ADMINISTRACIÓN DE SISTEMAS 2

PRÁCTICA 2

Pablo Moreno Muñoz 841972

Identificador W->E

ÍNDICE

Resumen

Se ha llevado a cabo una reestructuración de la red, introduciendo nuevas subredes para routers, servicios freeIPA a clientes y clientes.
Se ha agregado un nuevo router y tres máquinas Fedora para proporcionar servicios nuevos. Se incluyen dos VMs Fedora con IPv6 dinámica en la zona de clientes. Se detalla el despliegue y configuración de un servicio FreeIPA que da soporte a un servidor NFS y a dos máquinas clientes en una VLAN vecina.

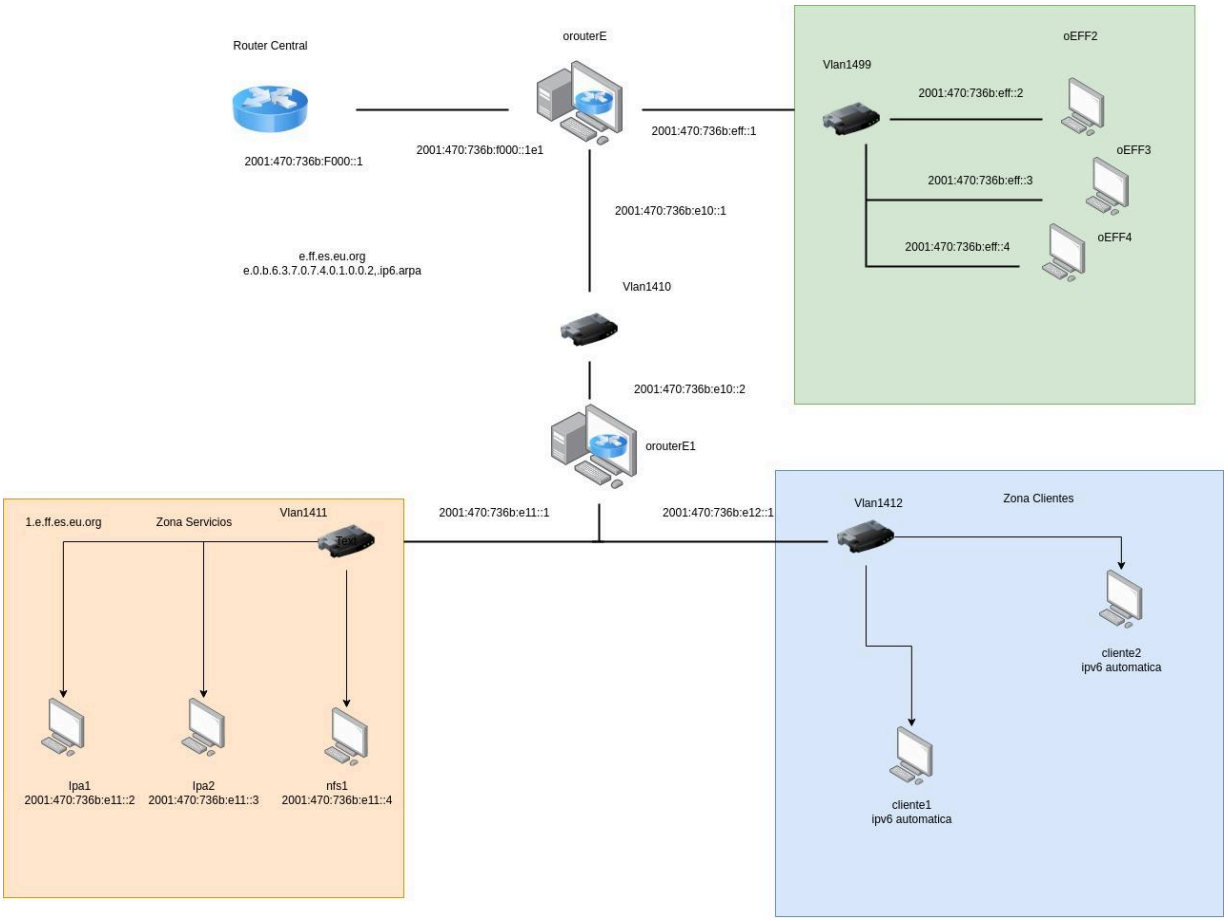
Introducción y objetivos

Los objetivos de esta práctica incluyen aprender y desplegar los servidores y clientes especificados, entender el funcionamiento de un servidor FreeIPA para proporcionar servicios DNS, autenticación y gestión de usuarios en red, así como comprender el funcionamiento de un servidor NFS y su servicio a las máquinas clientes.
Dentro de los objetivos establecidos, FreeIPA proporciona una solución compacta para configuración e integración, que incluye Kerberos para seguridad. Se utiliza NFS en formato Kerberizado para almacenamiento, contribuyendo a una mayor seguridad en la red.

