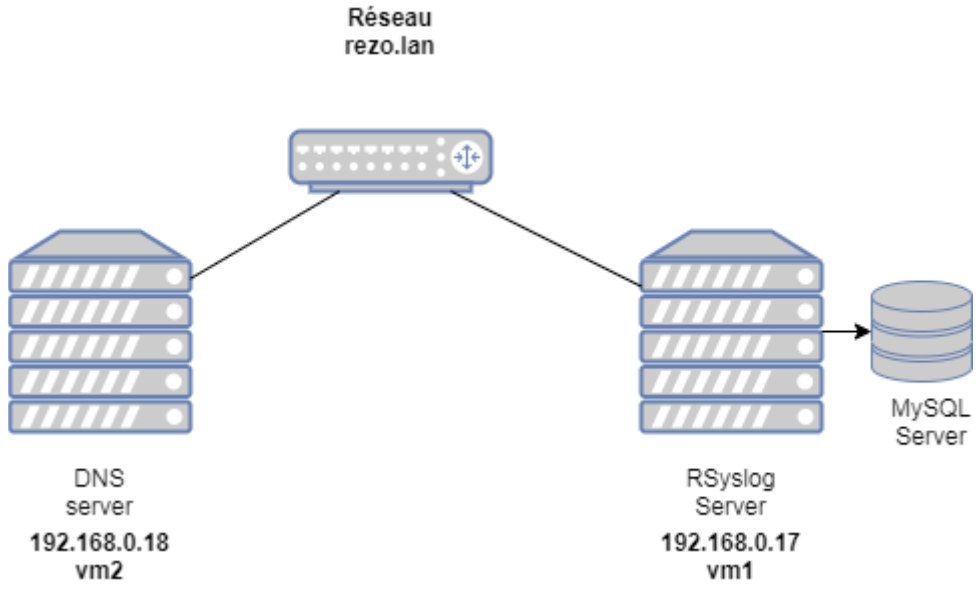
Installer et configurer un serveur DNS sur Linux

Introduction

Le DNS (Domain Name Service) est un service Internet qui trace les adresses IP en fonction du FQDN (Fully Qualified Domain Names) et vice versa.
BIND signifie Berkley Internet Naming Daemon. BIND est le programme le plus communément utilisé pour faire la maintenance d'un serveur DNS sous Linux.
Dans cet article, nous verrons comment installer et configurer un serveur DNS.

Informations réseau

Nous allons mettre en place un serveur local DNS pour le réseau montré sur le schéma ci-dessous.



Nous utiliserons le domaine « rezo.lan » comme exemple pour cette installation DNS. « vm1 », « vm2 » sont les hôtes sur le domaine.

Il est possible de configurer un simple système pour agir en tant que serveur DNS cache, Primaire/Master (Le serveur Primaire/Master est le serveur principal qui fonctionne tout le temps) et Secondaire/Slave (Le serveur Secondaire/Slave est un serveur qui peut être utiliser pour déléguer des tâches du serveur principal ou encore prendre le relais si le principal meurt). Nous configurons ce serveur DNS en tant que Master.

Nous installerons les serveurs DNS sur l'adresse « 192.168.0.18 ».

Installation de Bind

Installez le package bind9 en utilisant le package approprié pour votre distribution Linux.

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

Toutes les configurations DNS sont stockées sous le répertoire /etc/named. La configuration primaire est /etc/named.conf, laquelle inclura les autres fichiers nécessaires.

Configurer le serveur DNS Primaire/Master

Maintenant, nous allons configurer bind9 comme le Master pour le domaine « rezo.lan ».

Comme première étape dans la configuration de notre serveur DNS, nous devons Forward et Reverse la résolution de bind9.

