T: Instalacja i konfiguracja serwera DNS.

Cel ogólny lekcji to nauczenie się instalacji i konfiguracji serwera DNS oraz konfiguracji strefy przeszukiwania do przodu i wstecz oraz zrozumienie sposobu tworzenia rekordów jak korzystać z DNS oraz jak testować działanie uruchomionego serwera DNS oraz innych serwerów DNS.

Cele szczegółowe:

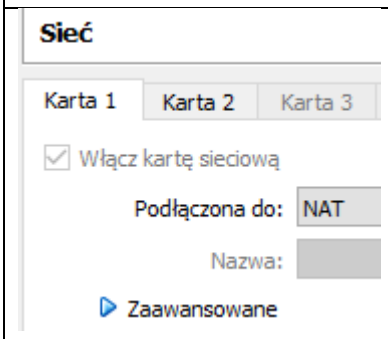
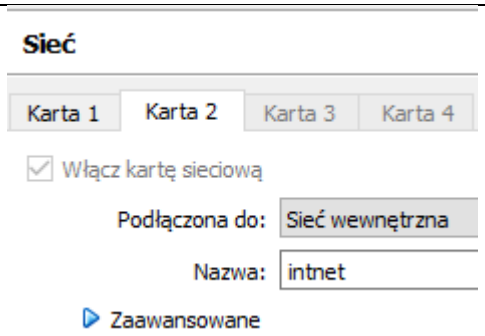
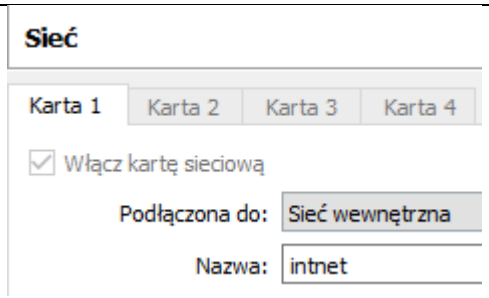
1. Wyjaśnienie pojęć związanych z DNS.
2. Instalacja serwera DNS BIND w wersji 9.
3. Konfiguracja serwera DNS wraz z ustawieniem stałego adresu IP oraz nazwy hosta.
4. Testowanie uruchomionego serwera DNS.
5. Testowanie innych serwerów DNS.
6. Zapisanie w zeszycie wszystkich poleceń konfiguracyjnych z wyjaśnieniem ich działania.
7. Skopiowanie przykładowego pliku konfiguracyjnego i nadanie mu odpowiedniej nazwy
8. Zmiana nazw localhost i root.localhost na nazwę domenową naszego serwera
9. Zmiana numeru seryjnego pliku o 1 po każdej zmianie
10. Dodanie interesujących nas rekordów, takich jak A, NS, CNAME, MX, AAAA, TXT, i zrozumienie ich składni
11. Utworzenie kopii pliku /etc/bind/db.127 i zmiana jego nazwy
12. Dodanie rekordów PTR używanych przy RevDNS, tyle ile zdefiniowanych jest subdomen w strefie przeszukiwania do przodu
13. Sprawdzenie i zaakceptowanie konfiguracji serwera DNS oraz poprawność konfiguracji strefy przeszukiwania do przodu dla naszej domeny.

Podczas wykonywania poniższych zadań w zeszycie w sprawozdaniu

1. podaj i wyjaśnij polecenia, które użyjesz, aby:
   - wyjaśnić pojęcia związane z dns,
   - zainstalować serwer dns,
   - uruchomić lub zatrzymać usługi sieciowe,
   - konfigurować serwer dns,
   - korzystać z dns.
2. podaj odpowiedzi na pytania zadane w treści zadań.

Przywróć migawkę „Migawka 1” zawierającą przygotowane do ćwiczeń maszyny Ubuntu serwer i desktop (klient). Przed przystąpieniem do ćwiczenia sprawdź czy ustawienie maszyny wirtualnej

pozwala na dostęp do Internetu, jeżeli ustawienia są niezgodne wykonaj konfigurację pierwszej i drugiej karty sieciowej według instrukcji, a następnie uruchom Ubuntu serwer i klienty zgodnie z wymaganiami w instrukcji.

Ubuntu serwer Adapter 1	Ubuntu serwer Adapter 2
	
	Ubuntu desktop Adapter 1
	

Po uruchomieniu Ubuntu serwer

podaj **login**: root **Password**: 1234 lub **login**: ubuntu **Password**: ubuntu

Jeśli zalogowałeś się do ubuntu wpisz sudo -s **Password**: ubuntu

Przygotowanie do ćwiczenia. Ustawienie statycznego adresu IP.

