AS2 : Práctica Nº 3

---

1. Resumen

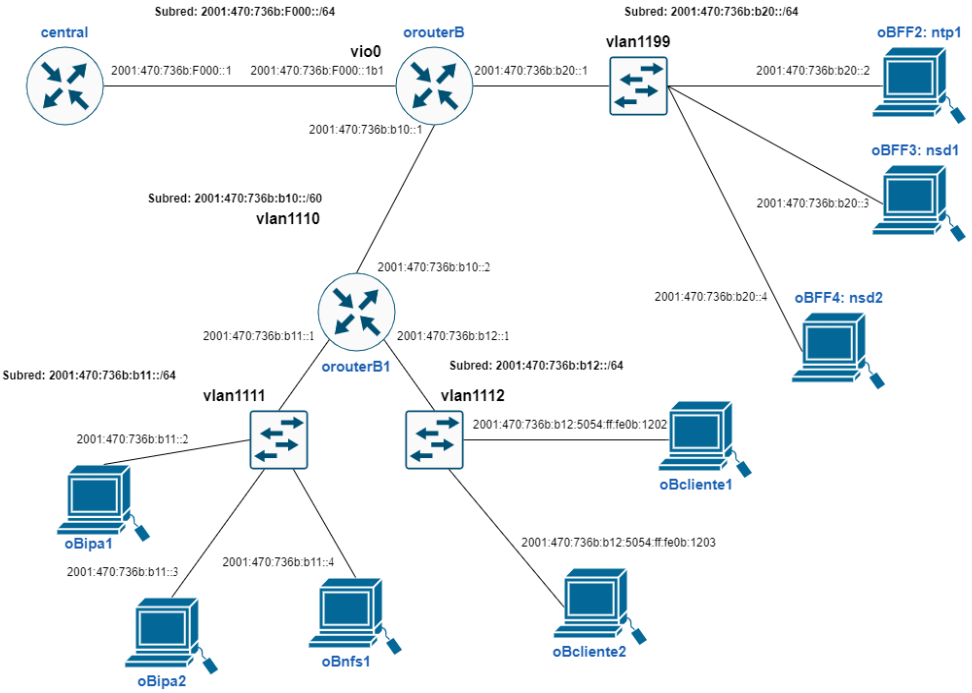
La siguiente práctica consiste en la puesta en marcha de un dominio FeeIpa y NFS mediante máquinas CentOS. Para ello, se ha tenido que configurar la red de máquinas virtuales. En primer lugar se han modificado las direcciones IP de la red obtenida como resultado de la práctica 2 cambiando las máquinas virtuales a la subred 2001:470:736b:b20::/64, y se ha añadido una nueva subred 2001:470:736b:b10::/60 en la que se desarrollará esta práctica, y bajo la cual salen dos subredes nuevas, 2001:470:736b:b11::/64, con el servidor maestro DNS , su réplica, y el servidor NFS, y 2001:470:736b:b12::/64, en la cuál se encuentran los clientes.

2. Introducción, objetivos y arquitectura de elementos relevantes

Entre los objetivos de está práctica, al igual que en prácticas anteriores, se encuentra la configuración de la red; en este caso la configuración de máquinas virtuales CentOS y una nueva subred, en la que se encuentra un router OpenBSD, el cual tiene que permitir el encaminamiento IPv6 entre las distintas subredes, y cinco máquinas CentOS, de las cuales 3 se van a configurar con una dirección estática y las restantes se configurarán dinámicamente.

Además, al igual que en la práctica anterior, se va a seguir trabajando con la configuración de un servidor DNS con la estructura maestro/réplica y algo nuevo como es un servidor NFS, mediante FreeIPA, una herramienta que integra varios componentes como un Directorio de Servicios (LDAP), Kerberos, NTP, DNS y un sistema de certificados.

A continuación se muestra el esquema de red que se ha configurado para la práctica, donde se muestran los elementos más relevantes.



