

Konfiguracja serwera DNS (z wykorzystaniem oprogramowania Bind9) w systemie Linux Debian 11.

Michał Pawełek

Spis treści

1	Instalacja Bind9	3
2	Generowanie klucza TSIG	3
2.1	Co to jest TSIG?	3
2.2	Generowanie klucza TSIG.	3
3	Konfiguracja serwera DNS, rekordów RR oraz samych stref	4
3.1	Konfiguracja pliku named.conf	4
3.2	Konfiguracja pliku named.conf.options	5
3.3	Konfiguracja pliku named.conf.local	6
3.4	Konfiguracja rekordów <i>Resource Records</i>	7
3.4.1	Co to są rekordy RR?	8
3.4.2	Rodzaje rekordów RR	8
3.5	Test za użyciem narzędzia dig	10

1 Instalacja Bind9

Instalacja aplikacji Bind9 na serwerze wykonuje się poprzez **apt-get install bind9**. Po zakończeniu procesu instalacji można przystąpić bezpośrednio do konfiguracji (oczywiście po ówczesnym przygotowaniu środowiska do pracy).

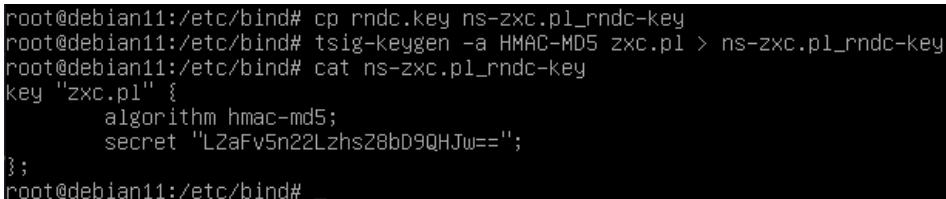
2 Generowanie klucza TSIG

2.1 Co to jest TSIG?

TSIG (transaction signature) to protokół umożliwiający aktualizację bazy danych DNS w bezpieczny sposób. Najczęściej wykorzystuje się go do aktualizacji dynamicznego DNS, bądź serwerów DNS działających w trybie *slave*. TSIG wykorzystuje klucze typu **shared secret** (w skrócie - te komputery, które biorą udział w komunikacji znają klucz shared secret) w celu szyfrowania (w jedną stronę) wymiany informacji. Różnica między aktualizacją serwerów DNS (ich konfiguracjami) jest inna od wysłania zapytania do serwera (tzw. *DNS query*).

2.2 Generowanie klucza TSIG.

Do generowania klucza można skorzystać z polecenia **tsig-keygen** (lub zamiennie **dnssec-keygen**). Wygenerowany klucz najlepiej zapisać w nowym pliku, który będzie dołączany do konfiguracji aplikacji bind9.



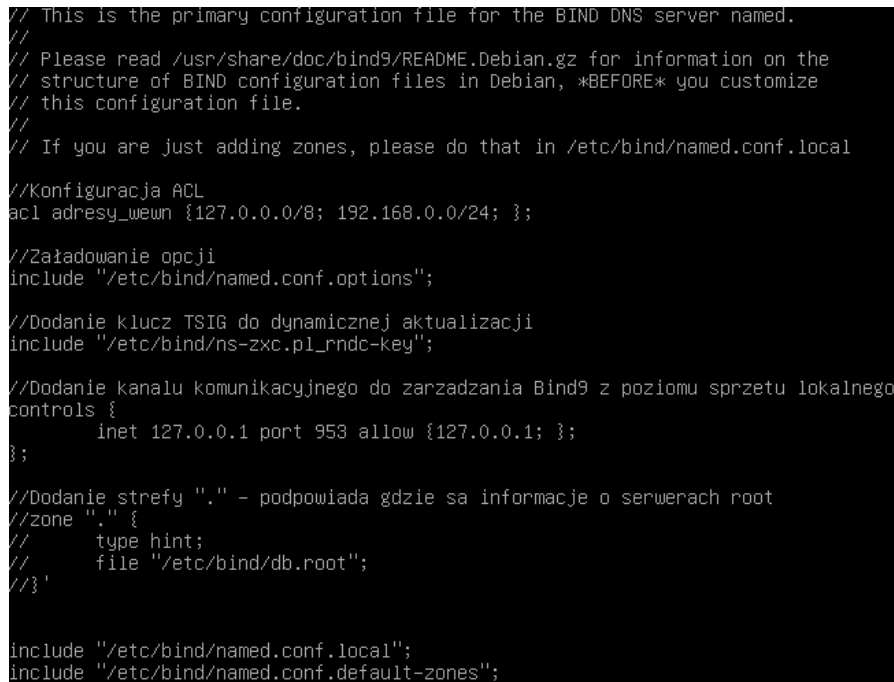
```
root@debian11:/etc/bind# cp rndc.key ns-zxc.pl_rndc-key
root@debian11:/etc/bind# tsig-keygen -a HMAC-MD5 zxc.pl > ns-zxc.pl_rndc-key
root@debian11:/etc/bind# cat ns-zxc.pl_rndc-key
key "zxc.pl" {
    algorithm hmac-md5;
    secret "LZaFv5n22Lzhs28bD9QHJw==";
};
root@debian11:/etc/bind# _
```

