

Konfiguracja serwera DNS z implementacją DNSsec

Konfiguracja Serwera DNS

[Scenariusz zadania](#)

[Testy](#)

[Połączenie z pawlaczkowo.pl](#)

[Połączenie z gliwice.pawlaczkowo.pl](#)

[Połączenie z poddomenami](#)

[Połączenie do poszczególnych serwerów](#)

[Pełna konfiguracja serwerów](#)

[DNS1](#)

[DNS2](#)

[DNS3](#)

[DNSsec](#)

[Założenia implementacji](#)

[Wdrożenie DNSsec na domenie podstawowej](#)

[DNSsec dla poddomeny](#)

[Testy](#)

[Lista zmian względem poprzedniego zadania](#)

[Serwer DNS1](#)

[Serwer DNS3](#)

Konfiguracja Serwera DNS

- Przygotowanie środowiska:

Do zadań należy wykorzystać trzy dowolne serwery VPS posiadające publiczny adres IPv4, oraz adres IPv6 unikalny globalny.

Do czynności wymagających systemu Windows należy użyć własnego systemu "gospodarza" na którym się pracuje.

Scenariusz zadania

Jesteś administratorem sieci w firmie Northwind Traders (nwtraders.msft).

W organizacji zapadła decyzja, aby kupić domenę {wybierz_co_chcesz}.pl, która ma działać w publicznym systemie DNS.

Z pewnych różnych powodów, otrzymałeś polecenie, aby dla tej zakupionej domeny DNS, utrzymywać jej strefę na dwóch serwerach własnych firmy (posiadających publiczny adres IP), jak również z wydelegowaną domeną na potrzeby jednego z oddziałów gliwice.{wybierz_co_chcesz}.pl, utrzymywaną również na jednym serwerze własnym firmy (posiadającym publiczny adres IP).

Twoim zadaniem jest ponadto:

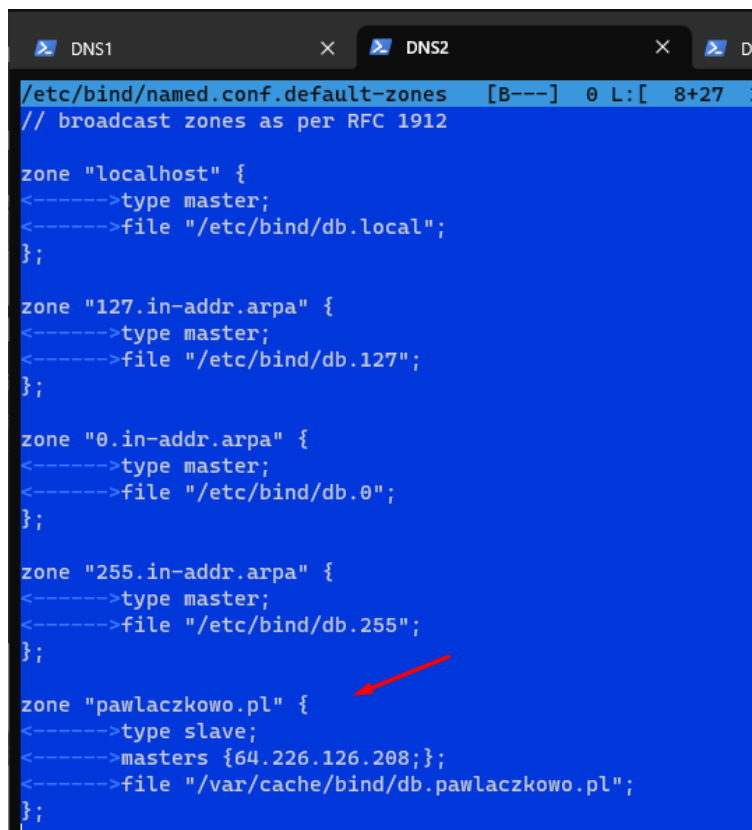
- zarejestrować/wykupić domenę {wybierz_co_chcesz}.pl (tutaj można wybrać sobie dowolną wolną w publicznym systemie DNS domenę z dowolną nazwą i dowolnym rozszerzeniem), która ma działać w publicznym systemie DNS

Na potrzeby zadania zakupiłem domenę pawlaczkowo.pl.

Wyniki poszukiwań dla pawlaczkowo.pl	
Nazwa domeny	pawlaczkowo.pl
Stan	Aktywna w DNS [REGISTERED]
Utworzona	2023.06.12 17:45:08
Ostatnia modyfikacja	2023.06.18 14:21:49
Koniec okresu rozliczeniowego	2024.06.12 17:45:08
Nazwy serwerów	dns1.pawlaczkowo.pl [64.226.126.208] dns2.pawlaczkowo.pl [46.101.153.232]
Abonent	dane niedostępne
Rejestrator	Thecamels Sp. z o.o. ul. Wróblewskiego 18 93-578 Łódź Polska/Poland +48.530887799 info@thecamels.org

- skonfigurować z wykorzystaniem dwóch dowolnych serwerów VPS (posiadających publiczny adres IPv4 oraz adres IPv6 unikalny globalny) zakupioną domenę DNS tak, aby na jednym była przechowywana strefa podstawowa, a na drugim strefa zapasowa

Ustawienia w serwerze zapasowym, serwer podstawowy punkt niżej.



```
/etc/bind/named.conf.default-zones [B---] 0 L:[ 8+27 3
// broadcast zones as per RFC 1912

zone "localhost" {
<----->type master;
<----->file "/etc/bind/db.localhost";
};

zone "127.in-addr.arpa" {
<----->type master;
<----->file "/etc/bind/db.127";
};

zone "0.in-addr.arpa" {
<----->type master;
<----->file "/etc/bind/db.0";
};

zone "255.in-addr.arpa" {
<----->type master;
<----->file "/etc/bind/db.255";
};

zone "pawlaczkowo.pl" {
<----->type slave;
<----->masters {64.226.126.208;};
<----->file "/var/cache/bind/db.pawlaczkowo.pl";
};
```

- skonfigurowanie podstawowego serwera DNS tak, aby automatycznie powiadamiał serwer podrzędny o zmianach dokonanych w strefie, i uniemożliwiał nikomu poza serwerem podrzędnym transferu strefy, jak również uniemożliwiał żadnemu urządzeniu dynamicznej modyfikacji rekordów w strefie domeny

Ustawienia strefy na serwerze podstawowym.

```
zone "pawlaczkowo.pl" {
<----->type master;
<----->file "/etc/bind/db.pawlaczkowo.pl";
<----->notify yes;
<----->allow-transfer{46.101.153.232;};
<----->allow-update{none;};
};
```

- skonfigurowanie podstawowego serwera DNS tak, aby rekordy które "trafią" do pamięci podręcznej klientów DNS (komputerów na których ktoś wpisał do jakiejś aplikacji naszą poddomenę), wygasły w tej pamięci podręcznej po 2 godzinach (czyli czas reakcji klientów w sieci, propagacji dokonanej zmiany w sieci, na dokonywane przez administratorów zmiany w ramach strefy, np. zmiana adresu IP dla poddomeny, ma być nie większy niż dwie godziny).

Konfiguracja pliku strefy:

```

DNS1  DNS2  DNS3
/etc/bind/db.pawlaczkowo.pl  [-M--] 31 L:[ 1+20 21/ 35] *(486 / 832b) 0049 0x031
$TTL<-->7200
@<----->IN<----->SOA<----->dns1.pawlaczkowo.pl. michpawlak.proton.me. (
<-----><-----><-----> 29<-----><-----> Serial
<-----><-----><-----> 604800<-----><-----> Refresh
<-----><-----><-----> 86400<-----><-----> Retry
<-----><-----><-----> 2419200<-----><-----> Expire
<-----><-----><-----> 604800 )<-----><-----> Negative Cache TTL
;
@<----->IN<----->NS<----->dns1.pawlaczkowo.pl.
@<----->IN<----->NS<----->dns2.pawlaczkowo.pl.
gliwice.pawlaczkowo.pl.>IN<----->NS<----->dns3gliwice

@<----->IN<----->A<----->64.226.126.208
@<----->IN<----->AAAA<----->2a03:b0c0:3:d0::920:6001
dns1<-->IN<----->A<----->64.226.126.208
dns1<-->IN<----->AAAA<----->2a03:b0c0:3:d0::920:6001

dns2<-->IN<----->A<----->46.101.153.232
dns2<-->IN<----->AAAA<----->2a03:b0c0:3:d0::f11:f001

```

- skonfigurować z wykorzystaniem jednego (tego trzeciego) serwera VPS tak, aby była na nim przechowywana strefa podstawowa domeny `gliwice.{wybierz_co_chcesz}.pl` (czyli chodzi o poddomenę "gliwice" dla wybranej wcześniej dowolnej domeny z dowolnym rozszerzeniem), a następnie skonfigurować dla niej delegację domeny w ramach strefy podstawowej `{wybierz_co_chcesz}.pl`

