ADMINISTRACIÓN DE SISTEMAS 2

Memoria práctica III

Grupo Viernes Mañana

21/03/2024

GUILLERMO BAJO LABORDA, 842748@unizar.es

Universidad Zaragoza
1542

Escuela de Ingeniería y Arquitectura Universidad Zaragoza

Índice

Resumen

Esta tercera práctica de la asignatura de administración de sistemas 2 se ha enfocado en desplegar un dominio FreeIPA compuesto por un servidor maestro y una réplica (esclavo), además de configurar un servidor NFS que a su vez actúa como cliente en el dominio IPA. Por otra parte se han conectado clientes a este dominio para operar con la gestión centralizada de usuarios y el almacenamiento de archivos.

Para llevar a cabo esta implementación, se ha trabajado con máquinas virtuales sobre el sistema operativo Fedora. Además, se ha ampliado el esquema de red utilizado en prácticas anteriores mediante la creación de nuevas VLANs y la introducción de un nuevo router interior.

A lo largo de la implementación, se ha seguido un enfoque metodológico, dividiendo la implementación en etapas y comprobando el correcto funcionamiento de cada componente antes de avanzar al siguiente paso. Esto ha permitido identificar y resolver problemas de manera más eficiente, lo que ha permitido no solo evitar la acumulación de problemas, sino también abordar los inconvenientes que han ido surgiendo de manera gradual a lo largo del proceso.

Introducción y objetivos

A grandes rasgos, el objetivo principal de esta práctica es la puesta en funcionamiento de un dominio FreeIPA y un sistema de archivos NFS sobre Fedora.

Por una parte se pretende establecer un dominio utilizando FreeIPA, encargado de gestionar aspectos cruciales de la red, como la autenticación de usuarios, la autorización de acceso a recursos y la resolución de nombres. Otro de los objetivos principales ha sido implementar un sistema de ficheros NFS para permitir el intercambio de datos entre diferentes sistemas de la red de forma eficiente y segura. Esto requiere la configuración adecuada del servidor NFS y la asignación de permisos de acceso para garantizar la seguridad de la información compartida.

Otro aspecto imprescindible de la práctica es la configuración de la infraestructura de red, que incluye la asignación de direcciones IPv6, la configuración del nuevo router interno y la gestión de las nuevas subredes VLAN para permitir la comunicación entre los diversos componentes del sistema.

Arquitectura de elementos relevantes

La infraestructura desplegada en esta práctica consta de varias máquinas virtuales y servidores configurados para llevar a cabo las funcionalidades requeridas. En primer lugar, se establece una red con dos subredes IPv6. El router exterior actúa como punto de conexión entre estas subredes y direcciona el tráfico adecuadamente. Además, se implementan servidores DNS maestro, esclavo y recursivo con caché en máquinas virtuales distintas en una de las subredes. En la otra subred se implementa un nuevo router que redirige el tráfico a nuevas máquinas que se encuentran en dos subredes bajo el router.

Las máquinas virtuales (VM2, VM3 y VM4) desempeñan roles específicos en la infraestructura. VM2 actúa como servidor NTP adicional y como servidor DNS recursivo con caché. VM3 se configura como servidor DNS maestro (primario), mientras que VM4 asume el papel de servidor DNS esclavo (secundario). Cada una de estas máquinas virtuales tiene asignada una dirección IPv6 según el esquema definido en el enunciado.

Las nuevas máquinas conectadas mediante la VLAN2711 toman el papel de servidor IPA maestro, esclavo y NFS kerberizado, respectivamente. En cambio, las dos máquinas conectadas mediante la VLAN2712 toman el papel de clientes IPA.

En cuanto a los servicios, se utiliza la herramienta unbound para configurar un servidor DNS recursivo y con caché en VM2, permitiendo la resolución eficiente de nombres y optimizando las consultas DNS. Se establecen servidores DNS autorizados (ns1 y ns2) en VM3 y VM4, respectivamente, para gestionar la resolución de nombres en la zona DNS definida.

