las siguientes órdenes:

```
$ORIGIN 2.0.10.in-addr.arpa.
$TTL 86400 ; 1 dia
@      IN      SOA      tienda      postmaster (
        1      ; serie
        6H     ; refresco (6 horas)
        1H     ; reintentos (1 hora)
        2W     ; expire (2 semanas)
        3H     ; mínimo (3 horas)
)
      NS      tienda.dominioempresa-jlcomesana-daw05.local.
15     PTR     tienda.dominioempresa-jlcomesana-daw05.local.
```

Comprobamos la zona inversa recién creada:

```
named-checkzone 2.0.10.in-addr.arpa /var/cache/bind/db.10.0.2
```

Reiniciamos el servicio:

```
service bind9 restart
```

Esta es la salida del proceso realizado:

```

root@joseluis-VirtualBox: /etc/bind
zone dominioempresa-jlcomesana-daw05.local/IN: loading from master file /var/lib
/bind/master/dominioempresa-jlcomesana-daw05.local failed: file not found
zone dominioempresa-jlcomesana-daw05.local/IN: not loaded due to errors.
root@joseluis-VirtualBox: /etc/bind# named-checkzone dominioempresa-jlcomesana-da
w05.local /var/lib/bind/master/db.dominioempresa-jlcomesana-daw05.local
zone dominioempresa-jlcomesana-daw05.local/IN: loaded serial 1
OK
root@joseluis-VirtualBox: /etc/bind# gedit /var/lib/bind/master/db.dominioempresa
-jlcomesana-daw05.local
root@joseluis-VirtualBox: /etc/bind# named-checkzone dominioempresa-jlcomesana-da
w05.local /var/lib/bind/master/db.dominioempresa-jlcomesana-daw05.local
zone dominioempresa-jlcomesana-daw05.local/IN: loaded serial 1
OK
root@joseluis-VirtualBox: /etc/bind# gedit /var/lib/bind/master/db.10.0.2
root@joseluis-VirtualBox: /etc/bind# named-checkzone 2.0.10.in-addr.arpa /var/lib
/bind/master/db.10.0.2
zone 2.0.10.in-addr.arpa/IN: loaded serial 1
OK
root@joseluis-VirtualBox: /etc/bind# service bind9 restart
* Stopping domain name service... bind9
waiting for pid 827 to die
[ OK ]
* Starting domain name service... bind9
[ OK ]
root@joseluis-VirtualBox: /etc/bind#

```

Revisamos el log para comprobar que todo ha ido bien:

```
tail /var/log/syslog
```

```

root@joseluis-VirtualBox: /etc/bind
* Stopping domain name service... bind9
waiting for pid 3510 to die
[ OK ]
* Starting domain name service... bind9
[ OK ]
root@joseluis-VirtualBox: /etc/bind# tail /var/log/syslog
Mar 31 18:34:25 joseluis-VirtualBox named[3562]: automatic empty zone: 8.B.D.0.1
.0.0.2.IP6.ARPA
Mar 31 18:34:25 joseluis-VirtualBox named[3562]: command channel listening on 12
7.0.0.1#953
Mar 31 18:34:25 joseluis-VirtualBox named[3562]: command channel listening on ::
1#953
Mar 31 18:34:25 joseluis-VirtualBox named[3562]: zone 0.in-addr.arpa/IN: loaded
serial 1
Mar 31 18:34:25 joseluis-VirtualBox named[3562]: zone 127.in-addr.arpa/IN: loade
d serial 1
Mar 31 18:34:25 joseluis-VirtualBox named[3562]: zone 255.in-addr.arpa/IN: loade
d serial 1
Mar 31 18:34:25 joseluis-VirtualBox named[3562]: zone dominioempresa-jlcomesana-
daw05.local/IN: loaded serial 1
Mar 31 18:34:25 joseluis-VirtualBox named[3562]: zone localhost/IN: loaded serla
l 2
Mar 31 18:34:25 joseluis-VirtualBox named[3562]: managed-keys-zone ./IN: loaded
serial 3
Mar 31 18:34:25 joseluis-VirtualBox named[3562]: running
root@joseluis-VirtualBox: /etc/bind#

```

Editamos el fichero `/etc/resolv.conf` para que nuestro servidor resuelva las peticiones DNS:

```
gedit /etc/resolv.conf
```

Cambiamos el primer servidor DNS por la IP del nuestro:

```
nameserver 10.0.2.15
nameserver 8.8.8.8.8
```

Probamos nuestro servidor de nombres:

```
dig dominioempresa-jlcomesana-daw05.local
```

```

root@joseluis-VirtualBox: /etc/bind
;; WHEN: Sun Mar 31 18:00:13 2013
;; MSG SIZE rcvd: 92

root@joseluis-VirtualBox:/etc/bind# dig dominioempresa-jlcomesana-daw05.local

; <<>> DiG 9.8.1-P1 <<>> dominioempresa-jlcomesana-daw05.local
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 39173
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;dominioempresa-jlcomesana-daw05.local. IN A

;; AUTHORITY SECTION:
dominioempresa-jlcomesana-daw05.local. 10800 IN SOA tienda.dominioempresa-jlcomesana-daw05.local. postmaster.dominioempresa-jlcomesana-daw05.local. 1 21600 3600 1209600 10800

;; Query time: 10 msec
;; SERVER: 10.0.2.15#53(10.0.2.15)
;; WHEN: Sun Mar 31 18:03:48 2013
;; MSG SIZE rcvd: 109

root@joseluis-VirtualBox:/etc/bind#

