RT 201 - Client DNS sous Linux : Oh My!

Jean-Marc Pouchoulon

mai 2024

La résolution de nom côté client s'est fortement complexifiée ces dernières années sur Linux avec l'arrivée de nouvelles technologies comme le DNS over TLS, le DNS over HTTPS, le DNSSEC, EDNS0, systemd-networkd, systemd-resolved, netplan, networkd-dispatcher...

On est passé d'un configuration simple dans /etc/resolv.conf à une configuration dynamique et ... complexe. L'objet de ce TP est de vous permettre de comprendre comment fonctionne la résolution de nom sous Linux et comment la configurer.

1 Instructions générales

La relecture du TP "persistance" est fortement conseillée. Installez le package tcpdump pour les besoins de ce TP. Pour voir l'activité DNS, vous pouvez utiliser la commande suivante :

```
tcpdump -n -i eth0 -n port 53
```

Les fichiers de configuration sont donnés sous la forme suivante appelée "heredoc" en bash:

```
cat << EOF > chemin_fichier
instructions
...
EOF
```

Un simple copié-collé de ces instructions créera le fichier avec les instructions. Un fichier texte sous Moodle avec les "heredoc" est à votre disposition pour copier-coller les instructions en conservant l'indentation.

NB: Le "man page" ne ment pas ce qui n'est pas forcément le cas pour votre IA préférée qui hallucine parfois... Les deux sont complémentaires. Vous serez évalué par QCM à la fin du TP.

2 Analyse de la configuration DNS standard de Debian

Vous utiliserez cette OVA VM debian 12 sous Virtualbox pour cette première partie du TP.

Quelques questions sur le sujet pour votre IA préférée

1. Quel est le fichier de configuration linux central pour la résolution DNS ?
2. Donnez la signification des instructions de ce fichier.
3. Quel est le rôle du fichier `/etc/nsswitch.conf` dans la résolution DNS ?
4. Comment se fait le lien entre ifdown et ifup et les scripts de configuration réseau ?
5. Expliquez ce qu'est le DNS over TLS ? le DNS over HTTPS ? le DNSSEC ? EDNS0 ?
6. Que fait la commande strace ?

Mise en pratique

1.
2. Installez le packages suivants:

```
apt install -y dnsutils strace resolvconf ifupdown ifupdown-extra
```

3. Configurez /etc/network/interfaces avec les serveurs dns 8.8.8.8 et 1.1.1.1 et avec une recherche dans le domaine iutbeziers.fr quand le nom de domaine n'est pas complet.
4. Pour que le fichier /etc/resolv.conf soit généré à partir /etc/network/interfaces, passez la commande suivante:

```
resolvconf -u
```

   Vérifiez que le fichier /etc/resolv.conf a bien été généré.
5. Configurez /etc/resolv.conf avec la bonne option pour alterner les requêtes sur les deux serveurs dns.
6. Vérifiez que la configuration est bien prise en compte : nb : Si la configuration est cassée, vous pouvez la réparer en passant la commande suivante:

```
dpkg-reconfigure resolvconf
```

   Pour "sniffez" le trafic DNS, vous pouvez utiliser la commande suivante:

```
tcpdump -i any -s0 -xX  port 53
```

   — Créez le script python suivant.

```
import socket
for x in range(5):
  print(socket.getaddrinfo('www.iutbeziers.fr', 443))
```

   — lancez le script avec la commande suivante et vérifiez que les deux serveurs dns sont bien alternés lors des demandes de résolutions.

```
strace -e trace=connect python3 resolv.py 2>&1|grep 53
```

   — Le traffic dns est-il chiffré ?

3 D'autres solutions pour le DNS client

Pour cette seconde partie vous utiliserez une VM Debian >=12 (lien sur Moodle dans le cours "Aide jmp"). Cette configuration est caractéristique d' Ubuntu mais s'applique aussi à Debian et plus généralement aux distributions supportant systemd.

Le mécanisme de résolution de nom sur ces VM est configurable via les outils suivants :

— Netplan
— systemd-networkd ou "Network Manager"
— system-resolved

On n'utilisera pas "Network Manager" dans ce TP. Il a plus de valeur ajoutée pour les postes de travail que pour les serveurs mais ça n'engage que l'auteur de ce TP.

Gestion du DNS avec Netplan

Netplan est un utilitaire de configuration réseau introduit dans Ubuntu 17.10. Il permet de configurer de manière persistante les interfaces réseau. Il fonctionne avec Debian aussi. Netplan génére des configurations pour systemd-networkd ou "Network Manager". Ici on ne s'intéressera qu'à systemd-networkd mais le principe reste le même pour "Network Manager".