Konfiguracja strefy na serwerze DNS3:

```

DNS1  DNS2  DNS3
/etc/bind/db.gliwice.pawlaczkowo.pl  [-M--] 32 L:[ 1+ 2 3/ 16] *(83 / 411b) 00
$TTL<-->7200
@<----->IN<----->SOA<----->dns3.gliwice.pawlaczkowo.pl. michpawlak.proton.me. (
<-----><-----><-----> 12<-----><-----> Serial
<-----><-----><-----> 604800<-----><-----> Refresh
<-----><-----><-----> 86400<-----><-----> Retry
<-----><-----><-----> 2419200<-----><-----> Expire
<-----><-----><-----> 604800 )<-----><-----> Negative Cache TTL
;
@<----->IN<----->NS<----->dns3.gliwice.pawlaczkowo.pl.
@<----->IN<----->A<----->167.99.254.113
@<----->IN<----->AAAA<----->2a03:b0c0:3:d0::ff2:5001
dns3<-->IN<----->A<----->167.99.254.113
dns3<-->IN<----->AAAA<----->2a03:b0c0:3:d0::ff2:5001
www<-->IN<----->A<----->167.99.254.113
www<-->IN<----->AAAA<----->2a03:b0c0:3:d0::ff2:5001

```

```

zone "gliwice.pawlaczkowo.pl" {
<----->type master;
<----->file "/etc/bind/db.gliwice.pawlaczkowo.pl";
};

```

Delegacja poddomeny na serwerze DNS1:

```

@<----->IN<----->NS<----->dns1.pawlaczkowo.pl.
@<----->IN<----->NS<----->dns2.pawlaczkowo.pl.
gliwice.pawlaczkowo.pl.>IN<----->NS<----->dns3.gliwice

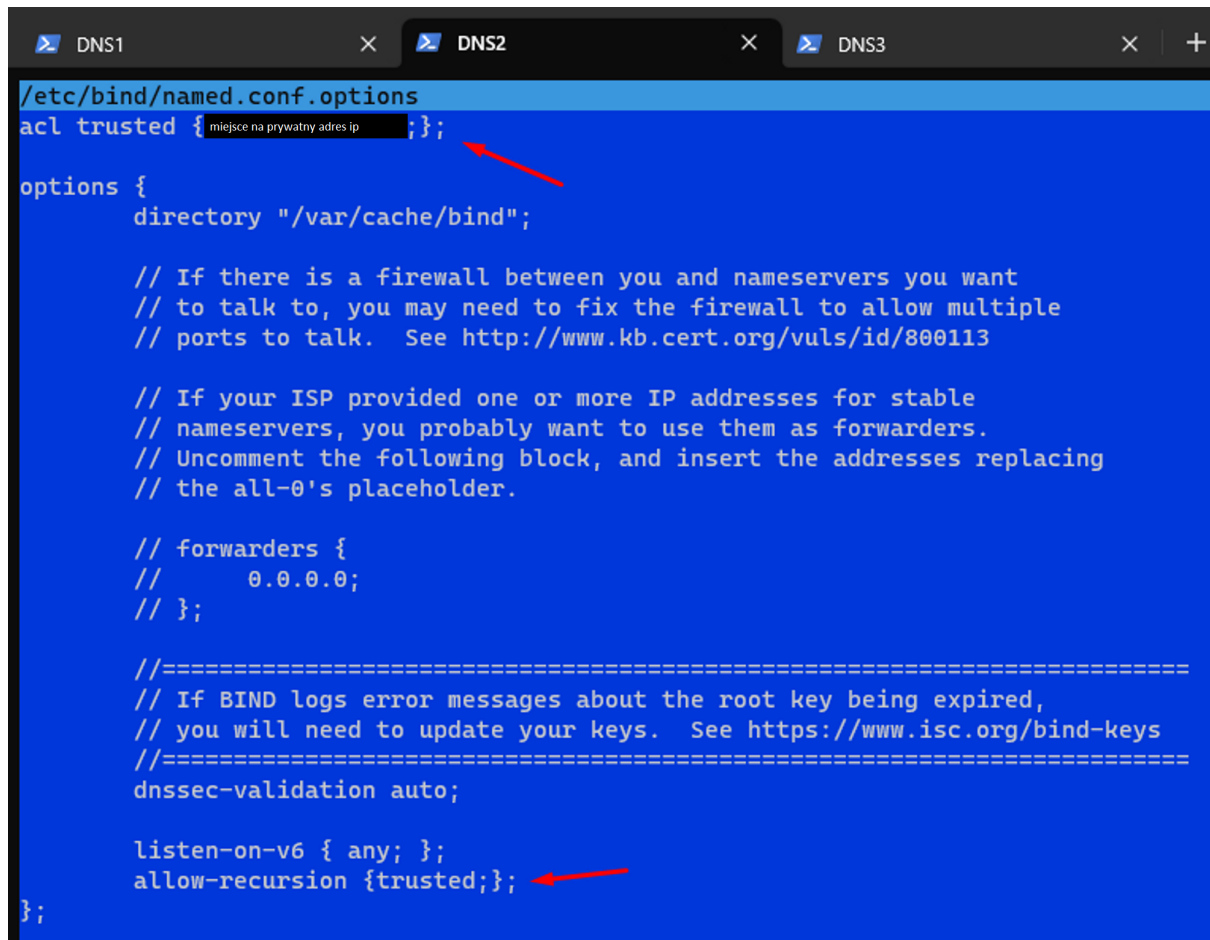
```

```
dns3.gliwice<-->IN<---->A<----->167.99.254.113
dns3.gliwice<-->IN<---->AAAA<---->2a03:b0c0:3:d0::ff2:5001
www.gliwice<-->IN<---->CNAME<-->dns3.gliwice
```

- na wszystkich serwerach VPS, poza serwerem podstawowym dla domeny *{wybierz_co_chcesz}.pl* należy wyłączyć możliwość obsługi zapytań rekursywnych, dla wszystkich za wyjątkiem własnego komputera (pozostawione tak na cele diagnostyczne)

W liście `acl` umieściłem publiczny adres ip komputera, z którego łączyłem się do serwerów.

Konfiguracja pliku `/etc/bind/named.conf.options` taka sama na systemach DNS2 i DNS3.



```
/etc/bind/named.conf.options
acl trusted { miejsce na prywatny adres ip };

options {
    directory "/var/cache/bind";

    // If there is a firewall between you and nameservers you want
    // to talk to, you may need to fix the firewall to allow multiple
    // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
    // the all-0's placeholder.

    // forwarders {
    //     0.0.0.0;
    // };

    //=====
    // If BIND logs error messages about the root key being expired,
    // you will need to update your keys.  See https://www.isc.org/bind-keys
    //=====
    dnssec-validation auto;

    listen-on-v6 { any; };
    allow-recursion {trusted};
};
```

- skonfigurować na serwerze utrzymującym podstawową strefę dla domeny *gliwice.{wybierz_co_chcesz}.pl*, dodatkowo strefę podstawową dla lokalnej domeny DNS "*{nazwisko}.pl*" (gdzie należy podstawić swoje własne nazwisko), i następnie skonfigurować na serwerze utrzymującym podstawową strefę domeny *{wybierz_co_chcesz}.pl* usługę warunkowego przesyłania dalej na potrzeby tej domeny "*{nazwisko}.pl*" (tak, aby jeżeli ktoś wyśle zapytanie DNS dotyczące dowolnej domeny DNS "*{nazwisko}.pl*" do serwera utrzymującego podstawową strefę domeny *{wybierz_co_chcesz}.pl*, to aby tenże potrafił w sposób właściwy obsłużyć to zapytanie)

Konfiguracja strefy na serwerze DNS3:

```
DNS1  X  DNS2  X  DNS3
/etc/bind/db.pawlak.pl  [----]  0 L:[ 1+11 12/ 12] *(248 / 248b)
$TTL<-->7200
@<----->IN<----->SOA<----->pawlak.pl.  bajojajo.pawlak.pl.  (
<-----><-----><----->      2<----->      ; Serial
<-----><-----><----->      604800<----->      ; Refresh
<-----><-----><----->      86400<----->      ; Retry
<-----><-----><----->      2419200<----->      ; Expire
<-----><-----><----->      604800 )<----->      ; Negative Cache TTL
)
@<----->IN<----->NS<----->pawlak.pl.
@<----->IN<----->A<----->167.99.254.113
@<----->IN<----->AAAA<----->2a03:b0c0:3:d0::ff2:5001
```

```
zone "pawlak.pl" {
<----->type master;
<----->file "/etc/bind/db.pawlak.pl";
<----->allow-transfer {64.226.126.208;};
};
```