El servidor IPA maestro actúa como el punto central de administración del dominio IPA, gestionando usuarios, grupos y más. Por otro lado, el servidor IPA esclavo replica la información del maestro para proporcionar redundancia y tolerancia a fallos. Esto garantiza que, en caso de fallo del maestro, el servicio proporcionado pueda seguir funcionando sin interrupciones.

El servidor NFS kerberizado ofrece un servicio de almacenamiento compartido. La integración de Kerberos con NFS añade una capa adicional de protección al sistema de archivos compartido, asegurando que solo los usuarios autorizados puedan acceder a los recursos compartidos.

Comprehensión de elementos significativos de la práctica

FreeIPA es una plataforma que ofrece servicios de gestión de identidad y acceso en sistemas linux. En esta práctica se han desplegado servidores maestros y réplicas de FreeIPA. El servidor maestro actúa como el componente principal que gestiona los servicios de directorio, autenticación y políticas de seguridad para la infraestructura de la red. La replicación entre los servidores FreeIPA garantiza la coherencia de los datos, lo que asegura la disponibilidad y redundancia de los servicios. La replicación aumenta la tolerancia a fallos.

El uso de NFS kerberizado implica la configuración de un servidor NFS que utiliza Kerberos para autenticar clientes y garantizar la seguridad en el acceso a los recursos compartidos. Esta configuración asegura que solo los usuarios autorizados puedan acceder a los archivos compartidos, proporcionando una capa adicional de protección.

El automontaje permite a los clientes montar automáticamente los sistemas de archivos compartidos cuando se accede a ellos, eliminando la necesidad de configurar manualmente cada punto de montaje en cada cliente. Esta funcionalidad garantiza un acceso transparente y seguro a los recursos compartidos del servidor NFS mediante autenticación Kerberos y autorización a través de IPA.

La introducción de nuevos routers implica la configuración adecuada tanto del router exterior como del router interior para enrutar los paquetes IP a las diferentes subredes definidas en el entorno, lo que garantiza la conectividad entre los diferentes componentes de la red. La implementación de VLANs (Virtual Local Area Networks) permite segmentar la red virtualmente.

Los clientes IPA son sistemas que se integran en el dominio FreeIPA y utilizan los servicios proporcionados por los servidores IPA para la autenticación, el acceso a recursos compartidos y otras funcionalidades.

Si profundizamos en aspectos más concretos de la práctica, en el contexto de Kerberos, un principal es una identidad única que puede ser autenticada dentro del sistema. Un principal puede representar un usuario, un servicio o una máquina en una red. Por otra parte, el archivo keytab es un archivo utilizado en sistemas que utilizan el protocolo Kerberos para autenticación de red. Este

contiene una o más claves secretas que representan las identidades de servicios en un sistema. A su vez, este archivo almacena las claves de autenticación de los principals del sistema.

Un mapa de montaje, (automount map) es una asociación entre directorios y ubicaciones en el sistema de archivos que se configuran para montarse automáticamente cuando se accede a ellos. Estos mapas son utilizados para gestionar de manera dinámica el montaje y desmontaje de recursos compartidos de red, sistemas de archivos remotos u otros dispositivos de almacenamiento. En otras palabras, se podría interpretar como un conjunto de instrucciones que le dicen al sistema operativo cómo encontrar y montar automáticamente carpetas compartidas desde otros lugares de la red cuando se necesiten.

Respecto a la segunda parte de la práctica, el script en ruby y los manifiestos, cabe destacar que los manifiestos de Puppet son archivos de configuración que contienen declaraciones que especifican los recursos que deben ser configurados una máquina, como paquetes a instalar, archivos a gestionar, servicios a ejecutar y configuraciones de red, entre otros aspectos.