1. Quelles sont les différences entre le fichier /etc/nsswitch.conf et celui de la VM précédente ? expliquez [UNAVAIL=return].
2. quel est le type du fichier /etc/resolv.conf ? Si vous le supprimez, la résolution DNS fonctionne-t-elle encore ? Qu'en déduisez-vous ? pourquoi y a -t il un lien symbolique vers /run/systemd/resolve/stub-resolv.conf ? recréez ensuite le lien avec la commande suivante:

   ```
   ln -s /run/systemd/resolve/stub-resolv.conf /etc/resolv.conf
   ```

3. Configurer un fichier yaml 01-netcfg.yaml sous /etc/netplan en passant la commande suivante:

   ```
   cat << EOF > /etc/netplan/01-netcfg.yaml
   network:
     version: 2
     renderer: networkd
     ethernets:
       eth0:
         dhcp4: true
         link-local: [ ipv4 ]
         dhcp4-overrides:
           use-dns: false
         nameservers:
           addresses:
           - 10.6.255.106
           search:
           - iutbeziers.fr
   EOF
   ```

   effectuez les commandes suivantes::

   ```
   netplan generate && netplan apply
   rm -f /etc/systemd/resolved.conf
   systemctl restart systemd-resolved
   ```

4. Quel est le but de cette configuration ?
5. Utilisez la commande "resolvectl status" afin de vérifier que la configuration a bien été prise en compte. Quel est le DNS utilisé pour la résolution de nom ? Quel est le DNS utilisé ?
6. Résout-il tous les noms de domaine ? utilisez la commande:

   ```
   resolvectl query --cache no votre_fqdn
   ```

7. Passez maintenant la commande "resolvectl default-route eth0 no" ? Que constatez-vous ? En déduire le rôle de l'option "default-route".
8. Utilisez la commande "networkctl -las status" pour retrouver l'emplacement du fichier de configuration généré par netplan pour systemd-networkd. Comment netplan fonctionne-t-il pour la configuration de systemd-networkd ?

   Veuillez notez au passage l'option -s de networkctl qui permet d'avoir des informations sur votre carte réseau ce qui peut être fort utile pour qualifier l'état d'une interface réseau.

Gestion du DNS avec systemd-networkd

1. Créez ce fichier de configuration pour systemd-networkd sous /etc/systemd/network/05-eth0.network et redémarrer le service (systemctl restart system-networkd)

```
cat << EOF > /etc/systemd/network/05-eth0.network
[Match]
Name=eth0
[Network]
DHCP=yes
DNS=8.8.8.8 1.1.1.1
Domains=iutbeziers.fr
EOF
```

   effectuez les commandes suivantes::

```
systemctl restart systemd-networkd
systemctl restart systemd-resolved
```

2. Faites un "resolvectl status" et sniffez le trafic sur le port 53 ? que constatez-vous ? Comment sont pris en compte les différents emplacements des fichiers de configuration de systemd-resolved (/run/-systemd généré par netplan versus /etc/systemd configuré statiquement) ? qui a rajouté le troisième DNS ? Dans quel ordre sont-ils utilisés ?
3. Supprimez mainenant le fichier de configuration /etc/systemd/network/05-eth0.network et redémarrez le service systemd-networkd.

Gestion du DNS avec systemd-resolved

1. Créez une seconde carte réseau eth1 en mode bridge sur votre VM (arrêt et redémarrage de la VM nécessaire). Modifiez le fichier Netplan comme suit afin de ne plus avoir de DNS imposé dans systemd-networkd par Netplan:
   Nb: link-local est une option qui désactive ici IPv6. C'est à retenir.

```
cat << EOF > /etc/netplan/01-netcfg.yaml
network:
    version: 2
    renderer: networkd
    ethernets:
            eth0:
                dhcp4: true
                dhcp4-overrides:
                  use-dns: false
                link-local: [ ipv4 ]
            eth1:
                dhcp4: true
                dhcp4-overrides:
                  use-dns: false
                link-local: [ ipv4 ]
EOF
```

   Appliquez la configuration avec "netplan apply".
2. Validez que plus aucun DNS n'est configuré pour les interfaces eth0 et eth1 avec la commande "resolvectl status".
3. La resolution de nom fonctionne-t-elle encore ?
4. Configurez maintenant systemd-resolved via /etc/systemd/resolved.conf:

```
cat << EOF > /etc/systemd/resolved.conf
[Resolve]
FallbackDNS=9.9.9.9#dns.quad9.net
EOF
```

Redémarrez le service systemd-resolved.

