**Serwer DNS - BIND- opis konfiguracji**

Na podstawie : http://www.iti.pk.edu.pl/attachments/category/29/ASK-04-DNS.pdf

**1. Plik konfiguracyjny pakietu BIND**

Plikiem konfiguracyjnym, z którego domyślnie korzysta named jest **/etc/bind/named.conf**. Składnia tego pliku przypomina język C, każda instrukcja i podinstrukcja kończy się średnikiem. Dozwolone są trzy rodzaje komentarzy:

# w stylu powłoki

/\* w stylu C \*/

// w stylu C++

Przykładowy plik **named.conf:**

options {

directory "/var/named";

listen-on port 53 {127.0.0.1;};

transfer-source 127.0.0.1;

allow-transfer {192.168.112.105;};

};

zone "iti.pk" {

type master;

file "iti.pk";

allow-update {127.0.0.1;};

};

zone "112.168.192.in-addr.arpa" {

type slave;

masters {192.168.112.105;};

File "112.168.192";

};

include \"/etc/bind/rndc.key\";

controls{

inet 127.0.0.1 port 953 allow {127.0.0.1;}

keys{rndc-key;};

};

**2. Opis konfiguracji**

* Instrukcja **options** konfiguruje opcje globalne:

|  |  |
| --- | --- |
| directory "/var/named" | definiuje katalog zawierający pliki danych strefowych |
| listen-on port 53 {127.0.0.1;} | określa adres IP oraz port, na którym serwer nazw będzie oczekiwał na zapytania |
| transfer-source 127.0.0.1 | określa adres IP, który będzie używany jako źródłowy podczas transferów stref |
| allow-transfer {192.168.112.105;} | transfery stref są dozwolone tylko z adresu  192.168.112.105 |

* Instrukcja **zone** konfiguruje strefy obsługiwane przez serwer:

|  |  |
| --- | --- |
| "iti.pk" | nazwa domenowa |
| type master | serwer nazw jest serwerem nadrzędnym dla tej strefy |
| file "iti.pk" | nazwa pliku w którym przechowywane są dane o strefie |
| allow-update {127.0.0.1;} | dynamiczna aktualizacja dla tej strefy dozwolona jest tylko z adresu 127.0.0.1 |
| "112.168.192.in-addr.arpa" | nazwa domenowa |
| type slave | serwer nazw jest serwerem podrzędnym dla tej strefy |
| masters {192.168.112.105;} | adresy serwerów z których będą pobierane dane o strefie |
| file "112.168.192" | nazwa pliku, w którym będą przechowywane dane o strefie |

* Linia **include \"/etc/bind/rndc.key\";** załącza plik z kluczami pozwalającymi na dostęp zdalny do serwera nazw.
* Plik rndc.key jest generowany dla naszego serwera DNS poleceniem

# rndc-confgen -a -u bind -t /lab-dns/dns1

|  |  |
| --- | --- |
| -a | tworzenie pliku z kluczem dla serwera DNS w zmienionym katalogu roota |
| -t katalog | Katalog domowy serwera DNS, dla którego generujemy pliki |
| -u użytkownik | użytkownik, dla którego generujemy klucz |

* Instrukcja **controls** konfiguruje dostęp zdalny do naszego serwera:

|  |  |
| --- | --- |
| inet 127.0.0.1 port 953 | adres oraz port, na którym nasłuchiwane będą  połączenia zdalne do serwera nazw |
| allow {127.0.0.1;} | adres, z którego akceptowane będą połączenia zdalne |
| keys{rndc-key;}; | nazwa klucza potrzebnego do autoryzacji połączenia zdalnego |

Pliki danych strefowych

Każdy rekord zapisany w pliku danych strefowych ma następujący format:

nazwa TTL klasa typ dane

|  |  |
| --- | --- |
| nazwa | zawiera nazwę domenową, do której odnosi się wpis. Pole nazwy może być puste wtedy za  nazwę domenową przyjmuje się domyślnie nazwę z poprzedniej  pozycji. Nazwy domenowe zakończone kropką są nazywane  bezwzględnymi i uważane za kompletne. Nazwy domenowe nie  zakończone kropką są nazywane względnymi, rzeczywista nazwa  domenowa jest złożeniem nazwy względnej oraz źródła |
| TTL | Time To Live - czas życia. Czas, przez który serwery mogą buforować dane. Jeśli zostawi  się to pole puste, zostanie przyjęty domyślny TTL (ustawiony  instrukcją $TTL na początku pliku) |
| klasa | IN – klasa Internet  CS – klasa CSNET  CH – klasa CHAOS  HS – klasa Hesiod  pole to określa typ rekordu. Oto niektóre typy:  A – adres  CNAME – nazwa kanoniczna  HINFO – informacje o hoście |
| Typ | MX – wymiennik poczty  NS – serwer nazw  PTR – wskaźnik  SOA – początek autorytatywnych danych  TXT – tekst |
| Dane | zawartość tego pola zależy od typu rekordu |

Przykładowy plik w wersji skróconej:

$TTL 1h

@ SOA dns1 root.dns1 1 1h 1h 1d 1d

NS dns1

NS dns2

dns1 A 127.0.0.1

dns2 A 192.168.112.105

t1 A 192.168.112.101

t2 A 192.168.112.102

t3 A 192.168.112.103

t4 A 192.168.112.104

t5 CNAME dns2

@ MX 10 t1

MX 20 t2

**3. Polecenie dig**

W celu wysłania zapytania do serwera nazw można użyć programu **dig** (Domain Information

Groper – Wyszukiwacz Informacji Domenowych).

Najczęściej polecenia **dig** używa się w następującej formie:

**dig @serwer nazwa typ**

|  |  |
| --- | --- |
| serwer | nazwa lub adres IP serwera nazw, który chcemy zapytać |
| nazwa | nazwa hosta lub adres IP, jeśli użyto opcji -x |
| typ | typ zapytania (SOA,NS,A,MX,CNAME,PTR,AXFR ...), domyślnym typem jest A |