```

Probamos también tienda:

```
dig tienda.dominioempresa-jlcomesana-daw05.local
```

```

root@joseluis-VirtualBox: /etc/bind
root@joseluis-VirtualBox:/etc/bind# dig tienda.dominioempresa-jlcomesana-daw05.local

; <<>> DiG 9.8.1-P1 <<>> tienda.dominioempresa-jlcomesana-daw05.local
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 55388
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;tienda.dominioempresa-jlcomesana-daw05.local. IN A

;; ANSWER SECTION:
tienda.dominioempresa-jlcomesana-daw05.local. 86400 IN A 10.0.2.15

;; AUTHORITY SECTION:
dominioempresa-jlcomesana-daw05.local. 86400 IN NS tienda.dominioempresa-jlcomesana-daw05.local.

;; Query time: 22 msec
;; SERVER: 10.0.2.15#53(10.0.2.15)
;; WHEN: Sun Mar 31 18:00:13 2013
;; MSG SIZE rcvd: 92

root@joseluis-VirtualBox:/etc/bind#

```

Como vemos que en `status` nos aparece `NOERROR`, podemos decir que tendremos concluido el punto 1 de la tarea

## 2. Configurar un servidor OpenLDAP con:

### 1º. El nombre de dominioempresa-xxxxx-daw05.local.

Antes de instalar LDAP se han de actualizar los repositorios y el sistema, pero como ya lo hicimos al comienzo del punto 1, no tendremos que realizarlo de nuevo.

Instalamos los paquetes necesarios para el funcionamiento de OpenLDAP, tecleando:

```
apt-get install slapd ldap-utils
```

Y cuando nos solicite la contraseña tendremos que recordarla ya que será la que nos pida para reiniciar los servicios LDAP.

Ahora comprobamos que el servicio está activo, por defecto en el puerto TCP 389, para lo que tecleamos:

```
netstat -natp | grep 389
```

Obteniendo la salida:

```
tcp 0 0 0.0.0.0:389 0.0.0.0:* ESCUCHAR 5668/slapd
tcp6 0 0 :::389 :::* ESCUCHAR 5668/slapd
```

Ahora configuramos LDAP utilizando su asistente:

```
dpkg-reconfigure slapd
```

Y nos preguntará:

- Deseas omitir la configuración** - Lógicamente contestamos que **NO**
- Nombre del dominio:** *dominioempresa-jlcomesana-daw05.local*
- Nombre de la organización:** *dominioempresa-jlcomesana-daw05.local*
- Contraseña administrador LDAP:** introducimos la que queramos y la volverá a solicitar como seguridad
- Motor de la base de datos a utilizar:** *HDB*
- Eliminar BD cuando quitemos slapd:** *SI*, para evitar confusiones con otras BD
- Desea mover la base de datos antigua:** *SI*
- Utilizar la versión 2 de LDAP:** *NO*, ya que está prácticamente obsoleta

**2º. Elabora un fichero `estructura.ldif` para crear una unidad organizacional "`tienda`".**

```
cd /etc/ldap
gedit estructura.ldif
```

En su interior tecleamos:

```
dn: ou=tienda, dc=dominioempresa-jlcomesana-daw05, dc=local
ou: tienda
objectclass: organizationalUnit
```

**3º. Elabora un fichero `grupo.ldif` para crear una unidad organizacional "`grupo`".**

```
gedit grupo.ldif
```

En su interior tecleamos:

```
dn: ou=grupo, dc=dominioempresa-jlcomesana-daw05, dc=local
ou: grupo
objectclass: organizationalUnit
```

**4º. Elabora un fichero `usuarios.ldif` para crear un grupo `users`.**

```
gedit usuarios.ldif
```

En su interior tecleamos:

```
dn: cn=users, ou=grupo, dc=dominioempresa-jlcomesana-daw05, dc=local
objectclass: posixGroup
objectclass: top
cn: users
userPassword: {crypt}*
gidNumber: 112
```

**5º. Agregar los contenidos de los ldif.**

```
ldapadd -x -W -D "cd=admin, dc=dominioempresa-jlcomesana-daw05, dc=local" -f estructura.ldif
ldapadd -x -W -D "cd=admin, dc=dominioempresa-jlcomesana-daw05, dc=local" -f grupo.ldif
ldapadd -x -W -D "cd=admin, dc=dominioempresa-jlcomesana-daw05, dc=local" -f usuarios.ldif
```