Objetivos

- Ser capaces de entender como funciona un servidor FreeIpa y como desplegarlo
- Acostumbrarse y dominar el uso de ruby
- Configurar de forma adecuada un servidor NFS y dar servicio a la maquinas cliente

Arquitectura de elementos relevantes



Comprehensión de elementos significativos de la práctica

Router Virtual Nuevo

La configuración fue muy similar al router antiguo teniendo que implementar las dos nuevas VLAN's 1411 y 1412 para comunicarse con los clientes y los servicios. Además de la VLAN1410 para comunicarse con el router antiguo y así reeexpedir los paquetes de las vlans inferiores al resto de l arquitectura

Router Virtual Antiguo
Se puede resaltar que se tuvo que modificar el fichero hostname.vlan1410 para añadir las nuevas sentencias de enrutamiento para encaminar los paquetes hacia los clientes y servicios nuevos desplegados

freeIPA MAESTRO

Se desplegó el servidor FreeIPA Maestro como parte de la infraestructura de la red. Este servidor se configuró para proporcionar servicios de autenticación, gestión de usuarios y DNS de forma centralizada.
Se actualiza el archivo /etc/hosts con la dirección IPv6 y nombre del servidor. Se instala y configura el servidor FreeIPA, seleccionando opciones como integración de DNS y especificando el nombre del servidor. Se ajustan las reglas de firewall para permitir los servicios necesarios. Se establecen los registros DNS y se configura el cliente NTP.

freeIPA REPLICA

Se implementó el servidor FreeIPA Réplica como un componente adicional para respaldar al servidor FreeIPA Maestro. Esta réplica se encarga de mantener actualizada la información de autenticación y usuarios, garantizando la disponibilidad del servicio.
Se ajusta el nombre del host y el DNS por defecto. Se configura la replicación DNS con el maestro, se instala y configura el cliente NTP y se instala el cliente FreeIPA. Se añade el host de replicación al grupo de servidores IPA y se configura la zona DNS inversa.

NFS

Se configuró un servidor NFS (Network File System) para proporcionar almacenamiento compartido a los clientes de la red. Se utilizó el formato Kerberizado para aumentar la seguridad de la red y garantizar la integridad de los datos compartidos.

Clientes

Se configuraron y desplegaron los clientes de la red, los cuales acceden a los servicios proporcionados por los servidores FreeIPA y NFS. Estos clientes pueden realizar autenticación de usuarios y acceder a los archivos compartidos.
Se instala y configura el cliente IPA, se añaden los registros DNS para los clientes y se configura el cliente NTP. Se monta el recurso compartido NFS y se configura el automontado. Se crea y prueba la autenticación de usuarios.

Configuración de máquinas base Fedora

Fedora

Primeramente tenemos que lanzar la máquina virtual y ejecutamos el comando

adduser -u 1000 a841972
usermod -aG wheel a841972
passwd a841972 #Aquí introducimos la contraseña

Introducimos el comando visudo para acceder al fichero de configuración sudoers
Y descomentamos la siguiente línea
Allow root to run any commands anywhere
root ALL=(ALL) ALL

Allows people in group wheel to run all commands
%wheel ALL=(ALL) ALL

Same thing without a password
%wheel ALL=(ALL) NOPASSWD: ALL

A continuación modificamos la configuración del fichero /etc/sysctl.conf (solo deben estar estas entradas activas) :
net.ipv6.conf.eth0.use_tempaddr = 0
net.ipv6.conf.eth0.autoconf = 0
net.ipv6.conf.eth0.accept_ra = 0

Una vez hecho esta pequeña configuración des-definimos la máquina con el siguiente comando:
virsh -c qemu+ssh://a841972@155.210.154.198/system undefine fed39

MODIFICACIONES DE LA RED PREVIA

MODIFICACIONES ROUTER

Para crear la VLAN 410:
Creamos el fichero /etc/hostname.vlan1410:

vlan 1410 vlandev vio0 up
inet6 2001:470:736b:e10::1 60
inet6 -temporary
inet6 -soii
!route add 2001:470:736b:e11::0/64 2001:470:736b:e10::2
!route add 2001:470:736b:e12::0/64 2001:470:736b:e10::2

Configuración inicial del orouterE1

Editamos el contenido del fichero /etc/hostname.vio0 y escribimos el siguiente:
up
-inet6

Creamos el fichero /etc/hostname.vlan1410 y su contenido es el siguiente:
vlan 1410 vlandev vio0 up
inet6 2001:470:736b:e10::2

Añadimos en /etc/mygate

2001:470:736b:e10::1

Ejecutamos el siguiente comando para reiniciar y aplicar todos los cambios:
sh /etc/netstart

Escribimos en el fichero /etc/sysctl.conf el siguiente contenido:
net.inet6.ip6.forwarding=1

CONFIGURACIÓN VLAN 1411

Creamos el fichero /etc/hostname.vlan1411 y su contenido es el siguiente:

vlan 1411 vlandev vio0 up
inet6 2001:470:736b:e11::1

CONFIGURACIÓN VLAN 1412

Creamos el fichero /etc/hostname.vlan1412 y su contenido es el siguiente:
vlan 1412 vlandev vio0 up
inet6 2001:470:736b:e12::1

Modificamos el fichero /etc/rad.conf con el siguiente contenido:
interface vlan1412

Hay que poner en funcionamiento el servicio de anuncio de prefijos IPv6 a la subred de la vlan mediante servicio rad : A través de /etc/rc.conf.local:

rad_flags=""

Guardamos el fichero y ejecutamos el siguiente comando para activar el servicio rad:
rcctl enable rad

Servicios de red DNS

Editar el fichero /etc/resolv.conf y escribir lo siguiente:
nameserver 2001:470:736b:eff::2
Para aplicar los cambios ejecutar el comando:
sh /etc/netstart