Rysunek 1: Generowanie klucza TSIG

3 Konfiguracja serwera DNS, rekordów RR oraz samych stref

3.1 Konfiguracja pliku named.conf

Plik *named.conf* jest głównym plikiem konfiguracyjnym serwera DNS.

A screenshot of a terminal window showing the content of the /etc/bind/named.conf file. The text is as follows:

```
// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind9/README.Debian.gz for information on the
// structure of BIND configuration files in Debian, *BEFORE* you customize
// this configuration file.
//
// If you are just adding zones, please do that in /etc/bind/named.conf.local

//Konfiguracja ACL
acl adresy_wewn {127.0.0.0/8; 192.168.0.0/24; };

//Załadowanie opcji
include "/etc/bind/named.conf.options";

//Dodanie klucz TSIG do dynamicznej aktualizacji
include "/etc/bind/ns-zxc.pl_rndc-key";

//Dodanie kanału komunikacyjnego do zarządzania Bind9 z poziomu sprzętu lokalnego
controls {
    inet 127.0.0.1 port 953 allow {127.0.0.1; };
};

//Dodanie strefy "." - podpowiada gdzie sa informacje o serwerach root
//zone "." {
//    type hint;
//    file "/etc/bind/db.root";
//};

include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";
```

Rysunek 2: Gotowy plik named.conf

W tym pliku należy wykonać poniższe czynności:

- **Konfiguracja ACL poleceniem: `acl nazwa_acl`:**
ACL to lista adresów IP, które będą mogły podłączyć się do serwera DNS i go konfigurować.
- **Dodanie klucza TSIG do dynamicznej aktualizacji:**
Jest to załączenie pliku z kluczem TSIG przy pomocy dyrektywy **include**.
- **Dodanie kanału komunikacyjnego do zarządzania BIND9 z poziomu komputera lokalnego z wykorzystaniem RNDC (`controls { ... }`):**
Zezwolenie na połączenie się z serwerem DNS przy pomocy RNDC z komputera o adresie 127.0.0.1 przy użyciu portu 953.

3.2 Konfiguracja pliku `named.conf.options`

Plik `named.conf.options` zawiera wszystkie opcje konfiguracyjne dla serwera DNS.

```
// you will need to update your keys. See https://www.isc.org/bind-keys
//=====
dnssec-validation auto;

//Konfiguracja portow i adresow z ktorymi serwery DNS beda sie wymieniac informacjami
query-source address * port *;

//Jesli ten serwer nie bedzie znac odpowiedzi na zapytanie
//to odeslij do serwera 192.168.1.1
forward only;
forwarders{192.168.1.1};

auth-nxofomain np;

//Wylaczenie skanowania interfejsow by zapobiec niechcianemu przerwaniu nasluchu
interface=interval 0;

//Nasluchiwanie tylko na lokalnych interfejsach IPv4
listen-on-v6 {none;};
listen-on {127.0.0.1; 192.168.0.1;};

//Zabronienie wymiany stref
allow-transfer {none;};

//Akceptacja zapytania tylko z sieci wewn.
allow-query {adresy_wewn;};

//Zezwolenie na rekurencyjne wysylanie zapytan do hostow wewn.
allow-recursion {adresy_wewn;};

//Nie tworzenie publicznej wersji Binda
version none;_
;
```

