BIND - konfiguracja serwera DNS

BIND jest jednym z najpopularniejszych serwerów DNS wykorzystywanym w systemach Linux i Unix. Stanowi on niezmiernie ważny składnik zapewniający poprawne działanie systemu nazw w Internecie. Wielu użytkowników globalnej sieci bezwiednie korzysta z serwera BIND, kiedy ich przeglądarka WWW odpytuje go o adres IP komputera udostępniającego interesującą ich stronę.
Nowa wersja BIND 9 została napisana od zera, aby rozwiązać część problemów z architekturą poprzednich wydań tego programu. Dlatego też warto byłoby nauczyć się go konfigurować dla swoich potrzeb. Artykuł ten będzie opisem konfiguracji serwera DNS pod kontrola systemu operacyjnego Linux Debian, jednak w rzeczywistości jedyne różnice jakie mogą wystąpić to inne ścieżki do plików konfiguracyjnych. Głównym plikiem konfiguracyjnym serwera jest

```
/etc/bind/named.conf
```

w nim też będziemy dodawać wszystkie domeny, przykładowo opiszę zaparkowanie domeny ziaja.name, na dole pliku *named.conf* dodajemy

```
zone "ziaja.name" IN {
type master;
file "/var/cache/bind/ziaja.name";
allow-update { none; };
allow-transfer { none; };
notify yes;
};
```

szczególną uwagę należy zwrócić na linie rozpoczynające się od *allow*, w *allow-update*dopisujemy IP serwerów, które będą mogły aktualizować naszą strefę, jeśli nasz serwer jest na domowe potrzeby powinniśmy wpisać *none*, drugi wpis tj. *allow-transfer* mówi o IP, które mogą widzieć wpisy w naszej domenie, jeśli przykładowo nie uwzględnimy przy parkowaniu *allow-transfer*, to każda osoba będzie mieć możliwość podglądu wszystkich wpisów w tej domenie po przez wydanie polecenia

```
dig @IPserweraDNS domena axfr
```

tak więc warto na to zwrócić uwagę, bo jednak często nawet największe serwisy o to nie dbają, m.in. gov.pl pozwala na taki export po przez dwa serwery dns cocos.fuw.edu.pl i dns3.atman.pl

```
dig @193.0.80.11 gov.pl axfr
dig @217.17.34.50 gov.pl axfr
```

również gmach.sejm.gov.pl pozwala na export, tylko w tym wypadku sejm.gov.pl

```
dig @195.187.137.108 sejm.gov.pl axfr
```

narzuca się pytanie, czy wszyscy muszą znać np. adres bramy

```
brama.sejm.gov.pl. 86400 IN A 195.187.136.89
```

czyli jak już wspomniałem wcześniej, nie jest to raczej korzystne i należy o to zadbać. Następnie powinniśmy utworzyć plik konfiguracyjny strefy

```
/var/cache/bind/ziaja.name
```

a w nim

```
$TTL 120 ; Domyślny TTL
$ORIGIN ziaja.name.
@ IN SOA dns.linux.pl. adam.ziaja.name. (
200901269 ; Numer seryjny
3600 ; Częstość odświeżania (refresh)
1800 ; Częstość powtórek (retry)
1209600 ; Czas wygaśnięcia (expire)
86400 ; Negatywne buforowanie TTL
)
@ IN NS dns.linux.pl.
@ IN A 213.135.50.73
```

gdzie fragment *adam.ziaja.name* to adres e-mail admina pisany z kropką zamiast małpy, a*dns.linux.pl* to adres naszego serwera DNS, przy czym należy pamiętać o kropkach na końcu i o każdorazowej zmianie numeru seryjnego np. na datę z godziną przy zmianie jakiegokolwiek elementu strefy oraz o odświeżeniu stref za pomocą komendy

```
rndc reload
```