Pour ajouter la résolution Forward et Reverse vers bind9, permettre les requêtes DNS sur le LAN local, supprimer la récurusion.

modifiez /etc/named.conf

```
options {
//      listen-on port 53 { 127.0.0.1; };
        listen-on port 53 { 127.0.0.1; 192.168.0.18; };
//      allow-query     { localhost; };
        allow-query     { localhost; 192.168.0.0/24; };

       /*
        - If you are building an AUTHORITATIVE DNS server, do NOT enable
recursion.
        - If you are building a RECURSIVE (caching) DNS server, you need to enable
          recursion.
        - If your recursive DNS server has a public IP address, you MUST enable
access
          control to limit queries to your legitimate users. Failing to do so will
          cause your server to become part of large scale DNS amplification
          attacks. Implementing BCP38 within your network would greatly
          reduce such attack surface
       */
//      recursion yes;
        recursion no;

zone "rezo.lan" IN {
     type master;
     file "forward.rezo.lan";
     allow-update { none; };
};

zone "0.168.192.in-addr.arpa" IN {
     type master;
     file "reverse.rezo.lan";
     allow-update { none; };
```

```
};


# named-checkconf -z
zone rezo.lan/IN: loading from master file forward.rezo.lan failed:
file not found
zone rezo.lan/IN: not loaded due to errors.
_default/rezo.lan/IN: file not found
zone 0.168.192.in-addr.arpa/IN: loading from master file
reverse.rezo.lan failed: file not found
zone 0.168.192.in-addr.arpa/IN: not loaded due to errors.
_default/0.168.192.in-addr.arpa/IN: file not found
zone localhost.localdomain/IN: loaded serial 0
zone localhost/IN: loaded serial 0
zone
1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.
arpa/IN: loaded serial 0
zone 1.0.0.127.in-addr.arpa/IN: loaded serial 0
zone 0.in-addr.arpa/IN: loaded serial 0
```

Il faut créer les fichiers de configuration indiqués.
Maintenant le fichier /var/named/forward.rezo.lan va avoir les détails pour résoudre (la résolution de nom est le fait de trouver le nom de l'hôte grâce à son adresse IP et vice-versa) le nom de l'hôte à son adresse IP pour ce domaine/zone, et le fichier /var/named/reverse.rezo.lan va avoir les détails pour résoudre l'adresse IP au nom d'hôte.

Mise en place de la Forward resolution pour le serveur DNS Primaire/Master

Maintenant nous allons ajouter les détails qui sont nécessaires pour la forward resolution dans le fichier /var/named/forward.rezo.lan.

```
$ cd /var/named
# vi forward.rezo.lan
$TTL 1D
@       IN SOA  @ vm2.rezo.lan. (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
@       IN  NS          vm2.rezo.lan.
@       IN  A           192.168.0.18
vm2     IN  A           192.168.0.18
vm1     IN  A           192.168.0.17
```

Mise en place de la Reverse resolution pour le serveur DNS Primaire/Master

Nous allons ajouter les détails nécessaires pour la Reverse Resolution dans le fichier /var/named/reverse.rezo.lan

```
$ cd /var/named
# vi reverse.rezo.lan
$TTL 1D
@       IN SOA  @ vm2.rezo.lan. (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
@       IN  NS          vm2.rezo.lan.
@       IN  PTR         rezo.lan.
vm2     IN  A           192.168.0.18
vm1     IN  A           192.168.0.17
18      IN  PTR         vm2.rezo.lan.
17      IN  PTR         vm1.rezo.lan.

# sudo chgrp named -R /var/named

# named-checkconf -z
zone rezo.lan/IN: loaded serial 0
zone 0.168.192.in-addr.arpa/IN: loaded serial 0
zone localhost.localdomain/IN: loaded serial 0
zone localhost/IN: loaded serial 0
zone
1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.
arpa/IN: loaded serial 0
zone 1.0.0.127.in-addr.arpa/IN: loaded serial 0
zone 0.in-addr.arpa/IN: loaded serial 0
```