Utworzenie strefy przesyłania dalej w serwerze DNS1:

```
zone "pawlak.pl" {
<----->type forward;
<----->forwarders {167.99.254.113;};
};
```

- utworzyć w ramach tejże domeny:
 - *{wybierz_co_chcesz}.pl* oraz *www.{wybierz_co_chcesz}.pl* nakierowane na adres IPv4 oraz IPv6 serwera VPS ze strefą podstawową
 - *sklep.{wybierz_co_chcesz}.pl* nakierowane w ramach mechanizmu pseudo-loadbalancingu na adres IPv4 oraz IPv6 obydwu serwerów VPS (ze strefą podstawową i zapasową)
 - *{wybierz_co_chcesz}.pl* nakierowane na adres na adres IPv4 oraz IPv6 serwera VPS ze strefą zapasową, na potrzeby usługi poczty elektronicznej (czyli zakładając, że w późniejszym czasie zostanie tam też uruchomiony serwer pocztowy)
 - *gliwice.{wybierz_co_chcesz}.pl* oraz *www.gliwice.{wybierz_co_chcesz}.pl* nakierowane na adres IPv4 oraz IPv6 serwera VPS ze strefą podstawową dla domeny *gliwice.{wybierz_co_chcesz}.pl*

Dodane rekordy w pliku strefy na serwerze podstawowym:

```

@<----->IN<----->A<----->64.226.126.208
@<----->IN<----->AAAA<----->2a03:b0c0:3:d0::920:6001
dns1<----->IN<----->A<----->64.226.126.208
dns1<----->IN<----->AAAA<----->2a03:b0c0:3:d0::920:6001

dns2<----->IN<----->A<----->46.101.153.232
dns2<----->IN<----->AAAA<----->2a03:b0c0:3:d0::f11:f001

www<----->IN<----->A<----->64.226.126.208
www<----->IN<----->AAAA<----->2a03:b0c0:3:d0::920:6001

sklep<----->IN<----->A<----->64.226.126.208
sklep<----->IN<----->AAAA<----->2a03:b0c0:3:d0::920:6001
sklep<----->IN<----->A<----->46.101.153.232
sklep<----->IN<----->AAAA<----->2a03:b0c0:3:d0::f11:f001

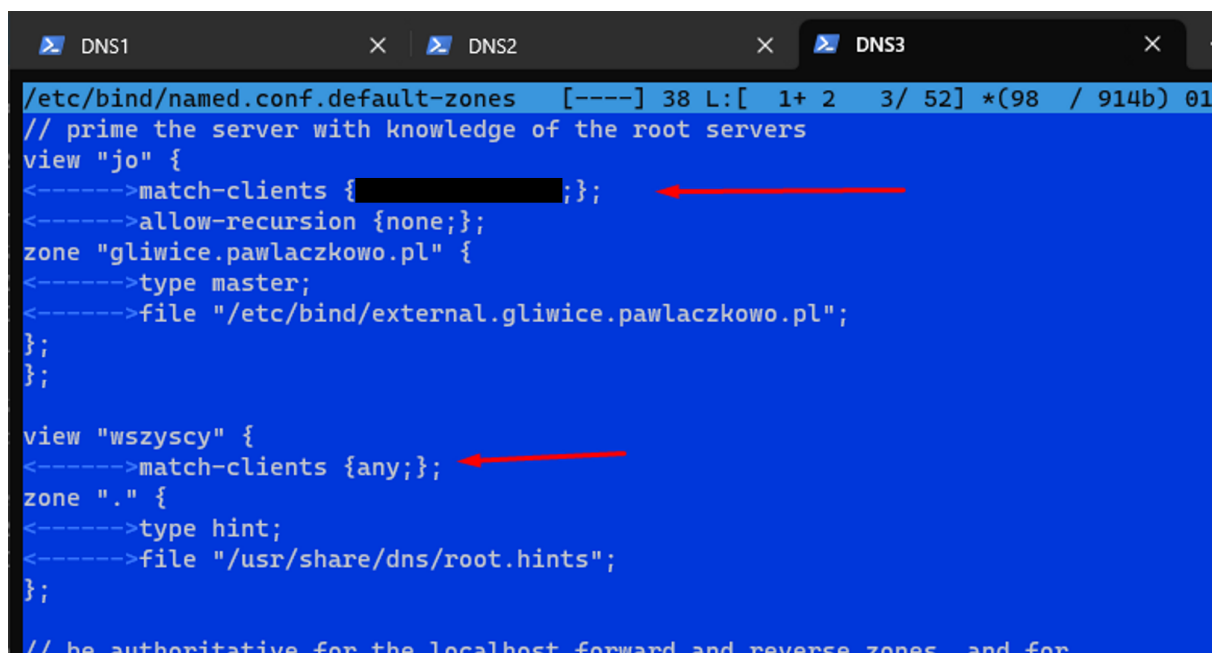
@<----->IN<----->MX<----->10<----->mail.pawlaczkowo.pl.
mail<----->IN<----->A<----->46.101.153.232
mail<----->IN<----->AAAA<----->2a03:b0c0:3:d0::f11:f001

dns3.gliwice<----->IN<----->A<----->167.99.254.113
dns3.gliwice<----->IN<----->AAAA<----->2a03:b0c0:3:d0::ff2:5001
www.gliwice<----->IN<----->CNAME<----->dns3.gliwice

```

- dokonać takiej konfiguracji na serwerze utrzymującym podstawową strefę domeny *gliwice.{wybierz_co_chcesz}.pl*, aby własny komputer w domu korzystał z osobnej konfiguracji strefy dla tej w/w domeny (np. nazwa *gliwice.{wybierz_co_chcesz}.pl* oraz *www.gliwice {wybierz_co_chcesz}.pl* mają być nakierowane na adres IP: 1.1.1.1) niż wszystkie pozostałe komputery, i nie były dla niego również obsługiwane zapytania rekursywne.

Konfiguracja widoków na serwerze poddomeny:



```

/etc/bind/named.conf.default-zones [----] 38 L: [ 1+ 2 3/ 52] *(98 / 914b) 01
// prime the server with knowledge of the root servers
view "jo" {
<----->match-clients { [redacted] };
<----->allow-recursion {none;};
zone "gliwice.pawlaczkowo.pl" {
<----->type master;
<----->file "/etc/bind/external.gliwice.pawlaczkowo.pl";
};
};

view "wszyscy" {
<----->match-clients {any;};
zone "." {
<----->type hint;
<----->file "/usr/share/dns/root.hints";
};
};

// be authoritative for the localhost forward and reverse zones, and for

```

Przykładowa podstawowa konfiguracja pliku strefy w widoku "jo":

```
DNS1  X  DNS2  X  DNS3  X  +
/etc/bind/external.gliwice.pawlaczkowo.pl  [----] 32 L:[ 1+ 2 3/ 12] *(78 / 272
$TTL<-->7200
@<----->IN<----->SOA<----->gliwice.pawlaczkowo.pl. michpawlak.proton.me. (
<-----><-----><-----> 12<-----><----->; Serial
<-----><-----><-----> 604800<-----><----->; Refresh
<-----><-----><-----> 86400<-----><----->; Retry
<-----><-----><-----> 2419200<-----><----->; Expire
<-----><-----><-----> 604800 )<-----><----->; Negative Cache TTL
;
@<----->IN<----->NS<----->dns3.gliwice.pawlaczkowo.pl.
@<----->IN<----->A<----->188.165.16.245
dns3<-->IN<----->A<----->188.165.16.245
```

Testy

Połączenie z pawlaczkowo.pl

```
> server 1.1.1.1
Default Server:  one.one.one.one
Address:  1.1.1.1

> pawlaczkowo.pl
Server:  one.one.one.one
Address:  1.1.1.1

Non-authoritative answer:
Name:  pawlaczkowo.pl
Addresses:  2a03:b0c0:3:d0::920:6001
            64.226.126.208

> www.pawlaczkowo.pl
Server:  one.one.one.one
Address:  1.1.1.1

Non-authoritative answer:
DNS request timed out.
    timeout was 2 seconds.
Name:  www.pawlaczkowo.pl
Address:  64.226.126.208

> www.pawlaczkowo.pl
Server:  one.one.one.one
Address:  1.1.1.1

Non-authoritative answer:
Name:  www.pawlaczkowo.pl
Addresses:  2a03:b0c0:3:d0::920:6001
            64.226.126.208
```



```

C:\Users\blumi>ping pawlaczkowo.pl

Pinging pawlaczkowo.pl [64.226.126.208] with 32 bytes of data:
Reply from 64.226.126.208: bytes=32 time=22ms TTL=51

Ping statistics for 64.226.126.208:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 22ms, Maximum = 22ms, Average = 22ms
Control-C
^C
C:\Users\blumi>ping www.pawlaczkowo.pl

Pinging www.pawlaczkowo.pl [64.226.126.208] with 32 bytes of data:
Reply from 64.226.126.208: bytes=32 time=21ms TTL=51
Reply from 64.226.126.208: bytes=32 time=20ms TTL=51

Ping statistics for 64.226.126.208:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 20ms, Maximum = 21ms, Average = 20ms

