Práctica 3

Asignatura: Administración de sistemas 2
Fecha: 18/4/2020
Autor: Diego Marco Beisty, 755232

RESUMEN

Se van a añadir a la arquitectura tres nuevas máquinas virtuales con sistema operativo Ubuntu.
Se va a configurar, en una subred interna de servidores, una nueva máquina que actúa como servidor NFS y servidor maestro del servicio LDAP. En esa misma subred se va a añadir otra máquina configurada como réplica del servicio LDAP para garantizar tolerancia a fallos.
Además se incluye una nueva máquina cliente de los servicios NFS y LDAP en una subred definida en la vlan 198. Este cliente accederá al servicio LDAP de forma cifrada con TLS.

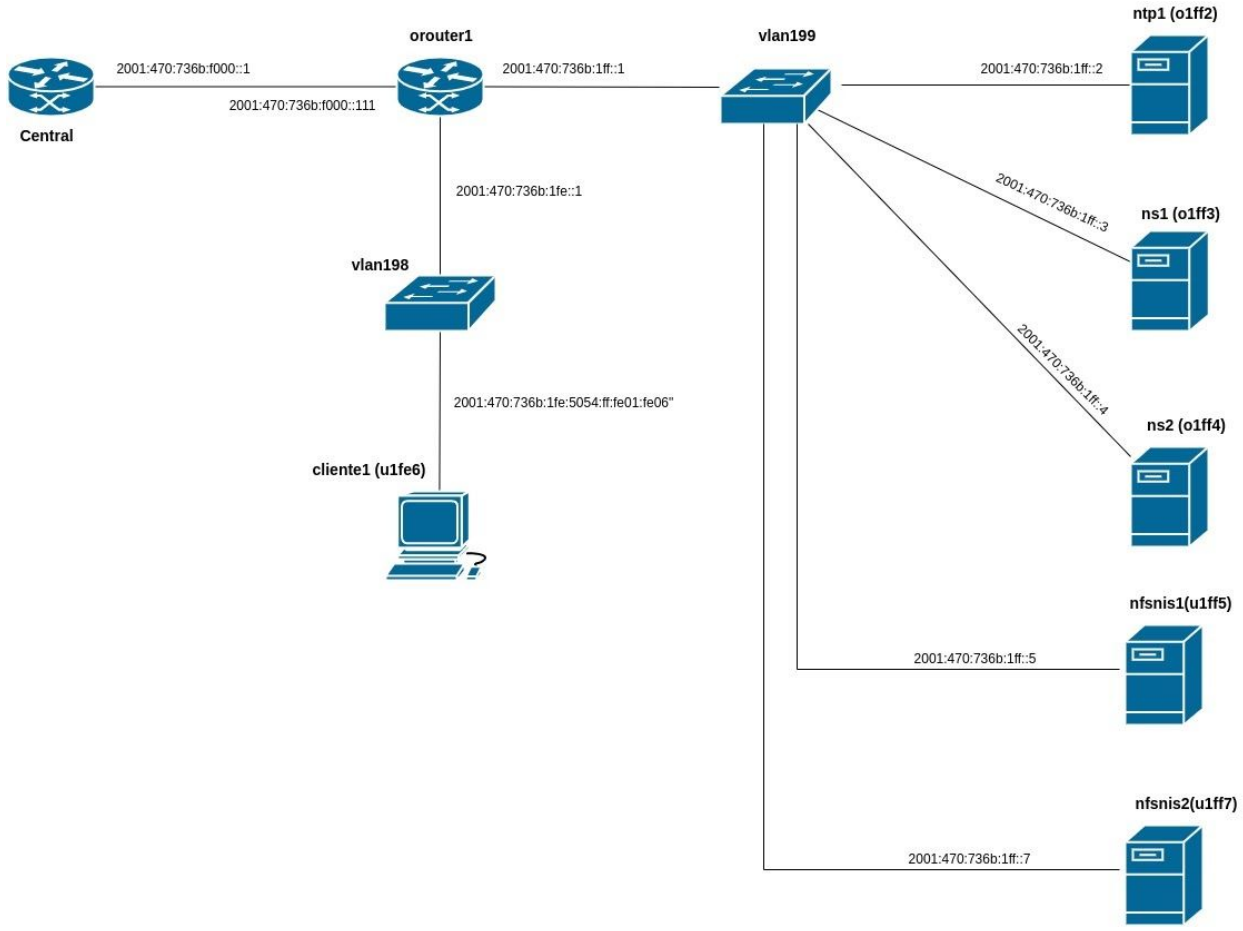
OBJETIVOS

El objetivo de esta práctica es centralizar y distribuir las cuentas de los usuarios de la nueva máquina cliente incluida en la arquitectura mediante el protocolo LDAP, así como sus directorios /home/usuario asociados mediante el servicio NFS.
Otro objetivo es la configuración de red y de servicios en un sistema operativo distinto de openBSD como es Ubuntu.

INTRODUCCIÓN

Inicialmente para que todas las máquinas puedan contar con los servicios básicos distribuidos implementados en la práctica dos, se van a configurar las nuevas máquinas “u1ff5”, “u1ff7” y “u1fe6” como clientes del servicio de resolución de nombres recursivo DNS configurado en la máquina “o1ff2”. También se configuran como clientes del servicio de sincronización de relojes NTP establecido en la máquina “o1ff2”.
Cabe destacar que se les ha configurado un usuario administrador llamado a755232 a todas las nuevas máquinas para mantener la consistencia con las máquinas configuradas en anteriores prácticas y poder acceder a todas ellas con ssh sin tener que distinguir el nombre de usuario.

