Instytut Teleinformatyki

Wydział Fizyki, Matematyki i Informatyki
Politechnika Krakowska

Administracja Systemami Komputerowymi

„DNS i Postfix”

laboratorium: 06
system operacyjny: Linux

Kraków, 2014

Spis treści

1. Wiadomości wstępne

Pierwsza część niniejszej instrukcji zawiera podstawowe wiadomości teoretyczne dotyczące zestawu oprogramowania DNS i serwera Postfix. Druga część obejmuje zestaw zadań do wykonania i opisania w sprawozdaniu z laboratorium. Na ocenę 3,0 konieczne jest wykonanie ćwiczeń z DNS, na 4,0 dodatkowo należy wykonać zadania z Postfiksa, zaś na 5,0 należy jeszcze wykonać ćwiczenie „Konfiguracja RoundCube”.

1.1. Tematyka laboratorium

Tematyką laboratorium są narzędzia do utworzenia serwera stron internetowych.

Zagadnienia do przygotowania

Przed przystąpieniem do realizacji laboratorium należy zapoznać się z zagadnieniami dotyczącymi:

- Architektura systemu DNS (hierarchia nazw domen, typy domen, popularne domeny TLD, rekordy SOA, A, AAAA, NS, MX, CNAME i ich zastosowanie) [3]
- Do czego służą wirtualne tablice kont [2]
- Na czym polega greylisting [4]
- Podstawowe polecenia POP3 (USER, PASS, QUIT, STAT, LIST, RETR, DELE) [5]
- Podstawowe polecenia SMTP (HELO, MAIL FROM, RCPT TO, DATA) [6]

Literatura:

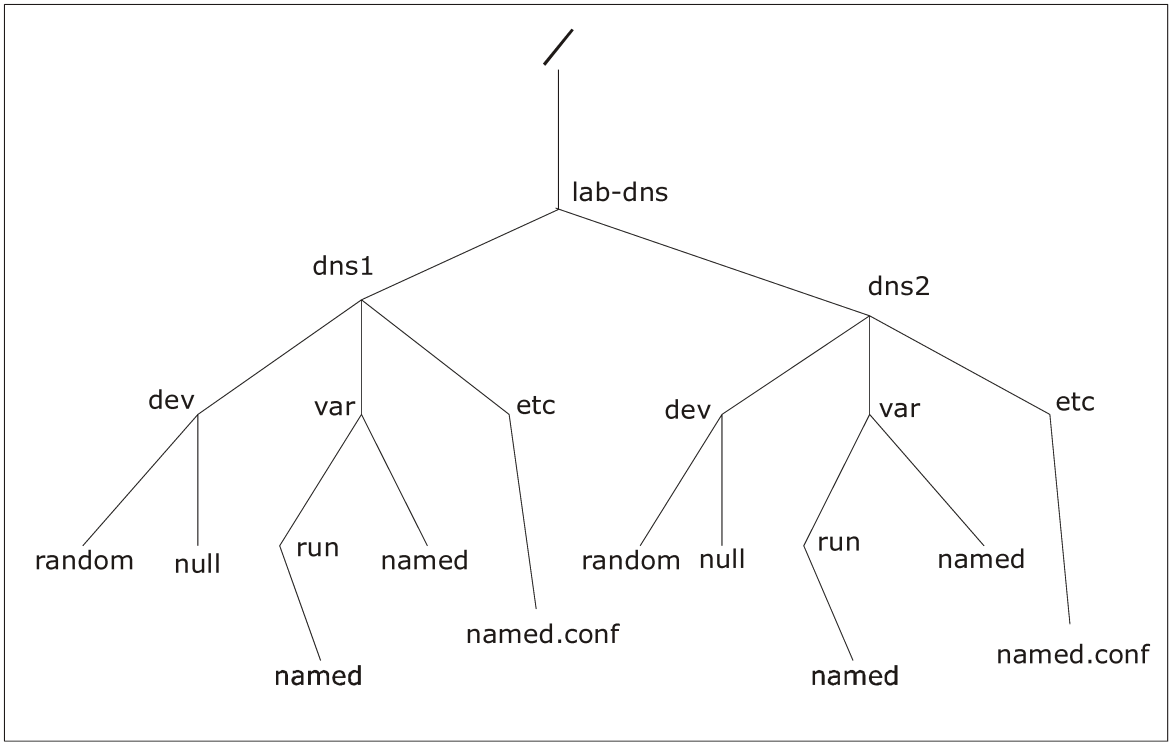
[1] Strony man dla …
[2] Dokumentacja Postfix 2.9 http://www.postfix.org/documentation.html
[3] “DNS i BIND” autorzy: Paul Albitz i Cricket Liu, wyd. O'Reilly
[4] http://www.greylisting.org/
[5] http://tools.ietf.org/html/rfc1081
[6] http://tools.ietf.org/html/rfc1123

2. Przebieg laboratorium

Druga część instrukcji zawiera zadania do praktycznej realizacji, które demonstrują zastosowanie technik z omawianego zagadnienia. Polecenia proszę wykonywać z terminala użytkownika root, chyba, że będzie zaznaczone inaczej.

