BIND (serwer nazw) – konfiguracja

Jak prosto skonfigurować własny serwer DNS.

Serwery DNS najłatwiej mówiąc są odpowiedzialne za zmianę nazwy domeny (np. *oke.gda.pl*) na adresy IP (np. *213.192.73.194*). Maszynom o wiele prościej jest posługiwać się liczbami, natomiast ludziom napisami.

W dzisiejszych czasach prawie każdy rejestrator pozwala korzystać z własnych serwerów DNS. Niestety udostępniają oni najczęściej bardzo prosty edytor bez możliwości większej ingerencji. Dlatego każdemu z nas, kto marzy np. o koncie Jabber/GoogleTalk we własnej domenie, czy podaniu wielu serwerów pocztowych przyda się własny serwer DNS. Nie wspominając, że prościej przenieść plik strefy między serwerami niż zapisy w panelu rejestratora.

Najpopularniejszym serwerem DNS jest BIND (nazywany *named*). Niestety nie jest on najpiękniejszym tworem ze względów bezpieczeństwa. O ile w dystrybucji PLD całość jest w więzieniu (jail) to niestety w takim Debianie nie.

Zabezpieczenie BIND-a

Pierwsze co musimy zrobić, aby posiadać własny serwer DNS to go zainstalować. W Debianie wystarczy wydać komendę:

```
# apt-get install bind9
```

Aby zwiększyć bezpieczeństwo. Całość BIND-a zamkniemy w katalogu */var/lib/named*. Wyłączmy serwer DNS.

BIND pozwala na definicję katalogu chrootowanego, dlatego zmieńmy parametr OPTIONS w pliku */etc/default/bind9* na:

```
OPTIONS="-u bind -t /var/lib/named"
```

Utwórzmy potrzebne katalogi i przenieśmy konfigurację:

```
mkdir -p /var/lib/named/etc
mkdir -p /var/lib/named/var/cache/bind
mkdir /var/lib/named/var/run
mkdir /var/lib/named/dev
mv /etc/bind /var/lib/named/etc
mv /var/run/bind /var/lib/named/var/run
```

W starych miejscach (np. */etc/bind*) możemy zostawić linki symboliczne dla pewności:

```
ln -s /var/lib/named/etc/bind /etc/bind
ln -s /var/lib/named/var/run/bind/ /var/run/bind
```

Na koniec utwórzmy potrzebne urządzenia (*null*, *random*) w naszym jail-u i nadajmy odpowiednie prawa:

```
mknod /var/lib/named/dev/null c 1 3
mknod /var/lib/named/dev/random c 1 8
chmod 666 /var/lib/named/dev/null /var/lib/named/dev/random
chown -R bind:nogroup /var/lib/named/var/*
chown -R bind:nogroup /var/lib/named/etc/bind
```

Jedynym problemem wydzielenia BIND do chroot'a jest problem z logowaniem zdarzeń. Musimy poinformować *syslog* jakie dodatkowe dane ma zbierać. Dlatego SYSLOGD w pliku /etc/default/syslogd powinien od teraz wyglądać następująco:

```
SYSLOGD="-a /var/lib/named/dev/log"
```

Skończone. Przeładujmy syslogd oraz bind na koniec:

```
# /etc/init.d/sysklogd restart
# /etc/init.d/bind9 start
```

Konfiguracja

Konfiguracja BIND-a jest bardzo prosta. W katalogu konfiguracyjnym (/var/lib/named/etc/bind/) znajdują się 2 pliki, które będą nas interesowały:

- /var/lib/named/etc/bind/named.conf.options – konfiguracja usługi
- /var/lib/named/etc/bind/named.conf.local – konfiguracja stref (domen), które obsługujemy

Mój plik named.conf.options wygląda następująco:

```
options {
version "matipl DNS";
directory "/var/cache/bind";

forwarders { XXX.XX.XX.XX; };

auth-nxdomain no;
listen-on { YYY.YYY.YYY.YY; 127.0.0.1; };
allow-recursion { 127.0.0.1; };
};
```

Znaczenie poszczególnych opcji:

- ze względów bezpieczeństwa możemy podać w **version** cokolwiek
- opcja **directory** to katalog roboczy BIND-a
- **forwarders** – każdorazowe odpytywanie się Root Servers może okazać się mało wydajne, jeśli chcemy przyspieszyć ten proces wpiszmy tutaj adresy IP serwerów DNS naszego ISP, do którego wpięty jest serwer (droga zapytań będzie o wiele krótsza)

