dnsmasq

Dnsmasq est un **relais DNS** et un **serveur DHCP** léger et facile à configurer. Il est conçu pour fournir le service DNS et éventuellement le service DHCP à un petit réseau. Il peut fournir le nom de machines locales qui ne sont pas dans le catalogue DNS global. Le serveur DHCP est intégré au serveur DNS et permet aux machines avec des adresses allouées grâce à DHCP d'apparaître dans le DNS avec des noms configurés soit dans chaque hôte ou dans un fichier de configuration central. **Dnsmasq** prend en charge les baux DHCP statiques et dynamiques et **BOOTP/TFTP** pour le démarrage par le réseau de machines sans disque.

Je détaille son installation et paramétrage pour Linux **Debian** / **Ubuntu** / **Mint** / **Zorin OS** / **Raspberry Pi OS**.

Avec Linux **Fedora** / **Red Hat**, vous pouvez suivre la procédure sur la page Use dnsmasq to provide DNS & DHCP services de Fedora Magazine.

1. Installation

Pour installer le paquet **dnsmasq**, il faut utiliser les bonnes commandes pour le bon système d'exploitation. Pour une distribution **Debian** et dérivée, c'est la commande **apt** et la paquet **dnsmasq** inclus dans la distribution officielle de Debian.

```
sudo apt update
sudo apt install dnsmasq
```

Le service **dnsmasq** démarre et est activé à la fin de la procédure d'installation.

2. Configurer dnsmasq

En standard, votre machine est configurée avec un ou plusieurs serveurs DNS externes. Cette déclaration est effectuée dans le fichier `/etc/resolv.conf`. Il se peut que d'autres noms d'hôtes (généralement des noms d'hôtes locaux) soient déclarés dans le fichier `/etc/hosts`)

> Plus d'infos : resolv.conf

Les options de **dnsmasq** peuvent être définies soit sur la ligne de commande lors du démarrage de **dnsmasq**, soit dans son fichier de configuration `/etc/dnsmasq.conf` ou dans un fichier de configuration spécifique présent dans le dossier `/etc/dnsmasq.d`

Pour que la machine où est exécuté dnsmasq, utilise **dnsmasq** comme résolveur DNS, vous devez modifier le fichier `/etc/resolv.conf` avec la valeur `127.0.0.1`.

Il faut également modifier le fournisseur DNS **upstream** dans **dnsmasq**. Pour cela il faut utiliser l'option `server` ou l'option `resolv-file` qui indique le nom d'un fichier contenant les noms des fournisseurs DNS **upstream**. Il est nécessaire de désactiver la consultation du fichier `/etc/resolv.conf` par **dnsmasq** avec l'option `no-resolv`.

3. fonction DHCP

dnsmasq lit le fichier `/etc/hosts` afin que les noms des machines locales soient disponibles dans le DNS. Cela fonctionne bien lorsque vous donnez à toutes vos machines locales des adresses IP statiques, mais cela ne fonctionne pas lorsque les machines locales sont configurées via DHCP. **Dnsmasq** est livré avec un service DHCP intégré pour résoudre ce problème.

Le service DHCP de **dnsmasq** alloue des adresses aux hôtes du réseau et essaie de déterminer leurs noms. S'il y parvient, il ajoute la paire nom/adresse au DNS. Il y a essentiellement deux façons d'associer un nom à une machine configurée par DHCP; soit la machine connaît son nom lorsqu'elle obtient un bail DHCP, soit **dnsmasq** lui donne un nom, basé sur l'adresse MAC de sa carte ethernet. Pour que la première solution fonctionne, une machine doit connaître son nom lorsqu'elle demande un bail DHCP. Les noms peuvent être n'importe quoi en ce qui concerne DHCP, mais **dnsmasq** ajoute quelques limitations. Par défaut, les noms ne doivent pas avoir de partie de domaine, c'est-à-dire qu'ils doivent juste être des noms alphanumériques, sans aucun point. Il s'agit d'une fonction de sécurité pour empêcher une machine sur votre réseau de dire à DHCP que son nom est “www.google.com” et ainsi de capter le trafic qui ne devrait pas lui être destiné. Une partie domaine n'est autorisée par **dnsmasq** dans les noms de machines DHCP que si l'option `domain-suffix` est définie, la partie domaine doit correspondre au suffixe.

4. Domaines locaux

Lorsque vous avez des domaines locaux que vous ne voulez pas faire suivre aux serveurs en amont, il suffit d'utiliser les options de serveur sans l'adresse IP du serveur. Par exemple, l'option `local=/localnet/` garantit que toute requête de nom de domaine se terminant par `.localnet` sera répondue si possible à partir de `/etc/hosts` ou DHCP, mais ne sera jamais envoyée à un serveur en amont.