Añadir al DNS

Añadimos en el fichero /var/nsd/zones/e.ff.es.eu.org.directo de la máquina ns1
router2 IN AAAA 2001:470:736b:e10::2
Dentro de /var/nsd/zones/e.0.b.6.3.7.0.7.4.0.1.0.0.2.ip6.arpa.
2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1 IN PTR router2.e.ff.es.eu.org.
Para comprobar y aplicar los cambios recargamos las zonas y hacemos notify al esclavo

Configuración VM de la vlan1411

Cambiamos el nombre de la máquina en /etc/hostname por:

ipa1E , ipa2E y nfs1E respectivamente

Para configurar la red principal tenemos que establecer solo la ip link-local y para eso tenemos que hacer hacer lo siguiente:

nmcli connection modify 'Wired connection 1' ipv6.method link-local

Para configurar la subred vlan1411 tenemos que configurarlo de la siguiente manera:
#Creamos la vlan
nmcli connection add type vlan con-name vlan1411 dev "ens3" id 1411
nmcli connection modify vlan1411 ipv6.method manual ipv6.address "2001:470:736b:e11::4/64"
nmcli connection modify vlan1411 ipv6.gateway 2001:470:736b:e11::1

Además añadimos en el /etc/systemd/resolved.conf el servidor unbound
DNS= 2001:470:736b:eff::2

Configuramos la zona Ipa en el DNS y en el UBOUND

Maquina UNBOUND
Añadimos al fichero /var/unbound/etc/unbound.conf :

forward-zone:
name: "1.e.ff.es.eu.org."
forward-addr: 2001:470:736b:e11::2
forward-first: yes

access-control 2001:470:736b:e10::1 /60 allow
Ejecutamos el comando
unbound-control reload

MAQUINA DNS MAESTRO

Añadimos al fichero /var/nsd/zones/e.0.b.6.3.7.0.7.4.0.1.0.0.2.ip6.arpa.

2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.1 IN PTR ipa1.1.e.ff.es.eu.org.
3.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.1 IN PTR ipa2.1.e.ff.es.eu.org.
4.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.1 IN PTR nfs1.1.e.ff.es.eu.org.

Ejecutamos el comando

nsd-control reload e.0.b.6.3.7.0.7.4.0.1.0.0.2.ip6.arpa.

CONFIGURACIÓN IPA MASTER

Actualizamos el contenido del fichero /etc/hosts añadiendo

2001:470:736b:e11::2 ipa1.1.e.ff.es.eu.org ipa1
2001:470:736b:e11::3 ipa2.1.e.ff.es.eu.org ipa2
2001:470:736b:e11::4 nfs1.1.e.ff.es.eu.org nfs1
2001:470:736b:e12::2 cliente1.1.e.ff.es.eu.org cliente1
2001:470:736b:e12::3 cliente2.1.e.ff.es.eu.org cliente2
2001:470:736b:e12::4 cliente3.1.e.ff.es.eu.org cliente3

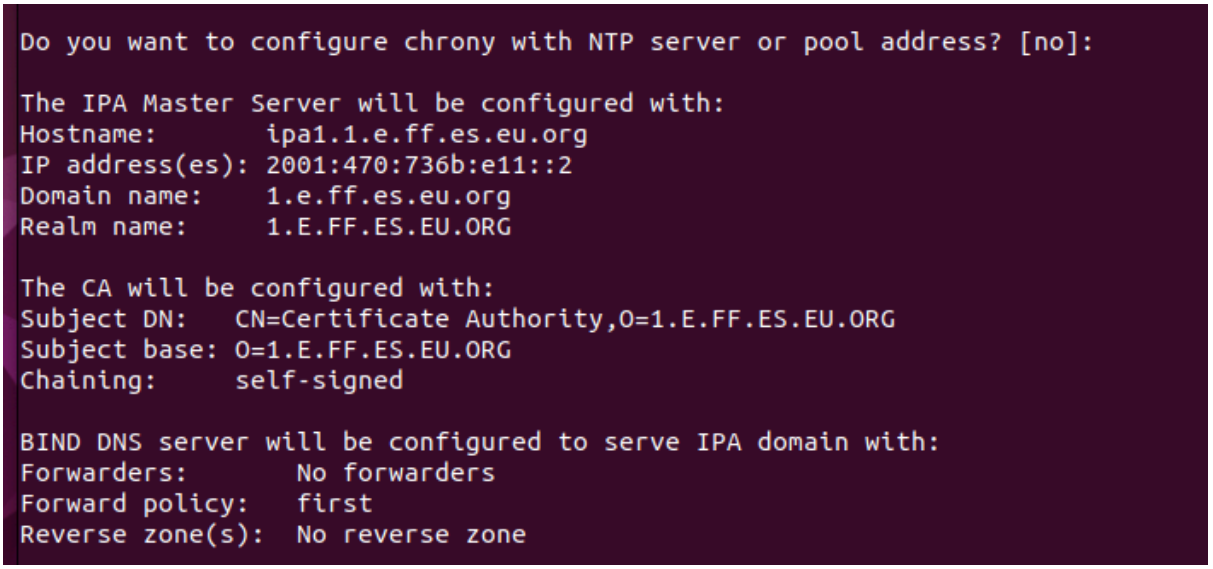
Añadimos al fichero /etc/sysconfig/network

HOSTNAME=nfs1.1.e.ff.es.eu.org

Ahora instalamos el servidor freeipa:

dnf -y install freeipa-server freeipa-server-dns freeipa-client
ipa-server-install --setup-dns

Durante la instalación hay que seleccionar las siguientes opciones:
DNS integrado:SI
SERVERHostname: ipa1.1.e.ff.es.eu.org
Las contraseñas de directory manager y IPA admin son las mismas que las de root
No dns forwarder
No reverse zones