2.1. Zadanie 1. DNS: Przygotowanie ćwiczenia

Do wykonania ćwiczenia niezbędne są następujące pliki i katalogi:



Aby utworzyć niezbędną strukturę plików i katalogów wystarczy uruchomić skrypt umieszczony na moodle:

```
# ./lab-dns start
```


Plik named.conf dla serwera DNS1 (/lab-dns/dns1/etc/bind/named.conf) powinien zawierać:

```
options {
      directory "/var/named";
      listen-on port 53 {127.0.0.1;};
      transfer-source 127.0.0.1;
};

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

controls{
      inet 127.0.0.1 port 953 allow {127.0.0.1;}
      keys{rndc-key;};
};
```

- 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 zapytania,
- transfer-souirce 127.0.0.1: określa adres IP który będzie używany jako źródłowy podczas transferów stref.

Podobnie plik named.conf dla serwera DNS2 (/lab-dns/dns2/etc/bind/named.conf) powinien zawierać:

```
options {
      directory "/var/named";
      listen-on port 53 {192.168.112.numer_komputera;};
      transfer-source 192.168.112.numer_komputera;
};

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

controls{
      inet 192.168.112.numer_komputera port 953 allow {127.0.0.1;}
      keys{rndc-key;};
};
```

Po wykonaniu się skryptu należy zmienić w pilikach konfiguracyjnych napisy numer_komputera tak aby adres zgadzał się z adresem IP maszyny, na której pracujemy oraz należy zwracać uwagę w kolejnych zadaniach aby podczas korygowania plików konfiguracyjnych wpisywać poprawny adres swojego komputera.

Kiedy mamy już gotowe drzewo katalogów i plików zatrzymujemy działanie demona programu named oraz generujemy pliki z kluczami rndc.

```
# /etc/init.d/bind9 stop
# rndc-confgen -a -u bind -t /lab-dns/dns1
# rndc-confgen -a -u bind -t /lab-dns/dns2
```

2.2. Zadanie 2. DNS: Rejestrowanie zdarzeń

BIND jest wyposażony w system rejestracji zdarzeń. Konfiguruje się go przy użyciu instrukcji logging. W plikach konfiguracyjnych serwerów nazw (/lab-dns/dns1/etc/bind/named.conf oraz /lab-dns/dns2/etc/bind/named.conf) należy dopisać:

```
logging {
      channel log {
      file “file.log”;
      severity info;
      print-time yes;
      print-category yes;
      };
      category default { log; };
      category queries { log; };
      category update {log; };
};
```

Instrukcja channel definiuje kanał:

- file „file.log”: w pliku file.log będą zapisywane komunikaty,
- severity info: określa ważność zapisywanych komunikatów,
- print-time yes: daty będą zapisywane w komunikacie,
- print-category yes: kategorie będą zapisywane w komunikacie,
- category default { log; }: określa kanał dla kategorii default,
- category queries { log; }: określa kanał dla kategorii queries (zapytania),
- category update { log; }: określa kanał dla kategorii update (dynamiczne aktualizacje).

2.3. Zadanie 3. DNS: Serwer nazw z pamięcią podręczną

Serwer nazw z pamięcią podręczną szuka odpowiedzi na zapytania o nazwy i pamięta odpowiedź. Przy kolejnych zapytaniach o tę samą nazwę czas odpowiedzi jest znacznie krótszy.

Serwer nazw musi wiedzieć, gdzie znajdują się serwery nazw strefy głównej. Odpowiada za to wpis w named.conf:

```
zone "." {
            type hint;
            file "root";
};
```

Plik root zawiera wskazania do głównych serwerów nazw.

Ponieważ BIND9 ma wbudowaną strefę hints, nie musisz umieszczać instrukcji zone dla tej strefy w pliku named.conf.

Aby sprawdzić działanie serwera nazw z pamięcią podręczną uruchom serwery nazw DNS1 i DNS2:

```
# /usr/sbin/named -u bind -t /lab-dns/dns1
# /usr/sbin/named -u bind -t /lab-dns/dns2
```

Upewnij się, że serwery działają:

```
# ps aux | grep named
```


powinno zwrócić trzy wyniki. Teraz korzystając z polecenia dig zapytaj serwer nazw o dowolny adres np.:

```
# dig @127.0.0.1 www.onet.pl
```

Zrób to jeszcze raz i porównaj czasy odpowiedzi(Query time).

Następnie obejrzyj komunikaty w pliku /lab-dns/dns1/var/named/file.log. Powinny tam znajdować się komunikaty podobne do tych:

```
13-Nov-2010 10:20:16.277 general: running
13-Nov-2010 10:22:55.223 queries: client 127.0.0.1#40188:  query:
www.onet.pl IN A + (127.0.0.1)
13-Nov-2010 10:24:00.188 queries: client 127.0.0.1#44199:  query:
www.onet.pl IN A + (127.0.0.1)
```

Każda linia w pliku zawiera jeden komunikat. Na początku znajduje się data oraz kategoria a następnie treść komunikatu. Pierwszy komunikat oznacza uruchomienie serwera nazw. Kolejne dwa to komunikaty dotyczące zapytań. 127.0.0.1#32780 to adres IP i port z którego nastąpiło zapytanie, natomiast www.onet.pl IN A oznacza, że pytano o adres IP hosta www.onet.pl.

