Escuela de
Ingeniería y Arquitectura
Universidad Zaragoza

adsis2-pr-3

Administración de Sistemas II

Autor 1:	Toral Pallás, Héctor - 798095
Grado:	Ingeniería Informática
Curso:	2022-2023

12 de abril de 2023

Índice

1. Introducción y objetivos

A continuación, se presenta el desarrollo de un proyecto que busca mejorar la seguridad y la eficiencia en la gestión de una red. En prácticas anteriores, se configuró una serie de servidores DNS para gestionar la subzona 7.ff.es.eu.org y un servidor NTP encargado de configurar la hora de los dispositivos conectados. Ahora, el objetivo es segmentar la red en tres zonas donde poder integrar nuevos servicios de una forma más organizada y profesional:

- La primera zona (720) albergará nuestros servidores DNS internos y NTP.
- La segunda zona (711) se encargará de gestionar otra zona DNS y todo lo relacionado con la autenticación de usuario mediante el uso de un servidor FreeIPA y un NFS Kerberizado.
- La tercera zona (712) será para los clientes de nuestra red.

Con esta segmentación, buscamos mejorar la seguridad y la eficiencia en la gestión de nuestra red, permitiendo una mayor organización y control sobre los servicios que se ofrecen.

2. Arquitectura del sistema

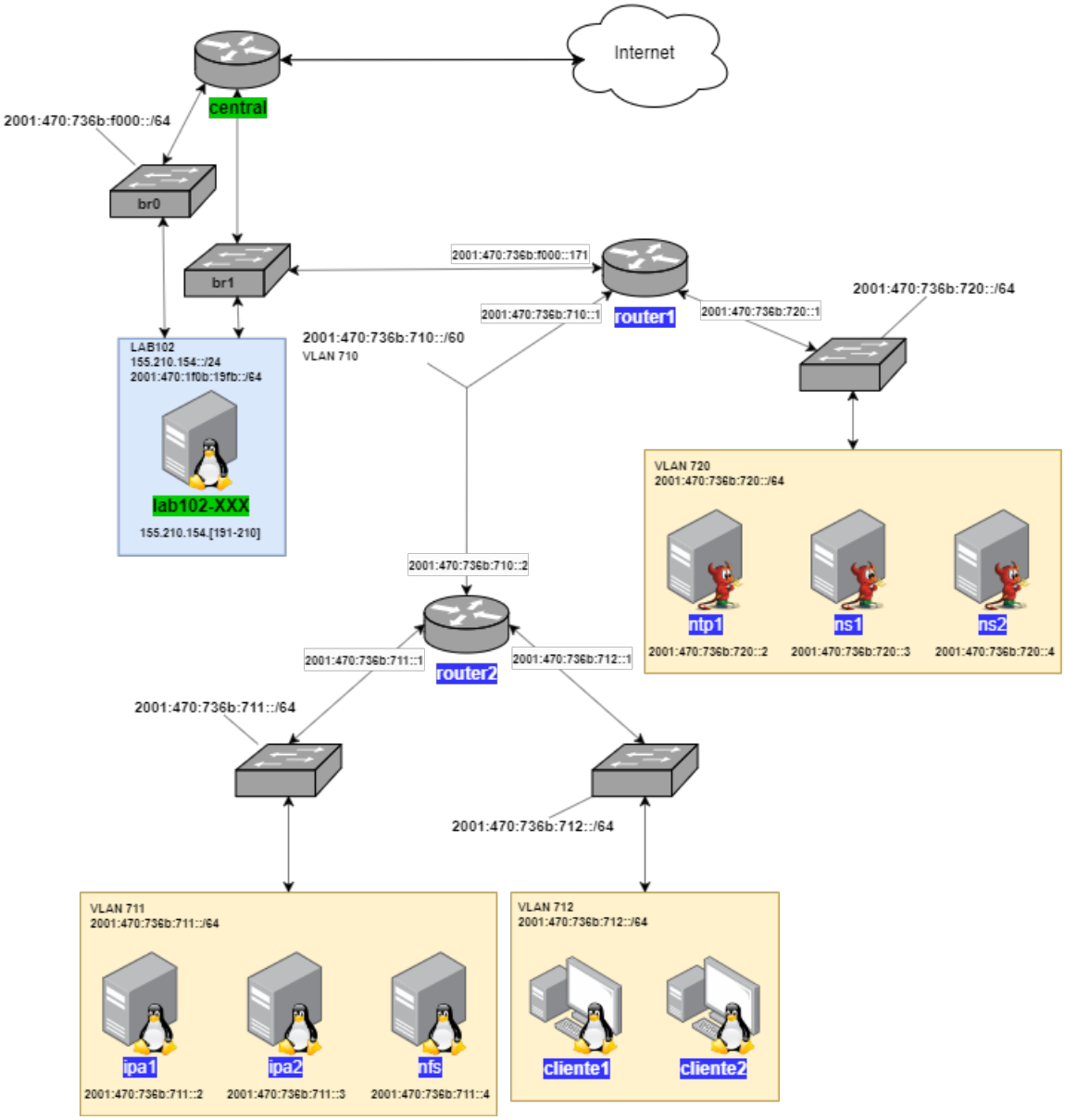

Figura 1: Arquitectura de red de la práctica 3

La infraestructura utilizada en el proyecto consiste en los servidores CentOS ubicados en el laboratorio 102 de la Universidad de Zaragoza. Estos servidores utilizan el sistema de virtualización QEMU, en el cual se han definido cada una de las máquinas virtuales. Para acceder a estas máquinas, se ha utilizado la interfaz br1, que se conecta a br0 mediante el enlace local de las tarjetas de red. De esta forma, se establece una comunicación con el servidor central, que actúa como gateway hacia el exterior.

Nuestra arquitectura cuenta con 2 routers, **router1** o router7 y **router2** o router71. Aunque ambos tienen la misma función de router, en el caso del router1, ha sido necesario configurar la redirección de paquetes de tal manera que los paquetes dirigidos a las subredes 711 y 712 sean redirigidos hacia la subred 710 permitiendo así continuar la búsqueda del destinatario de los paquetes en las diferentes subredes de manera eficiente.

2.1. Zona 710