5. Quelle est le DNS utilisé pour la résolution de nom ? Quel est le rôle de ce DNS et quand est-il utilisé ?
6. Quelle est l'adresse du DNS resolver dans /etc/resolv.conf ? Avec la commande "ss -tunelp" retrouvez le service en écoute sur ce port.
7. Configurez maintenant le DNS pour prendre en compte la carte réseau eth1 et en utilisant le DNS de l'IUT :

```
cat << EOF > /etc/netplan/01-netcfg.yaml
network:
   version: 2
   renderer: networkd
   ethernets:
            eth0:
               dhcp4: true
               dhcp4-overrides:
                 use-dns: false
               link-local: [ ipv4 ]
            eth1:
               dhcp4: true
               dhcp4-overrides:
                 use-dns: false
               link-local: [ ipv4 ]
               nameservers:
                 addresses:
                 - 10.6.255.106
                 search:
                 - iutbeziers.fr
EOF
```

Faites un "netplan apply"

8. Quel est maintenant le DNS courant utilisé pour la résolution de nom ? que constatez-vous ?
9. A l'aide de resolvectl, affichez les "_gateways" ? les "_outbounds". A quoi correspondent-ils ?
10. Modifiez maintenant la configuration de systemd-resolved comme suit:

```
cat << EOF > /etc/systemd/resolved.conf
[Resolve]
DNS=10.6.255.24
EOF
```

Redémarrez le service systemd-resolved.

11. Quel est le DNS utilisé pour les F.Q.D.N. du domaine iutbeziers.fr ? des autres domaines ?
12. Pourquoi seul le DNS 10.6.255.106 est-il utilisé ?
13. A quoi corresponde les modes "stub", "resolve" et "Off" de resolved.conf ?
14. Exécutez les commandes suivantes et expliquez les résultats:

```
resolvectl dns
resolvectl domain
resolvectl default-route
resolvectl statistics
```

15. Créez une configuration qui résolve le domaine iutbeziers.fr sur le dns 10.255.255.200. Puis configurez les autres domaines sur l'interface "global" en utilisant le DNS 1.1.1.1 (cf "routing domain et .."). Activer le chiffrement si le resolver 1.1.1.1 le supporte (traduire "opportunistic" dans la configuration.) avec DNSOverTLS.
16. Expliquez ce qu'est un routing-domain ? un search-domain ? une default-route ? (Vous pouvez vous aider du document RESOLVED-VPNS.md sur Moodle issu de la documentation systemd).

Fonctions de sécurité de la résolution DNS

1. Activez le chiffrement DNS avec systemd-resolved avec DNSOverTLS vers le resolver 1.1.1.1. Quel est le port utilisé pour le DNS over TLS ? Vérifiez que le trafic soit chiffré avec "tcpdump -Xx -s0 -i any port 853".
2. Depuis le navigateur Firefox de votre poste, activez maintenant le DNS over HTTPS vers CloudFlare (dns 1.1.1.1). Vérifiez que le trafic DNS soit chiffré en accédant à `https://one.one.one.one/help/`. Remettez la configuration initiale avant de passer à la question suivante.
3. Activez DNSSEC sur systemd-resolved. Installez le package "delv". Vérifiez que le trafic DNS soit signé via la commande "delv www.cloudflare.com" ? votre banque signe-t-elle ses enregistrements DNS ? brr ca fait peur...

Gestion dynamique du DNS avec systemd-networkd-dispatcher

On va tout créer une interface réseau virtuelle "dummy" pour illustrer le fonctionnement de systemd-networkd-dispatcher. Chaque fois que cette interface sera up , un script sera lancé pour modifier la configuration de systemd-resolved et gérer une "routed interface".

Le script suivant est à placer dans /etc/networkd-dispatcher/degraded.d/10-resolved. (degraded est l'état de l'interface réseau resolver0 une fois up pour systemd-networkd. Ce n'est pas un état normal mais c'est une interface dummy...)

```
#!/bin/bash
INTERFACE=resolver0
# Add your search domains here
SEARCH_DOMAINS="~umontpellier.fr"
resolvectl domain "$INTERFACE" $SEARCH_DOMAINS
resolvectl dns $INTERFACE 10.6.255.106
```

1. Créez le script 10-resolved dans /etc/networkd-dispatcher/degraded.d/10-resolved et rendez le exécutable.
2. Faites un "resolvectl status" pour vous permettre de voir les changements de configuration ensuite.
3. Créez l'interface réseau dummy0 et lancez les commandes suivantes:

```
apt -y install networkd-dispatcher
chmod +x /etc/networkd-dispatcher/10-resolved
# créer  l'interface dummy resolver0 et la "mettre up"
ip link add resolver0 type dummy
ip address add 127.0.0.52/32 dev resolver0
ip link set up dev resolver0
```

4. Vérifier que le script précédent a bien été exécuté et que le DNS est bien appelé.

   Nb : Linux se débrouille pour router les paquets vers l'interface réseau la plus appropriée pour joindre le DNS. mais c'est un peu magique...
5. Créez un script qui lorsque l'interface resolver0 est mise down, remet la configuration de systemd-resolved en état.
6. Dans quel cas cette technique est-elle utile ?