OpenSUSE Serwer DNS (BIND)

Domain Name System – hierarchiczny rozproszony system nazw sieciowych, który odpowiada na zapytania o nazwy domen. Dzięki DNS nazwa mnemoniczna, np. pl.wikipedia.org jest tłumaczona na odpowiadający jej adres IP, czyli 91.198.174.192.

Instalacja

```
sudo zypper install bind bind-utils
```

Status / Start /Stop

```
sudo systemctl status named
sudo systemctl start named
sudo systemctl stop named
```

Włączenie usługi do autostartu

```
sudo systemctl enable named
```

Konfiguracja

Głównym plikiem konfiguracyjnym serwera Bind jest `/etc/named.conf`. Znajdują się w nim podstawowe opcje usługi oraz informacje na temat obsługiwanych stref. Poniżej zamieszczono domyślne wpisy, które znajdują się w tym pliku

```
options {
  directory "/var/lib/named";
        pid-file "named.pid";
        auth-nxdomain yes;
        datasize default;
};
zone "localhost" IN {
        type master;
        file "localhost.zone";
        allow-update { none; };
```

```
        allow-transfer { any; };
};
zone "0.0.127.in-addr.arpa" IN {
        type master;
        file "127.0.0.zone";
        allow-update { none; };
        allow-transfer { any; };
};
zone "." IN {
        type hint;
        file "root.hint";
};
```

Przykładowy wpis dla strefy na serwerze podstawowym:

```
zone "example.net" in {
  type master;
  file "M/example.net";
  allow-transfer { 123.45.67.89; };
  notify yes;
};
```

- `zone "example.net"` - nazwa strefy - naszej domeny
- `type master` - rodzaj serwera
- `file "M/example.net"` - nazwa pliku z konfiguracją strefy
- `allow-transfer { 123.45.67.89; }` - adres serwera, który ma możliwość transferu całej strefy, Jeżeli posiadasz więcej niż jeden taki DNS, możesz je wpisać pomiędzy klamry pamiętając o tym, aby rozdzielić poszczególne adresy IP znakiem ';'.
- `notify yes` - opcja ta włącza powiadamianie zapasowego serwera DNS o zmianach w naszej domenie.

Musimy teraz utworzyć plik strefy dla domeny `example.net` wskazany przez opcję `file`. Poniżej zamieszczam treść przykładowego pliku strefy który w przypadku OpenSUSE 42.3 znajduje się w /var/lib/named/master:

```
$TTL 86400
$ORIGIN example.net.
@       IN      SOA     ns1.example.net. root.example.net. (
                                                2004022300 ;; serial
                                                1200       ;; refresh
                                                1200       ;; retry
                                                2419200    ;; expire
                                                86400      ;; TTL
                                                )
```

```
@               IN      NS      ns1.example.net.
@               IN      NS      ns2.example.net.
@               IN      MX      10    mail.example.net.
@               IN      A       123.45.67.8
ns1             IN      A       123.45.67.8
ns2             IN      A       90.12.34.237
mail            IN      A       123.45.67.8
www             IN      A       34.5.6.78
ftp             IN      CNAME   www
```

Plik strefy można podzielić na trzy odrębne sekcje. Pierwsza określa nazwę domeny oraz okres ważności wpisów. Druga, kto tą domeną zarządza. W trzeciej znajduje się cała jej zawartość.

Szczegółowy opis znajduje się poniżej.

Wszystkie wpisy poprzedzone *;;* będą ignorowane i traktowane jak komentarz. Kolejnym ważnym znakiem jest znak kropki.

```
@               IN      NS      ns1.example.net.
```

Jeżeli w powyższym wpisie pominęlibyśmy końcowy znak kropki, wówczas Bind dokleiłby na końcu nazwę domeny. Wówczas z ns1.example.net zrobiłby się wpis ns1.example.net.example.net, co oczywiście nie jest pożądane. następnym znakiem specjalnym na który warto zwrócić uwagę jest @. Otóż można go potraktować jako pewnego rodzaju zmienną, która przechowuje nazwę example.net. Jednym słowem, example.net i @ to to samo.