- **auth-nxdomain** jako parametry przyjmuje *yes*/*no*, ustawia czy negatywne odpowiedzi zbuforowane przez serwer mają być traktowane jako autorytatywne
- **listen-on** zawiera listę adresów IP, na których ma nasłuchiwać serwer nazw. Możemy wydzielić poszczególne IP (j.w) lub wpisać *any;*, wtedy będzie słuchał na wszelkich dostępnych
- **allow-recursion** po wpisaniu 127.0.0.1 nasz serwer DNS będzie zamknięty na cykliczne zapytania. Jeśli ma to być Open DNS usuńmy zupełnie tą linijkę

Aby zacząć przygodę z domenami utwórzmy jeszcze 2 katalogi. Osobny dla domen, dla których będziemy serwerem podstawowym, osobno dla zapasowych:

mkdir /var/lib/named/etc/bind/M
mkdir /var/lib/named/etc/bind/S

W pliku *named.conf.local* definiujemy jakie strefy (domeny) chcemy obsługiwać przez nasz serwer DNS. Jeśli nasz BIND ma być serwerem podstawowym (primary) dla domeny domena.pl powinniśmy dodać we wspomnianym pliku:

```
zone "domena.pl" {
type master;
file "/etc/bind/M/domena.pl";
notify yes;
allow-transfer { XXX.XXX.XXX.XX; };
};
```

Definicja strefy jest bardzo prosta:

- zone „domena.pl” – nazwa strefy
- type master – rodzaj serwera (master – primary, slave – secondary)
- file „/etc/bind/M/domena.pl” – nazwa pliku z konfiguracją naszej strefy
- notify yes – bardzo przydatna opcja, włącza automatyczne powiadamianie zapasowego serwera DNS o zmianach w strefie
- allow-transfer { XXX.XXX.XXX.XX; } – adres serwera, który ma możliwość transferu całej strefy, powinny znaleźć się tutaj wyłącznie adresy IP zapasowych serwerów nazw

W następnej kolejności dla domena.pl musimy utworzyć wspomniany plik strefy. Przykładowy plik strefy:

```
$TTL 86400
$ORIGIN domena.pl.
@ IN SOA dns1.domena.pl. root.domena.pl. (
2010111801 ;; serial
2H ;; refresh
1H ;; retry
7D ;; expire
1D ;; TTL
)
@ IN NS dns1.domena.pl.
@ IN NS dns2.domena.pl.
```

@ IN MX 10 mail.domena.pl.

@ IN A XXX.XX.XX.X
dns1 IN A XXX.XX.XX.X
dns2 IN A YYY.YY.YY.Y

www IN CNAME @
mail IN CNAME @
ftp IN CNAME www

Plik strefy dzieli się na 3 sekcje: nazwa domeny i okres ważności wpisów, kto zarządza domeną oraz zawartość. Kiedyś wszelkie **czasy podawane był w sekundach**, dzisiaj możemy tworzyć „skróty" podając 1D (Day) lub 2H (Hours).**Komentarze** oznaczamy podwójnym średnikiem (;;). Zauważyliście powyżej zapewne kropki podawane na końcach domen – dns1.domena.pl., gdyby zabrakło kropki BIND automatycznie dokleiłby domenę z $ORIGIN. Wtedy z dns1.domena.pl zrobiłoby się dns1.domena.pl.domena.pl. I ostatnia sprawa: **@ jest pewnego rodzaju zmienną**, która przechowuje nazwę domeny.

Omówmy powyższy przykład:

- **$TTL 86400** – czas ważności rekordów w domenie (jednostka – sekundy)
- **$ORIGIN domena.pl.** – nazwa domeny, którą plik strefy opisuje
- **@ IN SOA dns1.domena.pl. root.domena.pl**. – rekord typu Start Of Authority (SOA), informuje jaki jest adres serwera **primary DNS** (dns1.domena.pl) oraz **kto zarządza domeną** (root@domena.pl). W adresie e-mail należy pamiętać, że @ zamieniamy na kropkę (.). Dodatkowo rekord SOA posiada własną strukturę:
    - **2010111801 ;; serial** – numer seryjny domeny, przyjęło się że jego format to YYYYMMDDnn (rok – miesiąc – dzień – kolejny numer); po każdorazowej zmianie w tym pliku powinniśmy podbić numer
    - **2H ;; refresh** – jak często serwery slave mają sprawdzać czy dane domeny nie zmieniły się na primary DNS (wg RFC 1035 wartość powinna być z przedziału 1200-43200 sekund)
    - **1H;; retry** – czas, po którym secondary DNS na ponowić próbę kontaktu, gdy wcześniej się nie powiedzie (zalecana wartość 120-7200 sekund)
    - **14D ;; expire** – po jakim czasie dane domeny mają zostać uznane za nieaktualny, gdy serwer secondary DNS nie będzie mógł skontaktować się z primary (zalecana wartość 1209600-2419200 sekund, czyli 2-4 tygodni)
    - **1D ;; TTL** – Time To Live, długość ważności rekordu, czyli jak długo dane pobrane przez dany serwer DNS są ważne (zalecana wartość 86400-432000 sekund, czyli 1-5 dni)
- **@ IN NS dns1.domena.pl**. – definicja serwerów DNS, które obsługują domenę domena.pl; jest to pole wymagane, bez tego nasza domena nie będzie działać. Minimalnie musimy podać 2 serwery. Jeśli ich adresy są w ramach naszej domeny (czyli wcześniej nie pełniły roli serwerów DNS) musimy podać ich adresy IP poprzez rekord IN A.