Puesta en marcha y configuración

Primeramente se ha procedido a configurar la imágen fedora base. Para ello, se ha copiado la imagen a mi directorio personal y se ha adaptado el fichero XML correspondiente, tal y como se ha venido haciendo en prácticas anteriores. Respecto a la configuración de la imagen base, para empezar se ha añadido el usuario a842748 y se le ha añadido al grupo wheel. Por otra parte, para deshabilitar la configuración automática de IPv6 en la tarjeta de red base para tan solo tener comunicación por vlan, se ha modificado el fichero *etc/sysctl.conf* y se ha añadido el siguiente contenido:

```
Unset
#Desactivar el uso de @ temporales para la interfaz eth0
net.ipv6.conf.eth0.use_tempaddr = 0

#Desactivar la configuración automática de direcciones
net.ipv6.conf.eth0.autoconf = 0

#Desactivar la aceptación de mensajes de anuncio de router
net.ipv6.conf.eth0.accept_ra = 0
```

Para implementar el nuevo esquema de red, primero se ha añadido al **router central** ya existente la nueva VLAN 2710, esto se ha hecho creando el fichero */etc/hostname.vlan2710* y estableciendo el siguiente contenido:

```
Unset
inet6 2001:470:736b:1b10::1 60 vlan 2710 vlandev vio0
!route add 2001:470:736b:1b11::0/64 2001:470:736b:1b10::2
!route add 2001:470:736b:1b12::0/64 2001:470:736b:1b10::2
```

Las líneas de route especifican que cualquier tráfico destinado a las subredes especificadas debe enviarse a través de la dirección 2001:470:736b:1b10::2, la cual corresponde a la dirección IPv6 asignada a una de las interfaces del nuevo router que está conectado a la VLAN 2710.

También se ha modificado el */etc/rad.conf* y se ha añadido la línea “interface 2710”.

A continuación se ha creado el **nuevo router interior** a partir de la imagen base creada en anteriores prácticas y se han realizado ciertas configuraciones básicas:

- En el fichero /etc/hostname.vio0 se ha añadido *inet6 up* para configurar la interfaz de red vio0 para que utilice direcciones IPv6.
- Se han creado los ficheros */etc/hostname.vlan2710, vlan2711* y *2712* para configurar las nuevas VLANs, añadiendoles el siguiente contenido que especifican las direcciones IPv6 para cada una de las interfaces en el nuevo router interior, así como la interfaz física conectada a las vlans (vio0):

```
Unset
#En el /etc/hostname.vlan2710:
inet6 2001:470:736b:1b10::2 60 vlan 2710 vlandev vio0

#En el /etc/hostname.vlan2711:
inet6 2001:470:736b:1b11::1 64 vlan 2711 vlandev vio0

#En el /etc/hostname.vlan2712:
inet6 2001:470:736b:1b12::1 64 vlan 2712 vlandev vio0
```

- Se ha añadido al /etc/rad.conf la línea *interface vlan 2712* para que el servidor rad pueda autenticar y autorizar dispositivos que están conectados a dichas VLAN. También se ha añadido al /etc/rc.conf.local la línea *rad_flags=””*.
- Se ha añadido la línea *net.ipv6.ip_forward=1* al archivo */etc/sysctl.conf* para habilitar el reenvío de paquetes IPv6.
- Para la configuración como cliente DNS ha sido necesario modificar el fichero */etc/resolv.conf,* comentando su contenido y añadiendo la siguiente línea: *nameserver 2001:470:736b:1bff::2.* Esta dirección corresponde a la dirección de la máquina o1BFF2 implementada en prácticas anteriores, la cual funciona en el sistema como servidor ntp adicional y DNS recursivo con caché.