Aby móc kontrolować na bieżąco zapisy dokonywane w plikach logowania możemy w osobnych terminalach wprowadzić następujące polecenie:

```
# tail -f /lab-dns/dns1/var/named/file.log
```

oraz analogiczny wpis dla drugiego serwera DNS.

2.4. Zadanie 4. DNS: Konfiguracja serwera nadrzędnego dla strefy iti.pk

Załóżmy, że serwery nazw mają obsługiwać fikcyjną strefę iti.pk. Serwer DNS1 to serwer nadrzędny dla tej strefy, a serwer DNS2 podrzędny. Do pliku named.conf dla serwera DNS1 (/lab-dns/dns1/etc/bind/named.conf) dodaj wpis odpowiedzialny za strefę iti.pk:

```
zone "iti.pk" {
            type master;
            file "iti.pk";
};
```

- „iti.pk”: nazwa strefy
- type master: serwer nazw jest serwerem nadrzędnym dla tej strefy
- file „iti.pk”: nazwa pliku w którym przechowywane są dane o strefie

Następnie utwórz plik danych strefowych iti.pk:

```
# touch /lab-dns/dns1/var/named/iti.pk
```

i otwórz go używając dowolnego edytora.

Pierwszy wpis w pliku danych strefowych dotyczy domyślnego TTL dla strefy. TTL jest to “czas życia”, czyli okres, przez który inne serwery mogą buforować dane. Gdy ten czas upłynie, serwer musi usunąć buforowane dane i pobrać nowe z autorytatywnego źródła. Domyślny TTL ustawia się za pomocą instrukcji $TTL. Aby ustawić domyślny TTL na 1 godzinę wystarczy na początku pliku dodać instrukcje:

$TTL 1h

Drugim wpisem jest rekord SOA (Start Of Authority – początek autorytatywnych danych), który wskazuje na zwierzchność nad strefą. Rekord SOA dla strefy iti.pk wygląda tak:

```
iti.pk.  IN  SOA  dns1.iti.pk. root.dns1.iti.pk. (
              1     ; numer seryjny
              1h    ; okres odświeżania
              1h    ; okres ponownej próby
              1d    ; czas wygasania
              1d )  ; czas buforowania negatywnego
```

- „iti.pk”: nazwa strefy,
- IN: klasa danych; jest to skrót od Interneru,
- SOA: type rekordu (Start Of Authority – początek autorytatywnych danych),
- dns1.iti.pk.: nazwa podstawowego nadrzędnego serwera nazw dla strefy iti.pk,
- root.dns1.iti.pk.: adres e-mail osoby odpowiedzialnej za strefę („@” zostało zastąpione kropką).

Dane w nawiasie związane są z serwerem podrzędnym:

- numer seryjny: numer ten należy zwiększać po każdej modyfikacji pliku strefy, ponieważ serwer podrzędny próbując pobrać dane strefowe najpierw sprawdza numer seryjny i pobiera nową kopie strefy tylko wtedy, gdy numer strefy w serwerze podrzędnym jest mniejszy niż w nadrzędnym,
- okres odświeżania: określa jak często serwer podrzędny powinien sprawdzać, czy dane strefowe są aktualne (1h – oznacza jedną godzinę, 3d4h30m – oznacza 3 dni, 4 godziny i 30 minut),
- okres ponownej próby: jest to czas, po którym serwer spróbuje się ponownie połączyć z serwerem nadrzędnym, gdy nie udało się z nim skontaktować po upływie okresu odświeżania,
- czas wygasania: po jego upływie serwer podrzędny uznaje strefę za wygasłą i przestaje udzielać odpowiedzi na zapytania, które jej dotyczą,
- czas buforowania negatywnego: przez ten czas serwery mogą buforować odpowiedzi negatywne.

Następne wpisy to rekordy NS, dotyczące serwerów nazw. Każdy autorytatywny dla strefy iti.pk serwer nazw będzie miał jeden taki rekord:

```
iti.pk.          1h      IN NS   dns1.iti.pk.
iti.pk.          1h      IN NS   dns2.iti.pk.
```

- iti.pk.: nazwa strefy,
- 1h: TTL,
- IN: klasa danych,
- NS: typ rekordu (Name Server – serwer nazw),
- dns1.iti.pk.: hazwa hosta na którym działa serwer nazw.