Rysunek 3: Skonfigurowany plik `named.conf.options`

Poddane zmianom zostaną następujące aspekty:

- **Konfiguracja portów i adresów, którymi serwery DNS będą się wymieniać informacjami:**
Jak widać na powyższym obrazku poleceniem **query-source address * port *** zezwalamy serwerowi DNS na komunikację z serwerami o dowolnych adresach na dowolnych portach.
- **Konfiguracja serwera, do którego mają być przesyłane nierozwiązane zapytania:**
Opcje **forward only**; oraz **forwarders{...}** są informacją dla serwera, gdzie przesłać nierozwiązane zapytanie.
- **Nasłuchiwanie tylko na lokalnych interfejsach:**
Korzystając z poleceń **listen-on-v6: none**; oraz **listen-on {...}** powoduje, że serwer DNS nie będzie odpowiadał na zapytania pochodzące z adresów IPv6 oraz na zapytania przychodzące na adres inny niż wymieniony w nawiasach klamrowych.

-
- **Zablokowanie wymiany stref:**
Poleceniem **allow-transfer { none };** powoduje, że serwer nie będzie udostępniać informacji o strefach innym serwerom.
 - **allow-query {adresy_wewn;}::**
Polecenie powoduje, że zapytania do serwera DNS będą mogły pochodzić z podsieci 127.0.0.1/8 (localhost) oraz 192.168.0.0/24. Wynika to z konfiguracji pliku z obrazu 2.
 - **allow-recursion:**
Pozwala na wysyłanie przez serwer zapytań do hostów pochodzących z dodanych ACL.

3.3 Konfiguracja pliku named.conf.local

Plik konfiguruje lokalne strefy DNS. W ustawieniach strefy należy dodać informację o typie strefy, o serwerach działających jako *forwarder* oraz o bazach danych DNS i plikach z kluczami, które pozwalają na aktualizację wcześniej wspomnianych baz.

```
//  
// Do any local configuration here  
//  
  
// Consider adding the 1918 zones here, if they are not used in your  
// organization  
//include "/etc/bind/zones.rfc1918";  
  
//Dodawanie pliku do logow  
//include "/etc/bind/named.conf.log";  
  
zone "zxc.pl" {  
    type master;  
    file "var/lib/bind/db.test.pl";  
    //forwarders{};  
    allow-update {key ns-zxc.pl_rndc-key};  
};  
  
zone "0.168.192.in-addr.arpa"{  
    type master;  
    file "var/lib/bind/db.zxc.pl.inv";  
    //forwarders{};  
    allow-update {key ns-zxc.pl_rndc-key};  
};_
```

Rysunek 4: Skonfigurowany plik named.conf.local

Dodać do pliku trzeba dwie zależności:

- **zone "zxc.pl":**

W ten sposób została dodana strefa zxc.pl. Jej typ to *master*, a klucz, który zezwala na aktualizację tej strefy znajduje się w pliku "ns-zxc.pl_rndc-key";. Plik z rekordami RR tej strefy ustawiony paramterem **file** to **"/var/lib/bind/db.zxc.pl"**.

- **zone 0.168.192.in-addr.arpa:**

W ten sposób dodaje się strefę ARPA (czyli odwrotny DNS). Tak jak wcześniej dodana strefa zxc.pl strefa ARPA jest typu *master*, jej plik z rekordami RR to **"/var/lib/bind/db.zxc.pl.inv"**;. Nie posiada ona żadnych serwerów działających jako *forwarderzy*. Klucz umożliwiający aktualizację strefy to plik "ns-zxc.pl_rndc-key";.