```

Połączenie z gliwice.pawlaczkowo.pl

Zapytanie o domenę z innych serwerów:

```

C:\Users\blumi>nslookup
Default Server:  UnKnown
Address:  ::1

> server 9.9.9.9
Default Server:  dns9.quad9.net
Address:  9.9.9.9

> gliwice.pawlaczkowo.pl
Server:  dns9.quad9.net
Address:  9.9.9.9

Non-authoritative answer:
Name:    gliwice.pawlaczkowo.pl
Addresses:  2a03:b0c0:3:d0::ff2:5001
            167.99.254.113

> www.gliwice.pawlaczkowo.pl
Server:  dns9.quad9.net
Address:  9.9.9.9

Non-authoritative answer:
Name:    www.gliwice.pawlaczkowo.pl
Addresses:  2a03:b0c0:3:d0::ff2:5001
            167.99.254.113

```

Zapytanie wprost serwera DNS3:

```

C:\Users\blumi>nslookup
Default Server:  UnKnown
Address:  ::1

> server 167.99.254.113
Default Server:  [167.99.254.113]
Address:  167.99.254.113

> www.gliwice.pawlaczkowo.pl
Server:  [167.99.254.113]
Address:  167.99.254.113

*** [167.99.254.113] can't find www.gliwice.pawlaczkowo.pl: Non-existent domain
> gliwice.pawlaczkowo.pl
Server:  [167.99.254.113]
Address:  167.99.254.113

Name:    gliwice.pawlaczkowo.pl
Address: 188.165.16.245

```

Zapytanie "digiem":

```

C:\Users\blumi>dig @167.99.254.113 gliwice.pawlaczkowo.pl

; <<>> DiG 9.16.41 <<>> @167.99.254.113 gliwice.pawlaczkowo.pl
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56484
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: babfb667ca9cb95701000000648f5a9adb2df6002ccb7229 (good)
;; QUESTION SECTION:
;gliwice.pawlaczkowo.pl.          IN      A

;; ANSWER SECTION:
gliwice.pawlaczkowo.pl. 7200    IN      A      188.165.16.245

;; Query time: 20 msec
;; SERVER: 167.99.254.113#53(167.99.254.113)
;; WHEN: Sun Jun 18 21:28:15 ;; MSG SIZE rcvd: 95

```

Połączenie z poddomenami

- sklep

```

> server 1.1.1.1
Default Server:  one.one.one.one
Address:  1.1.1.1

> sklep.pawlaczkowo.pl
Server:  one.one.one.one
Address:  1.1.1.1

Non-authoritative answer:
Name:  sklep.pawlaczkowo.pl
Addresses:  2a03:b0c0:3:d0::920:6001
            2a03:b0c0:3:d0::f11:f001
            46 101.153.232
            64 226.126.208

> server 8.8.8.8
Default Server:  dns.google
Address:  8.8.8.8

> sklep.pawlaczkowo.pl
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:  sklep.pawlaczkowo.pl
Addresses:  2a03:b0c0:3:d0::f11:f001
            2a03:b0c0:3:d0::920:6001
            64 226.126.208
            46 101.153.232

```

Na zdjęciu widać sposób działania pseudo-loadbalancingu.

- mail

```

> mail.pawlaczkowo.pl
Server:  dns.google
Address:  8.8.4.4

Non-authoritative answer:
Name:  mail.pawlaczkowo.pl
Addresses:  2a03:b0c0:3:d0::f11:f001
            46 101.153.232

```

```

C:\Users\blumi>dig MX pawlaczkowo.pl

; <<>> DiG 9.16.41 <<>> MX pawlaczkowo.pl
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8677
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
pawlaczkowo.pl.                7200    IN      MX      10 mail.pawlaczkowo.pl.

;; Query time: 107 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Sun Jun 18 21:34:26 ;; MSG SIZE rcvd: 64

```

Połączenie do poszczególnych serwerów

```

> server 76.76.2.0
Default Server: p0.freedns.controld.com
Address: 76.76.2.0

> pawlaczkowo.pl
Server: p0.freedns.controld.com
Address: 76.76.2.0

Non-authoritative answer:
Name: pawlaczkowo.pl
Addresses: 2a03:b0c0:3:d0::920:6001
           64.226.126.208

> server 64.226.126.208
Default Server: [64.226.126.208]
Address: 64.226.126.208

> dns1.pawlaczkowo.pl
Server: [64.226.126.208]
Address: 64.226.126.208

Name: dns1.pawlaczkowo.pl
Addresses: 2a03:b0c0:3:d0::920:6001
           64.226.126.208

> dns2.pawlaczkowo.pl
Server: [64.226.126.208]
Address: 64.226.126.208

Name: dns2.pawlaczkowo.pl
Addresses: 2a03:b0c0:3:d0::f11:f001
           46.101.153.232

> dns3gliwice.pawlaczkowo.pl
Server: [64.226.126.208]
Address: 64.226.126.208

Name: dns3gliwice.pawlaczkowo.pl
Addresses: 2a03:b0c0:3:d0::ff2:5001
           167.99.254.113

```

Pełna konfiguracja serwerów

Adresy IP serwerów:

DNS1 — 64.226.126.208, 2a03:b0c0:3:d0::920:6001

DNS2 — 46.101.153.232, 2a03:b0c0:3:d0::f11:f001

DNS3 — 167.99.254.113, 2a03:b0c0:3:d0::ff2:5001

DNS1

- db.pawlaczkowo.pl

```

D$TTL 7200
@      IN      SOA    dns1.pawlaczkowo.pl. michpawlak.proton.me. (
                        30          ; Serial
                        604800       ; Refresh
                        86400        ; Retry
                        2419200      ; Expire
                        604800 )     ; Negative Cache TTL
;
@      IN      NS    dns1.pawlaczkowo.pl.
@      IN      NS    dns2.pawlaczkowo.pl.
gliwice.pawlaczkowo.pl. IN      NS    dns3.gliwice

@      IN      A      64.226.126.208
@      IN      AAAA   2a03:b0c0:3:d0::920:6001
dns1   IN      A      64.226.126.208

```

dns1	IN	AAAA	2a03:b0c0:3:d0::920:6001
dns2	IN	A	46.101.153.232
dns2	IN	AAAA	2a03:b0c0:3:d0::f11:f001
www	IN	A	64.226.126.208
www	IN	AAAA	2a03:b0c0:3:d0::920:6001
sklep	IN	A	64.226.126.208
sklep	IN	AAAA	2a03:b0c0:3:d0::920:6001
sklep	IN	A	46.101.153.232
sklep	IN	AAAA	2a03:b0c0:3:d0::f11:f001
@	IN	MX	10 mail.pawlaczkowo.pl.
mail	IN	A	46.101.153.232
mail	IN	AAAA	2a03:b0c0:3:d0::f11:f001
dns3.gliwice	IN	A	167.99.254.113
dns3.gliwice	IN	AAAA	2a03:b0c0:3:d0::ff2:5001
www.gliwice	IN	CNAME	dns3.gliwice

- Dodane strefy w named.conf.default-zones:

```
zone "pawlaczkowo.pl" {
    type master;
    file "/etc/bind/db.pawlaczkowo.pl";
    notify yes;
    allow-transfer {46.101.153.232;};
    allow-update {none;};
};

zone "pawlak.pl" {
    type forward;
    forwarders {167.99.254.113;};
};
```

- Dodanie zezwolenia na zapytania w named.conf.options:

```
options {
    /.../
    allow-query { any; };
};
```

DNS2

- Dodane strefy w named.conf.default-zones:

```
zone "pawlaczkowo.pl" {
    type slave;
    masters {64.226.126.208;};
    file "/var/cache/bind/db.pawlaczkowo.pl";
};
```

- zezwolenie na zapytania rekurencyjne tylko dla jednego komputera w named.conf.options:

```
acl trusted {XXX.XXX.XXX.XXX;};
options {
    /.../
    allow-recursion {trusted;};
};
```

DNS3

- db.gliwice.pawlaczkowo.pl

```
$TTL      7200
@         IN      SOA      dns3.gliwice.pawlaczkowo.pl. michpawlak.proton.me. (
                                12                                ; Serial
```

```

        604800      ; Refresh
        86400      ; Retry
        2419200    ; Expire
        604800 )    ; Negative Cache TTL
;
@      IN      NS      dns3.gliwice.pawlaczkowo.pl.
@      IN      A       167.99.254.113
@      IN      AAAA    2a03:b0c0:3:d0::ff2:5001
dns3   IN      A       167.99.254.113
dns3   IN      AAAA    2a03:b0c0:3:d0::ff2:5001
www    IN      A       167.99.254.113
www    IN      AAAA    2a03:b0c0:3:d0::ff2:5001