Si el Firewalld está activo hay que permitir los servicios

firewall-cmd --add-service={freeipa-ldap,freeipa-ldaps,dns,ntp}
firewall-cmd --runtime-to-permanent

CONFIGURACIÓN IPA REPLICA

Actualizamos el contenido del fichero /etc/hosts añadiendo

2001:470:736b:e11::3 ipa2.1.e.ff.es.eu.org ipa2

Añadimos al fichero /etc/sysconfig/network

HOSTNAME=ipa2.1.e.ff.es.eu.org

Cambiamos el dns por defecto en /etc/systemd/resolved.conf por:
DNS=2001:470:736b:eff::2

Tenemos que añadir al IPA-dns del maestro el nuevo record name ipa2 de la siguiente manera:
ipa dnsrecord-add 1.e.ff.es.eu.org ipa2 --aaaa-rec 2001:470:736b:e11::3

A continuación tenemos que configurar el cliente ntp mediante chrony
Para ello modificamos el fichero /etc/chrony.conf añadiendo

pool 2001:470:736b:eff::1 iburst

Y habilitamos el chrony

systemctl enable --now chronyd

A continuación descargamos el free ipa-cliente

dnf -y install freeipa-server freeipa-server-dns freeipa-client

Una vez instalado

sudo ipa-client-install --server=ipa1.1.e.ff.es.eu.org --domain 1.e.ff.es.eu.org

Proceed with fixed values and no DNS discovery? [no]: yes
Do you want to configure chrony with NTP server or pool address? [no]:
Continue to configure the system with these values? [no]: yes
User authorized to enroll computers: admin

En FreeIPA Master, tenemos que añadir un host de replicación al grupo [ipaservers].
Además, debe resolver la resolución de direcciones en el host maestro y el host réplica.
ipa hostgroup-add-member ipaservers --hosts ipa2.1.e.ff.es.eu.org

Añadimos la zona DNS para a continuación añadir la resolución inversa
ipa dnszone-add 1.e.0.b.6.3.7.0.7.4.0.1.0.0.2.ip6.arpa.

```
----------------------------
[root@ipa1 ~]# ipa dnszone-add e.0.b.6.3.7.0.7.4.0.1.0.0.2.ip6.arpa.
  Zone name: e.0.b.6.3.7.0.7.4.0.1.0.0.2.ip6.arpa.
  Active zone: True
  Authoritative nameserver: ipa1.1.e.ff.es.eu.org.
  Administrator e-mail address: hostmaster
  SOA serial: 1710325260
  SOA refresh: 3600
  SOA retry: 900
  SOA expire: 1209600
  SOA minimum: 3600
  BIND update policy: grant 1.E.FF.ES.EU.ORG krb5-subdomain
                      e.0.b.6.3.7.0.7.4.0.1.0.0.2.ip6.arpa. PTR;
  Dynamic update: False
  Allow query: any;
  Allow transfer: none;
[root@ipa1 ~]#
```

ipa dnsrecord-add 1.e.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.e.ff.es.eu.org.
ipa dnsrecord-add 1.e.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.e.ff.es.eu.org.

Si el Firewalld está activo hay que permitir los servicios

sudo firewall-cmd --add-service=freeipa-replication
sudo firewall-cmd --runtime-to-permanent

En Free-Ipa replica

Si el Firewalld está activo hay que permitir los servicios

sudo firewall-cmd
--add-service={freeipa-ldap,freeipa-ldaps,dns,ntp,freeipa-replication}
sudo firewall-cmd --runtime-to-permanent

A continuación descargamos los paquetes freeipa-server y service-dns

dnf -y install freeipa-server freeipa-server-dns

Ahora instalamos el free-ipa replica mediante el siguiente comando
ipa-replica-install --setup-ca --setup-dns --no-forwarders

Cuando acaba la instalación comprobamos los usuarios replicados con los siguiente comandos y comprobamos que son los mismos que en el maestro:

kinit admin
ipa user-find

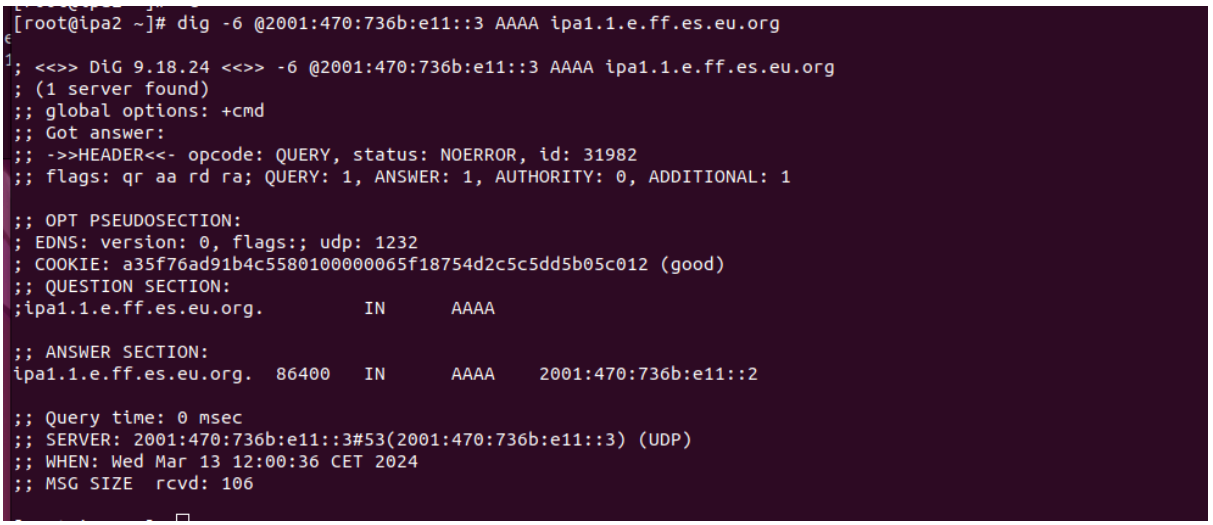
```
root@ipa1 ~]# ipa user-find
--------------
1 user matched
--------------
  User login: admin
  Last name: Administrator
  Home directory: /home/admin
  Login shell: /bin/bash
  Principal alias: admin@1.E.FF.ES.EU.ORG, root@1.E.FF.ES.EU.ORG
  UID: 1300800000
  GID: 1300800000
  Account disabled: False
----------------------------
Number of entries returned 1
----------------------------
root@ipa1 ~]#
root@ipa2 ~]# ipa user-find
--------------
1 user matched
--------------
  User login: admin
  Last name: Administrator
  Home directory: /home/admin
  Login shell: /bin/bash
  Principal alias: admin@1.E.FF.ES.EU.ORG, root@1.E.FF.ES.EU.ORG
  UID: 1300800000
  GID: 1300800000
  Account disabled: False
----------------------------
Number of entries returned 1
----------------------------
```

Podemos comprobar la correcta replicación del servicio dns con las siguientes sentencias:

dig -6 @2001:470:736b:e11::3 -x 2001:470:736b:e11::2

```
[root@ipa2 ~]# dig -6 @2001:470:736b:e11::3 -x  2001:470:736b:e11::2

; <<>> DiG 9.18.24 <<>> -6 @2001:470:736b:e11::3 -x 2001:470:736b:e11::2
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43167
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 47e86c3dd6b288db0100000065f186e358a54aa4282a3769 (good)
;; QUESTION SECTION:
;2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.1.e.0.b.6.3.7.0.7.4.0.1.0.0.2.ip6.arpa. IN PTR

;; ANSWER SECTION:
2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.1.e.0.b.6.3.7.0.7.4.0.1.0.0.2.ip6.arpa. 86400IN PTR ipa1.1.e.ff.es.eu.org.

;; Query time: 0 msec
;; SERVER: 2001:470:736b:e11::3#53(2001:470:736b:e11::3) (UDP)
;; WHEN: Wed Mar 13 11:58:43 CET 2024
;; MSG SIZE  rcvd: 164
```

dig -6 @2001:470:736b:e11::3 AAAA ipa1.1.e.ff.es.eu.org



Configurar NFS Kerberizado:

Actualizamos el contenido del fichero /etc/hosts y añadimos
2001:470:736b:e11::4 nfs1.1.e.ff.es.eu.org nfs1

Añadimos al fichero /etc/sysconfig/network
HOSTNAME=nfs1.1.e.ff.es.eu.org

Cambiamos el dns por defecto en /etc/systemd/resolved.conf:
DNS=2001:470:736b:eff::2

Tenemos que añadir al IPA-dns del maestro el nuevo record name nfs1 de la siguiente manera:

ipa dnsrecord-add 1.e.ff.es.eu.org nfs1 --aaaa-rec 2001:470:736b:e11::4
ipa dnsrecord-add 1.e.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.e.ff.es.eu.org.

Y habilitamos el chrony

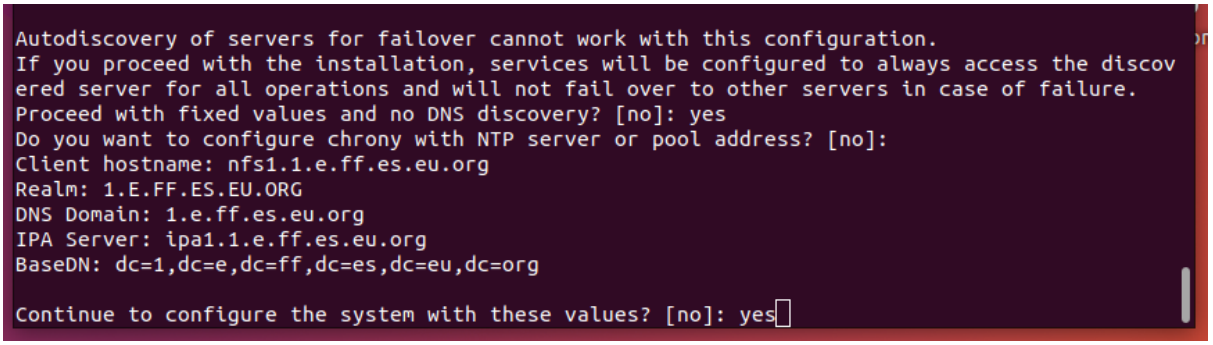
systemctl enable --now chronyd
chronyc sources

A continuación descargamos el free ipa-cliente
dnf install ipa-client

Una vez instalado

sudo ipa-client-install --server=ipa1.1.e.ff.es.eu.org --domain 1.e.ff.es.eu.org

Proceed with fixed values and no DNS discovery? [no]: yes
Do you want to configure chrony with NTP server or pool address? [no]:
Continue to configure the system with these values? [no]: yes
User authorized to enroll computers: admin