- `$TTL 86400` - czas ważności rekordów w domenie wyrażony w sekundach; 86400 s. to jedna doba
- `$ORIGIN example.net.` - domena jaką będzie opisywał bieżący plik strefy.
- `@ IN SOA ns1.example.net. root.example.net.` - Rekord typu SOA czyli Start Of Authority. Możemy się z niego dowiedzieć, kto zarządza domeną (root@example.net), jaki jest adres serwera primary DNS. Zwróć uwagę, że w adresie root@example.net zamiast znaku @ użyta została kropka. Rekord SOA posiada swoją własną strukturę o której poniżej. Zawarta jest ona pomiędzy znakami *( )*.
- `**2004022300 ;; serial**` - numer seryjny domeny. Powinien on być zwiększany wraz z każdą jej modyfikacją. W dobrym tonie jest utrzymywanie go w formacie *YYYYMMDDnn* czyli rok, miesiąc, dzień oraz numer modyfikacji w danym dniu.
- `**1200 ;; refresh**` - To pole rekordu SOA definiuje jak często serwery *slave* mają sprawdzać czy dane o domenie nie zmieniły się na *masterze*. Według RFC 1035 wartość ta powinna się zawierać pomiędzy 1200 a 43200 (czyli od dwudziestu minut do dwunastu godzin). W praktyce najlepsza wartość zawiera się między 3600 a 7200 sekund.
- `**1200 ;; retry**` - Czas po jakim *secondary* ma ponowić próbę kontaktu z *masterem*, gdy taka się nie powiedzie. Zalecana wartość pomiędzy 120 a 7200 sekund.
- `**2419200 ;; expire**` - Ta wartość określa czas po jakim dane domeny mają zostać uznane za nieaktualne gdy serwer *secondary* nie będzie mógł się skontaktować z *primary*. Zalecana wartość zawiera się pomiędzy 1209600 a 2419200 sekund, czyli od dwóch do czterech tygodni.
- `**86400 ;; TTL**` - Time To Live. Określa ile czasu informacja o danym rekordzie ma być ważna. Jest to okres przez jaki informacja o naszej domenie będzie przechowywana przez serwer DNS, który ją pobrał. Zalecana wartość zawiera się między 86400 a 432000 sekund, czyli przez okres od jednego do pięciu dni.

Bezpośrednio pod rekordem SOA definiujemy, które serwery DNS będą obsługiwały naszą domenę. Jeszcze raz przypominam aby właściwie zamknąć ten rekord. Bez tego nasza domena nie będzie działać. Do definiowania serwerów DNS służą wpisy typu `**IN NS**`.

```
@               IN      NS      ns1.example.net.
@               IN      NS      ns2.example.net.
```

Powyższy wpis mówi, że domenę *example.net* obsługuje serwer DNS *ns1.example.net* oraz *ns2.example.net*. Jeżeli obie nazwy dotyczą komputerów, które wcześniej nie pełniły roli serwerów DNS, powienieś dodać wpisy takie jak poniżej.

```
ns1             IN      A       123.45.67.8
ns2             IN      A       90.12.34.237
```

ns1 oczywiście może wskazywać na adres serwera DNS który zapewne konfigurujesz; *ns2* powinien wskazywać na Twojego *secondary*. Zrobiliśmy to posługując się wpisami typu `**IN A**`. Jak zapewne pamiętasz, brak końcowej kropki powoduje doklejenie do wpisanej nazwy tego co znajduje się w zmiennej `**$ORIGIN**`. Możemy więc uznać to co widzisz w powyższym przykładzie za postać skróconą poniższego wpisu.

```
ns1.example.net.            IN      A       123.45.67.8
ns2.example.net.            IN      A       90.12.34.237
```

Wpisy typu `**IN A**` służą do określania, że właśnie ten adres IP ma przypisaną taką a nie inną nazwę. Oczywiście do jednego adresu IP możesz stworzyć kilka takich wpisów. Jeżeli posiadasz serwer poczty, powinieneś zrobić wpis mówiący o tym, że będzie on obsługiwał pocztę dla domeny *example.net*.

```
@               IN      MX      10    mail.example.net
```

Dokładnie tak jak wcześniej wspomniałem, poczta, dla domeny *example.net* kierowana jest do serwera *mail.example.net* o priorytecie 10. Jest on tzw. MX'em. Rekord typu `**IN MX**` służy właśnie do definiowania w DNS serwera poczty. Priorytet przydaje się wtedy, kiedy posiadasz kilka serwerów poczty w swojej domenie. Służy on do ustalenia porządku; do którego serwera poczta ma trafić w pierwszej kolejności. Mniejszy priorytet zapewnia pierwszeństwo.

Pozostałe wpisy dotyczą takich standardowych usług jak www czy ftp. Umieszczanie ich w pliku strefy nie jest obowiązkowe. Jednak domenę rejestruje się zazwyczaj na potrzeby www, ftp czy poczty, dlatego zostały one wymienione w przykładzie.

```
ftp             IN      CNAME   www
```

Powyżej umieszczono przykład rekordu typu `IN CNAME`, tworzy on dodatkową subdomenę dla hosta przypisanego już do innej nazwy. Specjaliści radzą by tego rodzaju rekordy wskazywały wyłącznie na rekordy typu `**IN A**`.

Po zakończeniu konfiguracji musimy jeszcze uruchomić usługę.