```

- external.gliwice.pawlaczkowo.pl

```

$TTL      7200
@      IN      SOA      gliwice.pawlaczkowo.pl. michpawlak.proton.me. (
                                12              ; Serial
                                604800          ; Refresh
                                86400          ; Retry
                                2419200        ; Expire
                                604800 )        ; Negative Cache TTL
;
@      IN      NS      dns3.gliwice.pawlaczkowo.pl.
@      IN      A       188.165.16.245
dns3   IN      A       188.165.16.245

```

- db.pawlak.pl

```

$TTL      7200
@      IN      SOA      pawlak.pl. bajojajo.pawlak.pl. (
                                2              ; Serial
                                604800          ; Refresh
                                86400          ; Retry
                                2419200        ; Expire
                                604800 )        ; Negative Cache TTL
;
@      IN      NS      pawlak.pl.
@      IN      A       167.99.254.113
@      IN      AAAA    2a03:b0c0:3:d0::ff2:5001

```

- Dodane strefy w named.conf.default-zones:

```

view "jo" {
    match-clients {XXX.XXX.XXX.XXX;};
    allow-recursion {none;};
    zone "gliwice.pawlaczkowo.pl" {
        type master;
        file "/etc/bind/external.gliwice.pawlaczkowo.pl";
    };
    view "wszyscy" {
        match-clients {any;};
    };
    /.../
    zone "gliwice.pawlaczkowo.pl" {
        type master;
        file "/etc/bind/db.gliwice.pawlaczkowo.pl";
        allow-update{none;};
        allow-transfer {none;};
    };

    zone "pawlak.pl" {
        type master;
        file "/etc/bind/db.pawlak.pl";
        allow-update{none;};
        allow-transfer {none;};
    };
};

```

- zezwolenie na zapytania rekurencyjne tylko dla jednego komputera w named.conf.options:

```

acl trusted {XXX.XXX.XXX.XXX;};
options {

```

```
./.../  
allow-recursion {trusted;};  
};
```

DNSsec

Założenia implementacji

Dla skonfigurowanej w w/w zadaniu domeny zarejestrowanej w publicznym systemie DNS, należy skonfigurować pełną obsługę DNSsec, ze zgłoszonym do operatora rekordem DS, i z wdrożoną automatyczną rotacją kluczy ZSK - obsługa DNSsec ma zostać zrealizowana zarówno dla domeny głównej {wybierz_co_chcesz}.pl jak również delegowanej domeny gliwice.{wybierz_co_chcesz}.pl

Wdrożenie DNSsec na domenie podstawowej

- Przeniesienie plików strefy do /var/cache/bind/pawlaczkowo i zmiany w named.conf

Aby uprościć działanie na strefie powinno przenieść się jej pliki do folderu /var/cache/bind i nadać plikom odpowiednie uprawnienia.

- zmiana w named.conf.default-zones

```
zone "pawlaczkowo.pl" {  
    <----->type master;  
    <----->file "/var/cache/bind/pawlaczkowo/db.pawlaczkowo.pl";  
    <----->notify yes;  
    <----->allow-transfer{127.0.0.1; 46.101.153.232;};  
    <----->allow-update{none;};  
    <----->auto-dnssec maintain;  
    <----->inline-signing yes;  
    <----->key-directory "/var/cache/bind/pawlaczkowo/";  
};
```

- zmiana w named.conf.options

```
//-----  
>dnssec-enable yes;  
>dnssec-validation auto;  
>key-directory "/var/cache/bind/pawlaczkowo";  
>allow-query { any; };  
>listen-on-v6 { any; };
```

- utworzenie kluczy

```
root@DNS1:~# cd /var/cache/bind/pawlaczkowo/  
root@DNS1:/var/cache/bind/pawlaczkowo# dnssec-keygen -a ECDSA256SHA256 -3 pawlaczkowo.pl  
Generating key pair.  
Kpawlaczkowo.pl.+013+43010  
root@DNS1:/var/cache/bind/pawlaczkowo# dnssec-keygen -f KSK -a ECDSA256SHA256 -3 pawlaczkowo.pl  
Generating key pair.  
Kpawlaczkowo.pl.+013+59336  
root@DNS1:/var/cache/bind/pawlaczkowo# ls -la  
total 28  
drwxr-xr-x 2 root root 4096 Jun 18 23:50 .  
drwxrwxr-x 3 root bind 4096 Jun 18 23:46 ..  
-rw-r--r-- 1 root root 348 Jun 18 23:49 Kpawlaczkowo.pl.+013+43010.key  
-rw----- 1 root root 187 Jun 18 23:49 Kpawlaczkowo.pl.+013+43010.private  
-rw-r--r-- 1 root root 347 Jun 18 23:50 Kpawlaczkowo.pl.+013+59336.key  
-rw----- 1 root root 187 Jun 18 23:50 Kpawlaczkowo.pl.+013+59336.private
```

Wybrałem taki a nie inny algorytm, ponieważ mój rejestrator podał w zalecanej konfiguracji ten algorytm:

Key Setup ?

How the system creates the security key.

☒ Classic

Creates a ZSK (Zone Signing Key) and a KSK (Key Signing Key) keypair.

☐ Simple

Creates a CSK (Combined Signing Key) which will be used as both the ZSK and KSK.

Algorithm ?

The algorithm that the system will use to create the security key.

☐ RSA/SHA-256 (Algorithm 8) **Most Commonly Supported**

Most domain registrars support this algorithm.

☐ RSA/SHA-512 (Algorithm 10)

☒ ECDSA Curve P-256 with SHA-256 (Algorithm 13) **Zalecana(-e)**

We recommend that you use this algorithm if your domain registrar supports it.

☐ ECDSA Curve P-384 with SHA-384 (Algorithm 14)

Stan ?

Select whether to activate the newly-created key.

☒ Active

☐ Not Active

- nadanie uprawnień dla grupy bind

Wykorzystałem komendy:

```
chmod -R 760 /var/cache/bind/*
chown -R bind:bind /var/cache/bind/*
```

Ponieważ samo nadanie uprawnień odczytu i zapisu dla grupy bind może nie wystarczyć. Konfiguruje uprawnienia najlepiej sprawdzać logi (korzystając z komendy, np.: journalctl -xe).

- automatyczna rotacja kluczy ZSK

Pierwszy klucz ZSK:

```
Kpawlaczkowo.pl.+013+43010.key      Kpawlaczkowo.pl.+013+59336.key      db.pawlaczkowo.pl      db.pawlaczkowo.pl.signed
Kpawlaczkowo.pl.+013+43010.private  Kpawlaczkowo.pl.+013+59336.private  db.pawlaczkowo.pl.jbk  db.pawlaczkowo.pl.signed.jnl
root@DNS1:/var/cache/bind/pawlaczkowo# cat Kpawlaczkowo.pl.+013+43010.key
; This is a zone-signing key, keyid 43010, for pawlaczkowo.pl.
; Created: 20230618234949 (Sun Jun 18 23:49:49 2023)
; Publish: 20230618234949 (Sun Jun 18 23:49:49 2023)
; Activate: 20230618234949 (Sun Jun 18 23:49:49 2023)
pawlaczkowo.pl. IN DNSKEY 256 3 13 ZM07mNKw1ns4kBDsWQpwN4PxI1xqK16f3U5jJSYAiiRUa/gxv4gX107H SLcj66F7johi0bb3fhE8p5eHlQRtA==
```

Ustawienie dat ważności klucza i jego usunięcia, a także wygenerowanie dwóch następców tegoż klucza:


```

root@DNS1:/var/cache/bind/pawlaczkowo# dnssec-settime -I +3mo -D +4mo Kpawlaczkowo.pl.+013+43010.key
dnssec-settime: warning: Permissions on the file ./Kpawlaczkowo.pl.+013+43010.private have changed from 0760 to 0600 as a result of this operation.
./Kpawlaczkowo.pl.+013+43010.key
./Kpawlaczkowo.pl.+013+43010.private
root@DNS1:/var/cache/bind/pawlaczkowo# cat Kpawlaczkowo.pl.+013+43010.key
; This is a zone-signing key, keyid 43010, for pawlaczkowo.pl.
; Created: 20230618234949 (Sun Jun 18 23:49:49 2023)
; Publish: 20230618234949 (Sun Jun 18 23:49:49 2023)
; Activate: 20230618234949 (Sun Jun 18 23:49:49 2023)
; Inactive: 20230917084849 (Sun Sep 17 08:48:49 2023)
; Delete: 20231017084849 (Tue Oct 17 08:48:49 2023)
pawlaczkowo.pl. IN DNSKEY 256 3 13 ZM07mNKw1ns4kBDsWQpW4PxI1xqK16f3U5jJSYAiiRUa/gxv4gX107H SLcj66GF7joh10bb3fhE8p5eHLQRtA==
root@DNS1:/var/cache/bind/pawlaczkowo# dnssec-keygen -S Kpawlaczkowo.pl.+013+43010.key -I +6mo -D +7mo
Generating key pair.
Kpawlaczkowo.pl.+013+21196
root@DNS1:/var/cache/bind/pawlaczkowo# dnssec-keygen -S Kpawlaczkowo.pl.+013+21196.key -I +9mo -D +10mo
Generating key pair.
Kpawlaczkowo.pl.+013+22461
root@DNS1:/var/cache/bind/pawlaczkowo#

```

Oczywiście można ich wygenerować znacznie więcej, jednakże na potrzeby tego projektu powinna to być wystarczająca ilość. Niezależnie od tego, czy utworzy się ich dużo, czy mało trzeba pamiętać do kiedy jest ostatni z kluczy, aby za wczasu utworzyć nowe jeśli będzie taka potrzeba.