Filtre Windows

L'option `filterwin2k` permet à **dnsmasq** d'ignorer certaines requêtes DNS qui sont faites par Windows toutes les quelques minutes. Ces requêtes n'obtiennent généralement pas de réponses raisonnables dans le DNS global et causent des problèmes en déclenchant des liaisons Internet à la demande.

5. Exemple de configuration acegrp

Création d'un fichier de configuration spécifique dans `/etc/dnsmasq.d/acegrp.conf`

`server` permet d'indiquer le serveur **upstream** DNS. Il est nécessaire de l'indiquer car la consultation du fichier `/etc/resolv.conf` a été désactiver avec l'option `no-resolv`.

```
alias=8.8.8.8,192.168.100.1

listen-address=127.0.0.1,192.168.100.1

domain-needed
bogus-priv
filterwin2k

localise-queries
local=/acegrp.lan/
domain=acegrp.lan
expand-hosts
no-negcache
no-resolv
clear-on-reload
#resolv-file=/tmp/resolv.conf.auto

dhcp-authoritative
dhcp-leasefile=/tmp/dhcp.leases

#log-queries
log-dhcp

# use /etc/ethers for static hosts; same format as --dhcp-host
#read-ethers

# activez le serveur DHCP:
# Plage DHCP
dhcp-range=192.168.100.2,192.168.100.254,1h
# Netmask
dhcp-option=1,255.255.255.0
# Route
dhcp-option=3,192.168.100.254
dhcp-option=option:dns-server,192.168.100.3
# Set the NIS domain name to "acegrp.lan"
dhcp-option=40,acegrp.lan

# Send an empty WPAD option. This may be REQUIRED to get windows 7 to
behave.
dhcp-option=252,"\n"
# If a DHCP client claims that its name is "wpad", ignore that.
# This fixes a security hole. see CERT Vulnerability VU#598349
dhcp-name-match=set:wpad-ignore,wpad
dhcp-ignore-names=tag:wpad-ignore

#upstream
#server=192.168.100.3
#server=1.1.1.1
```

```
server=9.9.9.10
```

6. Lire et analyser les logs

Consulter les logs des actions du service **dnsmasq** dans le fichier `/var/log/syslog` :

```
Jun 10 17:50:00 dnsmasq[21796]: query[A] isatap.lan from 115.34.22.160
Jun 10 17:50:00 dnsmasq[21796]: cached isatap.lan is NXDOMAIN-IPv4
Jun 10 17:50:21 dnsmasq[21796]: query[A] isatap.lan from 115.34.22.160
Jun 10 17:50:21 dnsmasq[21796]: cached isatap.lan is NXDOMAIN-IPv4
Jun 10 17:50:31 dnsmasq[21796]: query[A] isatap.lan from 115.34.22.160
Jun 10 17:50:31 dnsmasq[21796]: cached isatap.lan is NXDOMAIN-IPv4
Jun 10 17:50:37 dnsmasq[21796]: query[A] isatap.lan from 115.34.22.160
Jun 10 17:50:37 dnsmasq[21796]: cached isatap.lan is NXDOMAIN-IPv4
Jun 10 17:50:40 dnsmasq[21796]: query[A] zyx.qq.com from 115.34.22.160
Jun 10 17:50:40 dnsmasq[21796]: forwarded zyx.qq.com to 114.114.114.114
Jun 10 17:50:40 dnsmasq[21796]: forwarded zyx.qq.com to 223.5.5.5
Jun 10 17:50:40 dnsmasq[21796]: reply zyx.qq.com is 123.151.43.51
Jun 10 17:50:40 dnsmasq[21796]: reply zyx.qq.com is 183.60.62.158
Jun 10 17:50:40 dnsmasq[21796]: reply zyx.qq.com is 113.108.1.90
Jun 10 17:50:42 dnsmasq[21796]: query[A] isatap.lan from 115.34.22.160
Jun 10 17:50:42 dnsmasq[21796]: cached isatap.lan is NXDOMAIN-IPv4
Jun 10 17:50:52 dnsmasq[21796]: query[A] isatap.lan from 115.34.22.160
Jun 10 17:50:52 dnsmasq[21796]: cached isatap.lan is NXDOMAIN-IPv4
Jun 10 17:50:58 dnsmasq[21796]: query[A] ic.wps.cn from 115.34.22.160
```

Extraire une liste des noms de domaine demandés :

```
awk '!seen[$6]++ {print $6}' /var/log/syslog
```