ARQUITECTURA DE ELEMENTOS RELEVANTES



En el diagrama quedan representados de izquierda a derecha los siguientes elementos:

- El router Central que conecta las MVs a internet.
- orouter1, que está conectado a la subred `2001:470:736b:f000` con Central, a la subred `2001:470:736b:1ff` con las máquinas servidores, mediante la vlan199 y a la subred 2001:470:736b:1fe con la máquina cliente, mediante la vlan198.
- u1fe6(nombre DNS cliente1), es el cliente NFS y LDAP.
- o1ff2 (nombre DNS ntp1), es el servidor ntp y DNS recursivo con caché.
- o1ff3 (nombreDNS ns1), es el servidor autoritario DNS primario.
- o1ff4 (nombre DNS ns2), es el servidor autoritario DNS secundario.
- u1ff5 (nombre DNS nfsnis1), es el servidor NFS y maestro LDAP.
- u1ff7 (nombre DNS nfsnis2), es el servidor réplica LDAP.

COMPREHENSIÓN DE ELEMENTOS RELEVANTES

Puesta en marcha máquinas virtuales Ubuntu

Inicialmente para poder crear tres nuevas máquinas virtuales ubuntu se ha descargado una imagen base llamada u1604 que a partir de la cual se han obtenido las imágenes diferenciales “u1ff5”, “u1ff7” y “u1fe6”.
Esta imagen base se ha configurado para que el shell funcione con entorno vi. Además se ha añadido un nuevo usuario a755232 que se usará como usuario administrador, añadiendo privilegios sudo y modificando su fichero profile para que guarde en variables globales la relación entre los nombres de las máquinas y su dirección ip para facilitar su acceso.

Configuración de red

Inicialmente se incorpora en “orouter1” una nueva interfaz sobre vio0 para añadir la subred vlan 198 sobre la cual levantar la máquina cliente.
Para ello se configura el fichero hostname.vlan198 con la siguiente información:

```
inet6 alias 2001:470:736b:1fe::1 64 vlan 198 vlandev vio0
-autoconfprivacy
```

En la que se disigna el prefijo 2001:470:736b:1fe:: para la nueva subred. Además se activa el servicio de prefijos para esta subred añadiendo en rad.conf la línea:

```
interface vlan198.
```

Respecto a la configuración de red de las nuevas máquinas, en anteriores prácticas la configuración se hacía mediante ficheros hostname puesto que eran sistemas operativos openBSD, pero estas tres nuevas máquinas son Ubuntu y por lo tanto la configuración se realiza sobre el fichero `/etc/network/interfaces`.
Para las máquinas servidores, como es el caso de “u1ff5” y “u1ff7” se les aplica una dirección IPv6 estática para facilitar el acceso de los clientes.
Para ello en el fichero interfaces se indica que en el interfaz ens3 no se va a configurar explícitamente ninguna dirección IP mediante las líneas:

```
auto ens3
iface ens3 inet6 manual.
```

Además se indica que al interfaz vlan ens3.199 sí que se le va a aplicar una configuración explícita mediante las líneas:

```
auto ens3.199
iface ens3.199 inet6 static
        address 2001:470:736b:1ff::5 | 2001:470:736b:1ff::7
        netmask 64
```

```
gateway 2001:470:736b:1ff::1
autoconf 0
vlan-raw-device ens3
```

Como se observa, se asocia una dirección estática IPV6 a la interfaz vlan ens3.199 en la que la dirección de subred es 2001:470:736b:1ff::, el encaminador por defecto es la máquina orouter1 con IPV6 2001:470:736b:1ff::1 y se indica que no se autoconfigure nada más. La última línea se incluye para indicar la interfaz sobre la cual se crea la vlan, en este caso ens3.
Respecto a la máquina cliente, la configuración del dispositivo vlan en el fichero interfaces varía un poco, puesto que la dirección se va a asignar de forma dinámica mediante el servicio rad, activo en “orouter1” y configurado para proveer prefijos ipv6 en la vlan 198 y 199.
Por ello su interfaz vlan está configurada de esta forma:

```
auto ens3.198
iface ens3.198 inet6 auto
          accept_ra 1
          autoconf 0
          vlan-raw-device ens3
```

Se observa la definición de la interfaz vlan en la que se acepta recibir un prefijo IPV6 mediante rad (accept_ra 1).

Posteriormente para las tres máquinas se les ha añadido su nombre dns en el fichero /etc/hostname y en /etc/hosts.

Se ha tenido en cuenta que la asignación dinámica de la dirección IPV6 de la máquina “cliente1” implica que su dirección IPV6 se forma mediante el prefijo IPV6 2001:470:736b:1fe:: obtenido por el servicio rad en “orouter1” y su direcciño MAC que nunca cambia. Por lo tanto en el contexto de las prácticas su dirección IPV6 siempre es la misma y no hay problema en mapear la máquina “cliente1” con su dirección en las zonas DNS.

Servicios básicos NTP y DNS

Estando las máquinas “u1ff5”,”u1fe6” y “u1ff7” accesibles desde la red, se procede a configurarlas como clientes del servicio de resolución de nombres recursivo añadiendo en el fichero /etc/resolvconf/resolv.conf.d/tail la línea:

```
nameserver 2001:470:736b:1ff::2
```

De esta forma se indica qué máquina ofrece este servicio.
Después se configuran como clientes del servicio de sincronización de tiempo añadiendo al fichero /etc/ntp.conf la línea:

```
 server ntp1.1.ff.es.eu.org
```

Donde se indica el servidor NTP que ofrece este servicio.

