4. DNS - cz. 3 - nslookup i dig (Windows Server 2012)

09.12.2012 18:25

W tej części opiszę 2 narzędzia służące do badania systemu DNS - nslookup i dig. Oba umożliwiają wysyłanie przygotowanych przez nas zapytań DNS i wyświetlanie odpowiedzi.

nslookup

Jest to konsolowy program wchodzący w skład systemu Windows. Jest on dostępny zarówno wersji serwerowej jak i desktopowej. Program działa w 2 trybach - interaktywnym i nie-interaktywnym. W trybie interaktywnym, nslookup jest uruchomiony przez cały czas. Możemy zmieniać ustawienia i odpytywać serwery o kolejne domeny, bez jego wyłączania. Uruchamiamy go za pomocą polecenia nslookup.

Pierwsze uruchomienie

Zaraz po włączeniu, nslookup wyświetla nazwę i adres IP domyślnego, rekursywnego serwera nazw z którego będzie korzystał (standardowo jest to serwer używany przez system), a następnie znak zachęty:

```
Default Server:  pdns1.vectranet.pl

Address:  95.160.170.92



>
```

Najprostsze "podpolecenie" które możemy wpisać, jest po prostu nazwą domeny o którą chcemy odpytać serwer. Musi być ona w formacie FQDN, czyli z kropką na końcu. Ponieważ domyślnym typem rekordu, o który odpytuje nslookup jest A, czyli adres IP, tylko ta informacja zostanie wyświetlona. Non-authoritative answer, oznacza że odpowiedź jest dostarczona przez serwer rekursywny.

```
> olo-web.eu.

Server:  pdns1.vectranet.pl

Address:  95.160.170.92



Non-authoritative answer:

Name:    olo-web.eu

Address:  46.41.129.59
```

Dzięki temu zapytaniu dowiedzieliśmy się, że host o adresie olo-web.eu ma adres IP 46.41.129.59.


```
> www.olo-web.eu.

Server:  pdns1.vectranet.pl

Address:  95.160.170.92



Non-authoritative answer:

Name:    olo-web.eu

Address:  46.41.129.59

Aliases:  www.olo-web.eu
```

Mimo że pytaliśmy o domenę www.olo-web.eu., została zwrócona odpowiedź dla domeny olo-web.eu., a dodatkowo pojawiło się nowe pole - Aliases. Oznacza to że w strefie znajduje się specjalny rekord - CNAME, który z jednej (sub)domeny przekierowuje na inną. W tym wypadku z www.olo-web.eu. na olo-web.eu. Serwer od razu dołącza odpowiedni rekord A dla przekierowanej (sub)domeny.

Zmiana typu rekordu

Jak już wspomniałem nslookup domyślnie odpytuje tylko o rekordy A.

Możemy to jednak zamienić za pomocą polecenia:

```
set type=[TYP REKORDU]
```

np:

- *set type=ns* - spowoduje to odpytanie o serwery DNS obsługujące daną domenę
- *set type=mx* - zwróci adres serwera SMTP przyjmującego pocztę dla danej danej domeny
- *set type=soa* - wyświetli rekord "konfiguracji domeny"

Jak widać, jedna z moich domen - http://olo-web.eu/ jest utrzymywana przez 3 serwery systemu CloudService firmy Home.pl. Oprócz adresów serwerów DNS, zostały zwrócone także odpowiadające im adresy IP.

```
> olo-web.eu.

Server:  pdns1.vectranet.pl

Address:  95.160.170.92



Non-authoritative answer:

olo-web.eu      nameserver = ns1.cloudservice.pl

olo-web.eu      nameserver = ns8.cloudservice.pl

olo-web.eu      nameserver = ns6.cloudservice.pl



ns6.cloudservice.pl     internet address = 62.129.250.8

ns1.cloudservice.pl     internet address = 62.129.250.7

ns8.cloudservice.pl     internet address = 62.129.250.9
```

Serwerem SMTP przyjmującą pocztę dla mojej domeny to natomiast mail.olo-web.eu, czyli 46.41.129.59.

```
> set type=mx

> olo-web.eu.

Server:  pdns1.vectranet.pl

Address:  95.160.170.92
```

```
Non-authoritative answer:

olo-web.eu      MX preference = 10, mail exchanger = mail.olo-web.eu



mail.olo-web.eu internet address = 46.41.129.59
```

Zamiast typu rekordu możemy wpisać słowo any, spowoduje to wyświetlenie wszystkich możliwych rekordów dla danej (sub)domeny.