1. Za pomocą polecenia ifconfig -a ustal dostępne interfejsy sieciowe.

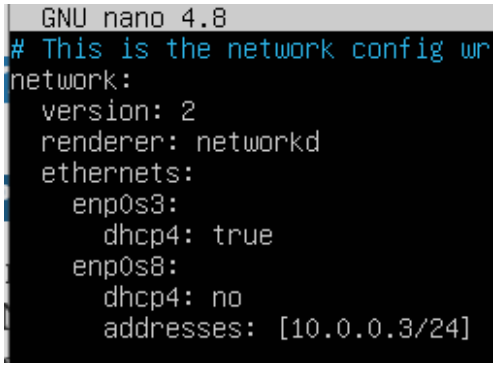
```
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe68:a08  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:68:0a:08  txqueuelen 1000  (Ethernet)
        RX packets 2712  bytes 2450820 (2.4 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1142  bytes 77401 (77.4 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
```

Plik nano /etc/netplan/00-installer-config.yaml - opisuje interfejsy sieciowe dostępne w systemie i jak je aktywować.

2. Zmień adres IP dla Ubuntu na enp0s8 (Adapter 2) na statyczny.

Otwórz plik, który opisuje interfejsy sieciowe nano /etc/netplan/0 tabulator – nazwa pliku zostanie uzupełniona do postaci *.yaml

Pozostaw zalecane wpisy w tym pliku jak poniżej pamiętaj o dokładności wpisów



3. Zastosuj ustawienia

root@ubuntusrv:~# netplan apply

4. Zmień nazwę hosta na stałe

root@ubuntusrv:~# hostnamectl set-hostname dlp

root@ubuntusrv:~# init 6

Opisz w zeszycie:

- procedurę instalacji i konfiguracji oraz uruchomienia serwera DNS,
- testowania uruchomionego serwera DNS,
- testowania innych serwerów DNS.

Wszystkie polecenia konfiguracyjne zapisz w zeszycie z wyjaśnieniem ich działania.

Ćwiczenie Instalacja i konfiguracja serwera DNS – bind

DNS to skrót od Domain Name System i jest to hierarchiczny, rozproszony system nazw sieciowych, odpowiadający na zapytania o nazwy domen. Stwierdzenie "jest to usługa zamieniająca domenę na nazwę IP" jest dość powierzchownym stwierdzeniem i nadaje się na lekcje Informatyki w szkole podstawowej. DNS nie tylko tłumaczy domeny na adresy IP, ale może np. tłumaczyć adresy IP na domeny (tzw. RevDNS), a nawet domeny na domeny (CNAME). Hierarchiczny oznacza, że opiera się na jakiejś hierarchii, w tym przypadku będziemy mieć 13 głównym serwerów zwanych root-servers, do których są podłączone mniejsze serwery w różnych krajach. Do tych serwerów mogą być podłączone inne serwery np. operatorów domen, operatorów internetowych itd. Z kolei do tych serwerów często podłączone są serwery mniejsze - firmowe, domowe. Rozproszony oznacza, że nie skupia się w jednym miejscu. Serwery DNS rozproszone są po krajach, kontynentach, miastach itd.

Znając to, możemy przejść do instalacji naszego serwera DNS. Użyjemy do tego implementacji o nazwie BIND w wersji 9. Jest to serwer stworzony przez Internet Systems Consortium. BIND to skrót od Berkley Internet Name Domain. Wpierw jednak warto zaktualizować repozytoria i pakiety na serwerze.

Zainstaluj BIND, aby skonfigurować serwer DNS, który rozpoznaje nazwę domeny lub adres IP.
DNS używa 53 / TCP, UDP.

1. Instalacja BIND 9 i czynności po instalacyjne.

A. Wykonaj aktualizację apt-get update - aktualizowanie listy pakietów i repozytoriów

B. Instalacja pakietów serwera DNS

root@dlp:~# apt install -y bind9 bind9utils bind9-doc

bind9 pakiet bind9; bind9utils pakiet diagnozujący; bind9-doc pakiet z dokumentacją

Jeśli pojawi się `Run 'apt list --upgradable' to see them.` można instalować powyższe pakiety.

Jeśli nie jest możliwe należy zapytać prowadzącego czy można wykonać apt-get upgrade - aktualizacja systemu.