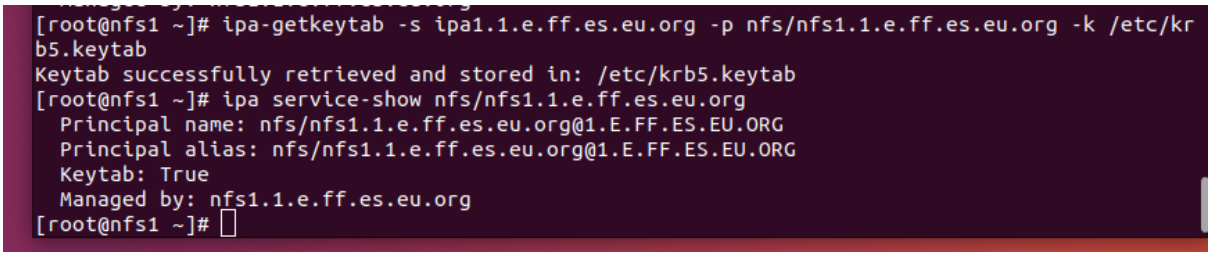


Desde el host:
kinit admin
ipa service-add nfs/nfs1.1.e.ff.es.eu.org

Desde el nfs:

ipa-getkeytab -s ipa1.1.e.ff.es.eu.org -p nfs/nfs1.1.e.ff.es.eu.org -k /etc/krb5.keytab
systemctl restart nfs-server
systemctl enable nfs-server

Comprobamos el funcionamiento con:
ipa host-del nfs1.1.e.ff.es.eu.org
ipa service-show nfs/nfs1.1.e.ff.es.eu.org



Configuramos el firewall del servidor nfs:

sudo firewall-cmd --add-service=nfs --add-service=mountd --add-service=rpc-bind
sudo firewall-cmd --runtime-to-permanent

Configuramos las exportaciones NFS compatible con Kerberos en el directorio /etc/exports que se utilizará.

/exports/home *(rw,sec=krb5:krb5i:krb5p, all_squash)

*: El asterisco significa que la exportación se aplica a todos los clientes. Permite que cualquier cliente acceda al directorio exportado.

rw: Significa "lectura-escritura". Concede permisos tanto de lectura como de escritura a los clientes que acceden al directorio exportado.
sec=krb5:b5i:krb5p: Esta parte especifica la configuración de seguridad para la exportación utilizando Kerberos.
krb5: Indica el uso de Kerberos para la autenticación.
krb5i: Especifica que se debe aplicar la verificación de integridad utilizando Kerberos.
krb5p: Indica que se debe encriptar el tráfico utilizando Kerberos.

A continuación ejecutamos el siguiente comando para que exporte el nuevo recurso compartido. (-r : reexportar todos los directorios, -a : exportar o desexportar todos los directorios)
exportfs -ra

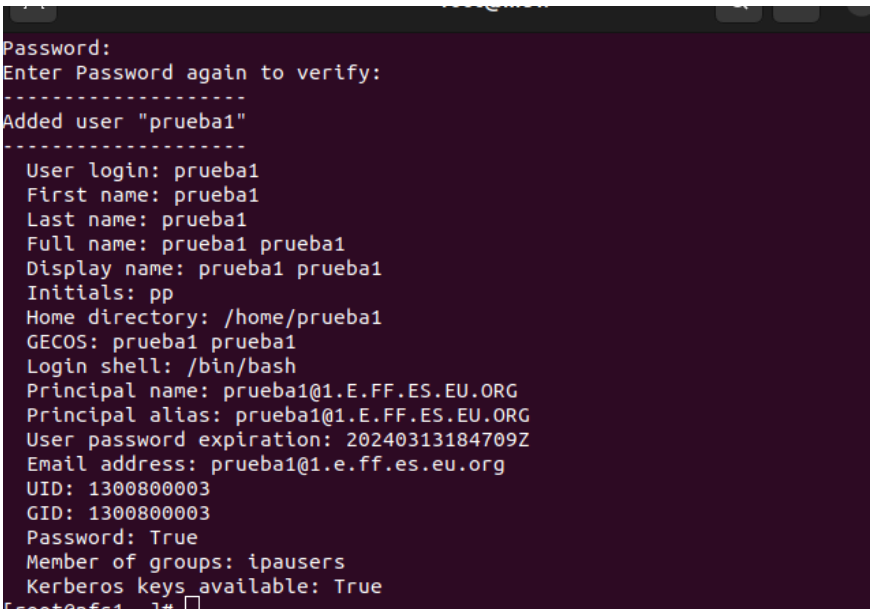
Habilitamos el nfs seguro *systemctl enable nfs-server --now* y mostramos los directorios a exportar con *showmount -e*

Creamos el mapa de montaje automático auto.home en la ubicación predeterminada y a continuación se crea una clave de montaje automático.

ipa automountmap-add default auto.home
ipa automountkey-add default --key "/home" --info auto.home auto.master
ipa automountkey-add default --key "*" --info "-fstype=nfs4,rw,sec=krb5,soft nfs1.1.e.ff.es.eu.org:/exports/home/&" auto.home