3.4 Konfiguracja rekordów *Resource Records*



```
$TTL      3600
; @ = zxc.pl.
@         IN      SOA     dns1.zxc.pl.  admin.zxc.gmail.com. (
                        200700      ; Serial
                        3600        ; Refresh [1h]
                        600         ; Retry [10m]
                        86400       ; Expire [1d]
                        600 )       ; Negative Cache TTL [1h]
;
@         IN      NS      dns1.zxc.pl.
@         IN      MX      10 dns1.zxc.pl.

dns1      In      A       192.168.0.1
etch      IN      A       192.168.0.2
ftp       IN      CNAME   dns1
www       IN      CNAME   dns1
mail      IN      CNAME   dns1_
```

Rysunek 5: Rekordy RR dla strefy zxc.pl

```
@      IN      SOA      dns1.zxc.pl. admin.zxc.gmail.com. (
                                200700
                                3600
                                600
                                86400
                                600 )
;

@      IN      NS       dns1.zxc.pl.
1      IN      PTR      dns1.zxc.pl.
2      IN      PTR      etch.zxc.pl._
```

Rysunek 6: Rekordy RR dla strefy 0.168.192.in-addr.arpa

3.4.1 Co to są rekordy RR?

Rekordy RR oznaczają jaki typ informacji przechowuje dana strefa DNS. Każdy rekord ma swój typ, czas, po którym wygasa oraz informacje specyficzne dla samego siebie.

3.4.2 Rodzaje rekordów RR

- **SOA - Start of authority record:**

Rekord ten przechowuje autorytatywne informacje o strefie DNS, włączając w to główny serwer rozpoznawania nazw, email administratora, numer seryjny strefy oraz kilka liczników czasu, które powiązane są z odświeżaniem informacji o strefie. Liczniki te są informacjami dla serwerów zapasowych, które mają synchronizować się z głównym serwerem.

- **Rekord NS:**

Informacja dla serwera DNS o adresach pozostałych serwerów. Rekordy te mają wskazywać na rekordy typu A, które należy utworzyć w pliku.

- **Rekord A:**

Rekord używany do mapowania nazw na adresy.

- **Rekord CNAME:**

Rekord ten jest rozszerzeniem rekordu A, czyli przekierowuje “nazwe2 na nazwe1”, gdzie nazwa1 jest wcześniej nakierowana np. na adres 192.168.0.1.

- **Rekord MX:**

Rekord *Mail Exchange* powstały na potrzeby usługi poczty elektronicznej. Przy pomocy tego rekordu oznacza się serwery poczty. Tak jak rekord NS, rekord MX musi być nakierowany na nazwę, która jest rozwiązana rekordem typu A.

- **Rekord PTR:**

Rekord mapujący adres IP na nazwę hosta. Używa się go w zapytaniach typu *reverse DNS*

3.5 Test za użyciem narzędzia dig

```
root@debian11:~# dig zxc.pl

;; <<>> DiG 9.16.48-Debian <<>> zxc.pl
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19175
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;zxc.pl.                                IN      A

;; ANSWER SECTION:
zxc.pl.                                3600    IN      A      79.96.226.30

;; Query time: 32 msec
;; SERVER: 1.1.1.1#53(1.1.1.1)
;; WHEN: Wed Feb 14 17:57:16 CET 2024
;; MSG SIZE rcvd: 51
```

Rysunek 7: Wynik komendy Dig dla domenty zxc.pl

```
root@debian11:~# dig dns1.zxc.pl

;; <<>> DiG 9.16.48-Debian <<>> dns1.zxc.pl
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61819
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;dns1.zxc.pl.                        IN      A

;; ANSWER SECTION:
dns1.zxc.pl.                        3301    IN      CNAME   zxc.pl.
zxc.pl.                             3301    IN      A      79.96.226.30

;; Query time: 12 msec
;; SERVER: 1.1.1.1#53(1.1.1.1)
;; WHEN: Wed Feb 14 17:57:50 CET 2024
;; MSG SIZE rcvd: 70
```

Rysunek 8: Wynik komendy Dig dla dns1.zxc.pl

Jak widać domena zwraca odpowiednie wartości rekordów, jeżeli zostanie “wypyтана” przez narzędzie *dig*.