C. Czynności po instalacyjne

Nie zamykaj konsoli z poleceniami

Po zakończeniu procesu instalacji sprawdź:

a) czy BIND9 działa.

root@dlp:~# nslookup google.com 127.0.0.1

Odpowiedź będzie mniej więcej taka:

```
root@dlp:~# nslookup google.com 127.0.0.1
Server:         127.0.0.1
Address:        127.0.0.1#53
```

b) Skonfiguruj plik /etc/hosts

root@dlp:~# nano /etc/hosts

```
127.0.0.1 localhost
127.0.1.1 openonevm
10.0.0.3 srv.local dlp
```

Adres IP serwera: 10.0.0.3

c) Skonfiguruj plik /etc/hostname

root@dlp:~# nano /etc/hostname

dlp

d) Otwórz także plik /etc/cloud/cloud.cfg i ustaw preserve_hostname: true

e) Dodaj adres IP serwera nazw jako adres IP swojego serwera do pliku /etc/resolv.conf

```
nameserver 10.0.0.3
options edns0
search srv.local
```
domena: srv.local

f) Uruchom ponownie serwer za pomocą polecenia. init 6

g) Za pomocą narzędzia DIG sprawdź, czy serwer DNS działa prawidłowo

```
root@dlp:~# dig -x 127.0.0.1

; <<>> DiG 9.16.1-Ubuntu <<>> -x 127.0.0.1
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 20518
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 47f9cf01f97ad81c01000000063793236ce30363ca0d5960a (good)
;; QUESTION SECTION:
;1.0.0.127.in-addr.arpa.                IN      PTR

;; ANSWER SECTION:
1.0.0.127.in-addr.arpa. 604800  IN      PTR     localhost.

;; Query time: 0 msec
;; SERVER: 10.0.0.30#53(10.0.0.30)
;; WHEN: Sat Nov 19 19:44:54 UTC 2022
;; MSG SIZE  rcvd: 102
```

Serwer DNS odpowie prawidłowo, jeśli zwróci nazwę hosta pętli zwrotnej: localhost

h) Po zakończeniu instalacji i przygotowań wstępnych wyświetl zawartość katalogu /etc/bind.

```
root@dlp:~# ls -l /etc/bind/
total 48
-rw-r--r-- 1 root root 1991 Apr 15  2020 bind.keys
-rw-r--r-- 1 root root  237 Apr 15  2020 db.0
-rw-r--r-- 1 root root  271 Apr 15  2020 db.127
-rw-r--r-- 1 root root  237 Apr 15  2020 db.255
-rw-r--r-- 1 root root  353 Apr 15  2020 db.empty
-rw-r--r-- 1 root root  270 Apr 15  2020 db.local
-rw-r--r-- 1 root bind  463 Apr 15  2020 named.conf
-rw-r--r-- 1 root bind  498 Apr 15  2020 named.conf.default-zones
-rw-r--r-- 1 root bind  165 Apr 15  2020 named.conf.local
-rw-r--r-- 1 root bind  846 Apr 15  2020 named.conf.options
-rw-r----- 1 bind bind  100 Nov 19 17:57 rndc.key
-rw-r--r-- 1 root root 1317 Apr 15  2020 zones.rfc1918
```

Zapisz w zeszycie

- db.127 - przykładowa konfiguracja strefy przeszukiwania wstecznego

- db.local - przykładowa konfiguracja strefy przeszukiwania do przodu
- named.conf - globalna konfiguracja DNS
- named.conf.default-zones - domyślne strefy przeszukiwania
- named.conf.local - lokalna konfiguracja DNS
- named.conf.options - konfiguracja serwera DNS

i) Wykonaj kopię named.conf.

```
root@dlp:~# cp /etc/bind/named.conf /etc/bind/named.confbackup
```

Przygotuj: zeszyt z notatką i niezamkniętą konsolę z wydanymi poleceniami

Zgłoszenie 1

UWAGA! ACHTUNG! ATTENTION!

Serwer BIND9 posiada dość wybredną składnię plików konfiguracyjnych. Należy uważać, aby WSZYSTKO było wpisane poprawnie. W przeciwnym wypadku serwer NIE ZADZIAŁA. Proszę się pilnować, aby NIE POMIJAĆ znaków ani NIE PRZEPISYWAĆ WSZYSTKIEGO NA ŚLEPO.

2. Skonfiguruj BIND 9.

Najważniejsze informacje:
- Adres IP serwera: 10.0.0.3
- Docelowa domena: srv.local
- Nazwa domenowa serwera: dlp.srv.local
- Nazwa domenowa klienta: klient1.srv.local

Oczywiście każdy może sobie wybrać inną domenę. Ważne jest, aby nie była to domena publiczna jak .com .pl .edu itd. Najlepiej korzystać z domeny .local przeznaczonej dla sieci lokalnej. Jednak nikt nie zabroni nam korzystać np. z domeny .zsl.

a. Edytuj pliku /etc/bind/named.conf.options stosując polecenie:

