Configurer un serveur DNS avec BIND sous CentOS 8 □□□□

Tuto depuis blog.microlinux.fr.

Installation

```
$ sudo yum install bind bind-utils
```

Serveur cache DNS

1. On fait une sauvegarde de fichier d'origine.
2. On édite un nouveau fichier named.conf

```
$ sudo mv /etc/named.conf /etc/named.conf.orig
$ sudo vim /etc/named.conf
```

```
// etc/named.conf
options {
  directory "/var/named";
};

// journalisation propre à BIND
logging {
  channel single_log {
    file "/var/log/named/named.log" versions 3 size 2m;
    severity info;
    print-time yes;
    print-severity yes;
    print-category yes;
```

```
  };
  category default {
    single_log;
  };
};

zone "." IN {
  type hint;
  file "named.ca";
};

include "/etc/named.rfc1912.zones";
// zone DNS afin de déclarer en serveur maître primaire
include "/etc/named.conf.local";
```

1. On attribut user:group du fichier.
2. On règle les permissions du fichier.
3. On active et démarre BIND.
4. On vérifie si le service tourne correctement.

```
$ sudo chown root:named /etc/named.conf
$ sudo chmod 0640 /etc/named.conf
$ sudo systemctl enable named --now
$ 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 Mon 2021-01-11 14:31:42 CET; 1 day 1h ago
```

Configurer la journalisation

Comme vu précédemment, la journalisation propre à BIND a été mise en place. Cependant, il ne peut pas créer ce fichier à la volée.
On le crée à sa place en attribuant les permissions correctes.

```
$ sudo mkdir /var/log/named
$ sudo touch /var/log/named/named.log
$ sudo chown -R named:named /var/log/named/
$ sudo chmod 0770 /var/log/named
```

1. Avec SELinux en mode renforcé, on réétiquette le répertoire.
2. On recharge la configuration de BIND.

```
$ sudo restorecon -R -v /var/log/named
$ sudo systemctl reload named
```

Serveur maître primaire

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

```
zone "<domaine.name>" {
  type master;
  file "zone.<domaine.name>";
};
```

On attribue les mêmes permissions que `named.conf`.

```
$ sudo chown root:named /etc/named.conf.local
$ sudo chmod 0640 /etc/named.conf.local
```

On édite le fichier `zone.<domaine.name>`.

```
$ sudo vim /var/named/zone.<domaine.name>
```

```
; /var/named/zone.<domaine.name>
$TTL 86400
$ORIGIN <domaine.name>.
@ IN SOA ns.<domaine.name>. <nom>.<domaine.name>. (
   2021011201   ; sn: serial number must be incremented each time
        10800   ; refresh (3 heures)
          600   ; retry (10 minutes)
      1814400   ; expiry (3 semaines)
        10800 ) ; minimum (3 heures)
□□□□□IN      NS      ns.<domaine.name>.
ownercheck□□□IN      TXT     "<hash>" ; to check owner with provider
<domaine.name>.□□IN      AAAA    2001:41d0:305:2100::100e
<domaine.name>.□□IN      A       51.38.177.69
ns□□□□□IN      AAAA    2001:41d0:305:2100::100e
ns□□□□□IN      A       51.38.177.69
shaarli□□□□IN      AAAA    2001:41d0:305:2100::100e
shaarli□□□□IN      A       51.38.177.69
www□□□□□IN      CNAME   <domaine.name>.
```

```
www.shaarli□□□IN      CNAME   shaarli
```

> La partie `<nom>.<domaine.name>.` correspond à une adresse e-mail joignable. Étant donné que le `@` à une signification particulière dans le fichier de configuration, il est substitué par un point (`.`). Si l'adresse e-mail contient un permier point de séparation (exemple `jean.dupond@example.com`) il doit être échappé (`jean\.dupond.example.com`).
>
> *Source : SOA Record Explained How to Perform an SOA Record Check (+Example) - IONOS*

1. On règle les droits de propriétés.
2. On règle les permissions qui vont bien.
3. On vérifie la définition correcte de la zone.
4. On recharge la configuration de BIND.
5. On refait une expansion des certificats au besoin.

```
$ sudo chown root:named /var/named/zone.<domaine.name>
$ sudo chmod 0640 /var/named/zone.<domaine.name>
$ sudo named-checkzone <domaine.name> /var/named/zone.<domaine.name>
zone <domaine.name>/IN: loaded serial 2021011201
OK
$ sudo systemctl reload named
$ sudo certbot --nginx # Si certbot est bien installé
```

Révision #4
Créé 5 juin 2021 13:55:05 par Mickaël G.
Mis à jour 9 août 2023 07:58:21 par Mickaël G.