Na końcu można dopisać dowolną ilość adresów różnego typu, w tym wypadku dopisany jest adres IP 213.135.50.73 IN A dla domeny ziaja.name (należy tutaj zaznaczyć że główny adres w domenie, ten bez subdomen musi wskazywać na IP IN A), kolejnym interesującym nas plikiem konfiguracyjnym będzie

```
/etc/bind/named.conf.options
```

w jego zawartości można wpisać np.

```
options {
directory "/var/cache/bind";
statistics-file "/var/cache/bind/bind.stats";
dump-file "/var/cache/bind/bind.dump";
allow-recursion { 127.0.0.1; };
allow-transfer { none; };
notify yes;
transfer-format many-answers;
listen-on { any; };
listen-on-v6 { any; };
auth-nxdomain yes;
query-source address * port 53;
transfer-source * port 53;
notify-source * port 53;
version "Microsoft DNS Server v1.5 (WinME)";
forwarders { 62.129.252.30; 213.25.47.166; 194.204.159.1; 194.204.152.34; 208.67.222.222; 208.67.220.220;
212.76.33.1; 62.179.1.60; 213.134.134.134; 217.17.34.10; 195.114.173.153; };
};

logging {
channel security_file { file "/var/log/named/security.log" versions 3 size 30m; severity dynamic; print-time yes; };
channel default_file { file "/var/log/named/default.log" versions 3 size 5m; severity dynamic; print-time yes; };
channel general_file { file "/var/log/named/general.log" versions 3 size 5m; severity dynamic; print-time yes; };
channel database_file { file "/var/log/named/database.log" versions 3 size 5m; severity dynamic; print-time yes; };
channel security_file { file "/var/log/named/security.log" versions 3 size 5m; severity dynamic; print-time yes; };
channel config_file { file "/var/log/named/config.log" versions 3 size 5m; severity dynamic; print-time yes; };
channel resolver_file { file "/var/log/named/resolver.log" versions 3 size 5m; severity dynamic; print-time yes; };
channel xfer-in_file { file "/var/log/named/xfer-in.log" versions 3 size 5m; severity dynamic; print-time yes; };
channel xfer-out_file { file "/var/log/named/xfer-out.log" versions 3 size 5m; severity dynamic; print-time yes; };
```

```
channel notify_file { file "/var/log/named/notify.log" versions 3 size 5m; severity dynamic; print-time yes; };
channel client_file { file "/var/log/named/client.log" versions 3 size 5m; severity dynamic; print-time yes; };
channel unmatched_file { file "/var/log/named/unmatched.log" versions 3 size 5m; severity dynamic; print-time yes; };
channel queries_file { file "/var/log/named/queries.log" versions 3 size 5m; severity dynamic; print-time yes; };
channel network_file { file "/var/log/named/network.log" versions 3 size 5m; severity dynamic; print-time yes; };
channel update_file { file "/var/log/named/update.log" versions 3 size 5m; severity dynamic; print-time yes; };
channel dispatch_file { file "/var/log/named/dispatch.log" versions 3 size 5m; severity dynamic; print-time yes; };
channel dnssec_file { file "/var/log/named/dnssec.log" versions 3 size 5m; severity dynamic; print-time yes; };
channel lame-servers_file { file "/var/log/named/lame-servers.log" versions 3 size 5m; severity dynamic; print-time yes;
};

category security { security_file; };
category default { default_file; };
category general { general_file; };
category database { database_file; };
category security { security_file; };
category config { config_file; };
category resolver { resolver_file; };
category xfer-in { xfer-in_file; };
category xfer-out { xfer-out_file; };
category notify { notify_file; };
category client { client_file; };
category unmatched { unmatched_file; };
category queries { queries_file; };
category network { network_file; };
category update { update_file; };
category dispatch { dispatch_file; };
category dnssec { dnssec_file; };
category lame-servers { lame-servers_file; };
};
```

gdzie *version* odpowiada za to jak będzie się przedstawiać nasz serwer DNS, jak zawsze nie jest wskazane korzystanie z oryginalnych bannerów ze względów bezpieczeństwa,*forwarders* są to adresy IP serwerów DNS do których będą przekazywane zmiany w strefach naszego serwera DNS w celu szybszego rozpropagowania dokonanych zmian, elementy w sekcji *logging* służą za logowanie poszczególnych zdarzeń, jedyne co można tutaj zmodyfikować to ścieżkę do logów, jeśli nie chcemy logować danych zdarzeń należy usunąć linię odpowiadająca za te zdarzenie. Jęśli posiadamy firewalla (np. iptables) to trzeba będzie dopisać jeszcze reguły

```
iptables -A INPUT -p tcp --dport 53 -j ACCEPT
iptables -A INPUT -p udp --dport 53 -j ACCEPT
```

To by było na tyle jeśli chodzi o podstawową konfigurację serwera BIND9 :-).