Servicio NFS

Este servicio está configurado en la máquina “u1ff5”. La implementación de NFS usada es la versión 4, que incluye in identity mapping que mapea entre los UID,GUID y strings en formato user@dominio. De esta forma se evita tener forzosamente el mismo UID y GUID en el cliente y el servidor ya que la correspondencia se hace entre nombres de usuario.
Para activar este mapeado, inicialmente se añade al fichero /etc/default/nfs-common la línea:

```
NEED_IDMAP=YES
```

Después en el fichero /etc/idmapd.conf se añade el dominio que comparten tanto cliente como servidor:

```
Domain = 1.ff.es.eu.org
```

Cabe destacar que si el identity mapping no encuentra en el passwd local una correspondencia entres el string user@dominio y su UID, GUID por defecto usa la cuenta nobody nogroup como se indica en las siguientes líneas del mismo fichero:

```
Nobody-User = nobody
Nobody-Group = nogroup
```

Posteriormente se añade en el servidor el directorio de un primer usuario llamado a755232, para ello se cera el directorio /srv/nfs4/home/a755232. Después se añade al directorio los ficheros básicos de usuario de /etc/skel. Finalmente se cambia el propietario del directorio y los ficheros con el comando chown al UID y GUID correspondientes al usuario a755232 ya creado en la máquina cliente.
(Posteriormente se usarán los UID y GUID del usuario creado en el directorio LDAP).
Cabe destacar que los permisos del directorio serán 0750 para que el usuario a755232 pueda leer y escribir y entrar al directorio, los usuarios de su grupo solo leer y entrar al directorio y otros usuarios no puedan acceder al directorio.

Para poder exportar este directorio a la máquina cliente, se añaden en el fichero /etc/exports las líneas:

```
/srv/nfs4/home
2001:470:736b:1fe::/64(rw,fsid=0,insecure,no_subtree_check,async,root_squash)
/srv/nfs4/home/a755232
2001:470:736b:1fe::/64(rw,nohide,insecure,no_subtree_check,async,root_squash)
```

Las primeras dos líneas implican que a la subred de clientes 2001:4070:736b:1fe:: se les permite montar el pseudo-sistema de ficheros que cuelga de /srv/nfs4/home (fsid=0) con permisos de lectura y escritura. Además se le permite al cliente que no use un puerto reservado para conectarse con el servidor NFS (insercure). Se elimina el chequeo interno de que el fichero requerido esté en el directorio exportado (no_subtree_check). Se le permite al servidor responder las peticiones de escritura antes de realizar cambios en disco (async). Además si el cliente realiza una petición con permisos root, el servidor automáticamente le cambia el uid a otro para quitarle los privilegios en el servidor (root_sqash).
Las segundas dos líneas se añaden para poder exportar el directorio concreto del usuario a755232 sin tener que montar los directorios /sev/nfs4/ en el cliente.

En el cliente, para montar su directorio home en el arranque, se van a añadir las siguientes líneas en el fichero /etc/fstab:

```
nfsnis1.1.ff.es.eu.org:a755232 /home/a755232 nfs4 rw,nolock,noauto,x-systemd.automount,x-systemd.device-timeout=30,retry=0,_netdev 0 0
```

Donde se indica que va a montar remotamente el directorio a755232 en el directorio local /home/a755232 alojado en el servidor NFS4, nfsnis1.1.ff.es.eu.org. Se añade además la opción x-systemd.automount para que sea el demonio systemd el que se encargue de montar el directorio en el arranque una vez se han inicializado todas las configuraciones de red del sistema.

Servicio LDAP

Se va a configurar un directorio LDAP en la máquina “u1ff5” en el que se definirán las cuentas de usuario que se usarán desde la máquina cliente “u1fe6”. Para garantizar tolerancia a fallos se va a configurar una réplica del directorio en el servidor “u1ff7”.
Además la comunicación entre el cliente y el servidor va a viajar cifrada mediante el protocolo TLS.
Inicialmente, en la instalación se define la cuenta LDAP de admin, desde la cual se podrá acceder a la base de datos y añadir nuevas entradas. Además se define el identificador básico de la base de datos, que se construye a partir del dominio:

```
dn: dc=1,dc=ff,dc=es,dc=eu,dc=org
```

Posteriormente se añaden dos nuevas entradas, la Unidad Organizacional alumnos y la OU grupos, que servirán como base para crear cuentas de usuarios y grupos.

```
dn: ou=people,dc=1,dc=ff,dc=es,dc=eu,dc=org
objectClass: organizationalUnit
ou: people

dn: ou=groups,dc=1,dc=ff,dc=es,dc=eu,dc=org
objectClass: organizationalUnit
ou: groups
```

Para añadir cada entrada a la base de datos se ejecuta el comando:

```
ldapadd -x -D cn=admin,dc=1,dc=ff,dc=es,dc=eu,dc=org -W -f base.ldif
```

Donde se indica con -D la cuenta usada para insertar las entradas contenidas en el fichero base.ldif
A continuación se va a añadir el usuario “pepe” a la OU alumnos mediante una entrada identificada como `dn: uid=pepe,ou=people,dc=1,dc=ff,dc=es,dc=eu,dc=org` con objectClass que indican que es una cuenta de usuario, (inetOrgPerson, posixAccount, shadowAccount) y otros atributos necesarios para completar la cuenta tales como la contraseña, el directorio home,etc. Además se añade el grupo “pepe” a la OU grupos mediante una entrada identificada como `dn: cn=pepe,ou=groups,dc=1,dc=ff,dc=es,dc=eu,dc=org`
Creada ya la cuenta LDAP “pepe”, se pasa a configurar la máquina cliente “u1fe6”.

