

## Problemas con el DNS en Ubuntu 17 y posteriores.

Tradicionalmente, en los sistemas UNIX para realizar la resolución de nombres, se usa el servicio Name Service Switch (NSS). Éste servicio forma parte de la biblioteca *glibc* escrita en C de los sistemas UNIX basados en GNU. Esta biblioteca contiene la API (código) que se utiliza para resolver nombres de dominio.

Con NSS se permite que ciertos datos del sistema sean proporcionados por servicios diferentes, cuyo orden de preferencia puede ser configurado por el administrador en el archivo `/etc/nsswitch.conf`. Así por ejemplo, los datos responsable de la resolución de nombres de dominio que se indican en `/etc/nsswitch.conf` podrían ser:

```
hosts: files mdns4_minimal [NOTFOUND = return] dns myhostname
```

En este caso, la resolución empezaría buscado en el archivo `/etc/hosts`, a continuación usaría el servicio mDNS (multicast Domain Name System), proseguiría con el servicio DNS, y por último se emplearía el método implementado por el *plugin* para NSS denominado *myhostname*.

*El servicio mDNS permite resolver nombres de dominio en redes pequeñas que no incluyen un servicio DNS. Cuando un cliente mDNS necesita resolver un nombre de dominio, envía un mensaje de multidifusión en el que pide al equipo que tenga ese nombre se identifique. La máquina que tiene dicho nombre envía un mensaje también de multidifusión con su IP.*

*De manera predeterminada, mDNS resuelve única y exclusivamente nombres de host que terminan en el dominio de nivel superior (TLD) .local. Existen diferentes implementaciones, siendo las más conocidas Bonjour (Apple) y Avahi (GNU/Linux y BSD).*

*El sistema de resolución implementado como plugin para NSS denominado myhostname intenta resolver el nombre de dominio examinando el archivo `/etc/hostname`.*

Pero actualmente, las nuevas distribuciones de Linux que usan *systemd* (sistema de inicio de los sistemas Linux que sustituye al sistema de inicio *System V init* tradicional), proporcionan un servicio denominado *systemd-resolved* que ofrece el servicio DNS a algunas aplicaciones locales (como por ejemplo a ciertos navegadores). Este servicio tiene 4 formas de manejar el archivo `/etc/resolv.conf` que es el que usa el *resolvedor* proporcionado por la librería *glibc*. En particular dos de ellas son:

1. El modo en el que *systemd-resolved* es en realidad un cliente de `/etc/resolv.conf`. Es decir, en este modo se conserva la información que contenga el archivo `/etc/resolv.conf` de forma que los servidores de nombres y dominio de búsqueda contenidos en dicho archivo son los que usará el servicio DNS proporcionado por la librería *glibc* y que anteriormente hemos comentado.

Este sistema sería el adecuado cuando el archivo `/etc/resolv.conf` es modificado directamente por el administrador o bien por otros programas, como es el caso de la

aplicación NetworkManager, o cuando usamos una configuración proporcionada por el servicio DHCP para las interfaces de red.

2. El segundo modo es el modo de operación recomendado por *systemd-resolved* e **implementado por defecto pero no por ello el más conveniente**. Consiste en usar un servidor DNS implementado de forma local en la interfaz de red 127.0.0.53, siendo este servidor el único servidor DNS, al cual normalmente se le acompaña con una lista de dominios de búsqueda (*search dominio*).

La información de dicho servidor DNS la podemos ver si seguimos el *link* desde */etc/resolv.conf* al archivo enlazado */run/systemd/resolve/stub\_resolv.conf*.

En este modo, los clientes locales que leen el archivo */etc/resolv.conf* realmente se dirigen a este servidor DNS local en lugar de usar el sistema DNS tradicional.

En realidad este DNS es muy adecuado cuando queremos resolver nombres de dominio locales, pero siempre que dichos dominios terminen su nombre de dominio de nivel superior (TLD) con *.local*, *.intranet*, *.net*, *.private* (ver salida del comando *systemd-resolve --status*). Si usamos otros nombres de dominio locales que no sean éstos, como suele suceder en muchas ocasiones, este servidor DNS intentará buscarlos redirigiendo las preguntas hacia el exterior, y evidentemente no los encontrará, a no ser que añadamos dichos dominios de búsqueda mediante la opción *search dominio*.

Por lo tanto, si queremos resolver nombres de dominio locales que no usen los nombres de dominio anteriores (con *.local*, *.intranet*, *.net*, *.private*) tendríamos que modificar manualmente el archivo */etc/resolv.conf* con la información que desea el administrador o bien dejar que sean las propias aplicaciones que lo necesiten las que modifiquen dicho archivo.

El problema de esta solución es que en el siguiente reinicio, el sistema volverá a la configuración por defecto (modo 2) donde */etc/resolv.conf* vuelve a ser enlazado con el archivo */run/systemd/resolve/stub\_resolv.conf*.

Para resolver este problema, debemos hacer que *systemd-resolved* opere en el tradicional modo 1, en vez del modo 2. Para ello el servicio *systemd-resolved* debe usar el contenido del archivo */run/systemd/resolve/resolv.conf* en lugar del contenido en */run/systemd/resolve/stub\_resolv.conf*

Para ello eliminamos el enlace de */etc/resolv.conf* a */run/systemd/resolve/stub\_resolv.conf* y creamos uno nuevo a */run/systemd/resolve/resolv.conf*.

```
root@localhost:~# ls -la /etc/resolv.conf
lrwxrwxrwx 1 root root 29 mar 7 20:20 /etc/resolv.conf ->
../run/systemd/resolve/stub_resolv.conf
```

```
root@localhost:~# rm -f /etc/resolv.conf
root@localhost:~# ln -s /run/systemd/resolve/resolv.conf /etc/resolv.conf
```

```
root@localhost:~# ls -la /etc/resolv.conf
lrwxrwxrwx 1 root root 32 mar 8 07:30 /etc/resolv.conf -> /run/systemd/resolve/resolv.conf
```