En esta zona encontramos nuestro router2 que actúa de encaminador hacia las subredes 711 y 712 permitiendo así poder tener conectadas las 3 subredes.

2.2. Zona 711

En esta zona se alojan los nuevos servicios a integrar en la práctica como lo son el servidor FreeIPA y el NFS.

- 2001:470:736b:711::1 Hace referencia a router2 que actúa como gateway para la VLAN 711.
- **2001:470:736b:711::2** Servidor maestro FreeIPA
- **2001:470:736b:711::3** Servidor réplica FreeIPA
- **2001:470:736b:711::4** Servidor NFS kerberizado que utiliza el servidor FreeIPA para la gestión de credenciales.

2.3. Zona 712

En la tercera zona, se encuentran los clientes de la red, los cuales hacen uso de los recursos y servicios implementados en las demás subredes. Las direcciones IPv6 de estos clientes son asignadas automáticamente a través del router2. En esta zona, se puede acceder al servicio FreeIPA para realizar la autenticación de los usuarios y acceder al montaje definido por el servidor NFS.

- Cliente 1: **2001:470:736b:712:...**
- Cliente 2: **2001:470:736b:712:...**

2.4. Zona 720

Los cambios aplicados en esta zona respecto a la práctica anterior han consistido en añádir 2 forwarders al servidor DNS unbound de tal manera que si se pregunta por un nombre DNS se consulte también a los servidores instalados en las máquinas ipa1 e ipa2 pudiendo asi resolver la subzona **1.7.ff.es.eu.org**

3. Pruebas realizadas

3.1. FreeIPA

3.1.1. ipa domainlevel-get

Con esta prueba comprobamos que nivel de dominio se ha utilizado en la creación

3.1.2. ipactl status

Comprueba el estado de instalación de las réplicas

3.1.3. Comprobación de zonas

```
ipa dnsrecord-find <zone>
```

Se ha comprobado que las zonas creadas fueran las creadas

3.1.4. Resolución de zonas

Se han realizado peticiones DNS utilizando la herramienta dig para comprobar que resuelve las direcciones

```
dig AAAA ipa1.1.7.ff.es.eu.org
dig -x 2001:470:736b:711::2
```

3.1.5. Creación de usuarios

Se ha creado un usuario y se ha iniciado sesión satisfactoriamente en una máquina que tiene un cliente ipa.

```
ipa user-add jonhdoe
ssh johndoe@cliente1.1.7.ff.es.eu.org
```

también, se ha creado un fichero dentro del home montado para dicho usuario, de tal manera que se comprueba que el usuario creado tiene permisos dentro de este directorio.