$ nano /etc/bind/named.conf.options

Musisz sobie odnaleźć w nim zakomentowaną opcję nazwaną forwarders. Odkomentujemy całą opcję, a następnie w miejsce 0.0.0.0 wpisujemy adres IP jakiegoś serwera DNS. Ja w swojej sieci domowej posiadam własny serwer DNS, więc tego też używam. Wy możecie, a nawet musicie, wpisać inny serwer. Zapisujemy plik i opuszczamy edytor.

```
// uncomment the following
// the all-0's placeholder.

forwarders {
        10.0.0.3;
};

//============================
```

Zgłoszenie 2

b. Skonfiguruj plik /etc/bind/named.conf.local. Dodamy sobie do niego dwie strefy przeszukiwania – naprzód i wstecz.

Zanim jednak to zrobimy, warto wyjaśnić znaczenie poszczególnych pól, które będą uzupełniane.

Zone (pol. Strefa) jest to wydzielony obszar w systemie nazw domenowych (Domain Name System) gdzie obowiązek administrowania został oddelegowany do pojedynczego menadżera. Aby to zrozumieć należy przypomnieć sobie czym jest DNS – jest to "hierarchiczny, rozproszony system nazw sieciowych, odpowiadający na zapytania o nazwy domen". System ten rozproszony jest na całym świecie i składa się z wielu domen. Strefa to jest obszar, który zajmuje się jedną domeną i wszystkimi subdomenami i innymi sprawami związanymi z daną domeną. Menadżerem jest główny serwer DNS danej domeny. Oczywiście jeden serwer może być menadżerem wielu domen, czyli wielu stref.

Strefa przeszukiwania naprzód jest strefą, która zawiera rekordy mapujące nazwy domenowe na adresy IP lub inne informacje. Zaś strefa przeszukiwania wstecz jest strefą, która zawiera rekordy mapujące adresy IP lub inne informacje na nazwy domenowe. Jest to element związany z usługą Reverse DNS, która właśnie mapuje adresy IP na domeny.

```
zone "srv.local" IN { //nazwa domeny
        type master; //serwer jest gwnym dns-em strefy
        file "/etc/bind/for.srv.local.db"; //zawiera info o strefie przeszukiwania do przodu
        allow-update {none;}; //pobiera info z innych stref jako strefa glowna
        allow-transfer {10.0.0.3;}; //pozwala innym serwerom dns pobierac info o strefie
        also-notify {10.0.0.3;}; //informuje doddatkowe serwery o zmianach w strefie

};

zone "0.0.10.in-addr.arpa" IN { //nazwa strefy przeszukiwania wstecznego
        type master;
        file "/etc/bind/rev.srv.local.db"; //zawiera onfo o strefie wyszukiwania wstecznego
        allow-update {none;}; //pobiera info z innych stref jako strefa glowna
        allow-transfer {10.0.0.3;}; //pozwala innym serwerom dns pobierac info o strefie
        also-notify {10.0.0.3;}; //informuje doddatkowe serwery o zmianach w strefie
};
```

c. Edytujemy poleceniem:

$ nano /etc/bind/named.conf.local

Utworzenie strefy rozpoczniemy od napisania słowa "zone"””, następnie w cudzysłowie podajemy adres naszej domeny "mydomain.local", a następnie "IN", czyli "w". Otwieramy nawiasy klamrowe "{}", w których podamy potrzebne parametry na podstawie, których BIND9 będzie obsługiwał domenę. Pierwszy z nich, czyli type master; informuje serwer, że będzie on głównym serwerem DNS dla strefy. Innym typem jest slave. Wtedy serwer pobiera dane o strefie (czyli domeny, subdomeny itd.) z serwera master. File "(…)" wskazuje nam na plik przechowywujący informacje o strefie. Później mamy allow-update {none;}; allow-transfer {adresip;}; oraz also-notify {adresip;};. Co te parametry oznaczają zostało wyjaśnione na screenie. Następnie dodamy do pliku drugą strefę jednak tym razem strefę przeszukiwania wstecznego. Zapis będzie taki sam jak wcześniej z tą różnicą, że wskazujemy inny plik, a domena ma następujący zapis:

X.in-addr.arpa Tam gdzie jest X podajemy odwrócony adres IP serwera DNS bez części hosta. Czyli dla adresu IP 192.168.10.10/24 piszemy 10.168.192.in-addr.arpa. Dla IP 10.0.0.1/8 piszemy 10.in-addr.arpa. Dla adresów publicznych np. 8.8.4.4 piszemy 4.4.8.8.in.addr.arpa. Kiedy nasz plik wygląda jak powyżej, to możemy go zapisać

Zgłoszenie 3

i przejść dalej.