Para integrar las distintas máquinas **fedora** en el esquema de red, se han llevado a cabo una serie de pasos utilizando la herramienta nmcli en la terminal de comandos:

```
Unset
# Creamos la conexión vlan
nmcli connection add type vlan con-name vlan2711 ifname vlan2711 vlan.parent
ens3 vlan.id 2711
```

```
# Modificamos la conexión vlan para configurar la dirección IPv6 y el encaminador por defecto
nmcli connection modify vlan2711 ipv6.addresses '2001:470:736b:1b11::2' ipv6.gateway '2001:470:736b:1b11::1' ipv6.method manual
# Modificamos la configuración de la conexión de red por defecto Wired connection 1 para que utilice link local
nmcli connection modify 'Wired connection 1' ipv6.method link-local

# Reiniciamos el NetworkManager
systemctl restart NetworkManager
```

Para cambiar el nombre de cada una de las máquinas se ha ejecutado el comando *hostnamectl set-hostname <nuevo_nombre>*.

También se han realizado algunas modificaciones en la **máquina NTP adicional y servidor DNS recursivo con caché,** así como en el servidor **DNS maestro**:

Se han añadido las siguientes líneas al fichero */var/unbound/etc/unbound.conf:*

```
Unset
access-control: 2001:470:736b:1b10::0/64 allow
access-control: 2001:470:736b:1b11::0/64 allow
access-control: 2001:470:736b:1b12::0/64 allow


stub-zone:
        name: "1.1b.ff.es.eu.org."
        stub-addr: 2001:470:736b:1b11::2
        stub-addr: 2001:470:736b:1b11::3
```

Las líneas de access-control permiten consultas DNS al servidor unbound a aquellas máquinas pertenecientes a las subredes especificadas. Mientras que el stub-zone establece una zona stub para el dominio 1.1b.ff.es.eu.org., lo que supone que el unbound utilizará directamente estos servidores DNS autorizados (servidores IPA maestro y esclavo) para resolver consultas relacionadas con el dominio 1.1b.ff.es.eu.org.

Por otra parte, se ha modificado el fichero de zonas del servidor DNS maestro, añadiendo los glue records correspondientes a las nuevas máquinas.

Fichero de zonas inverso (*/var/nsd/zones/1b.ff.es.eu.org.inverso*):

```
Unset
2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1  IN   PTR  orouter1B1.ff.es.eu.org.
2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.1  IN   PTR  ipa1.1.1b.ff.es.eu.org.
3.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.1  IN   PTR  ipa2.1.1b.ff.es.eu.org.
4.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.1  IN   PTR  nfs1.1.1b.ff.es.eu.org.
```

Una vez configurados el nuevo esquema de red, la imagen base fedora y realizadas las configuraciones correspondientes en los servidores DNS maestro y recursivo con caché, podemos proceder a la implementación del **servidor maestro IPA.**

Instalamos los paquetes necesarios con *dnf -y install freeipa-server freeipa-server-dns freeipa-client,* y a continuación configuramos el servidor de la siguiente manera:

Añadimos al fichero /etc/hosts el nombre y la IP del servidor: *2001:470:736b:1b11::2 ipa1.1.1b.ff.es.eu.org ipa1*. Esto permite mapear nombres de host a direcciones IP para poder resolver nombres de host localmente sin necesidad de consultar un servidor DNS externo.

Con ipa-server-install –setup-dns realizamos algunas configuraciones básicas como establecer el hostname, el nombre del dominio o el nombre del REALM.

Una vez configurados estos aspectos del servidor IPA, podemos iniciar sesión como admin utilizando el comando *kinit admin*. Este comando solicitará la contraseña del admin del dominio de IPA y a continuación se generará un ticket de autenticación que se puede utilizar para realizar acciones administrativas en el servidor IPA, como la administración de usuarios, grupos, etc.

Gracias al ticket de autenticación generado, se pueden realizar diversas acciones como ipa user-add, ipa hostgroup-add, ipa dnszone-add, ipa dnsrecord-add y más. Cabe destacar que no es lo mismo obtener el ticket con el comando sudo que sin él ya que al hacer sudo kinit admin se le otorga el ticket al usuario

Para configurar algunos servicios del firewall ejecutamos los comandos *firewall-cmd --add-service ={freeipa-ldap,freeipa-ldaps,dns, ntp}* y f*irewall-cmd --runtime-to-permanent.* El primero agrega los servicios especificados a las reglas de firewall de forma temporal, lo que permite que estén accesibles, mientras que el segundo convierte los cambios temporales en permanentes, lo cual asegura que persistan después de reinicios.