3.2. NFS

Se ha comprobado que una vez iniciado sesión con el usuario en las máquinas clientes el home se monta correctamente y se tienen permisos para modificar los ficheros del home.

4. Dificultades

Falta memoria para ejecutar el servidor IPA

Para solucionar el error se subió la memoria de la máquina virtual de 2GB a 4GB.

certmonger.service no inicia correctamente

Para solucionar el error:

```
sudo systemctl restart dbus
sudo systemctl retart certmonger.service
```

Falla al instalar la réplica

Al crear las máquinas hubo un problema de configuración en los ficheros xml y resulto en que las máquinas IPA1 e IPA2 tenían la misma dirección MAC.

Replica creation using 'ipa-replica-prepare' to generate replica file is supported only in 0-level IPA domain.

En el proceso de creación de la réplica se intento realizar con el comando ïpa-replica-prepare"que es solo válido para crear la replica con ipa-domain level 0. Para solucionar este error se siguieron los pasos descritos en el mensaje de error y se solucionó sin mucho problema.

- ipa-client-install
- ipa-replica-install

Mensaje de error al usar ipa-replica-prepare

```
Replica creation using 'ipa-replica-prepare' to generate replica file
is supported only in 0-level IPA domain.

The current IPA domain level is 1 and thus the replica must
be created by promoting an existing IPA client.

To set up a replica use the following procedure:
    1.) set up a client on the host using 'ipa-client-install'
    2.) promote the client to replica running 'ipa-replica-install'
        *without* replica file specified

'ipa-replica-prepare' is allowed only in domain level 0
The ipa-replica-prepare command failed.
```

El usuario creado no tiene permisos

Para solucionar el problema hay que darle la propiedad del home al usuario.

```
sudo chown johndoe:johndoe johndoe/
sudo chmod 700 johndoe/
```

5. ANEXOS

5.1. Configuración de red

5.1.1. Red 710::X

Para comenzar, se necesita configurar la interfaz 710 en el router1 para que pueda identificar la dirección de destino de los paquetes recibidos y dirigirlos correctamente hacia la 720 o la 710. Para ello, se ha utilizado la siguiente configuración de red:

Ejemplo de archivo hostname.vlan710

```
up
inet6 2001:470:736b:710::1 60 vlan 710 vlandev vio0 -temporary
!route add -inet6 2001:470:736b:711::/64 2001:470:736b:710::2
!route add -inet6 2001:470:736b:712::/64 2001:470:736b:710::2
```

Una vez realizada esta configuración, se reinicia la red con "doas sh /etc/netstartz procedemos a configurar el router 2.

En el router 2 hay que configurar 4 interfaces (vio0, vlan710, vlan711, vlan712). A continuación se muestran los ficheros de configuración empleados.

Ejemplo de archivo hostname.vio0

```
-inet6
up
```

Ejemplo de archivo hostname.vlan710

```
vlan 710 vlandev vio0 up
inet6 2001:470:736b:710::2
```

Ejemplo de archivo hostname.vlan711

```
vlan 711 vlandev vio0 up
inet6 2001:470:736b:711::1
```

Ejemplo de archivo hostname.vlan712

```
vlan 712 vlandev vio0 up
inet6 2001:470:736b:712::1
```

Una vez configuradas estas, reinicamos la red y procedemos a activar la redirección de paquetes mediante los siguientes pasos:

Copia el archivo de ejemplo sysctl.conf al archivo de configuración actual:

```
cp /etc/examples/sysctl.conf /etc/sysctl.conf
```

Este comando copia el archivo de ejemplo "sysctl.conf"del directorio /etc/examples/.ªl archivo de configuración actual /etc/sysctl.conf". El archivo "sysctl.conf.es utilizado para establecer valores de configuración de kernel en OpenBSD.

Edita el archivo /etc/sysctl.conf para habilitar el forwarding de paquetes IPv6:

```
net.inet6.ip6.forwarding=1      # 1=Permit forwarding (routing) of IPv6 packets
```

Este paso modifica el archivo /etc/sysctl.conf"para habilitar el forwarding de paquetes IPv6. Se agrega una línea que establece el valor de la variable "net.inet6.ip6.forwarding.en "1", lo que permite el forwarding de paquetes IPv6.

Comprueba que el forwarding de paquetes IPv6 está habilitado:

```
sysctl net.inet6.ip6.forwarding      # 1=Permit forwarding (routing) of IPv6 packets
```

Este comando muestra el valor actual de la variable "net.inet6.ip6.forwarding". Si el valor es "1", significa que el forwarding está habilitado. Si el valor es "0", significa que está deshabilitado.