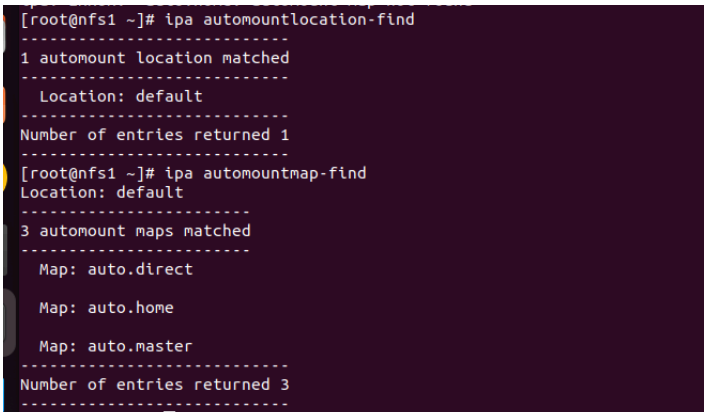
Podemos crear un usuario llamado prueba1

ipa user-add --first prueba1 --last prueba1 --password prueba1 --shell=/bin/bash



Creamos un directorio y un fichero dentro del directorio home que vamos a exportar

mkhomedir_helper prueba1
mkdir -p /exports/home
mv /home/prueba1 /exports/home/
touch /exports/home/prueba1/test.txt
chown :prueba1 /exports/home/prueba1/test.txt



Creación de clientes fedora

Cambiamos el nombre de la máquina en /etc/hostname por:

cliente1 y cliente2 respectivamente seguido .1.e.ff.es.eu.org

Modificamos el fichero hosts y añadimos la siguiente sentencia:
2001:470:736b:e11::2 ipa1.1.e.ff.es.eu.org ipa1

Cambiamos el dns por defecto en /etc/systemd/resolved.conf por:

DNS= 2001:470:736b:eff::2

Para configurar la red principal tenemos que establecer solo la ip link-local y para eso tenemos que hacer hacer lo siguiente:
nmcli connection modify 'Wired connection 1' ipv6.method link-local

Para configurar la subred vlan1412 tenemos que configurarlo de la siguiente manera:
#Creamos la vlan
nmcli connection add type vlan con-name vlan1412 dev "ens3" id 1412
nmcli connection modify vlan1412 ipv6.method auto
nmcli connection modify vlan1412 ipv6.address 2001:470:736b:e12::Z/64
#Se estableció esta conexión para facilitar la configuración, pero se usó la conexión automática para los servicios.
nmcli connection modify vlan1412 ipv6.gateway 2001:470:736b:e12::1

Ejecutamos el comando:

sudo systemctl restart NetworkManager

Ejecutamos el siguiente comando para poder instalar el cliente IPA:
dnf install ipa-client

Seguimos los pasos anteriores para instalar un cliente IPA

Añadimos al host IPA los siguientes DNS

 # Para la dirección IPv6 2001:470:736b:e12::2

ipa dnsrecord-add 1.e.ff.es.eu.org cliente1 --aaaa-rec 2001:470:736b:e12::2

 # Para el registro de resolución inversa correspondiente

ipa dnsrecord-add 1.e.0.b.6.3.7.0.7.4.0.1.0.0.2.ip6.arpa. 2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2 --ptr-rec cliente1.1.e.ff.es.eu.org.

 # Para la dirección IPv6 2001:470:736b:e12:fd65:e42e:6b79:52a8

ipa dnsrecord-add 1.e.ff.es.eu.org cliente2 --aaaa-rec 2001:470:736b:e12::3

 # Para el registro de resolución inversa correspondiente

ipa dnsrecord-add 1.e.0.b.6.3.7.0.7.4.0.1.0.0.2.ip6.arpa. 3.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2 --ptr-rec cliente2.1.e.ff.es.eu.org.

A continuación tenemos que configurar el cliente ntp mediante chrony
Para ello modificamos el fichero /etc/chrony.conf añadiendo

pool 2001:470:736b:eff::1 iburst

Y habilitamos el chrony

systemctl enable --now chronyd
chronyc sources

A continuación descargamos el free ipa-cliente
dnf install ipa-client

Una vez instalado

sudo ipa-client-install --server=ipa1.1.e.ff.es.eu.org --domain 1.e.ff.es.eu.org

Desde el host:
kinit admin
ipa host-add cliente1.1.e.ff.es.eu.org
ipa service-add nfs/clienteZ.1.e.ff.es.eu.org

sudo firewall-cmd --add-service=nfs --add-service=mountd --add-service=rpc-bind
sudo firewall-cmd --runtime-to-permanent

ipa-getkeytab -s ipa1.1.e.ff.es.eu.org -p nfs/clienteZ.1.e.ff.es.eu.org -k /etc/krb5.keytab

sudo mount -v -t nfs -o sec=krb5 nfs1.1.e.ff.es.eu.org:/exports/home /exports/home

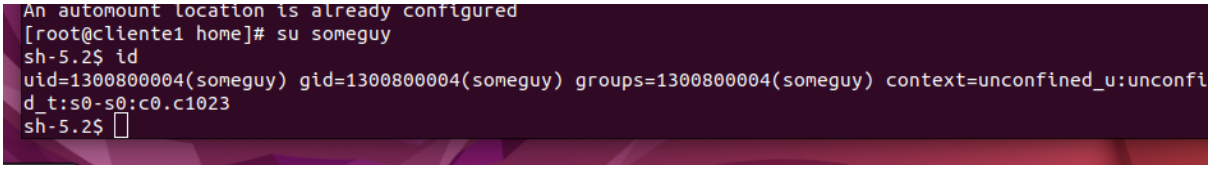
ipa-client-automount —location default -U

ssh prueba1@localhost
Aquí te hace actualizar la password y se cambia a prueba1234
Ahora podemos comprobar el acceso a los ficheros exclusivos para el usuario prueba1