3. Explicación de elementos significativos de la práctica.

Máquinas: en está práctica se han añadido 6 máquinas virtuales nuevas, entre las cuales se encuentra el **orouterb1**, está máquina es la única de las nuevas que es openBSD, es un nuevo router interior que va a permitir la comunicación entre las dos nuevas subredes en las que se distribuyen las nuevas máquinas, y las máquinas establecidas en la práctica anterior. Después encontramos las máquinas **ipa1**, donde se configurará el servidor IPA y la máquina **ipa2** que será la réplica de este. También dispondremos de la máquina nfs1 en la que se ha configurado un servidor NFS y por último dos máquinas clientes **cliente1** y **cliente2**.

Subredes: en primer lugar se ha añadido la subred **2001:470:736b:b10::/60** mediante la cual se comunicarán los routers orouterB (de prácticas anteriores), y el nuevo router (orouterB1). Esta subred se ha configurado con prefijo 60, ya que bajo está se van a configurar dos nuevas subredes adicionales con prefijo 64, **2001:470:736b:b11::/64** (donde se encuentran el ipa1, ipa2 y nfs1) y **2001:470:736b:b12::/64** (con los clientes).

FreeIpa y sus servicios: la herramienta de freeIPA permite crear en tu red un sistema de gestión de identidad que garantiza la seguridad de tu sistema. Además combina varios servicios como son:

- 389 Directory Server: el directorio de servicios, se encarga de almacenar los datos de estenuevo dominio de red. Además dispone de la BD de claves de kerberos.
- DNS: un servidor DNS, que simplemente resuelve las peticiones DNS (y como mucho las cachea).
- Kerberos: identifica, distribuye claves y provee comunicación confidencial e integra.
- NTP: servidor de tiempo.
- PKI: infraestructura de clave pública.

Servidor DNS y réplica con freeIPA: como ya hemos comentado en el punto anterior, freeIPA permite la gestión de servidores DNS. En nuestro sistema se ha configurado la máquina **ipa1** como el servidor DNS maestro y la máquina **ipa2** como su réplica. Está estructura permite que cualquier modificación que se realice en el servidor maestro, se propague y se vea reflejada en la réplica.

Servidor NFS con freeIPA: este servidor se ha montado en la máquina nfs1, y va a permitir a un sistema cliente de nuestro servidor (en nuestro caso las máquinas cliente1 y cliente2), para un usuario del dominio freeIPA, montar remotamente su sistema de ficheros del servidor NFS y acceder a él como si fuera un sistema de archivos local.

4. Explicación puesta en marcha y configuración de los diferentes aspectos requeridos.

Para la puesta en marcha y configuración de la práctica, en primer lugar se ha creado una imagen diferencial de la imagen oB (imagen base del sistema openBSD) y una nueva imagen base cB, con el sistema centOS, para la configuración de las máquinas virtuales centOS, que se crearán a partir de una imagen diferencial de esta imagen base cB.

Una vez añadidas las máquinas virtuales ya se puede configurar la red. Se ha configurado la **subred 2001:470:736b:b10::/60**, para ello se ha añadido en el router **orouterB** la **vlan1110**, mediante la cual se comunicará con el router **orouterB1**. Además, para permitir la comunicación desde el exterior de este router a las subredes internas **2001:470:736b:b11::/64** y **2001:470:736b:b12::/64**, se han añadido en la interfaz de la **vlan1110** dos rutas a la tabla de encaminamiento del orouterB:

```
echo '!route add -inet6 2001:470:736b:b11::/64 2001:470:736b:b10::2' > /etc/hostname.vlan1110
echo '!route add -inet6 2001:470:736b:b12::/64 2001:470:736b:b10::2' > /etc/hostname.vlan1110
```

Estas rutas indican que todos los paquetes que vayan hacia estas subredes, sean encaminados hacia el router orouterB1, el cual ya conoce las direcciones de destino.

El router **orouterB1**, se ha configurado como en prácticas pasadas, ya que es una máquina openBSD. Se ha habilitado el encaminamiento para ipv6 y se ha añadido la configuración para las distintas vlans, la **vlan1110**, **vlan1111** y **vlan1112**. Además, como las máquinas virtuales de la vlan1112 se configuran automáticamente, se ha modificado el fichero **/etc/rad.conf** -> interface vlan1112 y se ha activado el demonio **rad**, para que este este router envíe la información de prefijo a las máquinas de esta interfaz, y así puedan autoconfigurarse.