Habilita el forwarding de paquetes IPv6 en tiempo real:

```
doas sysctl net.inet6.ip6.forwarding=1
```

Este comando establece el valor de la variable "net.inet6.ip6.forwarding.[en] "1.[en] tiempo real, lo que habilita el forwarding de paquetes IPv6 sin necesidad de reiniciar el sistema.

5.1.2. Red 711::X

Para la generación de UUID únicos se puede utilizar el siguiente comando:

```
echo "UUID=$(uuidgen)" >> ifcfg-eth0.<n vlan>.
```

Ejemplo de archivo /etc/sysconfig/network-scripts/ifcfg-eth0

```
TYPE="Ethernet"
PROXY_METHOD="none"
BROWSER_ONLY="no"
DEFROUTE="yes"
IPV4_FAILURE_FATAL="no"
IPV6INIT="no"
IPV6_AUTOCONF="yes"
IPV6_DEFROUTE="yes"
IPV6_FAILURE_FATAL="no"
IPV6_ADDR_GEN_MODE="stable-privacy"
NAME="eth0"
DEVICE="eth0"
ONBOOT="yes"
IPV6_PRIVACY="no"
DNS1=2001:470:20::2
UUID="7f2813c5-c37c-4b77-ac7c-3b0dc20651e7"
```

Ejemplo de archivo /etc/sysconfig/network-scripts/ifcfg-eth0.711

```
VLAN=yes
TYPE=vlan
PHYSDEV=eth0
DEVICE=eth0.711
VLAN_ID=711
GVRP=no
REORDER_HDR=yes
MVRP=no
PROXY_METHOD=none
BROWSER_ONLY=no
IPV6INIT=yes
IPV6_AUTOCONF=no
IPV6ADDR=2001:470:736b:711::2
IPV6_DEFAULTGW=2001:470:736B:711::1
DNS1=2001:470:736b:720::2
DOMAIN=1.7.ff.es.eu.org
IPV6_DEFROUTE=yes
IPV6_FAILURE_FATAL=no
IPV6_ADDR_GEN_MODE=stable-privacy
NAME=eth0.711
ONBOOT=yes
UUID=74f3cca4-7e72-42f2-86d7-4dbbd3125eaf
```

Además hay que deshabilitar la configuración automática de IPv6 solo en la tajeta de red base (eth0), para que

solo se pueda establecer comunicación por vlan y para ello se tiene que configurar el fichero **/etc/sysctl.conf** de la siguiente manera:

Ejemplo de archivo sysctl.conf

```
net.ipv6.conf.eth0.use_tempaddr = 0
net.ipv6.conf.eth0.autoconf = 0
net.ipv6.conf.eth0.accept_ra = 0
```

Finalmente, es necesario configurar el nombre de host de la máquina. Como paso opcional en una fase temprana, se recomienda modificar el archivo /etc/hosts para permitir que el servidor IPA resuelva los nombres de host.

Ejemplo de archivo hosts

```
127.0.0.1   localhost localhost.localdomain localhost4 localhost4.localdomain4
::1         localhost localhost.localdomain localhost6 localhos
2001:470:736b:711::2  ipa1.1.7.ff.es.eu.org ipa1
2001:470:736b:711::3  ipa2.1.7.ff.es.eu.org ipa2
2001:470:736b:711::4  nfs.1.7.ff.es.eu.org  nfs
```

Ejemplo de archivo /etc/hostname

```
ipa1.1.7.ff.es.eu.org
```

Ejemplo de archivo /etc/sysconfig/network

```
ipa1.1.7.ff.es.eu.org
```

5.1.3. Red 712::X

Como la mayoría de ficheros son muy similares a los de la zona 711, solo se muestran a continuación los de la parte de configuración de la vlan 712 que son diferentes.