Una vez configurado el servidor IPA maestro, procedemos a configurar el **servidor IPA esclavo**. Para ello, es necesario configurarlo primeramente como cliente.

Para configurarlo como **cliente**, añadimos la correspondiente entrada directa DNS al servidor IPA maestro con *ipa dnsrecord-add 1.1b.ff.es.eu.org ipa2 --aaaa-rec 2001:470:736b:1bff::3.* Cabe destacar que en el entorno de FreeIPA los glue records se establecen mediante comandos directos en el servidor IPA maestro, y no a través de archivos de configuración de zonas como hemos visto anteriormente en el servidor DNS maestro.

A continuación, se ha de configurar la sincronización de tiempos con el servidor, ya que la sincronización adecuada con un servidor NTP entre otros aspectos, es clave para garantizar la funcionalidad segura y confiable de servicios como Kerberos, que son fundamentales para la autenticación y la autorización de usuarios en un entorno de dominio.

Para ello instalamos chrony con *dnf -y install chrony,* lo activamos con *systemctl enable --now chronyd,* y comprobamos que todo esté en correcto funcionamiento con *chronyd sources.* Se puede modificar el fichero /etc/chrony.conf para especificar el servidor NTP deseado con el que se pretende operar. En un principio se ha dejado ese fichero intacto con el servidor NTP que venía por defecto, una vez todo funcione correctamente se modificará y se establecerá el servidor NTP implementado en prácticas anteriores.

Una vez hecho esto podemos proceder a la configuración del cliente, para ello ejecutamos los comandos *nmcli connection modify vlan2711 ipv6.dns 2001:470:736b:1b11::2* y *nmcli connection up vlan2711.* Estos comandos modifican la configuración de la conexión de red del cliente, asignando el servidor DNS IPv6 correspondiente, lo que permite al cliente acceder a los servicios proporcionados por el servidor IPA de manera efectiva. A continuación, ejecutamos el comando *ipa-client-install --server=ipa1.1b.ff.es.eu.org --domain 1.1b.ff.es.eu.org* y terminamos de configurar el cliente.

Para configurarlo como **réplica**, desde el servidor maestro, añadimos un nuevo miembro al grupo de servidores con ipa hostgroup-add-member ipaservers --hosts ipa1.1.1b.ff.es.eu.org. Al igual que en el maestro deberemos modificar el el /etc/host para establecer el nombre e IP de los servidores FreeIPA.

También añadimos la nueva zona inversa y los glue records correspondientes a dicha zona con

```
Unset
ipa dnszone-add b.1.b.6.3.7.0.7.4.0.1.0.0.2.ip6.arpa.

ipa dnsrecord-add b.1.b.6.3.7.0.7.4.0.1.0.0.2.ip6.arpa.
2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.1 --ptr-rec ipa1.1.1b.ff.es.eu.org

ipa dnsrecord-add b.1.b.6.3.7.0.7.4.0.1.0.0.2.ip6.arpa.
3.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.1 --ptr-rec ipa2.1.1b.ff.es.eu.org
```

Con el comando ipa dnszone-find podemos verificar que tenemos tanto la zona directa como la inversa. El comando también proporciona otra información como el servidor autoritario, el nombre de la zona, si está activa, etc… Con *ipa dnsrecord-show* <*domain*> <*record*> se puede comprobar que un registro está correctamente añadido a la zona.