Kolejne rekordy będą dotyczyły odwzorowania nazw na adresy. Rekordem realizującym odwzorowanie nazwy na adres jest rekord A. W strefie iti.pk są następujące hosty:


```
dns1.iti.pk.    1h     IN A    127.0.0.1
dns2.iti.pk.    1h     IN A    192.168.112. numer_komputera
t1.iti.pk.      1h     IN A    192.168.112.101
t2.iti.pk.      1h     IN A    192.168.112.102
t3.iti.pk.      1h     IN A    192.168.112.103
t4.iti.pk.      1h     IN A    192.168.112.104
```

Do tworzenia aliasów służy rekord CNAME (Canonical Name), który odwzorowuje alias na nazwę kanoniczną :

```
t5.iti.pk.      1h      IN CNAME dns2.iti.pk.
```

Do realizacji trasowania poczty DNS używa rekordu zasobu MX (Mail Exchanger – wymiennik poczty). Rekord ten określa wymiennik poczty dla danej domeny. Oprócz nazwy domenowej rekord MX ma dodatkowy parametr, nazywany wartością preferencji, który określa priorytet wymiennika poczty. Program pocztowy próbuje skontaktować się z wymiennikiem poczty o najmniejszej wartości preferencji. Dla strefy iti.pk mamy dwa wymienniki poczty:

```
iti.pk.      IN  MX  10  t1.iti.pk.
iti.pk.      IN  MX  20  t2.iti.pk.
```

Po utworzeniu pliku z danymi strefy konieczne jest przeładowanie serwerów nazw. Wydaj polecenia:

```
# kill -HUP `cat /lab-dns/dns1/var/run/named/named.pid`
# kill -HUP `cat /lab-dns/dns2/var/run/named/named.pid`
```

lub skorzystaj ze skryptu:

```
# /root/lab-dns/lab-dns reload
```

Korzystając z polecenia dig sprawdź poprawność powyższej konfiguracji:

```
# dig @127.0.0.1 t1.iti.pk
# dig @127.0.0.1 t5.iti.pk
# dig @127.0.0.1 iti.pk ns
# dig @127.0.0.1 iti.pk mx
```

W pliku /lab-dns/dns1/var/named/file.log powinny pojawić się nowe wpisy:

```
13-Nov-2010 10:26:11.230 general: zone iti.pk/IN: loaded   serial 1
13-Nov-2010 10:26:11.231 notify: zone iti.pk/IN: sending   notifies
(serial 1)
13-Nov-2010 10:26:13.981 queries: client 127.0.0.1#48252:  query:
t1.iti.pk IN A + (127.0.0.1)
13-Nov-2010 10:26:19.412 queries: client 127.0.0.1#42122:  query:
t5.iti.pk IN A + (127.0.0.1)
13-Nov-2010 10:26:28.826 queries: client 127.0.0.1#43564:  query:
iti.pk IN NS + (127.0.0.1)
13-Nov-2010 10:26:32.542 queries: client 127.0.0.1#33642:  query:
iti.pk IN MX + (127.0.0.1)
```

Pierwszy wpis informuje, że została załadowana strefa iti.pk i jej numer seryjny to jeden. Drugi to informacja, że zostały wysłane powiadomienia o zmianie danych w strefie iti.pk. Kolejne to zapytania, które wysłałeś do serwera nazw przy użyciu programu dig.

2.5. Zadanie 5. DNS: Konfiguracja serwera nadrzędnego dla strefy 112.168.192.in-addr.arpa

Serwerem nadrzędnym dla strefy 112.168.192.in-addr.arpa będzie serwer DNS2. Do pliku named.conf dla serwera DNS2 (/lab-dns/dns2/etc/bind/named.conf)dodaj wpis odpowiedzialny za strefę 112.168.192.in-addr.arpa:

```
zone "112.168.192.in-addr.arpa" {
            type master;
            file "112.168.192";
};
```

- "112.168.192.in-addr.arpa": nazwa strefy,
- type master: serwer nazw jest serwerem nadrzędnym dla tej strefy,
- file „112.168.192”: nazwa pliku w którym przechowywane są dane o strefie.

Następnie utwórz plik danych strefowych 112.168.192:

```
# touch /lab-dns/dns2/var/named/112.168.192
```

i używając dowolnego edytora zapisz w nim:

```
$TTL 1h
112.168.192.in-addr.arpa. IN SOA  dns2.iti.pk. root.dns2.iti.pk. (
                                                                1
                                                                1h
                                                                1h
                                                                1d
                                                                1d )
112.168.192.in-addr.arpa.       1h      IN NS   dns1.iti.pk.
112.168.192.in-addr.arpa.       1h      IN NS   dns2.iti.pk.
numer_komputera.112.168.192.in-addr.arpa.         1h           IN  PTR
dns2.iti.pk.
101.112.168.192.in-addr.arpa.     1h      IN PTR  t1.iti.pk.
102.112.168.192.in-addr.arpa.     1h      IN PTR  t2.iti.pk.
103.112.168.192.in-addr.arpa.     1h      IN PTR  t3.iti.pk.
104.112.168.192.in-addr.arpa.     1h      IN PTR  t4.iti.pk.
```

Rekordy PTR (Pointer – wskaźnik) odwzorowują adresy na nazwy.

Po przeładowaniu serwerów nazw sprawdź poprawność powyższej konfiguracji:

```
# dig @192.168.112.numer_komputera -x 192.168.112.101
```

Obejrzyj plik /lab-dns/dns2/var/named/file.log. Jego zawartość powinna być podobna do pliku pokazanego w poprzednich punktach.

