

Systemd-resolved

Ja sabem que els servidors DNS que un sistema utilitza vénen llistats a l'arxiu `/etc/resolv.conf` (concretament a les seves línies *nameserver*). No obstant, a sistemes Systemd aquest fitxer no se sol editar manualment sinò que és gestionat per un servei anomenat "systemd-resolved". Aquest servei, cada cop que s'inicia recull les configuracions DNS als següents llocs...:

a) L'escrita a l'arxiu `/etc/systemd/resolved.conf`, el qual representa la configuració general del servei. Concretament, la IP dels servidors DNS es poden indicar a la línia "DNS=..." , una darrera l'altra separades per espais. Aquests servidors són globals per totes les tarjes de xarxa de la màquina

b) L'escrita a l'arxiu `.network` corresponent a cada tarja de xarxa. Concretament, cada IP dels servidors DNS s'ha d'indicar en una línia "DNS=..." diferent. Aquests servidors tenen preferència, per la tarja en qüestió, sobre els servidors indicats al punt anterior.

c) La provinent d'algun servidor DHCP de la xarxa que hagi estat rebuda per alguna tarja de xarxa.
NOTA: Cal saber que existeix la possibilitat d'obtenir del servidor DHCP totes les dades necessàries (direcció IP, porta d'enllaç, etc) però rebutjant els servidors DNS oferts (per tal de configurar estàticament uns altres mitjançant la línia "DNS=..." comentada al paràgraf anterior) ; això és possible si s'indica la següent secció dins de l'arxiu `.network` corresponent:

```
[DHCP]  
UseDNS=false
```

...i les guarda a memòria. A partir de llavors, tots els programes del sistema podran preguntar a systemd-resolved i ell sabrà accedir al servidor DNS adient en cada cas. Els programes del sistema saben que han de preguntar a systemd-resolved perquè l'arxiu `/etc/resolv.conf` (que, recordem, és l'únic on normalment els programes actualment van a buscar els servidors DNS) sol apuntar com a ÚNIC "servidor DNS" a la IP 127.0.0.53, la qual representa el propi systemd-resolved escoltant al port 53.

En realitat, l'arxiu `/etc/resolv.conf` sol ser un enllaç a l'arxiu `/run/systemd/resolve/stub-resolv.conf`. (el motiu de l'existència d'aquest link és que Systemd pretén a mig plaç que `/run` sigui la carpeta on es puguin modificar les configuracions del sistema deixant `/etc` com una carpeta de només lectura). No obstant, també podria donar-se el cas de què `/etc/resolv.conf` fos un link que apuntés a un altre fitxer diferent anomenat `/run/systemd/resolve/resolv.conf` , el qual conté la llista d'IPs de tots els servidors DNS recopilada durant l'últim arranc de systemd-resolved (cadascun indicat en una línia començada per la paraula *nameserver*); en aquest cas, però, els programes ja no utilitzaran a systemd-resolved com "servidor" sinò que consultaran aquest arxiu directament, el que és una solució més pobre perquè la llista allà existent és global i no distingeix si els servidors DNS només s'han d'usar per una determinada tarja, etc. De fet, en aquest cas no cal tenir ni tan sols systemd-resolved funcionant un cop `/run/systemd/resolve/resolv.conf` ja estigui construït.

NOTA: En el cas de què `/etc/resolv.conf` estigués gestionat per altres programes (com seria el cas, per exemple, de NetworkManager, del qual en parlarem més endavant), systemd-resolved (si estigués funcionant) es limitarà a usar els servidors DNS inclosos allà com a simple consumidor. NetworkManager, per exemple, el que sol fer és convertir `/etc/resolv.conf` en un link a `/var/run/NetworkManager/resolv.conf` i escriure-hi allà els servidors DNS que ell mateix recopila de la seva pròpia configuració o via DHCP.

ATENCIÓ: si en executar el client *dhclient* (o altres) l'arxiu `/etc/resolv.conf` és matxacat mostrant-se directament els servidors DNS obtinguts de la petició DHCP en comptes de la IP 127.0.0.53 (la qual hi tornarà a aparèixer quan systemd-resolved es reiniciï) vol dir que falta instal·lar una llibreria disponible en el paquet "libnss-resolve" (a Debian/Ubuntu aquest paquet no s'instal·la per defecte; a Fedora la llibreria en qüestió està dins del paquet "systemd-libs", el qual sí ve instal·lat per defecte). Aquesta llibreria permet que l'arxiu `/etc/resolv.conf` es mantingui sempre amb la IP 127.0.0.53, configurant-se llavors els DNS obtinguts per *dhclient* on toca (a memòria).