d. Konfiguracja strefy przeszukiwania do przodu. Skopiuj przykładowy plik konfiguracyjny (/etc/bind/db.local) i nadaj mu taką nazwę jaką podaliśmy w poprzednim pliku przy opcji file. Komenda:

$ cp /etc/bind/db.local /etc/bind/for.srv.local.db

```
root@dlp:~# cp /etc/bind/db.local /etc/bind/for.srv.local.db
```

e. Edytuj plik /etc/bind/for.srv.local.db poleceniem:

$ nano /etc/bind/for.srv.local.db

Widzimy oryginalną zawartość tego pliku, którą za chwilę zmienimy. Pierwsze co musimy zrobić to zmienić localhost. oraz root.localhost. na nazwę domenową jaką wybrałeś dla naszego serwera dlp.srv.local.

PROSZĘ PAMIĘTAĆ O KROPCE NA KOŃCU KAŻDEJ NAZWY DOMENOWEJ.

Później zmieniamy numer seryjny (Serial) pliku o 1. DOKONUJEMY TEGO ZAWSZE PO KAŻDORAZOWEJ ZMIANIE TEGO PLIKU. Jest to istotne, gdyż wtedy informujemy serwer DNS, że strefa uległa zmianie. Na samym końcu dodajemy już interesujące nas rekordy. Ich składnia wygląda następująco:

nazwa_domenowa IN typ_rekordu wartość

serwer IN A 10.0.0.3

Znak @ oznacza tutaj sam serwer.

```
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     dlp.srv.local. root.dlp.srv.local. (
                              3         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      localhost.
@       IN      A       127.0.0.1
@       IN      AAAA    ::1
;info o serwerach DNS
@       IN      NS      dlp.srv.local.
;adres ip serwera DNS
dlp     IN      A       10.0.0.3
;rekord A - domena na IP
klient1 IN      A       10.0.0.35
```

Zapisz w zeszycie:

Rekordy to są poszczególne wpisy w strefie, które mapują odpowiednie informacje. Typów rekordów jest wiele jednak takimi najpopularniejszymi są:

- A - mapuje nazwę domenową na adres IP

- NS - informuje o serwerach DNS

- CNAME - mapuje nazwę domenową na nazwę domenową

- MX - informuje o serwerze poczty

- AAAA - mapuje nazwę domenową na adres IPv6

- TXT - przechowuje czysty tekst. Używany przez chociażby przez Google do autoryzacji właściciela

Zgłoszenie 4

f. Strefa przeszukiwania wstecznego. Utwórz kopię pliku /etc/bind/db.127 Nadaj mu taką nazwę jaką podana wcześniej przy opcji file. Komenda będzie wyglądać następująco:

$ cp /etc/bind/db.127 /etc/bind/rev.srv.local.db

```
dlp:~# cp /etc/bind/db.127 /etc/bind/rev.srv.local.db
```

g. Kiedy to już zrobiliśmy to możemy przejść do edycji tego pliku znanym już poleceniem:

$ nano /etc/bind/rev.srv.local.db

Widzimy oryginalną zawartość tego pliku i postępujemy tak samo jak w poprzednim przypadku (zmiana localhost i numeru seryjnego). Aż do momentu dodawania rekordów. Najpierw tak jak poprzednio dodajemy dwa rekordy - NS i A informujące o serwerze DNS. Na samym końcu dodajemy interesujące nas rekordy, a ich składnia wygląda następująco:

część_hosta_ip IN PTR adres_domenowy

np. 10 IN PTR dlp.srv.local.

PAMIĘTAJMY O KROPCE NA KOŃCU.

```
$TTL    604800
@       IN      SOA     dlp.srv.local. root.dlp.srv.local. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      localhost.
1.0.0   IN      PTR     localhost.
;info o serwerach DNS
@       IN      NS      dlp.srv.local.
dlp     IN      A       10.0.0.3
;przeszukiwanie wsteczne dla serwera DNS
10      IN      PTR     dlp.srv.local.
;rekordy PTR - adres ip na domene
11      IN      PTR     klient1.srv.local.
```

Dodajemy tyle rekordów PTR, używanych przy RevDNS ile mamy zdefiniowanych subdomen w strefie przeszukiwania do przodu. Mam dwa - serwer oraz klienta, więc dodaję dwa rekordy.

Jeżeli nasz plik wygląda jak powyżej to zapisujemy w nim zmiany

Zgłoszenie 5

i zamykamy go.

h. Sprawdź i zaakceptuj konfigurację serwera DNS i poprawność konfiguracji stref:

$ named-checkconf

Powyższa komenda sprawdzi nam konfigurację serwera DNS.