2.6. Zadanie 6. DNS: Konfiguracja serwera podrzędnego

Serwer DNS2 będzie serwerem podrzędnym dla stref iti.pk a serwer DNS1 dla strefy 112.168.192.in-addr.arpa. Do pliku konfiguracyjnego (named.conf) serwera DNS2 dodaj:

```
zone "iti.pk" {
            type slave;
```



```
                masters {127.0.0.1;};
                file "iti.pk";
        };
```

- „iti.pk”: nazwa strefy,
- type slave: serwer nazw jest serwerem podrzędnym dla tej strefy,
- masters {127.0.0.1;}: adres IP serwera nadrzędnego dla tej strefy,
- file „iti.pk”: nazwa pliku w którym będą przechowywane dane o strefie.

Natomiast do pliku konfiguracyjnego serwera DNS1 dodaj:

```
        zone "112.168.192.in-addr.arpa" {
                type slave;
                masters {192.168.112.numer_komputera;};
                file "112.168.192";
        };
```

- "112.168.192.in-addr.arpa": nazwa strefy,
- type slave: serwer nazw jest serwerem podrzędnym dla tej strefy,
- masters {192.168.112.numer_komputera;}: adres IP serwera nadrzędnego dla tej strefy,
- file "112.168.192";: nazwa pliku w którym będą przechowywane dane o strefie.

Po przeładowaniu serwerów sprawdź działanie serwera podrzędnego:

```
# dig @192.168.112.numer_komputera t5.iti.pk
# dig @127.0.0.1 -x 192.168.112.101
```

W pliku /lab-dns/dns1/var/named/file.log powinny pojawić się wpisy:

```
        13-Nov-2010 11:28:30.170 xfer-in: transfer of  '112.168.192.in-
addr.arpa/IN' from 192.168.112.5#53:     connected using 127.0.0.1#58359
        13-Nov-2010     11:28:30.171     general:     zone     112.168.192.in-
        addr.arpa/IN: transferred serial 1
        13-Nov-2010 11:28:30.171 xfer-in: transfer of  '112.168.192.in-
addr.arpa/IN' from 192.168.112.5#53:     Transfer completed: 1 messages, 9
records, 255 bytes,     0.001 secs (255000 bytes/sec)
        13-Nov-2010 11:28:30.212 xfer-out: client      192.168.112.5#39754:
transfer of 'iti.pk/IN': AXFR      started
        13-Nov-2010 11:28:30.212 xfer-out: client      192.168.112.5#39754:
transfer of 'iti.pk/IN': AXFR      ended
```

Pierwszy oznacza pobranie przez serwer nazw strefy 112.168.192.in-addr.arpa, natomiast drugi informuje, że z serwera nazw została pobrana strefa iti.pk.
Plik /lab-dns/dns2/var/named/file.log zawiera analogiczne wpisy.

2.7. Zadanie 7. DNS: Transfer stref

Wykonaj polecenia:

```
# dig @127.0.0.1 iti.pk axfr
# dig @192.168.112.numer_komputera 112.168.192.in-addr.arpa axfr
```

W wyniku ich działania powinieneś otrzymać całą strefę iti.pk i 112.168.192.in-addr.arpa. Takie działanie serwera nazw nie jest zbyt bezpieczne, ponieważ każdy może dokonać

transferu strefy. Podinstrukcja allow-transfer pozwala zapobiegać nieautoryzowanym transferom stref. Aby transferu stref mógł dokonać tylko serwer podrzędny do plików konfiguracyjnych serwerów nazw dodaj w instrukcji options następujące linie:

- dla serwera DNS1
  ```
  allow-transfer {192.168.112.numer_komputera;};
  ```
- dla serwera DNS2
  ```
  allow-transfer {127.0.0.1;};
  ```

  Przeładuj serwery nazw. Teraz używając polecenia:

```
# dig @127.0.0.1 iti.pk axfr
```

nie otrzymasz transferu strefy, ponieważ transfer strefy iti.pk może być dokonany tylko z adresu 192.168.112.numer_komputera.

W pliku /lab-dns/dns1/var/named/file.log wyraźnie widać działanie podinstrukcji allow-transfer:

```
13-Nov-2010 10:40:56.559 queries: client 127.0.0.1#59144: query:
iti.pk IN AXFR -T (127.0.0.1)
13-Nov-2010 10:40:56.560 xfer-out: client 127.0.0.1#59144:
transfer of 'iti.pk/IN': AXFR started
13-Nov-2010 10:40:56.560 xfer-out: client 127.0.0.1#59144:
transfer of 'iti.pk/IN': AXFR ended
```

Przed dodaniem wpisu można było dokonać transferu strefy z adresu 127.0.0.1 natomiast po dodaniu allow-transfer {192.168.112.numer_komputera;}; transfer nie jest już możliwy z adresu 127.0.0.1:

```
13-Nov-2010 10:48:04.829 queries: client 127.0.0.1#57100: query:
iti.pk IN AXFR -T (127.0.0.1)
13-Nov-2010 10:48:04.829 security: client 127.0.0.1#57100: zone
transfer 'iti.pk/AXFR/IN' denied
```