NOTA: Aquesta llibreria també fa una altra cosa: anteposa la paraula "resolve" davant de "dns" a la línia "hosts:..." del fitxer `/etc/nsswitch.conf`. Amb això el que s'aconsegueix és que tots els programes utilitzin com a "resolver" a systemd-resolve abans que el mètode tradicional

En els sistemes que no fan servir Systemd (o, com a mínim, no fan servir systemd-networkd/systemd-resolved, com podria ser els sistemes que utilitzen el sistema "networking" tradicional) la "recopilació" dels diferents servidors DNS obtinguts des de diferents llocs la fa un altre programa anomenat "resolvconf". Aquest programa és l'encarregat de generar dinàmicament el contingut de /etc/resolv.conf a partir, per exemple, del que ofereixen eventuais servidors DHCP, el propi NetworkManager o del que estigui escrit dins de /etc/network/interfaces. En aquest sentit, per fer que una tarja de xarxa utilitzi determinats servidors DNS fixes, a les línies corresponents dins de /etc/network/interfaces s'haurà d'afegir la línia...:

```
dns-nameservers x.x.x.x y.y.y.y z.z.z.z
```

...on "x.x.x.x", "y.y.y.y" i "z.z.z.z" representen les IPs dels servidors DNS escollits. Un cop reiniciat el servei "networking", aquestes IPs seran integrades dins de l'arxiu /etc/resolv.conf gràcies a resolvconf.

Dominis "search":

Dins de l'arxiu /etc/resolv.conf no només hi ha la informació sobre a qui llençar les peticions DNS sinó que també hi ha una altra dada important: els dominis "search". Aquests dominis són "les cues" que automàticament s'afegeixen a qualsevol nom de màquina simple per tal de completar-lo i convertir-lo en un nom plenament qualificat. Així, per exemple, si el nostre sistema tingués "cocacola.com" com a domini "search", quan executéssim la comanda `ping www` automàticament el nostre sistema realment el que executaria seria la comanda `ping www.cocacola.com`. Es poden definir més d'un domini "search", en ordre; si, seguint amb l'exemple, el nostre sistema tingués primer "cocacola.com" i després "pepsicola.com" com a dominis "search", quan executéssim la comanda `ncat www 80` automàticament el nostre sistema provaria de fer `ncat www.cocacola.com 80` i, si no funciona, llavors provaria a executar `ncat www.pepsicola.com 80`

Les maneres de definir els dominis "search" d'una màquina són dues: l'estàtica o la dinàmica. La primera consisteix simplement en afegir a la secció [Network] de l'arxiu .network de la tarja de xarxa en qüestió la línia `Domains=` contenint una llista (separada per espais) dels dominis "search" desitjats. La segona consisteix en rebre la llista de dominis "search" des d'un servidor DHCP. Concretament, si utilitzem com a servidor DHCP el programa Dnsmasq, la directiva pertinent és `dhcp-option=option:domain-search,cocacola.com pepsicola.com` (el codi numèric de l'opció és 119); si utilitzem com a servidor DHCP el programa isc-dhcp-server, llavors la directiva pertinent és `option domain-search "cocacola.com", "pepsicola.com"`;

En el cas de voler muntar un servidor DNS...:

...cal tenir en compte que per a què *systemd-resolved* reconegui els noms de màquines com de tipus DNS (en comptes de noms de tipus LLMNR), aquests hauran de ser sempre plenament qualificats (és a dir, hauran de ser FQDN). Això vol dir que els noms simples "sense domini" seran invisibles. A la pràctica, això vol dir que si tenim, per exemple, un servidor Dnsmasq autoritatiu agafant els noms del seu arxiu /etc/hosts, els noms que han d'aparèixer en aquest arxiu han de ser plenament qualificats (o, si no, ha de tenir configurades convenientment les seves directives `local=`, `domain=` i `expand-hosts`)

Client systemd-resolve:

De clients DNS n'hi ha per tot arreu: quasi qualsevol aplicació de xarxa porta integrada a dins un client DNS: des d'un navegador fins la comanda `ping` han de primer preguntar a un servidor DNS la IP corresponent al nom introduït per l'usuari per poder començar a realitzar la seva tasca. No obstant, existeixen clients DNS "per se" per poder enviar peticions DNS més personalitzades i estudiar més en profunditat les respostes DNS rebudes. Exemples de clients DNS són la comanda `host`, la comanda `nslookup` o la comanda `dig` (més completa)

Un client DNS una mica especial és *systemd-resolve*, ja que està dissenyat específicament per preguntar al servei *systemd-resolved* de la màquina. Bàsicament té les següents opcions:

systemd-resolve --status : Obté la llista de servidors DNS que *systemd-resolved* té recopilats, mostrant-los separats per cada tarja de xarxa. També informa dels dominis *search* configurats per cadascuna d'elles (i de si hi està activat DNSSEC o altres protocols alternatius a DNS com ara LLMNR o mDNS)

systemd-resolve nomMaquina : Retorna la IP de la màquina indicada

systemd-resolve direccioIP : Retorna el nom de la màquina associat a la IP indicada

systemd-resolve -t registre domini : Retorna el valor del registre indicat (A, AAAA, CNAME, MX, NS ...) emmagatzemat al servidor DNS primari del domini indicats

systemd-resolve { --statistics | --reset-statistics } : Informa sobre les estadístiques de peticions/respostes

systemd-resolve --flush-caches : Elimina tota la catxé del client amb les respostes DNS obtingudes fins ara