Primero se añade en el fichero nsswitch la opción ldap para que al autenticar este usuario consulte primero el servidor LDAP y no los ficheros locales /etc/passwd y /etc/shadow.

```
passwd:     compat ldap
group:     compat ldap
shadow:     compat ldap
```

Después se configura PAM para que no fuerce a comprobar la contraseña localmente eliminando del fichero /etc/pam.d/common-password la línea `use_authok.`
Además para que cree a nivel local el fichero home del usuario si este no existe, añado en /etc/pam.d/common-session la línea: `session optional pam_mkhomedir.so skel=/etc/skel umask=077.`
Para cifrar las comunicaciones entre el servidor y el cliente sobre TLS se genera el certificado del servidor y lo se guarda en `/etc/ldap/sasl2/`. Se añade una nueva entrada `dn: cn=config` que añade el certificado al directorio LDAP.
Finalmente se le indica al cliente que pida el certificado del servidor añadiendo al fichero /etc/default/slapd la línea `TLS_REQCERT allow` y se activa el protocolo start TLS descomentando en el fichero /etc/ldap.conf la línea `ssl start_tls.`
Para añadir replicación, en el master “u1ff5” se añaden las entradas identificadas como:

```
dn: cn=module,cn=config
dn: olcOverlay=syncprov,olcDatabase={1}mdb,cn=config
```

Y en la réplica se añaden las entrada que referencian a las unidades organizacionales de personas, grupos y otra entrada identificada como:
`dn: olcDatabase={1}mdb,cn=config` que habilita la sincronización con el master.

PROBLEMAS ENCONTRADOS

- En la máquina cliente “u1fe6” haciendo ip a show ens3.198 se observa que el servicio rad de orouter1 le asigna dos direcciones públicas ipv6:

  ```
  inet6 2001:470:736b:1fe:d49f:9d48:8c4b:20a8/64 scope global temporary dynamic
  inet6 2001:470:736b:1fe:5054:ff:fe01:fe06/64 scope global mngtmpaddr dynamic
  ```

  No he conseguido arreglar esta incorrección y para la realización de la práctica he referenciado a esta máquina con la segunda dirección IPV6.

- Al montar en el arranque con fstab el directorio remoto nfsnis1.1.ff.es.eu.org:/a755232, se observaba en /var/log/syslog, que cuando se montaba el directorio, la red todavía no estaba iniciada, esto ocasionaba que nfs devolviese un error de timeout al intentar montar el directorio y no obtener respuesta del servidor nfs en u1ff5. Esto se soluciono añadiendo las opciones ,x-systemd.automount,noauto en fstab para que el montaje lo hiciese systemd una vez que la red estaba lista.
  Esta configuración impide montar con mount -a, pero permite tener el directorio montado en el arranque.

ANEXO

VERIFICACIÓN

1) Configuración de red:

Desde la máquina 155.210.154.199 del laboratorio ejecuto el comando traceroute a las nuevas máquinas para comprobar que están accesibles desde la red.

u1ff5:

```
traceroute to 2001:470:736b:1ff::5 (2001:470:736b:1ff::5), 30 hops max, 80 byte packets
1  2001:470:1f0b:19fb::1 (2001:470:1f0b:19fb::1)  0.231 ms  0.215 ms  0.202 ms
 2  2001:470:736b:f000::111 (2001:470:736b:f000::111)  0.595 ms  0.580 ms  0.561 ms
3  2001:470:736b:1ff::5 (2001:470:736b:1ff::5)  0.860 ms  0.815 ms  0.799 ms
```

Máquina u1ff7:

```
traceroute to 2001:470:736b:1ff::7 (2001:470:736b:1ff::7), 30 hops max, 80 byte packets
 1  2001:470:1f0b:19fb::1 (2001:470:1f0b:19fb::1)  0.223 ms  0.184 ms  0.204 ms
 2  2001:470:736b:f000::111 (2001:470:736b:f000::111)  0.523 ms  0.502 ms  0.497 ms
 3  2001:470:736b:1ff::7 (2001:470:736b:1ff::7)  0.649 ms  0.648 ms  0.633 ms
```

Máquina u1fe6:

```
traceroute to 2001:470:736b:1fe:5054:ff:fe01:fe06 (2001:470:736b:1fe:5054:ff:fe01:fe06), 30 hops max, 80 byte packets
 1  2001:470:1f0b:19fb::1 (2001:470:1f0b:19fb::1)  0.201 ms  0.163 ms  0.162 ms
 2  2001:470:736b:f000::111 (2001:470:736b:f000::111)  0.657 ms  0.634 ms  0.635 ms
   3  2001:470:736b:1fe:5054:ff:fe01:fe06  (2001:470:736b:1fe:5054:ff:fe01:fe06)  0.700 ms  0.693 ms  0.683 ms
```

2) Servicios básicos:

Desde cada máquina compruebo la resolución recursiva de nombres haciendo ping6 a la dirección IPV6 ipv6.google.com con resultado satisfactorio.

Para comprobar la sincronización correcta con el servidor NTP “o1ff2” se ejecuta el comando “sudo ntpq -p” obteniendo:

Máquina u1ff5:

```
 remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
```

```
*ntp1.1.ff.es.eu 200.98.196.212   2 u    6   64   37    0.415   -4.886   3.432
```

Máquina u1ff7:

```
 remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*ntp1.1.ff.es.eu 200.98.196.212   2 u   22   64   77    0.326   -0.156   0.414
```

Máquina u1fe6:

```
    remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*ntp1.1.ff.es.eu 200.98.196.212   2 u   63   64   77    0.739   -6.707   4.770
```

Para comprobar la correcta resolución directa e inversa de los nombres de dominio asignados a cada máquina, desde mi máquina local ejecuto los comandos:

Máquina u1ff5:

dig nfsnis1.1.ff.es.eu.org AAAA @8.8.8.8 +trace

```
; <<>> DiG 9.11.3-1ubuntu1.11-Ubuntu <<>> nfsnis1.1.ff.es.eu.org AAAA @8.8.8.8
+trace
;; global options: +cmd
.                   86578  IN     NS     a.root-servers.net.
.                   86578  IN     NS     b.root-servers.net.
.                   86578  IN     NS     c.root-servers.net.
.                   86578  IN     NS     d.root-servers.net.
.                   86578  IN     NS     e.root-servers.net.
.                   86578  IN     NS     f.root-servers.net.
.                   86578  IN     NS     g.root-servers.net.
.                   86578  IN     NS     h.root-servers.net.
.                   86578  IN     NS     i.root-servers.net.
.                   86578  IN     NS     j.root-servers.net.
.                   86578  IN     NS     k.root-servers.net.
.                   86578  IN     NS     l.root-servers.net.
.                   86578  IN     NS     m.root-servers.net.
.                   86578  IN     RRSIG  NS 8 0 518400 20200430170000
org.                172800 IN     NS     d0.org.afilias-nst.org.
org.                172800 IN     NS     a0.org.afilias-nst.info.
org.                172800 IN     NS     c0.org.afilias-nst.info.
org.                172800 IN     NS     a2.org.afilias-nst.info.
org.                172800 IN     NS     b0.org.afilias-nst.org.
org.                172800 IN     NS     b2.org.afilias-nst.org.
org.                86400  IN     DS     17883 7 1
org.                86400  IN     DS     9795 7 2 FE7FF8E5
org.                86400  IN     DS     17883 7 2 1EB4E6EE
org.                86400  IN     DS     9795 7 1
org.                86400  IN     RRSIG  DS 8 1 86400 20200501170000
eu.org.                    86400  IN     NS     ns.bortzmeyer.eu.org.
eu.org.                    86400  IN     NS     oz.wolfhugel.eu.
eu.org.                    86400  IN     NS     pl.wolfhugel.eu.
eu.org.                    86400  IN     NS     ns1.eu.org.
eu.org.                    86400  IN     NS     ns1.eriomem.net.
eu.org.                    86400  IN     NS     ns3.keltia.net.
eu.org.                    86400  IN     NS     dns4.gandi.net.
```

```
eu.org.                 86400  IN     NS     auth1.dns.elm.net.
eu.org.                 86400  IN     NS     canada.wolfhugel.eu.
eu.org.                 86400  IN     NS     hobbes.bsd-dk.dk.
eu.org.                 86400  IN     DS     36406 8 2 36A6F4D2
eu.org.                 86400  IN     RRSIG  DS 7 2 86400 20200505163700
es.eu.org.          86400  IN     NS     ns.ankh.fr.eu.org.
es.eu.org.          86400  IN     NS     ns1.eu.org.
es.eu.org.          86400  IN     NS     ns1.eriomem.net.
es.eu.org.          86400  IN     NS     canada.wolfhugel.eu.
es.eu.org.          86400  IN     DS     56470 8 2 960B5514
es.eu.org.          86400  IN     RRSIG  DS 8 3 86400 20200512072044
ff.es.eu.org.       172800 IN     NS     ns1.ff.es.eu.org.
ff.es.eu.org.       172800 IN     NS     ns2.ff.es.eu.org.
1.ff.es.eu.org.             86400  IN     NS     ns1.1.ff.es.eu.org.
1.ff.es.eu.org.             86400  IN     NS     ns2.1.ff.es.eu.org.
;; Received 143 bytes from 2001:470:736b:f000::2#53(ns1.ff.es.eu.org) in 488 ms
nfsnis1.1.ff.es.eu.org.    3600   IN     AAAA   2001:470:736b:1ff::5
1.ff.es.eu.org.             3600   IN     NS     ns1.1.ff.es.eu.org.
1.ff.es.eu.org.             3600   IN     NS     ns2.1.ff.es.eu.org.
;; Received 171 bytes from 2001:470:736b:1ff::4#53(ns2.1.ff.es.eu.org) in 168 ms
```

Máquina u1ff7:

dig nfsnis2.1.ff.es.eu.org AAAA @8.8.8.8 +trace

```
; <<>> DiG 9.11.3-1ubuntu1.11-Ubuntu <<>> nfsnis2.1.ff.es.eu.org AAAA @8.8.8.8
+trace
;; global options: +cmd
.                   86961  IN     NS     k.root-servers.net.
.                   86961  IN     NS     m.root-servers.net.
.                   86961  IN     NS     b.root-servers.net.
.                   86961  IN     NS     g.root-servers.net.
.                   86961  IN     NS     j.root-servers.net.
.                   86961  IN     NS     c.root-servers.net.
.                   86961  IN     NS     h.root-servers.net.
.                   86961  IN     NS     f.root-servers.net.
.                   86961  IN     NS     l.root-servers.net.
.                   86961  IN     NS     d.root-servers.net.
.                   86961  IN     NS     e.root-servers.net.
.                   86961  IN     NS     a.root-servers.net.
.                   86961  IN     NS     i.root-servers.net.
.                   86961  IN     RRSIG  NS 8 0 518400 20200501050000
;; Received 525 bytes from 8.8.8.8#53(8.8.8.8) in 23 ms
org.                172800 IN     NS     a0.org.afilias-nst.info.
org.                172800 IN     NS     a2.org.afilias-nst.info.
org.                172800 IN     NS     b0.org.afilias-nst.org.
org.                172800 IN     NS     b2.org.afilias-nst.org.
org.                172800 IN     NS     c0.org.afilias-nst.info.
org.                172800 IN     NS     d0.org.afilias-nst.org.
org.                86400  IN     DS     9795 7 1
org.                86400  IN     DS     9795 7 2 FE7FF8E5
org.                86400  IN     DS     17883 7 1
org.                86400  IN     DS     17883 7 2 1EB4E6EE
org.                86400  IN     RRSIG  DS 8 1 86400 20200501170000 S6UhCQ==
;; Received 908 bytes from 2001:500:2f::f#53(f.root-servers.net) in 237 ms
```

```
eu.org.                  86400  IN     NS     ns.bortzmeyer.eu.org.
eu.org.                  86400  IN     NS     oz.wolfhugel.eu.
eu.org.                  86400  IN     NS     pl.wolfhugel.eu.
eu.org.                  86400  IN     NS     ns1.eu.org.
eu.org.                  86400  IN     NS     ns1.eriomem.net.
eu.org.                  86400  IN     NS     ns3.keltia.net.
eu.org.                  86400  IN     NS     dns4.gandi.net.
eu.org.                  86400  IN     NS     auth1.dns.elm.net.
eu.org.                  86400  IN     NS     canada.wolfhugel.eu.
eu.org.                  86400  IN     NS     hobbes.bsd-dk.dk.
eu.org.                  86400  IN     DS     36406 8 2 36A6F4D2
eu.org.                  86400  IN     RRSIG  DS 7 2 86400 20200505163700
es.eu.org.          86400  IN     NS     ns.ankh.fr.eu.org.
es.eu.org.          86400  IN     NS     ns1.eu.org.
es.eu.org.          86400  IN     NS     ns1.eriomem.net.
es.eu.org.          86400  IN     NS     canada.wolfhugel.eu.
es.eu.org.          86400  IN     DS     56470 8 2 960B5514
es.eu.org.          86400  IN     RRSIG  DS 8 3 86400 20200512072044 20200416051206
44709 eu.org.
FF.ES.EU.ORG.       172800 IN     NS     NS2.FF.ES.EU.ORG.
FF.ES.EU.ORG.       172800 IN     NS     NS1.FF.ES.EU.ORG.
;; Received 430 bytes from 46.165.221.137#53(ns1.eriomem.net) in 54 ms
1.ff.es.eu.org.            86400  IN     NS     ns1.1.ff.es.eu.org.
1.ff.es.eu.org.            86400  IN     NS     ns2.1.ff.es.eu.org.
;; Received 143 bytes from 2001:470:736b:f000::3#53(NS2.FF.ES.EU.ORG) in 615 ms


nfsnis2.1.ff.es.eu.org.    3600   IN     AAAA   2001:470:736b:1ff::7
1.ff.es.eu.org.            3600   IN     NS     ns1.1.ff.es.eu.org.
1.ff.es.eu.org.            3600   IN     NS     ns2.1.ff.es.eu.org.
;; Received 171 bytes from 2001:470:736b:1ff::4#53(ns2.1.ff.es.eu.org) in 611 ms
```