$ named-checkzone srv.local for.local.db

Ta komenda sprawdzi nam poprawność konfiguracji strefy przeszukiwania do przodu dla naszej domeny.

$ named-checkzone 0.0.0.10.in-addr.arpa rev.local.db

Ostatnia komenda sprawdzi nam poprawność konfiguracji strefy przeszukiwania wstecznego dla naszej domeny.

Jeżeli komendy te zachowają się tak samo jak na screenie to gratuluję! Wszystko zostało skonfigurowane poprawnie. Jeżeli coś pójdzie nie tak to komendy te poinformują nas, gdzie jest błąd i co nim jest.

```
root@dlp:/etc/bind# named-checkconf
root@dlp:/etc/bind# named-checkzone srv.local for.srv.local.db
zone srv.local/IN: loaded serial 3
OK
root@dlp:/etc/bind# named-checkzone 0.0.0.10.in-addr.arpa rev.srv.local.db
zone 0.0.0.10.in-addr.arpa/IN: loaded serial 2
OK
```

Wnioski:

- Jeśli wszystkie trzy komendy zwracają brak błędów, to oznacza, że konfiguracja serwera DNS oraz konfiguracja stref przeszukiwania do przodu i wstecznego są poprawne.
- W przypadku wystąpienia błędów, komendy te powinny dostarczyć informacji o konkretnej lokalizacji błędu, co ułatwia identyfikację i naprawę problemów z konfiguracją DNS.
- Po wykryciu i naprawieniu ewentualnych błędów można ponownie uruchomić te komendy, aby potwierdzić, że konfiguracja serwera DNS jest teraz poprawna.

Zgłoszenie 6

3. Konfiguracja serwera do świadczenia usług.

a. przygotowanie serwera do świadczenia usług DNS-owych. W tym celu musimy dodać w Netplanie do karty LAN adres IP serwera DNS, czyli samego siebie. Wpisujemy zatem polecenie:

$ nano /etc/netplan/00-installer-config.yaml

I dodajemy serwer DNS i jego adres IP 10.0.0.3

```
network:
  version: 2
  renderer: networkd
  ethernets:
    enp0s3:
      dhcp4: true
    enp0s8:
      dhcp4: no
      addresses: [10.0.0.3/24]
      nameservers:
        addresses: [10.0.0.3]
```

Sprawdzamy poprawność konfiguracji poleceniami:

$ netplan try

$ netplan apply

```
root@dlp:/etc/bind# netplan apply
root@dlp:/etc/bind# _
```

Jeśli uzyskamy powyższy efekt, to znaczy, że wszystko jest ok.

b. Przetestuj działanie serwera DNS korzystając z dwóch poleceń. Pierwsze wchodzi w skład pakietu bind9utils, czyli dig wyświetla nam więcej informacji o danej domenie. Istotna dla nas jest sekcja ANSWER SECTION. Tutaj wyświetlana jest informacja o rekordzie. Prostszym poleceniem jest nslookup. Wyświetla ono tylko podstawowe informacje. Wpisujemy:

$ dig dlp.srv.local

$ nslookup dlp.srv.local

```
root@dlp:~# dig dlp.srv.local

; <<>> DiG 9.16.1-Ubuntu <<>> dlp.srv.local
;; global options: +cmd
;; Got answer:
;; WARNING: .local is reserved for Multicast DNS
;; You are currently testing what happens when an mDNS query is leaked to DNS
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38234
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: ac5dc6316aeb7c4e01000000637a3d35a0a1a573af7cd07b (good)
;; QUESTION SECTION:
;dlp.srv.local.                 IN      A

;; ANSWER SECTION:
dlp.srv.local.          604800  IN      A       10.0.0.3

;; Query time: 0 msec
;; SERVER: 10.0.0.3#53(10.0.0.3)
;; WHEN: Sun Nov 20 14:44:05 UTC 2022
;; MSG SIZE  rcvd: 86

root@dlp:~# nslookup dlp.srv.local
Server:         10.0.0.3
Address:        10.0.0.3#53

Name:   dlp.srv.local
Address: 10.0.0.3
```

Wnioski:

- Polecenie **dig** jest bardziej wszechstronne i pozwala na uzyskanie obszernych informacji o domenie, co jest przydatne w bardziej zaawansowanych przypadkach diagnozowania problemów z DNS.
- Polecenie **nslookup** jest bardziej uproszczone i nadaje się do szybkiego sprawdzenia podstawowych informacji o domenie.
- Wybór między tymi dwoma narzędziami zależy od konkretnego przypadku i poziomu szczegółowości potrzebnej do diagnozowania problemów z DNS.