Ejemplo de archivo /etc/sysconfig/network-scripts/ifcfg-eth0

```
TYPE="Ethernet"
PROXY_METHOD="none"
BROWSER_ONLY="no"
DEFROUTE="yes"
IPV4_FAILURE_FATAL="no"
IPV6INIT="no"
IPV6_AUTOCONF="yes"
IPV6_DEFROUTE="yes"
IPV6_FAILURE_FATAL="no"
IPV6_ADDR_GEN_MODE="stable-privacy"
NAME="eth0"
DEVICE="eth0"
ONBOOT="yes"
IPV6_PRIVACY="no"
DNS1=2001:470:20::2
UUID="7f2813c5-c37c-4b77-ac7c-3b0dc20651e7"
```

Ejemplo de archivo /etc/sysconfig/network-scripts/ifcfg-eth0.712

```
VLAN=yes
TYPE=vlan
PHYSDEV=eth0
DEVICE=eth0.712
VLAN_ID=712
REORDER_HDR=yes
GVRP=no
MVRP=no
PROXY_METHOD=none
BROWSER_ONLY=no
IPV6_INIT=yes
```

```
IPV6_AUTOCONF=yes
DNS1=2001:470:736b:711::2
DNS2=2001:470:736b:711::3
DOMAIN=1.7.ff.es.eu.org
IPV6_DEFROUTE=yes
IPV6_FAILURE_FATAL=no
IPV6_ADDR_GEN_MODE=stable-privacy
NAME=eth0.712
UUID=353eed5f-5d30-46dc-8f21-e13988dbdb21
ONBOOT=yes
```

5.2. FreeIPA

5.2.1. FreeIPA Maestro

Instalamos el servidor FreeIPA

```
yum install freeipa-server ipa-server-dns
```

Una vez instalado el servidor Free IPA haya sido instalado de manera exitosa, procederemos a configurar la zona DNS mediante los siguientes comandos:

Ejemplo de configuración directa por consola

```
ipa dnsrecord-add 1.7.ff.es.eu.org ipa1 --aaaa-ip-address=2001:470:736b:711::2
ipa dnsrecord-add 1.7.ff.es.eu.org ipa2 --aaaa-ip-address=2001:470:736b:711::3
ipa dnsrecord-add 1.7.ff.es.eu.org nfs  --aaaa-ip-address=2001:470:736b:711::4

ipa dnsrecord-add 1.7.ff.es.eu.org cliente1 --aaaa-ip-address=2001:470:736b:712:5054:ff:fe01
    :1202
ipa dnsrecord-add 1.7.ff.es.eu.org cliente2 --aaaa-ip-address=2001:470:736b:712:5054:ff:fe01
    :1203
```

Ejemplo de configuración inversa por consola

```
ipa dnsrecord-add 1.7.0.b.6.3.7.0.7.4.0.1.0.0.2.ip6.arpa. 2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1
    --ptr-rec=ipa1.1.1.ff.es.eu.org.
ipa dnsrecord-add 1.7.0.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=ipa2.1.1.ff.es.eu.org.
ipa dnsrecord-add 1.7.0.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=nfs1.1.1.ff.es.eu.org.

ipa dnsrecord-add 1.7.0.b.6.3.7.0.7.4.0.1.0.0.2.ip6.arpa. 2.f.8.0.9.4.2.3.6.0.8.a.c.8.f.7.2
    --ptr-rec=cliente1.1.7.ff.es.eu.org.
ipa dnsrecord-add 1.7.0.b.6.3.7.0.7.4.0.1.0.0.2.ip6.arpa. 1.0.0.9.9.4.d.d.4.6.c.c.5.9.c.f.2
    --ptr-rec=cliente2.1.7.ff.es.eu.org.
```

Cabe destacar que la configuración de los clientes ha sido configurada de igual manera que que las demás máquinas para poder simplificar la operativa. Esto ha sido posible gracias a que las direcciones asignadas a las máquinas clientes es siempre la misma, en caso contrario hubiese sido necesario configurar algún mecanismo que nos permitiese tener un DNS dinámico.

5.2.2. FreeIPA Réplica

Debido a que nuestro dominio IPA no es de nivel 0 no podemos hacer uso de ipa-replica-prepare, es por eso que los pasos a seguir para instalar la réplica son:

En el servidor cliente que desea promocionar a una réplica, instale el paquete IPA client

```
sudo yum install ipa-client
```

Una vez que se complete la instalación, ejecute el siguiente comando para unirse al servidor FreeIPA:

```
sudo ipa-client-install
```

Ahora, en el servidor principal de FreeIPA, ejecute el siguiente comando para promover el cliente recién instalado a una réplica:

```
sudo ipa-replica-install
```

5.3. NFS

Para la configuración del servidor NFS se requieren de los siguientes paquetes:

```
yum install freeipa-client nfs-utils
```

Una vez tengamos nuestro cliente ipa configurado y el servicio nfs corriendo, procederemos con la configuración del servicio:

Tareas a realizar en las réplicas IPA

Añada la entidad de seguridad del servicio NFS al servidor y el cliente a Kerberos.

```
[root@ipa1 ~]# ipa service-add nfs/nfs.1.7.ff.es.eu.org
[root@ipa1 ~]# ipa service-add nfs/cliente1.1.7.ff.es.eu.org
[root@ipa1 ~]# ipa service-add nfs/cliente2.1.7.ff.es.eu.org
```

Añadir el mapa auto.home en el servidor ipa

```
[root@ipa1 ~]# ipa automountmap-add default auto.home
------------------------------
Added automount map "auto.home"
------------------------------
  Map: auto.home
```

Y añade el mapa auto.home a auto.master

```
[root@ipa1 ~]# ipa automountkey-add default --key "/home" --info auto.home auto.master
---------------------------
Added automount key "/home"
---------------------------
  Key: /home
  Mount information: auto.home
```

Por último, añade la clave al mapa auto.home

```
[root@ipa1 ~]# ipa automountkey-add default --key "*" --info "-fstype=nfs4,rw,sec=krb5,soft,
    rsize=8192,wsize=8192 nfs.example.com:/exports/home/&" auto.home
-----------------------
Added automount key "*"
-----------------------
  Key: *
  Mount information: -fstype=nfs4,rw,sec=krb5i,soft,rsize=8192,wsize=8192 nfs.example.com:/
    exports/home/&
```

Configura el servidor NFS

Cree un Keytab Kerberos para su servidor NFS

```
[root@nfs ~]# kinit admin
[root@nfs ~]# ipa-getkeytab -s ipa1.1.7.ff.es.eu.org -p nfs/nfs.1.7.ff.es.eu.org -k /etc/
    krb5.keytab
```

Indica a tu servicio NFS que utilice NFSv4

```
[root@nfs ~]# perl -npe 's/#SECURE_NFS="yes"/SECURE_NFS="yes"/g' -i /etc/sysconfig/nfs
```

Crea un recurso compartido NFS e inicie el servidor NFS

```
[root@nfs ~]# mkdir /exports/home
[root@nfs ~]# echo "/exports/home  *(rw,sec=sys:krb5:krb5i:krb5p)" >> /etc/exports
[root@nfs ~]# service nfs start
[root@nfs ~]# chkconfig nfs on
```

Configura los clientes

```
[root@cliente1 ~]# sudo yum install ipa-client
```

Obtener el keytab de Kerberos

```
[a798095@cliente1 ~]# kinit admin
[root@cliente1 ~]# ipa-getkeytab -s ipa1.1.7.ff.es.eu.org -p nfs/cliente1.1.7.ff.es.eu.org -
    k /etc/krb5.keytab
```

Por último, hay que configurar los clientes para que utilicen los mapas automount proporcionados por IPA

```
[root@cliente1 ~]# sudo yum install ipa-client
[root@client1 ~]# ipa-getkeytab -s ipa1.1.7.ff.es.eu.org -p nfs/cliente1.1.7.ff.es.eu.org -k
     /etc/krb5.keytab
[root@cliente1 ~]# ipa-client-automount --location=default
```

5.3.1. Creación de un usuario

Para crear un usuario hay que realizar 2 pasos esencialmente:

- 1. Crear el usuario
- 2. Exportar el home del usuario

Para poder crear el usuario necesitaremos realizar los siguientes pasos:

```
[root@nfs ~]# kinit admin
[root@nfs ~]# ipa user-add johndoe
[root@nfs ~]# ipa passwd johndoe
[root@nfs ~]# ipa user-mod johndoe --shell=/bin/bash
```

Una vez tengamos el usuario creado, podremos proceder a exportar un ”home”para este.

```
[root@nfs ~]# mkdir -p /exports/home/johndoe
[root@nfs ~]# chown johndoe:johndoe johndoe/
[root@nfs ~]# chmod 700 exports/home/johndoe/
[root@nfs ~]# exportfs -a
```

6. Bibliografia

- Luc de Louw's Blog
- NFS and FreeIPA
- How to Set Up NFS Server and Client on CentOS 8
- Como Configurar Servidor Replica en FreeIPA
- How to Install FreeIPA Server on RHEL 8 — Rocky Linux 8 — AlmaLinux 8
- FreeIPA NFS krb5p (Spanish)
- Lab: Montando Volúmenes Gluster via nfs
- Setup NFS Server on CentOS
- Configuring a Red Hat Enterprise Linux System as an IPA Client
- Managing Dynamic DNS Updates
- Replica$_{S}etup$