Máquina u1fe6:

dig cliente1.1.ff.es.eu.org AAAA @8.8.8.8 +trace

```
; <<>> DiG 9.11.3-1ubuntu1.11-Ubuntu <<>> cliente1.1.ff.es.eu.org AAAA @8.8.8.8
+trace
;; global options: +cmd
.                   87091  IN     NS     e.root-servers.net.
.                   87091  IN     NS     h.root-servers.net.
.                   87091  IN     NS     l.root-servers.net.
.                   87091  IN     NS     i.root-servers.net.
.                   87091  IN     NS     a.root-servers.net.
.                   87091  IN     NS     d.root-servers.net.
.                   87091  IN     NS     c.root-servers.net.
.                   87091  IN     NS     b.root-servers.net.
.                   87091  IN     NS     j.root-servers.net.
.                   87091  IN     NS     k.root-servers.net.
.                   87091  IN     NS     g.root-servers.net.
.                   87091  IN     NS     m.root-servers.net.
```

```
.                   87091  IN     NS     f.root-servers.net.
.                   87091  IN     RRSIG  NS 8 0 518400 20200430170000
;; Received 525 bytes from 8.8.8.8#53(8.8.8.8) in 19 ms
org.                172800 IN     NS     b2.org.afilias-nst.org.
org.                172800 IN     NS     d0.org.afilias-nst.org.
org.                172800 IN     NS     c0.org.afilias-nst.info.
org.                172800 IN     NS     a2.org.afilias-nst.info.
org.                172800 IN     NS     a0.org.afilias-nst.info.
org.                172800 IN     NS     b0.org.afilias-nst.org.
org.                86400  IN     DS     9795 7 1
org.                86400  IN     DS     9795 7 2 FE7FF8E5
org.                86400  IN     DS     17883 7 1
org.                86400  IN     DS     17883 7 2 1EB4E6EE
org.                86400  IN     RRSIG  DS 8 1 86400 20200501170000
;; Received 937 bytes from 199.9.14.201#53(b.root-servers.net) in 92 ms
eu.org.                     86400  IN     NS     ns.bortzmeyer.eu.org.
eu.org.                     86400  IN     NS     oz.wolfhugel.eu.
eu.org.                     86400  IN     NS     pl.wolfhugel.eu.
eu.org.                     86400  IN     NS     ns1.eu.org.
eu.org.                     86400  IN     NS     ns1.eriomem.net.
eu.org.                     86400  IN     NS     ns3.keltia.net.
eu.org.                     86400  IN     NS     dns4.gandi.net.
eu.org.                     86400  IN     NS     auth1.dns.elm.net.
eu.org.                     86400  IN     NS     canada.wolfhugel.eu.
eu.org.                     86400  IN     NS     hobbes.bsd-dk.dk.
eu.org.                     86400  IN     DS     36406 8 2 36A6F4D2
eu.org.                     86400  IN     RRSIG  DS 7 2 86400 20200505163700 37022
org.
;; Received 601 bytes from 2001:500:48::1#53(b2.org.afilias-nst.org) in 234 ms
FF.ES.EU.ORG.       172800 IN     NS     NS1.FF.ES.EU.ORG.
FF.ES.EU.ORG.       172800 IN     NS     NS2.FF.ES.EU.ORG.
;; Received 431 bytes from 2a00:c98:2030:a006:1::1#53(ns1.eriomem.net) in 204 ms
1.ff.es.eu.org.             86400  IN     NS     ns1.1.ff.es.eu.org.
1.ff.es.eu.org.             86400  IN     NS     ns2.1.ff.es.eu.org.
;; Received 144 bytes from 2001:470:736b:f000::2#53(NS1.FF.ES.EU.ORG) in 534 ms
cliente1.1.ff.es.eu.org. 3600     IN     AAAA   2001:470:736b:1fe:5054:ff:fe01:fe06
1.ff.es.eu.org.             3600   IN     NS     ns1.1.ff.es.eu.org.
1.ff.es.eu.org.             3600   IN     NS     ns2.1.ff.es.eu.org.
;; Received 172 bytes from 2001:470:736b:1ff::3#53(ns1.1.ff.es.eu.org) in 611 ms
```

3) Servicio NFS:

Para verificar la correcta configuración de este servicio, en el servidor se actualiza el fichero /etc/exports mediante el comando `exportfs -a` y se comprueba el pseudosistema de ficheros exportado con `exportfs -v`.