Uwzględnienie tych kluczy w pliku strefy:

```

DNS1  DNS2  DNS3
/var/cache/bind/pawlaczkowo/db.pawlaczkowo.pl [-M--] 31 L: [ 1+ 6
$TTL<--->7200
$INCLUDE /var/cache/bind/pawlaczkowo/Kpawlaczkowo.pl.+013+43010.key
$INCLUDE /var/cache/bind/pawlaczkowo/Kpawlaczkowo.pl.+013+59336.key
$INCLUDE /var/cache/bind/pawlaczkowo/Kpawlaczkowo.pl.+013+21196.key
$INCLUDE /var/cache/bind/pawlaczkowo/Kpawlaczkowo.pl.+013+22461.key
@<----->IN<----->SOA<----->dns1.pawlaczkowo.pl. michpawlak.proton.me. (
<-----><-----><-----> 33|<-----> Serial
<-----><-----><-----> 604800<-----> Refresh

```

- przekazanie rekordu DS do rejestratora:

```

root@DNS1:/var/cache/bind/pawlaczkowo# dnssec-dsfromkey Kpawlaczkowo.pl.+013+59336.key
pawlaczkowo.pl. IN DS 59336 13 2 5B5E70ED848DB9B6CF213BC117FD6AF89B672646E58BA0ABC5398B4B7DCC5765
root@DNS1:/var/cache/bind/pawlaczkowo# cat Kpawlaczkowo.pl.+013+59336.key
; This is a key-signing key, keyid 59336, for pawlaczkowo.pl.
; Created: 20230618235014 (Sun Jun 18 23:50:14 2023)
; Publish: 20230618235014 (Sun Jun 18 23:50:14 2023)
; Activate: 20230618235014 (Sun Jun 18 23:50:14 2023)
pawlaczkowo.pl. IN DNSKEY 257 3 13 o1M4KfSkq5soLH9i6eIpFo9qMkfsa8B2mqg5EkjNf4H/15MF1YQwDQN5 7bb+E5Gqx5L8YvLwuqhRahyZn6d6QQ==

```

Zarządzaj
Przegląd
Autoodnowienie
Konfiguracja serwerów DNS
Registry Lock
Dane kontaktowe domeny
Prywatne serwery DNS
Cesja
Zarządzanie DNSsec

Zarządzaj pawlaczkowo.pl

START / PANEL KLIENTA / MOJE DOMENY / PAWLACZKOWO.PL / DNSSEC MANAGEMENT

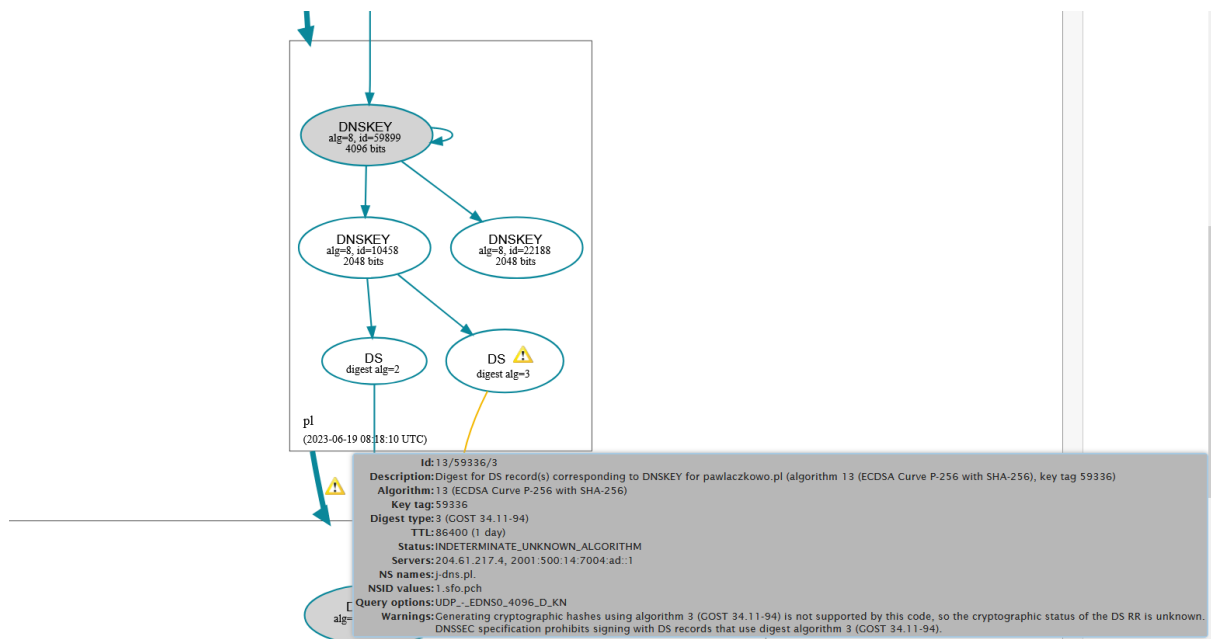
DNSSec Management

Changes saved succesfully.

Key Tag	Algorithm	Digest Type	Digest
59336	13	3	5B5E70ED848DB9B6CF213BC117F

Jeśli tak jak na zdjęciu wyżej, popełni się błąd przy wklejaniu danych do panelu webowego rejestratora, nie trzeba się tym martwić. Można poprawić błąd, jednakże przez jakiś czas będą widniały oba rekordy DS.

Po naprawieniu błędu przez zmienienie "Digest Type" na 2:



Sprawdzając następnego dnia, widoczny był już tylko jeden, prawidłowy, rekord ds. (Zdjęcie w sekcji "Testy")

DNSsec dla poddomeny

Konfiguracja przebiega podobnie jak na podstawowej domenie.

- Przeniesienie plików strefy do /var/cache/bind/gliwice.pawlaczkowo
- Zmiany w named.conf
- Utworzenie kluczy
- W tym wypadku utworzyłem tylko jednego następcę klucza ZSK

```
root@DNS3:/var/cache/bind/gliwice.pawlaczkowo# cat Kgliwice.pawlaczkowo.pl.+013+26736.key
; This is a key-signing key, keyid 26736, for gliwice.pawlaczkowo.pl.
; Created: 20230619002758 (Mon Jun 19 00:27:58 2023)
; Publish: 20230619002758 (Mon Jun 19 00:27:58 2023)
; Activate: 20230619002758 (Mon Jun 19 00:27:58 2023)
gliwice.pawlaczkowo.pl. IN DNSKEY 257 3 13 l+ZGWHaYknnYvxQ6uD5FMKM4zE7U19V4/+At3mjsBG3MmABv4NnXgZtw FM4VbujTzexZGhQ5uJQErS0IF1M7lg==
root@DNS3:/var/cache/bind/gliwice.pawlaczkowo# cat Kgliwice.pawlaczkowo.pl.+013+56670.key
; This is a zone-signing key, keyid 56670, for gliwice.pawlaczkowo.pl.
; Created: 20230619002737 (Mon Jun 19 00:27:37 2023)
; Publish: 20230619002737 (Mon Jun 19 00:27:37 2023)
; Activate: 20230619002737 (Mon Jun 19 00:27:37 2023)
; Inactive: 20231017010520 (Tue Oct 17 01:05:20 2023)
; Delete: 20231116010520 (Thu Nov 16 01:05:20 2023)
gliwice.pawlaczkowo.pl. IN DNSKEY 256 3 13 emrk8q/571DRDQZx+WpMzX6pqRys/xL8FTdw104z52CITombCpmNKn8k TFjjmOtBjhAReC9LT7zA0dxTQx6dvQ==
root@DNS3:/var/cache/bind/gliwice.pawlaczkowo# cat Kgliwice.pawlaczkowo.pl.+013+65423.key
; This is a zone-signing key, keyid 65423, for gliwice.pawlaczkowo.pl.
; Created: 20230619010629 (Mon Jun 19 01:06:29 2023)
; Publish: 20230917010520 (Sun Sep 17 01:05:20 2023)
; Activate: 20231017010520 (Tue Oct 17 01:05:20 2023)
; Inactive: 20231216010629 (Sat Dec 16 01:06:29 2023)
; Delete: 20240115010629 (Mon Jan 15 01:06:29 2024)
gliwice.pawlaczkowo.pl. IN DNSKEY 256 3 13 wEy618tz44sCn/p1JyikR2xRzUGERcWXYxwj1hdEyq9aa5b4y8F5aoAw UpxS+yLaZS/qqrJHaEa/j594AdH5Dg==
```

