Tuto DNS

Centos7

Prérequis

Dans le [pare-feu](https://blog.microlinux.fr/firewalld-dedibox/), ouvrir le port 53 en TCP et en UDP pour les requêtes DNS.

$ **sudo firewall-cmd --permanent --add-service=dns**

$ **sudo firewall-cmd --reload**

$ **sudo firewall-cmd --list-all**

public (active)

target: default

icmp-block-inversion: no

interfaces: eth0

sources:

services: **dns** ssh

ports:

protocols:

masquerade: no

forward-ports:

source-ports:

icmp-blocks:

rich rules:

Installation

Outre le serveur bind à proprement parler, on installera le paquet bind-utils, qui fournit une collection d’outils comme dig, host et nslookup.

$ **sudo yum install bind bind-utils**

Serveur cache DNS

La configuration par défaut fournie par Red Hat est déjà assez sophistiquée. On va la sauvegarder pour partir sur quelque chose de plus simple.

$ **cd /etc**

$ **sudo mv named.conf named.conf.orig**

Éditer /etc/named.conf comme ceci.

// /etc/named.conf

options {

directory "/var/named";

};

zone "." IN {

type hint;

file "named.ca";

};

include "/etc/named.rfc1912.zones";

Régler les permissions de ce fichier.

$ **sudo chown root:named /etc/named.conf**

$ **sudo chmod 0640 /etc/named.conf**

Activer et démarrer BIND.

$ **sudo systemctl enable named --now**

Vérifier si le service tourne correctement.

$ **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 2020-03-11 09:47:39 CET; 31s ago

Exécuter dig sur un domaine extérieur en vérifiant le temps de requête.

**$ dig centos.org @localhost**

...

;; ANSWER SECTION:

centos.org. 60 IN A 85.12.30.226

;; AUTHORITY SECTION:

centos.org. 14400 IN NS ns4.centos.org.

centos.org. 14400 IN NS ns1.centos.org.

centos.org. 14400 IN NS ns3.centos.org.

;; ADDITIONAL SECTION:

ns4.centos.org. 86400 IN A 62.141.54.220

ns3.centos.org. 86400 IN A 88.208.217.170

ns1.centos.org. 86400 IN A 199.187.126.93

;; Query time: **141 msec**

;; SERVER: 127.0.0.1#53(127.0.0.1)

;; WHEN: Wed Mar 11 11:13:02 CEST 2017

;; MSG SIZE rcvd: 157

Le temps de réponse devrait être bien plus court après une deuxième invocation de dig.

$ **dig centos.org @localhost**

...

;; Query time: **1 msec**

Configurer la journalisation

Dans notre configuration actuelle, les logs inondent /var/log/messages. Pour éviter ça, on va configurer une journalisation propre à BIND en ajoutant la stance correspondante à /etc/named.conf.

options {

directory "/var/named";

};

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;

};

};

BIND ne peut pas créer ce fichier à la volée. On va donc le faire 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**

Si l’on utilise [SELinux en mode renforcé](https://blog.microlinux.fr/selinux/), il faut impérativement réétiqueter le répertoire /var/log/named et son contenu.

$ **sudo restorecon -R -v /var/log/named**

Recharger la configuration de BIND.

$ **sudo systemctl reload named**

Désactiver l’IPv6

Si l’on n’utilise pas l’IPv6, on peut désactiver le protocole en éditant /etc/sysconfig/named.

OPTIONS="-4"

Il faudra également ajouter une option à /etc/named.conf.

options {

directory "/var/named";

filter-aaaa-on-v4 yes;

};

Redémarrer BIND pour prendre en compte les modifications.

$ **sudo systemctl restart named**

Utiliser les DNS de base de chez Online

Online met à disposition deux serveurs DNS de base que nous allons utiliser de préférence.

options {

directory "/var/named";

filter-aaaa-on-v4 yes;

forwarders {

62.210.16.6;

62.210.16.7;

};

};

À partir de là, on pourra utiliser notre propre serveur cache DNS par défaut.

# /etc/resolv.conf

nameserver 127.0.0.1

Recharger la configuration de BIND.

$ **sudo systemctl reload named**

Serveur maître primaire

À présent, nous allons configurer BIND comme serveur maître primaire du domaine slackbox.fr. Le nom de domaine sera réservé au bureau d’enregistrement (*registrar*) [BookMyName.com](https://www.bookmyname.com/).

Pour ajouter une zone DNS à BIND afin de le transformer en serveur maître primaire, il faut tout d’abord indiquer l’emplacement du fichier de zone à /etc/named.conf. Pour plus de lisibilité, nous allons créer un fichier /etc/named.conf.local.