Zgłoszenie 7

4. Konfiguracja klienta.

Przygotowanie do ćwiczenia.

Włącz klienta - Ubuntu desktop

Po uruchomieniu Ubuntu desktop podaj **login**: ubuntu **Password**: ubuntu

Jeśli zalogowałeś się do ubuntu wpisz sudo -s **Password**: ubuntu

Ustaw statyczny adresu IP 10.0.0.35/24 brama 10.0.0.3

```
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gr
oup default qlen 1000
    link/ether 08:00:27:9a:ee:8e brd ff:ff:ff:ff:ff:ff
    inet 10.0.0.35/24 brd 10.0.0.255 scope global noprefixroute enp0s3
```

a. zpinguj naszego klienta. Najpierw na samą subdomenę (klient1) wpisujemy:

$ ping klient1

Sprawdzić, czy zadziała na pełną nazwę domenową:

$ ping klient1.srv.local

```
root@dlp:~# ping klient1
PING klient1.srv.local (10.0.0.35) 56(84) bytes of data.
64 bytes from 10.0.0.35 (10.0.0.35): icmp_seq=1 ttl=64 time=0.469 ms
64 bytes from 10.0.0.35 (10.0.0.35): icmp_seq=2 ttl=64 time=0.958 ms
64 bytes from 10.0.0.35 (10.0.0.35): icmp_seq=3 ttl=64 time=0.931 ms
^C
--- klient1.srv.local ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 0.469/0.786/0.958/0.224 ms
root@dlp:~# ping klient1.srv.local
PING klient1.srv.local (10.0.0.35) 56(84) bytes of data.
64 bytes from 10.0.0.35 (10.0.0.35): icmp_seq=1 ttl=64 time=0.280 ms
64 bytes from 10.0.0.35 (10.0.0.35): icmp_seq=2 ttl=64 time=0.284 ms
^C
--- klient1.srv.local ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.280/0.282/0.284/0.002 ms
```

b. Przetestuj działanie serwera DNS korzystając z dwóch poleceń. Pierwszym poleceniem jest nslookup. Wyświetla ono tylko podstawowe informacje. Drugie wchodzi w skład pakietu bind9utils, czyli dig

wyświetla nam więcej informacji o danej domenie. Istotna dla nas jest sekcja ANSWER SECTION. Tutaj wyświetlana jest informacja o rekordzie. Wpisujemy:

$ nslookup klient1

$ dig klient1.srv.local

```
root@dlp:~# nslookup klient1
Server:         10.0.0.3
Address:        10.0.0.3#53

Name:   klient1.srv.local
Address: 10.0.0.35

root@dlp:~# dig klient1.srv.local

; <<>> DiG 9.16.1-Ubuntu <<>> klient1.srv.local
;; global options: +cmd
;; Got answer:
;; WARNING: .local is reserved for Multicast DNS
;; You are currently testing what happens when an mDNS query is leaked to DNS
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27060
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 515fddf483b5e0a101000000637a523773af8f15ee172118 (good)
;; QUESTION SECTION:
;klient1.srv.local.             IN      A

;; ANSWER SECTION:
klient1.srv.local.      604800  IN      A       10.0.0.35

;; Query time: 0 msec
;; SERVER: 10.0.0.3#53(10.0.0.3)
;; WHEN: Sun Nov 20 16:13:43 UTC 2022
;; MSG SIZE  rcvd: 90
```

Podaj wnioski:

- Jeśli klient był dostępny po nazwie hosta "klient1" i pełnej nazwie domenowej "klient1.srv.local", to oznacza, że serwer DNS działa poprawnie i przekierowuje zapytania DNS do odpowiednich adresów IP.
- Polecenie **nslookup** jest przydatne do podstawowego testowania działania DNS, podczas gdy **dig** dostarcza bardziej szczegółowych informacji, w tym rekordy DNS.
- Ustawienie statycznego adresu IP jest przydatne w sytuacjach, gdy konkretny adres IP musi być przypisany do klienta, aby zapewnić stałą konfigurację sieciową.