- Uwzględnienie kluczy w pliku strefy (strefa external.gliwice.pawlaczkowo.pl, bez dnsseca bo jest to konfiguracja testowa)

```

DNS1 X DNS2 X DNS3 X Windows Power
/var/cache/bind/gliwice.pawlaczkowo/db.gliwice.pawlaczkowo.pl [-M--] 32 L:[ 1+ 5 6/ 19]
$TTL<-->7200
$INCLUDE /var/cache/bind/gliwice.pawlaczkowo/Kgliwice.pawlaczkowo.pl.+013+26736.key
$INCLUDE /var/cache/bind/gliwice.pawlaczkowo/Kgliwice.pawlaczkowo.pl.+013+56670.key
$INCLUDE /var/cache/bind/gliwice.pawlaczkowo/Kgliwice.pawlaczkowo.pl.+013+65423.key
@<----->IN<----->SOA<----->dns3.gliwice.pawlaczkowo.pl. michpawlak.proton.me. (
<-----><-----><-----> 14<-----><-----><-----> Serial
<-----><-----><-----> 604800<-----><-----><-----> Refresh
<-----><-----><-----> 86400<-----><-----><-----> Retry

```

- Nadanie odpowiednich uprawnień dla plików w /var/cache/bind

```

root@DNS3:/var/cache/bind/gliwice.pawlaczkowo# ls -la
total 52
drwxrwxrwx 2 bind bind 4096 Jun 19 01:06 .
drwxrwxrwx 3 bind bind 4096 Jun 19 08:38 ..
-rwxrwxrwx 1 bind bind 363 Jun 19 00:27 Kgliwice.pawlaczkowo.pl.+013+26736.key
-rwxrwxrwx 1 bind bind 187 Jun 19 00:27 Kgliwice.pawlaczkowo.pl.+013+26736.private
-rwxrwxrwx 1 bind bind 470 Jun 19 01:06 Kgliwice.pawlaczkowo.pl.+013+56670.key
-rwxrwxrwx 1 bind bind 252 Jun 19 01:06 Kgliwice.pawlaczkowo.pl.+013+56670.private
-rwxrwxrwx 1 bind bind 470 Jun 19 01:06 Kgliwice.pawlaczkowo.pl.+013+65423.key
-rwxrwxrwx 1 bind bind 254 Jun 19 01:06 Kgliwice.pawlaczkowo.pl.+013+65423.private
-rwxrwxrwx 1 bind bind 579 Jun 19 00:36 db.gliwice.pawlaczkowo.pl
-rwxrwxrwx 1 bind bind 512 Jun 19 00:54 db.gliwice.pawlaczkowo.pl.jbk
-rwxrwxrwx 1 bind bind 2966 Jun 19 01:06 db.gliwice.pawlaczkowo.pl.signed
-rwxrwxrwx 1 bind bind 1738 Jun 19 01:06 db.gliwice.pawlaczkowo.pl.signed.jnl
-rwxrwxrwx 1 bind bind 272 Jun 18 19:03 external.gliwice.pawlaczkowo.pl

```

- Przekazanie rekordu DS do serwera strefy podstawowej

```

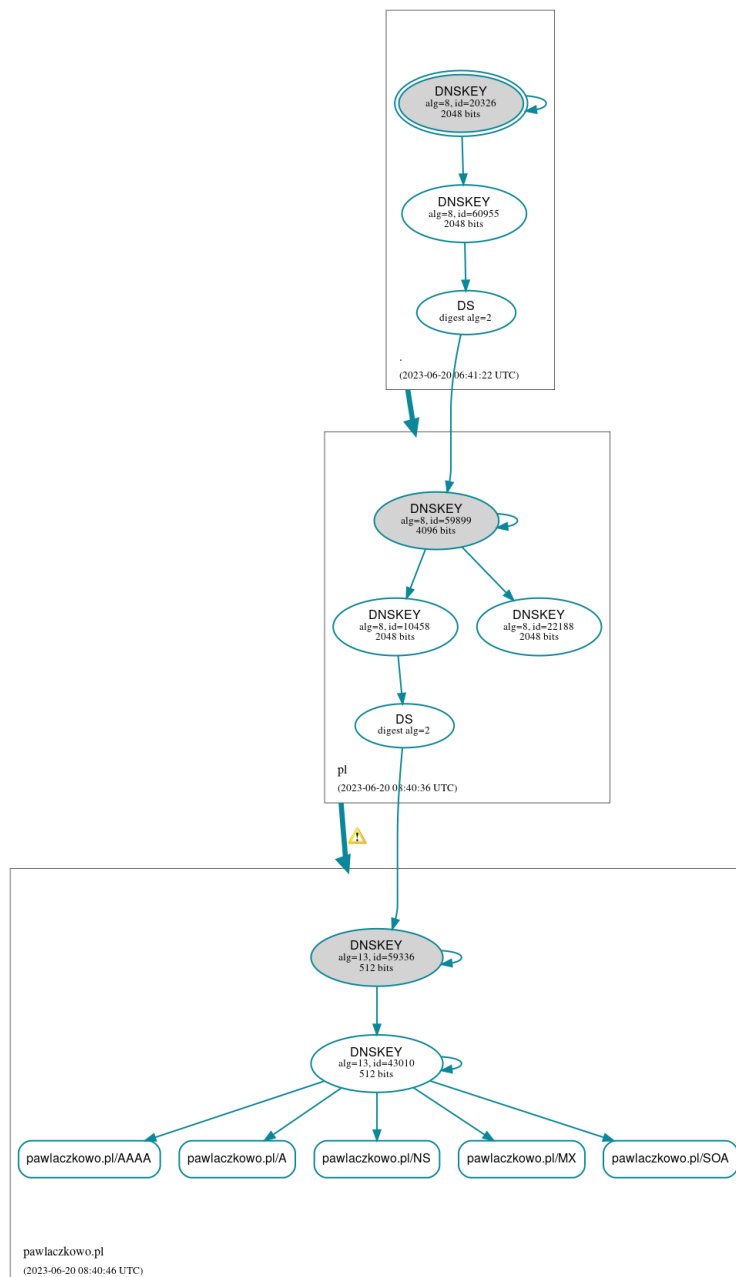
; Negative Cache TTL:
;
; IN NS dns1.pawlaczkowo.pl.
; IN NS dns2.pawlaczkowo.pl.
gliwice.pawlaczkowo.pl. IN NS dns3.gliwice
gliwice.pawlaczkowo.pl. IN DS 26736 13 2 1B7EC751BCA4346A506F22192060439043004BE7CAD116C1CC3ABA10FF348002

```

Testy

Sprawdzenie konfiguracji przez dnsviz.pl

- pawlaczkowo.pl



Description: Delegation from pl. to pawlaczkowo.pl.
Status: SECURE
Warnings: Authoritative AAAA records exist for dns1.pawlaczkowo.pl, but there are no corresponding AAAA glue records.
 Authoritative AAAA records exist for dns2.pawlaczkowo.pl, but there are no corresponding AAAA glue records.

Niestety mój rejestrator domeny nie przewidział utworzenia w panelu webowym glue rekordów dla ipv6, więc wprost nic nie można z tym zrobić.

Podgląd panelu do rejestracji serwera:

Serwery nazw



Tutaj możesz określić własne serwery nazw (np. ns1., ns2., itp.)