**6º. Revisar el resultado de la inserción.**

```
ldapsearch -x -b "dc=dominioempresa-jlcomesana-daw05, dc=local"
```

Y obtenemos la siguiente salida:

```
# extended LDIF
#
# LDAPv3
# base <dc=dominioempresa-jlcomesana-daw05, dc=local> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#
# dominioempresa-jlcomesana-daw05.local
dn: dc=dominioempresa-jlcomesana-daw05, dc=local
objectClass: top
objectClass: dcObject
objectClass: organization
o: dominioempresa-jlcomesana-daw05.local
dc: dominioempresa-jlcomesana-daw05

# admin, dominioempresa-jlcomesana-daw05.local
dn: cn=admin, dc=dominioempresa-jlcomesana-daw05, dc=local
```

```

objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator

# tienda, dominioempresa-jlcomesana-daw05.local
dn: ou=tienda,dc=dominioempresa-jlcomesana-daw05,dc=local
ou: tienda
objectClass: organizationalUnit

# grupo, dominioempresa-jlcomesana-daw05.local
dn: ou=grupo,dc=dominioempresa-jlcomesana-daw05,dc=local
ou: grupo
objectClass: organizationalUnit

# users, grupo, dominioempresa-jlcomesana-daw05.local
dn: cn=users,ou=grupo,dc=dominioempresa-jlcomesana-daw05,dc=local
objectClass: posixGroup
objectClass: top
cn: users
gidNumber: 112

# search result
search: 2
result: 0 Success

# numResponses: 6
# numEntries: 5

```

### 7º. Elabora un fichero `miusuario.ldif` para crear un usuario con tu nombre.

```
gedit miusuario.ldif
```

Tecleando en su interior:

```

dn: uid=joseluis,ou=tienda,dc=dominioempresa-jlcomesana-daw05,dc=local
uid: joseluis
cn: José Luis
objectClass: account
objectClass: posixAccount
objectClass: top
objectClass: shadowAccount
userPassword: {crypt}3kYWXeItEYp1.
shadowLastChange: 14001
shadowMax: 99999
shadowWarning: 7
loginShell: /bin/bash
uidNumber: 1012
gidNumber: 112
homeDirectory: /home/joseluis

```

el `password` lo hemos averiguado mediante la orden `slappasswd -h {CRYPT}` la cual cuando pulsamos *Intro* nos pregunta una contraseña por duplicado para confirmarla y cuando terminamos nos indica cual es su contraseña cifrada, por ejemplo:

```

slappasswd -h {CRYPT}
New password: hola
Re-enter new password: hola
{CRYPT}XMOQyPNgth5WE

```

### 8º. Agrega el nuevo usuario al nuevo árbol de LDAP.

```
ldapadd -x -W -D "cn=admin,dc=dominioempresa-jlcomesana-daw05,dc=local" -f miusuario.ldif
```

Tras introducir la contraseña de LDAP que nos solicita, y si todo es correcto, nos pone un mensaje indicando que ha añadido una nueva entrada

### 9º. Revisa el resultado de la inserción.

```
ldapsearch -x -b "dc=dominioempresa-jlcomesana-daw05,dc=local"
```

Y el mensaje nos indica que todo se ha realizado de forma correcta

```

# extended LDIF
#
# LDAPv3
# base <dc=dominioempresa-jlcomesana-daw05,dc=local> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

```

```
# dominioempresa-jlcomesana-daw05.local
dn: dc=dominioempresa-jlcomesana-daw05,dc=local
objectClass: top
objectClass: dcObject
objectClass: organization
o: dominioempresa-jlcomesana-daw05.local
dc: dominioempresa-jlcomesana-daw05

# admin, dominioempresa-jlcomesana-daw05.local
dn: cn=admin,dc=dominioempresa-jlcomesana-daw05,dc=local
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator

# tienda, dominioempresa-jlcomesana-daw05.local
dn: ou=tienda,dc=dominioempresa-jlcomesana-daw05,dc=local
ou: tienda
objectClass: organizationalUnit

# grupo, dominioempresa-jlcomesana-daw05.local
dn: ou=grupo,dc=dominioempresa-jlcomesana-daw05,dc=local
ou: grupo
objectClass: organizationalUnit

# users, grupo, dominioempresa-jlcomesana-daw05.local
dn: cn=users,ou=grupo,dc=dominioempresa-jlcomesana-daw05,dc=local
objectClass: posixGroup
objectClass: top
cn: users
gidNumber: 112

# joseluis, tienda, dominioempresa-jlcomesana-daw05.local
dn: uid=joseluis,ou=tienda,dc=dominioempresa-jlcomesana-daw05,dc=local
uid: joseluis
cn:: Sm9zw6kgTHVpcw==
objectClass: account
objectClass: posixAccount
objectClass: top
objectClass: shadowAccount
shadowMax: 99999
shadowWarning: 7
loginShell: /bin/bash
uidNumber: 1012
gidNumber: 112
homeDirectory: /home/joseluis

# search result
search: 2
result: 0 Success

# numResponses: 7
# numEntries: 6
```