// /etc/named.conf.local

zone "slackbox.fr" {

type master;

file "zone.slackbox.fr";

};

Le fichier named.conf.local aura les mêmes permissions que named.conf.

$ **sudo chown root:named /etc/named.conf.local**

$ **sudo chmod 0640 /etc/named.conf.local**

Éditer /etc/named.conf en incluant ce fichier.

zone "." IN {

type hint;

file "named.ca";

};

include "/etc/named.rfc1912.zones";

**include "/etc/named.conf.local";**

Le fichier /var/named/zone.slackbox.fr devra être édité comme ceci.

; /var/named/zone.slackbox.fr

$TTL 86400

$ORIGIN slackbox.fr.

@ IN SOA ns.slackbox.fr. hostmaster.slackbox.fr. (

2020031101 ; sn

10800 ; refresh (3 heures)

600 ; retry (10 minutes)

1814400 ; expiry (3 semaines)

10800 ) ; minimum (3 heures)

IN NS ns.slackbox.fr.

IN NS nssec.online.net.

IN MX 10 mail.slackbox.fr.

slackbox.fr. A 163.172.220.174

ns IN A 163.172.220.174

mail IN A 163.172.220.174

www CNAME slackbox.fr.

Définir les permissions qui vont bien.

$ **sudo chown root:named /var/named/zone.slackbox.fr**

$ **sudo chmod 0640 /var/named/zone.slackbox.fr**

Quelques remarques sur la syntaxe et les options utilisées.

* La directive $TTL (*Time To Live*) définit le temps en secondes qu’un enregistrement pourra être gardé dans le cache par un autre serveur de noms.
* La directive $ORIGIN définit le nom de domaine automatiquement ajouté à tous les noms de domaine incomplets (c’est-à-dire « non qualifiés ») définis dans un enregistrement DNS. Le nom de domaine est toujours un FQDN (*Fully Qualified Domain Name*) et se termine en conséquence par un point.
* L’enregistrement SOA (*Start Of Authority*) définit les principales caractéristiques pour la zone ou le domaine avec un certain nombre de paramètres.
* Le symbole @ se substitue à la valeur de $ORIGIN, concrètement à slackbox.fr.
* IN définit la classe *Internet*. D’autres valeurs existent, mais elles sont rarement utilisées.
* L’enregistrement NS définit le serveur de noms primaire pour la zone.
* hostmaster.slackbox.fr définit l’adresse mail de l’administrateur de la zone. L’adresse hostmaster est recommandée, mais n’importe quelle adresse mail valide peut être définie ici. Étant donné que le symbole @ a une signification spécifique dans le contexte, on utilise les points comme séparateurs, ce qui explique la syntaxe bizarre. L’adresse mail définie ici est donc hostmaster@slackbox.fr.
* 2020031101 définit le numéro de série associé à la zone. Par convention, on utilise le format AAAAMMJJSS. Le numéro de série doit impérativement être mis à jour à chaque fois que l’on modifie le domaine.
* La valeur refresh contrôle la mise à jour des informations du serveur de noms esclave de la zone. Les valeurs typiques se situent entre 3 heures (10800) et 24 heures (86400).
* La valeur retry définit le temps d’attente avant une deuxième tentative lorsque le serveur de noms esclave n’arrive pas à contacter le serveur maître pour rafraîchir les informations. Les valeurs typiques se situent entre 10 minutes (600) et 60 minutes (3600).
* La valeur expiry définit le laps de temps au bout duquel les enregistrements de zone sont considérés comme ne faisant plus autorité. On choisira une valeur assez élevée, située entre une semaine (604800) à trois semaines (1814400).
* La valeur minimum définit le laps de temps durant lequel des réponses négatives (NXDOMAIN) peuvent être gardées en cache par le serveur de noms esclave. Cette valeur se situera entre 0 et 3 heures (10800).
* L’enregistrement NS (*NS Resource Record*) définit le ou les serveurs de noms pour le domaine ou la zone.
* L’enregistrement A (*A Resource Record*) définit l’adresse IPv4 d’un hôte du domaine ou de la zone.

Vérifier la définition correcte de la zone.

$ **sudo named-checkzone slackbox.fr /var/named/zone.slackbox.fr**

zone slackbox.fr/IN: loaded serial 2020031101

OK

À chaque fois que l’on modifie le fichier de zone, on doit obligatoirement incrémenter le numéro de série. Ne pas oublier de recharger la configuration de BIND après chaque modification.

$ **sudo systemctl reload named**