Rejestracja serwera DNS

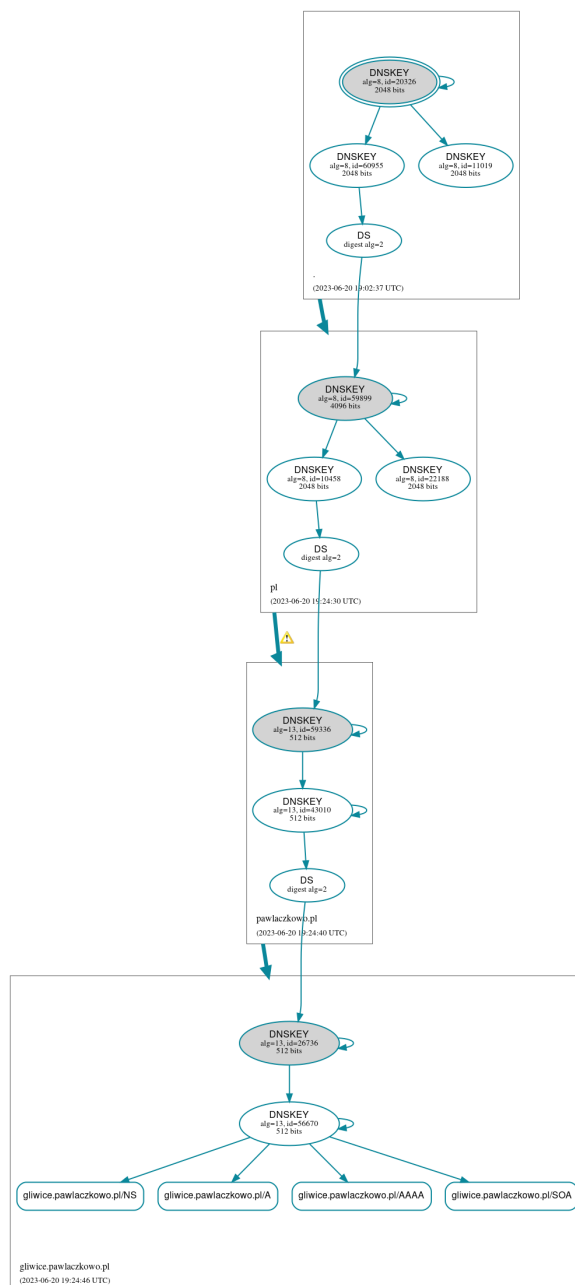
DNS

 .pawlaczkowo.pl

Adres IP

Zapisz zmiany

- gliwice.pawlaczkowo.pl



Lista zmian względem poprzedniego zadania

Serwer DNS1

Pliki strefy przeniesione do `/var/cache/bind/pawlaczkowo`.

Utworzenie kluczy KSK i ZSK oraz ustawienie automatycznej wymiany.

Zmiana uprawnień w katalogu:

```

root@DNS1:/var/cache/bind/pawlaczkowo# ls -la
total 60
drwxrw---- 2 bind bind 4096 Jun 19 09:00 .
drwxrwxr-x 3 bind bind 4096 Jun 19 09:00 ..
-rwxrw---- 1 bind bind 454 Jun 19 08:50 Kpawlaczkowo.pl.+013+21196.key
-rwxrw---- 1 bind bind 271 Jun 19 08:50 Kpawlaczkowo.pl.+013+21196.private
-rwxrw---- 1 bind bind 454 Jun 19 08:50 Kpawlaczkowo.pl.+013+22461.key
-rwxrw---- 1 bind bind 254 Jun 19 08:50 Kpawlaczkowo.pl.+013+22461.private
-rwxrw---- 1 bind bind 454 Jun 19 08:49 Kpawlaczkowo.pl.+013+43010.key
-rwxrw---- 1 bind bind 252 Jun 19 08:49 Kpawlaczkowo.pl.+013+43010.private
-rwxrw---- 1 bind bind 347 Jun 18 23:50 Kpawlaczkowo.pl.+013+59336.key
-rwxrw---- 1 bind bind 187 Jun 18 23:50 Kpawlaczkowo.pl.+013+59336.private
-rwxrw---- 1 bind bind 1252 Jun 19 09:00 db.pawlaczkowo.pl
-rwxrw---- 1 bind bind 512 Jun 19 00:53 db.pawlaczkowo.pl.jbk
-rwxrw---- 1 bind bind 5408 Jun 19 01:04 db.pawlaczkowo.pl.signed
-rwxrw---- 1 bind bind 4034 Jun 19 01:04 db.pawlaczkowo.pl.signed.jnl

```

- db.pawlaczkowo.pl

```

$TTL      7200
$INCLUDE /var/cache/bind/pawlaczkowo/Kpawlaczkowo.pl.+013+43010.key
$INCLUDE /var/cache/bind/pawlaczkowo/Kpawlaczkowo.pl.+013+59336.key
$INCLUDE /var/cache/bind/pawlaczkowo/Kpawlaczkowo.pl.+013+21196.key
$INCLUDE /var/cache/bind/pawlaczkowo/Kpawlaczkowo.pl.+013+22461.key
@         IN      SOA      dns1.pawlaczkowo.pl. michpawlak.proton.me. (
/.../)
/.../
gliwice.pawlaczkowo.pl. IN      DS      26736  13      2      1B7EC751BCA4346A506F22192060439043004BE7CAD116C1CC3ABA10FF348002
/.../

```

- named.conf.default-zones:

```

zone "pawlaczkowo.pl" {
<----->type master;
<----->file "/var/cache/bind/pawlaczkowo/db.pawlaczkowo.pl";
<----->notify yes;
<----->allow-transfer {127.0.0.1; 46.101.153.232;};
<----->allow-update {none;};
<----->auto-dnssec maintain;
<----->inline-signing yes;
<----->key-directory "/var/cache/bind/pawlaczkowo/";
};

```

zezwole nie na transfer do 127.0.0.1 utworzone na cele diagnostyczne.

- named.conf.options:

```

options {
/.../
<----->dnssec-enable yes;
<----->dnssec-validation auto;
<----->key-directory "/var/cache/bind/pawlaczkowo";
/.../
};

```

Serwer DNS3

Pliki strefy przeniesione do /var/cache/bind/gliwice.pawlaczkowo.

Utworzenie kluczy KSK i ZSK oraz ustawienie automatycznej wymiany.

Zmiana uprawnień w katalogu:

```

root@DNS3:/var/cache/bind/gliwice.pawlaczkowo# ls -la
total 52
drwxrw---- 2 bind bind 4096 Jun 19 11:15 .
drwxrwxr-x 3 bind bind 4096 Jun 19 08:38 ..
-rwxrw---- 1 bind bind 363 Jun 19 00:27 Kgliwice.pawlaczkowo.pl.+013+26736.key
-rwxrw---- 1 bind bind 187 Jun 19 00:27 Kgliwice.pawlaczkowo.pl.+013+26736.private
-rwxrw---- 1 bind bind 470 Jun 19 01:06 Kgliwice.pawlaczkowo.pl.+013+56670.key
-rwxrw---- 1 bind bind 252 Jun 19 01:06 Kgliwice.pawlaczkowo.pl.+013+56670.private
-rwxrw---- 1 bind bind 470 Jun 19 01:06 Kgliwice.pawlaczkowo.pl.+013+65423.key
-rwxrw---- 1 bind bind 254 Jun 19 01:06 Kgliwice.pawlaczkowo.pl.+013+65423.private
-rwxrw---- 1 bind bind 663 Jun 19 11:15 db.gliwice.pawlaczkowo.pl
-rwxrw---- 1 bind bind 512 Jun 19 00:54 db.gliwice.pawlaczkowo.pl.jbk
-rwxrw---- 1 bind bind 2966 Jun 19 01:06 db.gliwice.pawlaczkowo.pl.signed
-rwxrw---- 1 bind bind 1738 Jun 19 01:06 db.gliwice.pawlaczkowo.pl.signed.jnl
-rwxrw---- 1 bind bind 272 Jun 18 19:03 external.gliwice.pawlaczkowo.pl

```

- db.gliwice.pawlaczkowo.pl

```

$TTL<-->7200
$INCLUDE /var/cache/bind/gliwice.pawlaczkowo/Kgliwice.pawlaczkowo.pl.+013+26736.key
$INCLUDE /var/cache/bind/gliwice.pawlaczkowo/Kgliwice.pawlaczkowo.pl.+013+56670.key
$INCLUDE /var/cache/bind/gliwice.pawlaczkowo/Kgliwice.pawlaczkowo.pl.+013+65423.key
/.../

```

- named.conf.default-zones

```

zone "gliwice.pawlaczkowo.pl" {
<----->type master;
<----->file "/var/cache/bind/gliwice.pawlaczkowo/db.gliwice.pawlaczkowo.pl";
<----->allow-update{none;};
<----->allow-transfer {none;};
<----->auto-dnssec maintain;
<----->inline-signing yes;
<----->key-directory "/var/cache/bind/gliwice.pawlaczkowo/";
};

```

- named.conf.options

```

options {
/.../
<----->dnssec-enable yes;
<----->dnssec-validation auto;
<----->key-directory "/var/cache/bind/pawlaczkowo";
/.../
};

```