De nuevo modificamos el firewall del maestro para añadir el servicio de replicación con *firewall-cmd --add-service=freeipa-replication* y *firewall-cmd --runtime-to-permanent.* En la réplica añadimos también los servicios correspondientes al firewall con *firewall-cmd --add-service={freeipa-ldap,freeipa-ldaps,dns,ntp,freeipa-replication}* y *firewall-cmd –runtime-to-permanent.*

A continuación, instalamos y configuramos la réplica con *dnf -y install freeipa-server freeipa-server-dns* y *ipa-replica-install --setup-ca --setup-dns --no-forwarders.*

De cara a la configuración del **servidor NFS kerberizado**, primeramente se ha instalado y configurado como cliente IPA de la manera anteriormente descrita, y una vez verificado su correcto funcionamiento como cliente, se ha procedido a configurar los aspectos de NFS.

Para ello, primeramente utilizaremos *sudo kinit admin*, autenticando al usuario admin en el sistema de autenticación Kerberos, lo que nos permitirá realizar operaciones administrativas

utilizando el ticket Kerberos obtenido. Con klist podemos listar los tickets de Kerberos activos que no han expirado aún.

Para crear un principal de servicio para NFS ejecutamos *sudo ipa service-add nfs/nfs1.1.1b.ff.es .eu.org.* A continuación generamos el keytab para el principal de servicio NFS con el comando *sudo ipa-getkeytab -s ipa1.1.1b.ff.es.eu.org -p nfs/nfs1.1.1b.ff.es.eu.org -k /etc/krb5.keytab.* Ipa-getkeytab se utiliza para obtener un keytab para un principal, -s especifica el servidor IPA maestro del cual se obtendrá el keytab, -p el principal para el que se está generando el keytab, y -k la ubicación donde se almacenará el archivo keytab.

Para permitir el tráfico necesario para el funcionamiento del servicio NFS en el sistema, agregamos la siguiente regla al firewall: *firewall-cmd --add-service=nfs --add-service=mountd --add-service=rpc-bind --permanent.*

Para configurar el automontaje ejecutamos el comando *ipa-client-automount.* A continuación, creamos el directorio /etc/exports en el servidor NFS, el cual controla qué directorios se exportan. Cada línea contiene un punto de exportación, así como los clientes que tienen permitido montar el directorio y algunas opciones adicionales. Añadimos la línea */exports/home *(rw,sec=krb5i),* la cual indica que el directorio /exports/home está disponible para montaje a través de NFS para cualquier cliente, con permisos de lectura y escritura, y utilizando Kerberos v5 para la autenticación con integridad de datos (krb5i). Con *exportfs -ra* exportamos el nuevo directorio añadido al */etc/exports*. Activamos e iniciamos el servidor NFS con s*ystemctl enable nfs-server –now* y con *showmount -e* podemos ver la lista de exportaciones, podemos observar que aparece el /exports/home.

Creamos un mapa de montaje automático, lo que establecerá un mecanismo automático para montar el directorio /home desde un servidor NFS cuando se acceda a él desde otros sistemas en la red. Esto se hace con el comando *sudo ipa automountmap-add-indirect default auto.home --mount=/home,* y con *ipa automountkey-add default auto.home --key "*" --info "nfs1.1.1b.ff.es.eu.org:/export/home/&"* creamos una clave de montaje automático.

Una vez configurado el servidor NFS kerberizado, procedemos a **crear un usuario y su directorio home**. Primero creamos el usuario con ipa user-add <nombre_usuario> y establecemos su contraseña con ipa passwd <nombre_usuario>. A continuación, en el servidor

nfs1, creams un directorio con su nombre dentro del /exports/home y con chown lo configuramos para que el nuevo usuario sea el propietario.