Seguidamente se han configurado las máquinas centOS. Para las máquinas de la subred **2001:470:736b:b11::/64** se ha seguido el siguiente esquema de configuración, modificando la dirección ipv6 dependiendo de la máquina:

- vi /etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0       //nombre interfaz
TYPE=Ethernet     //tipo interfaz
ONBOOT=yes        //activar interfaz en el arranque
IPV6INIT="no"     //no se establece dirección ipv6
```

- vi /etc/sysconfig/network-scripts/ifcfg-eth0.1111

```
DEVICE=eth0.1111
BOOTPROTO=static
ONBOOT=yes
VLAN=yes
IPV6INIT=yes
IPV6ADDR="2001:470:736b:b11::2/64"
IPV6_DEFAULTGW="2001:470:736b:b11::1"
```

Para las máquinas de la subred 2001:470:736b:b12::/64, el esquema cambia un poco, ya que en este caso no le indicamos la dirección ipv6, sino que hay que activar la opción de autoconfiguración:

- Configuracion vlan: vi /etc/sysconfig/network-scripts/ifcfg-eth0.1112

  DEVICE=eth0.1112
  BOOTPROTO=none
  ONBOOT=yes
  VLAN=yes
  IPV6INIT=yes
  IPV6_AUTOCONF=yes

Una vez ya tenemos las vlan bien configuradas y se puede hacer ping entre las distintas máquinas, en el nsd1 de la práctica anterior añadimos en las zonas DNS, esta nueva zona (glue records) que van a formar las máquinas ipa1 e ipa2, y se ha seguido configurando el servicio IPA.

Para la instalación del servidor IPA se han instalado en primer lugar los paquetes necesarios que van a permitir su instalación, y se ha instalado mediante el comando **ipa-server-install --domain-level 0**, indicando el nivel de dominio 0 para permitirnos más adelante la instalación de la réplica.

Antes de configurar las zonas DNS, hay que asegurarse que el servidor esté en buen estado, los puertos estén abiertos (netstat -tulpn | grep LISTEN) y comprobar que todos los servicios están encendidos (sudo ipactl status); por consiguiente ya se puede proceder a solicitar un ticket de Kerberos con **kinit admin**, lo que nos permitirá utilizar las herramientas IPA.

Una vez disponemos del ticket de Kerberos ya se pueden establecer las zonas DNS [2] que falten y sus respectivos records. Para ver las zonas DNS de la máquina se ha ejecutado el comando **ipa dnszone-find** , en nuestro caso, en la instalación del servidor ya se habia establecido la zona directa 1.b.ff.es.eu.org.. La zona inversa se ha añadido con el comando **ipa dnszone-add 1.b.0.b.6.3.7.0.7.4.0.1.0.0.2.ip6.arpa.**.

Además se ha añadido la resolucion directa e inversa de nombres de esa subred.

Directa:

```
ipa dnsrecord-add 1.b.ff.es.eu.org. ipa2 --aaaa-rec 2001:470:736b:b11::3
ipa dnsrecord-add 1.b.ff.es.eu.org. nfs1 --aaaa-rec 2001:470:736b:b11::4
ipa dnsrecord-add 1.b.ff.es.eu.org. router2 --aaaa-rec 2001:470:736b:b11::1
```

Inversa:

```
ipa dnsrecord-add 1.b.0.b.6.3.7.0.7.4.0.1.0.0.2.ip6.arpa. 3.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1
--ptr-rec ipa2.1.b.ff.es.eu.org.
ipa dnsrecord-add 1.b.0.b.6.3.7.0.7.4.0.1.0.0.2.ip6.arpa. 4.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1
--ptr-rec nfs1.1.b.ff.es.eu.org.
ipa dnsrecord-add 1.b.0.b.6.3.7.0.7.4.0.1.0.0.2.ip6.arpa. 1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1
--ptr-rec router2.1.b.ff.es.eu.org.
```

Para comprobar que las entradas se han añadido correctamente a sus respectivas zonas se puede ejecutar el comando **ipa dnsrecord-find** para cada una de las zonas:

```
ipa dnsrecord-find 1.b.0.b.6.3.7.0.7.4.0.1.0.0.2.ip6.arpa.
```

ipa dnsrecord-find 1.b.ff.es.eu.org.

A continuación se procede a realizar la creación de la **réplica** [3] en la máquina **ipa2**, para ello desde la máquina **ipa1** se prepara el fichero de información de réplica que contiene el REALM y otros datos básicos que se extraen del servidor maestro para configurar la réplica:

sudo ipa-replica-prepare ipa2.1.b.ff.es.eu.org --ip-address 2001:470:736b:b11::3

Y se transmite a la máquina **ipa2**:

scp /var/lib/ipa/replica-info-ipa2.1.b.ff.es.eu.org.gpg root@[2001:470:736b:b11::3]:/var/lib/ipa/

Con esto, la máquina **ipa2** ya puede proceder para la instalación de la réplica:

ipa-replica-install /var/lib/ipa/replica-info-ipa2.1.b.ff.es.eu.org.gpg

Es importante, una vez se ha creado la réplica, comprobar que las zonas se han replicado correctamente. Además se puede comprobar que si se añaden nuevos records, como podrían ser los de los clientes, estos también se transfieren a la réplica.

Una vez creada la réplica, como se especifica en el enunciado se ha procedido a la creación de dos nuevos usuarios de ipa mediante el comando **ipa user-add**, y a la instalación del **servidor NFS** y sus **clientes**.

Para la instalación y configuración del **servidor NFS**, en primer lugar (obviando la instalación de los paquetes necesarios), en el servidor **ipa1** se ha agregado el servicio NFS con el nombre **nfs/nfs1.1.b.ff.es.eu.org** al sistema, lo que permite a los clientes acceder a recursos compartidos de archivos a través de NFS utilizando la identidad y autentificación proporcionadas por freeIPA. También se ha establecido una relación de confianza entre FreeIPA y el servidor NFS en los dominios de los clientes, lo que permitirá a los clientes acceder a los recursos compartidos de archivos a través de NFS utilizando las credenciales gestionadas por FreeIPA.

Una vez establecidas estas relaciones, ya se puede proceder a gestionar el sistema de automontaje, para que sea posible montar automaticamente sistemas de archivos remotos en un directorio local cuando se accede a él, en lugar de montar manualmente los sistemas de archivos remotos. Para ello, en primer lugar se ha creado un mapa de montaje automático **auto.home** en la ubicación por defecto del servidor **ipa1**, se le ha agregado la clave **/home** al mapa de montaje automatico **auto.master** y se ha configurado la información para que busque en el mapa **auto.home**, para obtener la información de cómo se debe montar la ubicacion **/home**.

Por último, se ha añadido una nueva clave al mapa **auto.home**, donde la clave es cualquier cosa, y la información se ha configurado para que se monte en la ubicación **nfs1.1.b.ff.es.eu.org:/exports/home/&**, sustituyendo el & por la clave que le llegue.

Es decir, se ha establecido una configuración de montaje automática para el directorio /home en el servidor, donde este se encargará de buscar en el mapa auto.home cómo establecer ese montaje.

Una vez creados los mapas de automontaje, en el servidor NFS ya se puede proceder a crear el directorio **/exports/home**, y en este los directorios correspondientes a cada uno de los usuarios clientes. Por último exportamos e iniciamos el demonio nfs, y en los clientes

instalamos nfs, obtenemos el keytab de kerberos y montamos los mapas de automount de IPA.

Pruebas realizadas para comprobar el funcionamiento del sistema.

Pruebas:

- Server ipa1

  Directo: dig -6 AAAA router2.1.b.ff.es.eu.org

```
;; ANSWER SECTION:
router2.1.b.ff.es.eu.org. 86400 IN      AAAA
2001:470:736b:b11::1

;; AUTHORITY SECTION:
1.b.ff.es.eu.org.       86400   IN      NS
ipa1.1.b.ff.es.eu.org.
1.b.ff.es.eu.org.       86400   IN      NS
ipa2.1.b.ff.es.eu.org.

;; ADDITIONAL SECTION:
ipa1.1.b.ff.es.eu.org.  1200    IN      AAAA
2001:470:736b:b11::2
ipa2.1.b.ff.es.eu.org.  1200    IN      AAAA
2001:470:736b:b11::3

;; Query time: 0 msec
;; SERVER: ::1#53(::1)
```

  Inversa: dig -6 -x 2001:0470:736b:b11::4

```
;; ANSWER SECTION:
4.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.1.b.0.b.6.3.7.0.7.4.0.
.0.0.2.ip6.arpa. 86 400     IN PTR nfs1.1.b.ff.es.eu.org.