2.8. Zadanie 8. DNS: Dynamiczna aktualizacja

Wszystkie zmiany, jakich dokonywałeś w tym ćwiczeniu wymagały przeładowania serwera nazw. Dynamiczne aktualizacje pozwalają na aktualizacje danych strefowych podczas pracy serwera nazw. Aby zezwolić na dynamiczne aktualizacje z localhost'a dodaj w plikach konfiguracyjnych serwerów DNS1 i DNS2 następujące linie:

- w instrukcji zone “iti.pk”pliku konfiguracyjnego serwera DNS1:
  ```
  allow-update {127.0.0.1;};
  ```
- a w instrukcji zone “112.168.192.in-addr-arpa” pliku konfiguracyjnego serwera DNS2:
  ```
  allow-update {192.168.112.numer_komputera;};
  ```

  Następnie, po przeładowaniu serwerów nazw, uruchom program nsupdate:

```
# nsupdate
> server 127.0.0.1
> prereq nxdomain t6.iti.pk.
> update add t6.iti.pk. 3600 A 192.168.112.6
> show
```



```
> send
> server 192.168.112.numer_komputera
> prereq nxdomain 6.112.168.192.in-addr.arpa.
> update add 6.112.168.192.in-addr.arpa. 3600 PTR t6.iti.pk.
> show
> send
> quit
```

Teraz poleceniem dig sprawdź czy dane strefowe zostały zaktualizowane:

```
# dig @127.0.0.1 t6.iti.pk.
# dig @192.168.112.numer_komputera -x 192.168.112.6
```

Zobacz także, jakie zmiany zostały wprowadzone w plikach iti.pk i 112.168.192.in-addr.arpa (jeśli obok tych plików pojawią się pliki *.jnl, wykonaj program sync).

W pliku /lab-dns/dns1/var/named/file.log powinny znaleźć się podobne wpisy:

```
13-Nov-2010 11:34:53.600 update: client 127.0.0.1#36606: updating zone 'iti.pk/IN': adding an RR at 't6.iti.pk' A
13-Nov-2010 11:34:53.604 notify: zone iti.pk/IN: sending notifies (serial 2)
```

Pierwszy wpis informuje, że został dodany rekord zasobów do strefy iti.pk. Drugi natomiast – wysłanie powiadomień o zmianie danych strefy iti.pk. Plik /lab-dns/dns2/var/named/file.log zawiera analogiczne wpisy.

2.9. Zadanie 9. DNS: Zakończenie ćwiczenia

Po zakończeniu ćwiczenia należy uruchomić:

```
# /root/lab-dns/lab-dns stop
```

w celu przywrócenia stanu wyjściowego systemu.

2.10. Zadanie 10. Postfix: Przygotowanie

Proszę upewnić się, że ma się otwarty terminal roota. Następnie proszę utowrzyć katalog /home/student/postfix:

```
# cd /home/student
# mkdir postfix
```

2.11. Zadanie 11. Postfix: Konfiguracja serwera Postfix

Zadanie to polega na skonfigurowaniu serwera pocztowego. Zacznijmy od stworzenia kopii zapasowych plików konfiguracyjnych postfiksa i skopiujmy je do wyżej utworzonego katalogu. Plik, który będziemy modyfikować ma ścieżkę dostępu /etc/postfix/main.cf. Przed edycją tego pliku należy wykonać polecenie hostname:

```
# hostname
```

Otwórzmy wymieniony wcześniej plik w edytorze i wklejmy do niego następującą konfigurację:


```
command_directory = /usr/sbin
mail_owner = postfix
mydomain = debian   //wpisujemy co zwróci hostname
myhostname = debian  //wpisujemy co zwróci hostname
myorigin = /etc/mailname
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
mydestination = $mydomain, $myhostname, localhost,
localhost.localdomain,
mynetworks = 127.0.0.0/8
inet_interfaces = all
inet_protocols = ipv4
home_mailbox = Maildir/
mail_spool_directory = /home/
smtpd_banner = ESMTP on $myhostname !
mailbox_size_limit = 0
recipient_delimiter = +
biff = no
append_dot_mydomain = no
relayhost =
```

Po wpisaniu tej konfiguracji wykonujemy polecenie, które sprawdzi nam poprawność konfiguracji.

```
# postfix check
```

Przy poprawnym pliku powyższe wywołanie nie wypisze niczego na terminal. Następnie tworzymy bazę aliasów poleceniem:

```
# newaliases
```

I restartujemy demona

```
# /etc/init.d/postfix restart
```

Sprawdzamy teraz czy nasza konfiguracja poprawnie zadziała:

```
# telnet 127.0.0.1 25
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.
220 ESMTP on myhostname !
EHLO myhostname   //to co wpisywaliśmy w main.cf
250-nazwa_komputera
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
quit
221 2.0.0 Bye
Connection closed by foreign host.
```


Pogrubione są polecenia które wpisujemy. Jeśli wynik jest taki jak powyżej wtedy wszystko działa poprawnie.