Finalmente, procedemos a configurar los clientes del servicio NFS. Para ello, ejecutamos de nuevo el *ipa-client-automount* en las máquinas clientes para poder acceder automáticamente a los recursos compartidos NFS. Habilitamos los servicios necesarios para que el cliente pueda interactuar correctamente con los servicios NFS en la red con *systemctl enable rpc-gssd nfs-idmapd rpcbind --now:*

- El servicio *rpc-gssd* proporciona autenticación segura para las comunicaciones RPC.
- El servicio *nfs-idmapd* asigna identificadores de usuario y grupo entre diferentes sistemas NFS.
- El servicio *rpcbind* actúa como un mapa de puerto para las solicitudes RPC

Una vez configurados tanto servidor NFS como cliente, podemos conectarnos con uno de los usuarios de la siguiente forma: ssh <nombre_usuario>@cliente1.1.1b.ff.es.eu.org, y al hacer ls veremos que se ha montado automáticamente el directorio home con los subdirectorios correspondientes.

Pruebas para comprobar el funcionamiento el sistema

Al haberse convertido en un sistema algo más complejo, no es una técnica muy recomendable montarlo todo y probarlo todo al final, dado que podemos enfrentarnos a una gran variedad de errores. Es por ello por lo que se ha seguido una metodología de implementación por etapas, tras las cuales han sido probados los diferentes componentes implementados.

Lo primero en ser implementado fue el nuevo esquema de red, antes de proceder a configurar los servidores ni clientes IPA, se configuró lo básico de cada una de las máquinas para integrarlas en el esquema de red, y se procedió a probar el correcto funcionamiento del sistema con pings a las nuevas máquinas. Primero desde el nuevo router interior y posteriormente desde el router exterior, máquinas de la VLAN 2799, y desde las propias máquinas del laboratorio.

Una vez configurados los aspectos básicos de red, se realizaron los cambios comentados anteriormente en los servidores DNS implementados en prácticas anteriores. Esto fue probado principalmente con el uso del comando *dig* y de sus diferentes opciones como *+trace,* tanto al servidor DNS recursivo, como al DNS maestro y al esclavo.

A continuación se procedió a la instalación y configuración del servidor IPA, en el cual se probaron diferentes aspectos de Kerberos como obtener el ticket y listarlos con *kinit* y *klist*, y otros aspectos como la adición de nuevos usuarios, la conexión mediante ssh a estos nuevos usuarios, etc… Para ello fueron útiles comandos como *ipa user-add nuevo_usuario* para añadirlo*, ipa passwd nuevo_usuario* para cambiarle la contraseña*, ssh nuevo_usuario@nombre _del_servidor_ipa* para verificar que se podía acceder remotamente*, ipa user-find <nombre_usuario>* para buscarlos, *o ipa user-del >nombre>* para eliminarlos. También se probaron aspectos como el DNS, de nuevo realizando diferentes digs, creando zonas, añadiendo glue records, etc… Para comprobar el correcto funcionamiento de los clientes de ambas subredes, se realizaron también pruebas de conexión al servidor, así como de resolución de nombres.

Una vez el maestro IPA funcionaba correctamente, se procedió a la implementación de la réplica, la cual fue probada de forma bastante similar al maestro, realizando peticiones DNS a la réplica directamente, creando usuarios en el maestro y visualizándolos en la réplica (y viceversa). Se puede utilizar el comando *ipa-replica-manage list* para listar las réplicas de servidores dentro de la infraestructura FreeIPA.

Tras haber configurado correctamente tanto el servidor como la réplica, se ha procedido a configurar el servidor NFS kerberizado. Para ello, primeramente se ha configurado como cliente, y se ha probado de la misma manera que se han probado anteriormente los clientes. Una vez verificado su correcto funcionamiento como cliente, se ha procedido a implementar el servidor NFS.

Para verificar la correcta exportación de directorios por parte del servidor NFS y el automontaje, se ha creado un nuevo usuario y se le ha asignado su respectivo directorio de usuario dentro del /exports/home. A continuación, se ha realizado la conexión mediante ssh al usuario y se ha comprobado que todo estuviera montado correctamente, así como los permisos de escritura y lectura funcionasen correctamente, probando a escribir en un fichero.

Una vez comprobado que todo funciona con normalidad, se ha procedido a crear un par de usuarios más y añadir ficheros y subdirectorios a sus homes, para comprobar que efectivamente al realizar la conexión, pueden leer sus archivos y modificarlos.