Zgłoszenie 8

c. Sprawdź poprawność działania serwera DNS z klienta. Dokonaj zmian w pliku /etc/resolv.conf

```
nameserver 10.0.0.3
options edns0
search srv.local
```

```
ubuntu@ubunu2004:~$ sudo nano /etc/resolv.conf
ubuntu@ubunu2004:~$ nslookup dlp
Server:         10.0.0.3
Address:        10.0.0.3#53

Name:   dlp.srv.local
Address: 10.0.0.3

ubuntu@ubunu2004:~$ nslookup dlp.srv.local
Server:         10.0.0.3
Address:        10.0.0.3#53

Name:   dlp.srv.local
Address: 10.0.0.3
```

```
ubuntu@ubunu2004:~$ ping dlp
PING dlp.srv.local (10.0.0.3) 56(84) bytes of data.
64 bytes from 10.0.0.3 (10.0.0.3): icmp_seq=1 ttl=64 time=0.189 ms
64 bytes from 10.0.0.3 (10.0.0.3): icmp_seq=2 ttl=64 time=0.597 ms
64 bytes from 10.0.0.3 (10.0.0.3): icmp_seq=3 ttl=64 time=0.894 ms
^C
--- dlp.srv.local ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2036ms
rtt min/avg/max/mdev = 0.189/0.560/0.894/0.289 ms
ubuntu@ubunu2004:~$ ping dlp.srv.local
PING dlp.srv.local (10.0.0.3) 56(84) bytes of data.
64 bytes from 10.0.0.3 (10.0.0.3): icmp_seq=1 ttl=64 time=0.189 ms
64 bytes from 10.0.0.3 (10.0.0.3): icmp_seq=2 ttl=64 time=0.973 ms
^C
--- dlp.srv.local ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1019ms
rtt min/avg/max/mdev = 0.189/0.581/0.973/0.392 ms
```

Jak widać serwer DNS poprawnie podaje adres IP dla pełnej domeny (dlp.srv.local) oraz dla samej subdomeny (dlp). Poprawnie pinguje na serwer korzystając z subdomeny.

Zgłoszenie 9

d. Łączność z komputerem z internetu

```
ubuntu@ubunu2004:~$ ping google.pl
PING google.pl (216.58.208.195) 56(84) bytes of data.
^C
--- google.pl ping statistics ---
9 packets transmitted, 0 received, 100% packet loss, time 8171ms
```

Nie działa pingowanie do google.pl, gdyż serwera DNS nie ma routingu.

Najszybszym sposobem na konfigurację dostępu do sieci Internet serwera DNS jest:

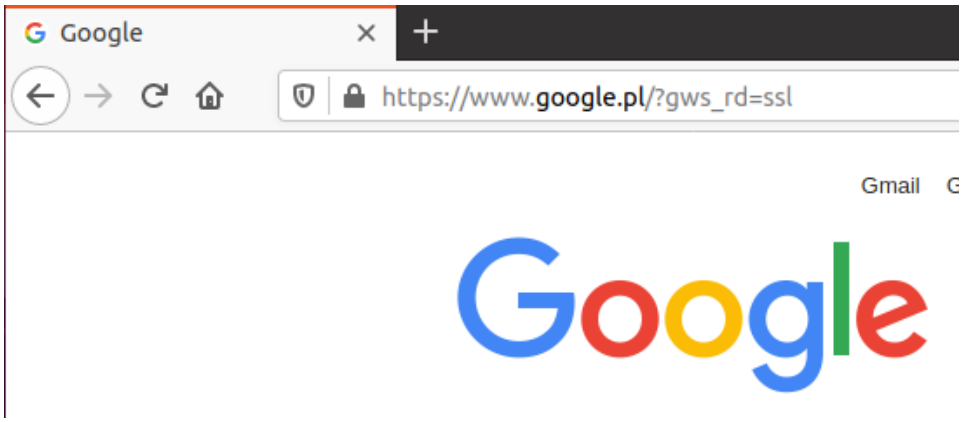
echo 1 > /proc/sys/net/ipv4/ip_forward

iptables -t nat -A POSTROUTING -j MASQUERADE

```
root@dlp:~# echo 1 > /proc/sys/net/ipv4/ip_forward
root@dlp:~# iptables -t nat -A POSTROUTING -j MASQUERADE
```

Sprawdź

```
ubuntu@ubunu2004:~$ ip a |grep enp0s3 |grep inet
    inet 10.0.0.35/24 brd 10.0.0.255 scope global noprefixroute enp0s3
ubuntu@ubunu2004:~$ ping www.google.pl
PING www.google.pl (142.250.75.3) 56(84) bytes of data.
64 bytes from waw07s03-in-f3.1e100.net (142.250.75.3): icmp_seq=1 ttl=115 time=
2.7 ms
```



Zgłoszenie 10

Zgłoś zakończenie ćwiczenia w celu sprawdzenia.

Przywróć pierwszą migawkę

Podsumowanie:

Po wykonaniu wszystkich czynności z powyższej instrukcji przeczytaj ponownie z zrozumieniem cel ogólny i cele szczegółowe, które znajdują się na pierwszej stronie instrukcji. Jeżeli one zostały niezrealizowane to powtarzaj wykonie tej instrukcji w szkole lub/i w domu do momentu zrealizowania.