;; Query time: 0 msec
;; SERVER: ::1#53(::1)
```

- Réplica ipa2

  Directo: dig -6 @2001:470:736b:b11::3 AAAA nfs1.1.b.ff.es.eu.org

```
;; ANSWER SECTION:
nfs1.1.b.ff.es.eu.org.  1200    IN      AAAA
2001:470:736b:b11::4
;; Query time: 0 msec
;; SERVER: 2001:470:736b:b11::3#53(2001:470:736b:b11::3)
```

Inversa: dig -6 -x 2001:0470:736b:b11::4

```
;; ANSWER SECTION:
4.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.1.b.0.b.6.3.7.0.7.4.0.
.0.0.2.ip6.arpa. 86 400     IN PTR nfs1.1.b.ff.es.eu.org.

;; Query time: 0 msec
;; SERVER: 2001:470:736b:b11::3#53(2001:470:736b:b11::3)
```

- Creación nuevo usuario, los pasos seguidos son los siguientes:
    1. Crear usuario sin contraseña:
       `ipa user-add`
    2. Añadir contraseña a usuario <nombre>
       `ipa user-mod <nombre> --password`
    3. Comprobar creación del usuario:
       `ipa user-find`
    4. Crear directorio en nfs1:
       `mkdir /exports/home/<nombre>`
    5. Dar permisos a ese usuario:
       `chown <nombre>:<nombre> /exports/home/<nombre>`

  Por último, comprobar que podemos entrar a la máquina cliente1 o cliente2 con usuario <nombre> y ver que monta su sistema de ficheros.
  Con pwd, podemos comprobar el directorio en el que está es el home de ese usuario, por lo que se puede concluir que sí que funciona el automontaje del sistema de ficheros para un usuario freeIPA.

```
-sh-4.2$ pwd
/home/prueba
-sh-4.2$ id
uid=234800005(prueba) gid=234800005(prueba)
groups=234800005(prueba)
```

5. Problemas encontrados y su solución

Alguno de los probemas que se han encontrado durante la realización de la práctica son el espacio de memoria de las máquinas, este no era suficiente para que se pudiera completar la instalación del servidor IPA, por lo que se ha modificado en el fichero correspondiente de la máquina, <nombre_maquina>.xml, aumentando la memoria ram.
Otros de los problemas encontrados ha sido la instalación de la réplica, desde la máquina maestro no pérmitía crear el fichero de preparación de la réplica, debido a que el servidor maestro desde el que se estaba intentando crear ese fichero de preparación tenía un nivel de dominio 1, y el comando requería un nivel de dominio superior del servidor maestro con

respecto a la réplica, para solucionarlo se desinstaló el servidor maestro ipa1, y volvió a instalarse indicando un nivel de dominio 0.
Por último, otro de los problemas que han surgido han sido en la configuración del servidor NFS, principalmente que funcione de forma correcta el montaje automático del sistema de ficheros de cada cliente, debido a que los pasos que se estaban ejecutando y la reacción de los mapas de automontaje no se estaban realizando correctamente.

Bibliografia

1. 2.3. Installing an IdM Server: Introduction.
   https://access.redhat.com/documentation/es-es/red_hat_enterprise_linux/7/html/linux_domain_identity_authentication_and_policy_guide/install-server
2. Creación de zonas DNS, añadir records,etc. Red Hat, 33.4. Managing Master DNS Zones
   https://access.redhat.com/documentation/es-es/red_hat_enterprise_linux/7/html/linux_domain_identity_authentication_and_policy_guide/managing-master-dns-zones
3. Creación de la réplica, Red Hat, D.2. Creating Replicas
   https://access.redhat.com/documentation/es-es/red_hat_enterprise_linux/7/html/linux_domain_identity_authentication_and_policy_guide/creating-replicas-old
4. Red Hat. Chapter 2. Installing and Uninstalling an Identity Management Server
   https://access.redhat.com/documentation/es-es/red_hat_enterprise_linux/7/html/linux_domain_identity_authentication_and_policy_guide/installing-ipa