Problemas encontrados y su solución

A lo largo de esta práctica han surgido diferentes problemas, los cuales han sido resueltos y comentaremos a continuación.

Los primeros problemas surgieron por temas de red. Inicialmente, el router exterior reexpedía los paquetes que iban al router interior a través de la vlan2710, pero no aquellos que iban destinados a las máquinas fédora. Sin embargo, descarté que se tratase de un problema con las VLANs, dado que los paquetes enviados del router interior a las fédora se enviaban sin problema, por lo que debía haber algún problema con los encaminadores. Finalmente, se añadió la línea !route add 2001:470:736b:1b1X::0/64 2001:470:736b:1b10::2 al /etc/hostname.vlan2710 del router exterior y se solucionó el problema. Al agregar estas rutas, se corrigieron las configuraciones de enrutamiento del router exterior para garantizar que los paquetes destinados a las máquinas Fedora fueran enviados correctamente a través del router interior.

Por otra parte, la VLAN estaba mal añadida en la máquina en la que posteriormente se implementaría el servidor IPA, ya que esta se desconectaba y conectaba parcialmente. Me percaté de este problema al instalar paquetes pesados como los paquetes FreeIPA. La descarga finalizaba repentinamente con un error y tras revisar los logs observé que daba el error “Network unreachable”, lo cual se corroboró realizando diferentes pruebas con la herramienta ping en los momentos de desconexión. Eliminé la vlan y la configuré de nuevo correctamente.

Respecto a la descarga de paquetes, hubo también algunos problemas ya que las descargas no se llegaban a completar y ni siquiera se podía hacer un *dnf update.* Esto era causado por temas de espacio, lo cual se solucionó añadiendo a la imagen cierto espacio hasta llegar a los 2 gigas en *memory unit.*

Durante la implementación del NFS, se encontraron dificultades debido a la ejecución inconsistente de comandos. Algunas acciones se realizaron utilizando sudo kinit admin, lo que otorga privilegios de administrador, mientras que otras se llevaron a cabo sin el uso de sudo. Esta variación en la ejecución de comandos pudo haber resultado en discrepancias en los permisos y la autorización de los recursos compartidos NFS.

Bibliografía

Configuración de red en máquinas fédora:
https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html-single/configuring_and_managing_networking/index

Instalación y configuración de servidor IPA:
https://www.server-world.info/en/note?os=Fedora_39&p=freeipa&f=1

Instalación y configuración de réplica IPA:
https://www.server-world.info/en/note?os=AlmaLinux_9&p=freeipa&f=7#google_vignette

Instalación y configuración clientes IPA:
https://www.server-world.info/en/note?os=AlmaLinux_9&p=freeipa&f=3

https://www.server-world.info/en/note?os=AlmaLinux_9&p=ntp&f=2

Algunas funciones útiles para manejo de usuarios y grupos con IPA
https://www.server-world.info/en/note?os=Fedora_39&p=freeipa&f=2

https://www.server-world.info/en/note?os=Fedora_39&p=freeipa&f=4

Aspectos de NFS y montaje:
https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html/configuring_and_using_network_file_services/deploying-an-nfs-server_configuring-and-using-network-file-services

https://linux.die.net/man/1/ipa-client-automount

Guía de automontaje en un entorno con IPA y NFS Kerberizado
https://blog.khmersite.net/p/automating-home-directory-with-ipa/

Funciones útiles para tratado de strings utilizadas en el script
https://www.rubyguides.com/2015/05/working-with-files-ruby/
https://ruby-doc.org/3.2.2/String.html#method-i-lstrip

Las memorias realizadas en prácticas anteriores también han sido de gran utilidad a la hora de algunos aspectos como configurar el nuevo router o las nuevas VLANs.

Las transparencias suministradas en la plataforma Moodle también han sido una útil fuente de información.