La configuration est testée et ne donne pas d'erreur.
Enfin, redémarrez le service bind9 :

```
# systemctl status named
? named.service - Berkeley Internet Name Domain (DNS)
     Loaded: loaded (/usr/lib/systemd/system/named.service;
disabled; vendor preset: disabled)
     Active: inactive (dead)

# systemctl enable named
Created symlink /etc/systemd/system/multi-
```

```
user.target.wants/named.service ?
/usr/lib/systemd/system/named.service.


# systemctl start named
# systemctl status named
? named.service - Berkeley Internet Name Domain (DNS)
     Loaded: loaded (/usr/lib/systemd/system/named.service; enabled; vendor preset:
disabled)
     Active: active (running) since Wed 2020-07-15 08:12:29 CEST; 2s ago
    Process: 11218 ExecStartPre=/bin/bash -c if [ ! "$DISABLE_ZONE_CHECKING" ==
"yes" ]; then /usr/sbi>
    Process: 11220 ExecStart=/usr/sbin/named -u named -c ${NAMEDCONF} $OPTIONS
(code=exited, status=0/>
   Main PID: 11221 (named)
      Tasks: 4 (limit: 2251)
     Memory: 55.1M
        CPU: 46ms
     CGroup: /system.slice/named.service
             +-11221 /usr/sbin/named -u named -c /etc/named.conf


juil. 15 08:12:29 vm2 named[11221]: zone 0.168.192.in-addr.arpa/IN: loaded serial 0
juil. 15 08:12:29 vm2 named[11221]: zone rezo.lan/IN: loaded serial 0
juil. 15 08:12:29 vm2 named[11221]: zone localhost/IN: loaded serial 0
juil. 15 08:12:29 vm2 named[11221]: all zones loaded
juil. 15 08:12:29 vm2 systemd[1]: Started Berkeley Internet Name Domain (DNS).
juil. 15 08:12:29 vm2 named[11221]: running
juil. 15 08:12:29 vm2 named[11221]: zone 0.168.192.in-addr.arpa/IN: sending
notifies (serial 0)
juil. 15 08:12:29 vm2 named[11221]: zone rezo.lan/IN: sending notifies (serial 0)
juil. 15 08:12:29 vm2 named[11221]: managed-keys-zone: Key 20326 for zone .
acceptance timer complete:>
juil. 15 08:12:29 vm2 named[11221]: resolver priming query complete
```

Reconfigurer le resolver pour qu'il utilise le nouveau serveur DNS
La configuration de networkManager est modifiée pour le plus générer automatiquement le fichier resolv.conf (dns=none)

```
# cd /etc/NetworkManager
# vi NetworkManager.conf


[main]
dns=none
#plugins=ifcfg-rh


# cd /etc
# vi resolv.conf


nameserver 192.168.0.18
```

Tester le serveur DNS

```
# dig @192.168.0.18 vm1.rezo.lan

; <<>> DiG 9.11.20-RedHat-9.11.20-1.fc32 <<>> @192.168.0.18
vm1.rezo.lan
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 64446
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: d048e25f4d192e9fb9aa86075f0ea85ff568d4e33be46d8c (good)
;; QUESTION SECTION:
;vm1.rezo.lan.                  IN      A

;; ANSWER SECTION:
vm1.rezo.lan.           86400   IN      A       192.168.0.17

;; AUTHORITY SECTION:
rezo.lan.               86400   IN      NS      vm2.rezo.lan.

;; ADDITIONAL SECTION:
vm2.rezo.lan.           86400   IN      A       192.168.0.18

;; Query time: 0 msec
;; SERVER: 192.168.0.18#53(192.168.0.18)
;; WHEN: mer. juil. 15 08:55:27 CEST 2020
;; MSG SIZE  rcvd: 119

]# dig vm2.rezo.lan

; <<>> DiG 9.11.20-RedHat-9.11.20-1.fc32 <<>> vm2.rezo.lan
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2859
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
```

```
; COOKIE: 95e3b798752c6edcc2847eba5f0ea88c505ec39966a0e8dd (good)
;; QUESTION SECTION:
;vm2.rezo.lan.                  IN      A

;; ANSWER SECTION:
vm2.rezo.lan.           86400   IN      A       192.168.0.18

;; AUTHORITY SECTION:
rezo.lan.               86400   IN      NS      vm2.rezo.lan.

;; Query time: 0 msec
;; SERVER: 192.168.0.18#53(192.168.0.18)
;; WHEN: mer. juil. 15 08:56:12 CEST 2020
;; MSG SIZE  rcvd: 99

# ping -c 3 vm1.rezo.lan
PING vm1.rezo.lan (192.168.0.17) 56(84) bytes of data.
64 bytes from vm1.rezo.lan (192.168.0.17): icmp_seq=1 ttl=64
time=0.234 ms
64 bytes from vm1.rezo.lan (192.168.0.17): icmp_seq=2 ttl=64
time=0.500 ms
64 bytes from vm1.rezo.lan (192.168.0.17): icmp_seq=3 ttl=64
time=0.546 ms

--- vm1.rezo.lan ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2030ms
rtt min/avg/max/mdev = 0.234/0.426/0.546/0.137 ms
```