Reszta pliku strefy jest dowolna, ale omówimy co znaczą poszczególne wpisy.

Każda domena, musi mieć **zdefiniowane swoje serwery DNS**:

@ IN NS dns1.domena.pl.
@ IN NS dns2.domena.pl.

Mogą to być oczywiście serwery spoza naszej domeny, np.:

@ IN NS dns1.example.com.
@ IN NS dns2.example.com.

Jeśli jest to definicja serwerów nazw, które sami obsługujemy musimy rozwiązać nazwę *dns1.domena.pl* na adres IP:

@ IN A XXX.XX.XX.X
dns1 IN A XXX.XX.XX.X
dns2 IN A YYY.YY.YY.Y

W ten oto sposób powiedzieliśmy światu, że *domena.pl* obsługuje maszyna o IP XXX.XX.XX.X, ma primary DNS na XXX.XX.XX.X, a secondary na YYY.YY.YY.Y. Gdybyśmy musieli „podpiąć" inne IP-ki pod domeną posługujemy się właśnie wpisami **IN A**.

Jeśli chcemy ustawić serwer poczty dla naszej domeny musimy posłużyć się rekordem **IN MX**:

@ IN MX 10 mail.domena.pl.

Wpis ten mówi, że wszelka poczta kierowana na @domena.pl ma być kierowana na **serwer pocztowy** mail.domena.pl o priorytecie 10. Priorytet przydaje się nam wtedy, gdy podamy kilka serwerów pocztowych.

Z naszego przykładu zostały nam jeszcze wpisy **IN CNAME**.

www IN CNAME @
mail IN CNAME @
ftp IN CNAME www

Najprościej mówiąc **IN CNAME** to alias, który tworzy sub-domenę. Najlepiej wskazywać na rekord **IN A**, niż inny **IN CNAME**.

Po wszystkim należy ponownie uruchomić usługę bind:

/etc/init.d/bind9 restart

Secondary DNS

Dla naszego zapasowego serwera DNS konfiguracja usługi (*named.conf.options*) wygląda dokładnie tak samo (ew. zmieńmy IP). W tym wypadku nie tworzymy pliku strefy DNS, ponieważ będzie on ściągany z primary DNS. Jedyne co należy zrobić to w pliku *named.conf.local* zdefiniować strefy, które obsługujemy. Dla przykładu domena.pl:

```
zone "domena.pl" {
type slave;
file "/etc/bind/S/domena.pl";
masters { ZZZ.ZZZ.ZZZ.ZZ; };
};
```

Jak zapewne zauważyliście nie ma wpisu dotyczącego notify oraz allow-transfer, natomiast pojawia się opcja masters. Masters wskazuje nam na podstawowy serwer nazw naszej domeny. To wszystko. Po przeładowaniu BIND:

```
# /etc/init.d/bind9 reload
```

powinna pojawić się definicja strefy domena.pl w katalogu */etc/bind/S*.

Sprawdzanie pliku ze strefą

Na początku naszej przygody z definiowaniem stref DNS na pewno przyda nam się program *named-checkzone* (paczka *bind9utils*), który służy do sprawdzenia poprawności naszego pliku strefy. Wywołanie jest bardzo proste.:

```
# named-checkzone domena.pl /etc/bind/M/domena.pl
```

Jako pierwszy parametr podajemy nazwę domeny, natomiast po nim ścieżkę do pliku strefy tej domeny.

Na podstawie:
https://matipl.pl/2010/11/19/bind-serwer-nazw-konfiguracja/