Desde la máquina cliente se comprueban los directorios que exporta el servidor con el comando `showmount -e nfsnis1.1.ff.es.eu.org`.

Si están visibles, se monta manualmente el directorio remoto sobre un punto de montaje.

`sudo mount -v -t nfs4 nfsnis1.1.ff.es.eu.org:/remoto punto_montaje`.

Finalmente si el directorio se monta satisfactoriamente se añade al fichero fstab y se comprueba que monta en el arranque.

4)Servicio LDAP:

Cada vez que se añade una entrada se comprueba que se ha añadido a LDAP observando si al ejecutar `sudo slapcat` esta aparece en pantalla.
Además al añadir un nuevo usuario como el caso de “pepe”, tanto desde el servidor como desde el cliente ejecuto el siguiente comando verificando que se encuentra en ldap:
`ldapsearch -xLLL -b “dc=1,dc=ff,dc=es,dc=eu,dc=org” uid=pepe, sn cn`
Posteriormente se comprueba que se puede acceder a la cuenta “pepe” desde la máquina cliente: `su pepe`
Para verificar que funciona el protocolo TLS, desde el cliente y desde el servidor ejecuto:

```
ldapwhoami  -H ldap://nfsnis1.1.ff.es.eu.org -x -ZZ
```

Si las peticiones se hacen sobre TLS este comando devuelve anonymous.
Finalmente para comprobar que la máquina “u1ff7” mantiene una réplica del directorio LDAP hago una búsqueda desde esta máquina de una entrada existente en el directorio LDAP del master como puede ser la unidad organizacional personas:

```
ldapsearch -x -b 'ou=people,dc=1,dc=ff,dc=es,dc=eu,dc=org'
```

FICHEROS DE CONFIGURACIÓN

Máquina orouter1:

/etc/rad.conf

```
interface vlan199
interface vlan198
```

/etc/hostname.vlan198

```
inet6 alias 2001:470:736b:1fe::1 64 vlan 198 vlandev vio0
-autoconfprivacy
```

Máquina o1ff3:

/var/nsd/zones/1.ff.es.eu.org.directo

```
$ORIGIN 1.ff.es.eu.org.
    @       IN      SOA     ns1.1.ff.es.eu.org.  a755232.1.ff.es.eu.org. (
                            2020031107          ; numero serie
                            21600               ; Refresca cada 6 horas
                            3600                ; Reintenta cada 1 hora
                            604800              ; Expira despues de 1 semana
                            86400 )             ; TTL minimo cliente de 1
dia
            IN      NS      ns1.1.ff.es.eu.org.
            IN      NS      ns2.1.ff.es.eu.org.
    ntp1    IN      AAAA    2001:470:736b:1ff::2
    ns1     IN      AAAA    2001:470:736b:1ff::3
    ns2     IN      AAAA    2001:470:736b:1ff::4
    router1 IN      AAAA    2001:470:736b:f000::111
    otro_servidor   IN      AAAA    2001:470:736b:1ff::f
    nfsnis1         IN      AAAA    2001:470:736b:1ff::5
    cliente1        IN      AAAA    2001:470:736b:1fe:5054:ff:fe01:fe06
    nfsnis2         IN      AAAA    2001:470:736b:1ff::7
    o1ff3   IN      CNAME   ns1
    o1ff4   IN      CNAME   ns2
```

/var/nsd/zones/1.ff.es.eu.org.inverso

```
    @       IN      SOA     ns1.1.ff.es.eu.org.  a755232.1.ff.es.eu.org. (
                            2020031103          ; numero serie
                            21600               ; Refresca cada 6 horas
                            3600                ; Reintenta cada 1 hora
                            604800              ; Expira despues de 1 semana
                            86400 )             ; TTL minimo cliente de 1 dia
    IN      NS      ns1.1.ff.es.eu.org.
    IN      NS      ns2.1.ff.es.eu.org.
3.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.f     IN      PTR     ns1.1.ff.es.eu.org.
4.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.f     IN      PTR     ns2.1.ff.es.eu.org.
1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.f     IN      PTR     router1.1.ff.es.eu.org.
```

```
f.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.f     IN      PTR
otro_servidor.1.ff.es.eu.org.
5.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.f     IN      PTR     nfsnis1.1.ff.es.eu.org.
6.0.0.0.0.0.0.0.0.0.0.0.0.0.0.e.f     IN      PTR     cliente1.1.ff.es.eu.org.
7.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.f     IN      PTR     nfsnis2.1.ff.es.eu.org.
2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.f     IN      PTR     ntp1.1.ff.es.eu.org.
```

Máquina u1ff5:

/etc/network/interfaces

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet6 loopback

# The primary network interface
# This is an autoconfigured IPv6 interface
#auto ens3
#iface ens3 inet6 auto
#      dns-nameservers 2001:470:20::2

auto ens3
iface ens3 inet6 manual

auto ens3.199
iface ens3.199 inet6 static
address 2001:470:736b:1ff::5
netmask 64
gateway 2001:470:736b:1ff::1
autoconf 0
vlan-raw-device ens3
```

/etc/exports

```
# /etc/exports: the access control list for filesystems which may be
exported to NFS clients.  See exports(5).
/srv/nfs4/home
2001:470:736b:1fe::/64(rw,fsid=0,insecure,no_subtree_check,async,root_
squash)
/srv/nfs4/home/a755232
2001:470:736b:1fe::/64(rw,nohide,insecure,no_subtree_check,async,root_
squash)
```

base.ldif (fichero LDAP)