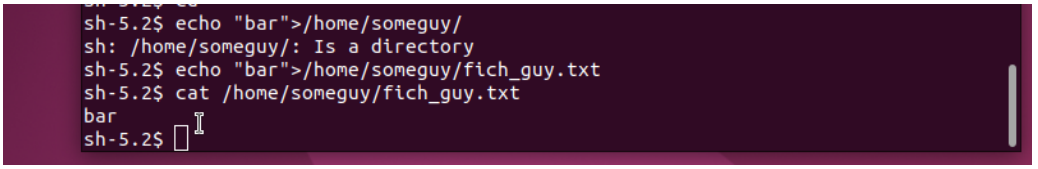
Ahora podemos crear otro usuario para comprobar que funciona correctamente.
Desde el servidor nfs con credenciales hacemos lo siguiente:

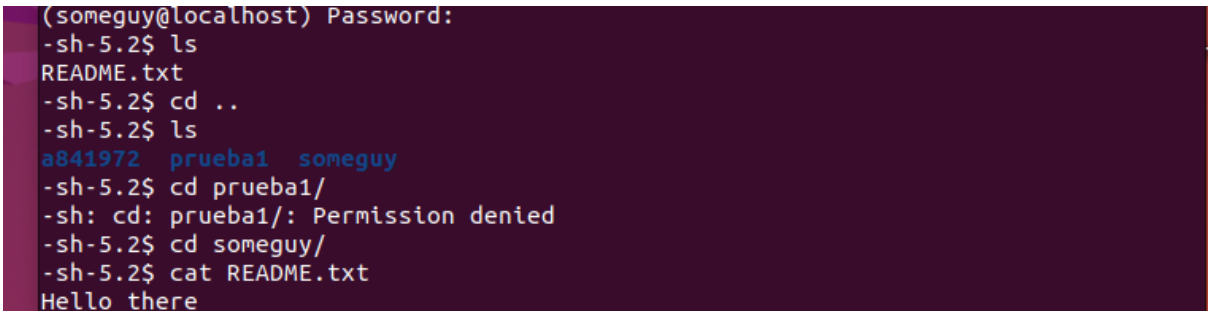
ipa user-add someguy
ipa passwd someguy
New Password = someguy123

Comprobamos en los clientes que funciona el nuevo usuario:



Creamos un nuevo fichero para el usuario someguy





Problemas encontrados y su solución.

Un problema fue a la hora de configurar el nuevo router e intentar hacer ping6 a las vlan1411 y 12 desde el router antiguo lo cual no funcionaba a pesar de que habíamos modificado /etc/sysctl.conf con el siguiente contenido:

net.inet6.ip6.forwarding=1
Se soluciono haciendo un reboot del sistema ya que con el comando sh /etc/netstart no era suficiente

Otro problema encontrado fue la configuración de la red en los sistemas Fedora ya que en un principio se intentó configurar mediante los scripts ifcfg. Lo cual resultó estar deprecated y se tuvo que configurar la red mediante comandos nmcli

Otro problema encontrado fue a la hora de instalar el cliente feeIpa. Debido a que daba error ya que no estaba sincronizado el NTP para solucionar este problema se estableció en el fichero /etc/chronyd.conf el servidor NTP del routerE común para el servidor y para todos los clientes FreeIpa

Otro problema encontrado fue a la hora de hacer un mount en el cliente daba problemas de permisos pero tras mirar los logs daba un error de pre-autenticación de Kerberos: Para solucionarlo tuve que reinstalar el servidor ya que tenía un problema en la autentificación requerida al propagar el TGT de kerberos

Finalmente a lo largo del desarrollo de la práctica hubo ciertos problemas debido principalmente al firewall de Unizar el cual no permitía a varias conexiones SSH sucesivas a el lab. lo que provocaba una privación de los recursos tanto de Moodle como de central para mi IP, por lo tanto se decidió traspasar el script que se usaba desde el escritorio para las máquinas de laboratorio lo cual cesó este problema

Otro problema encontrado fue a la hora del montaje de los directorios kerberizado de NFS, esto se solucionó teniendo en cuenta que el comando kinit admin administraba unos tickets distintos si lo hacías con sudo o si lo hacías con el usuario a841972 , debido a que el fichero /etc/krb5.conf tiene de owner el root se tenía que hacer los comandos con sudo para primero conseguir las keytabs y posteriormente hacerlo sin el sudo para que le diera las keytabs también al usuario a841972 para asi poder hacer al final el comando mount y se montara correctamente.

ANEXO

https://blog.khmersite.net/p/automating-home-directory-with-ipa/

A parte de lo requerido en la práctica se ha realizado un pequeño script en bash que combinado con las nuevas funcionalidades del script de la primera práctica, permite una vez definidos y iniciados las máquinas, abrir automáticamente una terminal por máquina virtual encendida y conectarse a cad auna de estas máquinas mediante la lectura de un fichero con sus ip's

Unset

```
#!/bin/bash

# Verifica si el archivo m1.txt existe
if [ ! -f "m1.txt" ]; then
  echo "El archivo m1.txt no existe."
  exit 1
fi

# Itera sobre cada línea del archivo m1.txt
while IFS= read -r ip_address; do
  gnome-terminal -- ssh -t -Y a841972@central.cps.unizar.es "ssh -t -Y
a841972@$ip_address"
done < "m1.txt"
```