Cache DNS : installer et configurer

OS testé : **Fedora 24**
Date de test : **12 novembre 2016**

Installer ''bind''

Lancer l'installation de `bind` et `bind-utils` en utilisant le programme `dnf`.

`bind-utils` inclus les programmes `nslookup`, `dig` and `host`.

```
sudo dnf install bind bind-utils
```

Le résultat est le suivant :

```
Vérification de l'expiration des métadonnées effectuée il y a 1:07:23 sur
Fri Nov 11 20:10:48 2016.
Le paquet bind-utils-32:9.10.4-2.P3.fc24.x86_64 est déjà installé, ignorer
Dépendances résolues.
================================================================================
========================
 Package           Architecture        Version
Dépôt                Taille
================================================================================
========================
Installation de:
 bind              x86_64              32:9.10.4-2.P3.fc24
updates              1.9 M

Résumé de la transaction
================================================================================
========================
Installation  1 Paquet

Taille totale des téléchargements : 1.9 M
Taille d'installation : 4.0 M
Est-ce correct [o/N] : o
Téléchargement des paquets :
bind-9.10.4-2.P3.fc24.x86_64.rpm                                 555 kB/s
| 1.9 MB     00:03
--------------------------------------------------------------------------------
------------------------
Total                                                            382 kB/s
| 1.9 MB     00:05
Test de la transaction en cours
La vérification de la transaction a réussi.
Lancement de la transaction de test
```

```
Transaction de test réussie.
Exécution de la transaction
  Installation de               : bind-32:9.10.4-2.P3.fc24.x86_64
1/1
  Vérification                  : bind-32:9.10.4-2.P3.fc24.x86_64
1/1

Installé:
  bind.x86_64 32:9.10.4-2.P3.fc24

Terminé !
```

Les programmes `bind` et `bind-utils` sont installés.

Editer ''named.conf''

1. Modifier le fichier de configuration `/etc/named.conf`

```
sudo vim /etc/named.conf
```

2. Remplacer la ligne suivante (~11)

```
listen-on port 53 { 127.0.0.1; };
```

par le bloc suivant

```
listen-on port 53 { goodclients; };
allow-query { goodclients; };
allow-query-cache { goodclients; };
recursion yes;
```

3. Supprimer la ligne suivante

```
allow-query { localhost;};
```

Voilà a quoi pourrait correspondre le fichier de configuration `named.conf`

```
acl goodclients {
    192.168.100.0/24;
    127.0.0.1;
    localhost;
};

options {
        listen-on port 53 { goodclients; };
        allow-query { goodclients; };
        allow-query-cache { goodclients; };
```

```
        listen-on-v6 port 53 { ::1; };
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
```

Redémarrer le service ''named''

```
systemctl restart named
```

systemctl enable named # systemctl status named

Modifier le paramétrage DNS

```
sudo vim /etc/resolv.conf
```

```
nameserver 127.0.0.1
```

Tester l'interrogation DNS

Executer le code suivant

```
dig google.com
```

```
; <<>> DiG 9.10.4-P3-RedHat-9.10.4-2.P3.fc24 <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15768
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 5

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;google.com.            IN    A

;; ANSWER SECTION:
google.com.     300    IN    A    172.217.18.238

;; AUTHORITY SECTION:
google.com.     171791    IN    NS    ns1.google.com.
google.com.     171791    IN    NS    ns2.google.com.
google.com.     171791    IN    NS    ns4.google.com.
google.com.     171791    IN    NS    ns3.google.com.

;; ADDITIONAL SECTION:
```

```
ns2.google.com.     171791    IN    A    216.239.34.10
ns1.google.com.     171791    IN    A    216.239.32.10
ns3.google.com.     171791    IN    A    216.239.36.10
ns4.google.com.     171791    IN    A    216.239.38.10

;; Query time: 116 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: ven. nov. 11 21:47:14 CET 2016
;; MSG SIZE  rcvd: 191
```

```
; <<>> DiG 9.10.4-P3-RedHat-9.10.4-2.P3.fc24 <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 64308
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 5

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;google.com.            IN    A

;; ANSWER SECTION:
google.com.     248    IN    A    172.217.18.238

;; AUTHORITY SECTION:
google.com.     171739    IN    NS    ns4.google.com.
google.com.     171739    IN    NS    ns3.google.com.
google.com.     171739    IN    NS    ns1.google.com.
google.com.     171739    IN    NS    ns2.google.com.

;; ADDITIONAL SECTION:
ns2.google.com.     171739    IN    A    216.239.34.10
ns1.google.com.     171739    IN    A    216.239.32.10
ns3.google.com.     171739    IN    A    216.239.36.10
ns4.google.com.     171739    IN    A    216.239.38.10

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: ven. nov. 11 21:48:06 CET 2016
;; MSG SIZE  rcvd: 191
```

Activer le service au démarrage de l'OS

1. Vérifier le status

```
systemctl list-unit-files|grep named
```

Résultat

```
named-setup-rndc.service                    static
named.service                               disabled
systemd-hostnamed.service                   static
```

2. Activer le démarrage du service

```
sudo systemctl enable named
```

Résultat

```
Created symlink from /etc/systemd/system/multi-
user.target.wants/named.service to /usr/lib/systemd/system/named.service.
```

3. Vérifier

```
systemctl list-unit-files|grep named
```

```
named-setup-rndc.service                    static
named.service                               enabled
systemd-hostnamed.service                   static
```

Modifier le parefeu

1. Activer le port

Si vous voulez utiliser le cache mis en place par d'autres machines du réseau, il sera nécessaire de lever les restrictions du parefeu.

```
sudo iptables -A INPUT -p tcp -m tcp --dport 53 -m conntrack --ctstate NEW -
j ACCEPT

sudo service iptables save
```

2. Vérifier les règles mises en place

```
sudo iptables -L|grep domain
```

Résultat

```
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:domain
ctstate NEW
```

3. Vérifier l'accessbilité depuis un autre poste

Depuis un autre poste, effectuer une commande **nmap** sur l'adresse du serveur (192.168.100.1 dans notre cas).

```
nmap -v 192.168.100.1
```

Résultat

```
Starting Nmap 7.12 ( https://nmap.org ) at 2016-11-12 09:49 CET
Initiating Ping Scan at 09:49
Scanning 192.168.100.1 [2 ports]
Completed Ping Scan at 09:49, 0.00s elapsed (1 total hosts)
Initiating Connect Scan at 09:49
Scanning srv-prod (192.168.100.1) [1000 ports]
Discovered open port 53/tcp on 192.168.100.1
Completed Connect Scan at 09:49, 0.04s elapsed (1000 total ports)
Nmap scan report for srv-prod (192.168.100.1)
Host is up (0.00025s latency).
Not shown: 999 closed ports
PORT     STATE SERVICE
53/tcp   open  domain
```

From:
https://www.abonnel.fr/ - **notes informatique & technologie**

Permanent link:
https://www.abonnel.fr/informatique/divers/installer-configurer-dns-cache-server-fedora

Last update: **2020/04/17 20:06**