2.12. Zadanie 12. Postfix: Konfiguracja serwera POP3 oraz IMAP wraz z SSL

Wykorzystamy w tym ćwiczeniu zestaw pakietów dovecot. POP3s oraz IMAPs są to protokoły do odbierania poczty z szyfrowaniem transmisji przez SSL. Jeśli w pliku dovecot.conf przy opcji protocols mamy wpisane imap imaps pop3 pop3s. Oznacza to, że na naszym komputerze działają proste serwery IMAP i POP3 jak i serwery szyfrowane.

Ustawiamy prawa do katalogów:

```
# chmod 755 /var/run/dovecot
# chgrp dovecot /var/run/dovecot/login/
```

Kolejnym krokiem jest stworzenie katalogu, w którym będziemy przechowywać nasz certyfikat:

```
# mkdir –p /etc/postfix/ssl
```

Przechodzimy do tego katalogu i z jego poziomu tworzymy certyfikat:

```
# openssl req -new -x509 -nodes -out mail.pem -keyout mail.pem -days 365
      Country Name (2 letter code) [AU]:PL
      State or Province Name (full name) [Some-State]:POLAND
      Locality Name (eg, city) []:Krakow
      Organization Name (eg, company) [Internet Widgits Pty Ltd]:Moj
certyfikat
      Organizational Unit Name (eg, section) []:POCZTA
      Common Name (eg, YOUR name) []:myhostname
      Email Address []:root@myhostname
```

W celu konfiguracji tworzymy kopię zapasową pliku, który znajduje się w lokalizacji /etc/dovecot/dovecot.conf, do naszego katalogu postfix. Edytujemy go i wklejamy poniższą konfigurację:

```
      base_dir = /var/run/dovecot/
      protocols = imap pop3
      listen = *
      disable_plaintext_auth = no
      shutdown_clients = yes

      #logi
      log_path=/var/log/dovecot.log
      info_log_path = /var/log/mail.log
      log_timestamp = "%Y-%m-%d %H:%M:%S "
      syslog_facility = mail
      login_greeting = Welcome. I’m ready ...
      login_log_format_elements = user=<%u> method=%m rip=%r lip=%l %c
      login_log_format = %$: %s
      mail_location = maildir:~/Maildir
```



```
verbose_ssl = yes
ssl_cert = </etc/postfix/ssl/mail.pem
ssl_key = </etc/postfix/ssl/mail.pem

mail_access_groups = postfix
protocol imap {
}
protocol pop3 {
            pop3_uidl_format = %08Xu%08Xv
}
protocol lda {
            postmaster_address = postmaster@debian
}
auth_verbose = yes
auth_debug = yes
auth_mechanisms = plain login
passdb {
            driver = pam
}
userdb {
            driver = passwd
}
service auth {
            user = dovecot
}

dict {
}
plugin {
}
```

Dodatkowo musimy włączyć SSL w pliku /etc/dovecot/conf.d/10-ssl.conf ustawiając wartość ssl na yes oraz podając ścieżki do plików z certyfikatami:

```
ssl_cert = </etc/postfix/ssl/mail.pem
ssl_key = </etc/postfix/ssl/mail.pem
```

Teraz uruchamiamy demona dovecot:

```
# /etc/init.d/dovecot start
```

oraz sprawdzamy poprawność powyższej konfiguracji. W tym celu musimy stworzyć dwóch użytkowników w systemie ustawiając im hasła "haslo".

```
# useradd –m nadawca
# passwd nadawca
# useradd –m odbiorca
# passwd odbiorca
```

Dalsze czynności wykonamy z użyciem programu telnet:

```
# telnet 127.0.0.1 25
      Trying 127.0.0.1...
```



```
Connected to localhost.
Escape character is '^]'.
220 ESMTP on myhostname !
EHLO myhostname
250-debian
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
mail from: nadawca@myhostname
250 2.1.0 Ok
rcpt to: odbiorca@myhostaname
250 2.1.5 Ok
data
354 End data with <CR><LF>.<CR><LF>
Subject: mail testowy

to jest testowy mail
zaraz zobaczymy czy dojdzie:)
.
250 2.0.0 Ok: queued as A912CBACD
quit
221 2.0.0 Bye
Connection closed by foreign host.
```

Pogrubione są polecenia, które wprowadzamy.

Teraz sprawdzamy czy wyżej wysłany mail doszedł. W tym celu wykonujemy polecenie.

```
# ls -l /home/odbiorca
```

Powinniśmy zobaczyć folder Maildir. Teraz sprawdzamy szyfrowany serwer POP3

```
# openssl s_client –connect localhost:995
      //tu pojawi się informacja o certyfikacie, który wcześniej //został utworzony
      +OK Welcome. I’m ready …
      user odbiorca
      +OK
      pass haslo
      +OK Logged in.
      stat
      +OK 1 485
      list
      +OK 1 messages:
      1 485
      .
```



```
retr 1
+OK 485 octets
Return-Path: <nadawca@debian>
X-Original-To: odbiorca@ debian
Delivered-To: odbiorca@ debian
Received: from pk.edu.pl (localhost [127.0.0.1])
            by debian (Postfix) with ESMTP id A912CBACD
            for <odbiorca@debian >; Sat,  3 Nov 2007 15:54:52 +0100
(CET)
Subject: mail testowy
Message-Id: <20071103145513.A912CBACD@debian>
Date: Sat,  3 Nov 2007 15:54:52 +0100 (CET)
From: nadawca@pk.edu.pl
To: undisclosed-recipients:;

to jest testowy mail
zaraz zobaczymy czy dojdzie:)
.
quit
+OK Logging out.
Connection closed by foreign host.
```

Uzyskanie podobnego efektu oznacza, że wszystko poszło pomyślnie.