```
objectClass: organizationalUnit
ou: people

dn: ou=groups,dc=1,dc=ff,dc=es,dc=eu,dc=org
```

```
objectClass: organizationalUnit
ou: groups
```

ldapuser.ldif (fichero LDAP)

```
dn: uid=pepe,ou=people,dc=1,dc=ff,dc=es,dc=eu,dc=org
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: pepe
sn: ubuntu
userPassword: {SSHA}eHhsh5tF0RxcH6pbIf05EzpiTxHghSbf
loginShell: /bin/bash
uidNumber: 2000
gidNumber: 2000
homeDirectory: /home/pepe

dn: cn=pepe,ou=groups,dc=1,dc=ff,dc=es,dc=eu,dc=org
objectClass: posixGroup
cn: pepe
gidNumber: 2000
memberUid: pepe
```

mod_ssl.ldif (fichero LDAP)

```
dn: cn=config
changetype: modify
add: olcTLSCACertificateFile
olcTLSCACertificateFile: /etc/ldap/sasl2/ca-certificates.crt
-
replace: olcTLSCertificateFile
olcTLSCertificateFile: /etc/ldap/sasl2/server.crt
-
replace: olcTLSCertificateKeyFile
olcTLSCertificateKeyFile: /etc/ldap/sasl2/server.key
```

mod_syncprov.ldif (fichero LDAP)

```
dn: cn=module,cn=config
objectClass: olcModuleList
cn: module
olcModulePath: /usr/lib/ldap
olcModuleLoad: syncprov.la
```

syncprov.ldif (fichero LDAP)

```
dn: olcOverlay=syncprov,olcDatabase={1}hdb,cn=config
objectClass: olcOverlayConfig
objectClass: olcSyncProvConfig
olcOverlay: syncprov
olcSpSessionLog: 100
```

Máquina u1ff7:

/etc/network/interfaces

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet6 loopback

# The primary network interface
# This is an autoconfigured IPv6 interface
#auto ens3
#iface ens3 inet6 auto
#      dns-nameservers 2001:470:20::2

auto ens3
iface ens3 inet6 manual

auto ens3.199
iface ens3.199 inet6 static
address 2001:470:736b:1ff::7
netmask 64
gateway 2001:470:736b:1ff::1
autoconf 0
vlan-raw-device ens3
```

base.ldif (fichero LDAP)

```
dn: ou=people,dc=1,dc=ff,dc=es,dc=eu,dc=org
objectClass: organizationalUnit
ou: people

dn: ou=groups,dc=1,dc=ff,dc=es,dc=eu,dc=org
objectClass: organizationalUnit
ou: groups
```

syncrepl.ldif

```
dn: olcDatabase={1}hdb,cn=config
changetype: modify
add: olcSyncRepl
olcSyncRepl: rid=001
  provider=ldap://nfsnis1.1.ff.es.eu.org:389/
  bindmethod=simple
  binddn="cn=admin,dc=1,dc=ff,dc=es,dc=eu,dc=org"
  credentials=adminope1
  searchbase="dc=1,dc=ff,dc=es,dc=eu,dc=org"
  scope=sub
  schemachecking=on
  type=refreshAndPersist
  retry="30 5 300 3"
  interval=00:00:05:00
```

Máquina u1fe6:

/etc/network/interfaces

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet6 loopback

# The primary network interface
# This is an autoconfigured IPv6 interface
#auto ens3
#iface ens3 inet6 auto
#      dns-nameservers 2001:470:20::2

auto ens3
iface ens3 inet6 manual

auto ens3.198
iface ens3.198 inet6 auto
accept_ra 1
autoconf 0
vlan-raw-device ens3
```

/etc/fstab

```
# /etc/fstab: static file system information.
#
# Use 'blkid' to print the universally unique identifier for a
# device; this may be used with UUID= as a more robust way to name devices
# that works even if disks are added and removed. See fstab(5).
#
# <file system> <mount point>   <type>  <options>       <dump>  <pass>
# / was on /dev/vda1 during installation
UUID=0191e2f0-1d0b-4133-9797-0f0b74cef492 /               ext4    errors=remount-ro
0       1
# swap was on /dev/vda2 during installation
UUID=20ad38c6-a2b0-4fa4-8829-6cf166f65566 none            swap    sw              0
0
nfsnis1.1.ff.es.eu.org:a755232 /home/a755232 nfs4
rw,nolock,noauto,x-systemd.automount,x-systemd.device-timeout=30,retry=0,_netdev 0
0
```

SCRIPTS USADOS

Se ha usado el programa u desarrollado como trabajo de la asignatura para testear que las máquinas nuevas estén accesibles desde la red y para configurar los servicios NTP y unbound mediante los manifiestos puppet desarrollados para el trabajo.

Además se han guardado en dos scripts llamados define.sh y undefine.sh el conjunto de instrucciones necesarias para realizar la puesta en marcha y parada de todas las máquinas de forma automática.

Fichero define.sh

```
#!/bin/bash
maquinas=( "orouter1.xml" "o1ff2.xml" "o1ff3.xml" "o1ff4.xml" )
for vm in "${maquinas[@]}";do
    sudo virsh define /misc/alumnos/as2/as22019/a755232/$vm
done
sudo virsh list --all
virt-manager
```

Fichero undefine.sh

```
#!/bin/bash
read -p "HAS APAGADO TODAS LAS MAQUINAS?? [yes|no]: " response
if [ $response = "yes" ];then
      maquinas=( "orouter1" "o1ff2" "o1ff3" "o1ff4" )
      for vm in "${maquinas[@]}";do
            sudo virsh undefine $vm &> /dev/null
      done
       pkill virt-manager
       sudo virsh list --all
else
    echo "Abortando..."
fi
```