2.13. Zadanie 13. Postfix: Konfiguracja wirtualnych tablic kont

Dzięki tablicom wirtualnych kont możemy pozwolić konkretnym użytkownikom w systemie na dobieranie maili na adresy, które sami zdefiniujemy. Żeby poprawnie skonfigurować wirtualne domeny wykonujemy następujące polecenia.

Pierwszym krokiem jest stworzenie w systemie kont na potrzeby tego ćwiczenia. Nadajemy im jednakowe hasło np. haslo. Przykładowo:

```
# useradd -m virtual1
# useradd -m virtual2
```

Tworzymy lub edytujemy plik /etc/postfix/virtual i wpisujemy do niego następującą konfigurację:

```
example                 domain //ten tekst jest ignorowany
postmaster@example      postmaster
address1@example        virtual1
address2@example        virtual2
@example                odbiorca
```

Teraz musimy wskazać postfixowi gdzie ma szukać tych wirtualnych kont. W tym celu dodajemy do pliku main.cf konfigurację:

```
virtual_alias_maps = hash:/etc/postfix/virtual
```

Pozostaje nam tylko restart demona postfix oraz aktualizujemy wpisy w pliku virtual.

```
# postfix reload
```



```
# postmap /etc/postfix/virtual
```

Żeby sprawdzić czy to działa wystarczy spróbować wysłać mail na adres address1@example i zobaczyć czy został on dostarczony do użytkownika virtual1. Wykonujemy to tak jak w ćwiczeniu poprzednim, poleceniem telnet localhost 25. Po wysłaniu maila sprawdzamy, czy użytkownik virtual1 ma w swoim katalogu domowym folder Maildir:

```
# ls -l /home/virtual1
```

Jeśli tak, to oznacza, że nasz e-mail doszedł.

2.14. Zadanie 14. Postfix: Konfiguracja autoryzacji START TLS

Zajmijmy się teraz konfiguracją uwierzytelniania użytkowników za pomocą START TLS. Edytujemy plik main.cf i wpisujemy następującą konfigurację:

```
#TLS
smtpd_tls_auth_only = yes
smtp_use_tls = yes
smtpd_use_tls = yes
smtp_tls_note_starttls_offer = yes
smtpd_tls_key_file = /etc/postfix/ssl/mail.pem
smtpd_tls_cert_file = /etc/postfix/ssl/mail.pem
smtpd_tls_CAfile = /etc/postfix/ssl/mail.pem
smtpd_tls_loglevel = 1
smtpd_tls_received_header = yes
smtpd_tls_session_cache_timeout = 3600s
smtpd_tls_session_cache_database = btree:$
{queue_directory}/smtpd_scache
smtp_tls_session_cache_database = btree:$
{queue_directory}/smtp_scache
tls_random_source = dev:/dev/urandom
```

Następnie restartujemy postfixa i sprawdzamy czy działa:

```
# /etc/init.d/postfix restart
# telnet localhost 25
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 ESMTP on myhostname !
EHLO myhostname
250-debian
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
```



```
250-8BITMIME
250 DSN
quit
221 2.0.0 Bye
Connection closed by foreign host.
```

Jeśli widzimy linijkę 250-STARTTLS to znaczy, że konfiguracja jest poprawna.

2.15. Zadanie 15. Postfix: Konfiguracja narzędzi do zarządzania pocztą

Zadanie to polega na konfiguracji narzędzia RoundCube na podstawie http://trac.roundcube.net/wiki/Howto_Install .

2.16. Zadanie 16. Postfix: Zakończenie ćwiczenia

Usuń utworzonych użytkowników: nadawcę, odbiorcę i dwóch do tablic kont wirtualnych:

```
# deluser nadawca
# deluser odbiorca
# deluser virtual1
# deluser virtual2
```

Następnie usuń utworzone wcześniej katalogi:

```
# rm -rf /etc/postfix/ssl
# rm -rf /etc/postfix/virtual
```


3. Opracowanie i sprawozdanie

Realizacja laboratorium pt. „DNS i Postfix” polega na wykonaniu wszystkich zadań programistycznych podanych w drugiej części tej instrukcji. Wynikiem wykonania powinno być sprawozdanie w formie wydruku papierowego. Sprawozdanie powinno zawierać:

- opis wykonanych czynności,
- uwagi oceniające ćwiczenie: trudne/łatwe, nie/wymagające wcześniejszej znajomości zagadnień (wymienić jakich),
- wskazówki dotyczące ewentualnej poprawy instrukcji celem lepszego zrozumienia sensu oraz treści zadań.