Jak widać pojawiły się tutaj 2 nowe rekordy - SOA i TXT (SPF).


```
olo-web.eu

        primary name server = ns1.cloudservice.pl

        responsible mail addr = akurczyk.outlook.com

        serial  = 1352402998

        refresh = 10800 (3 hours)

        retry   = 3600 (1 hour)
```

```
        expire  = 604800 (7 days)

        default TTL = 10800 (3 hours)

olo-web.eu      text =



        "v=spf1 +a +mx -all"
```

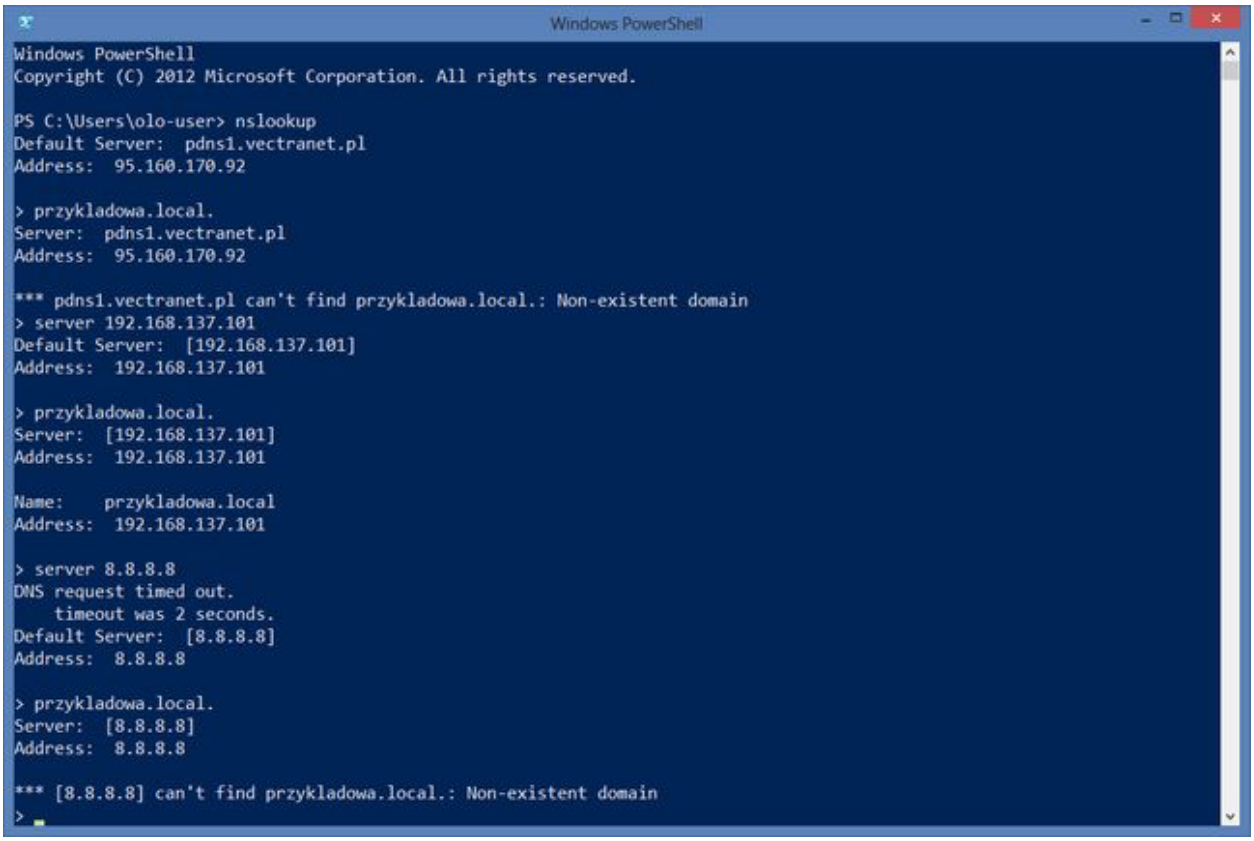
Pierwsza część to rekord SOA, zawierający "ustawienia domeny":

- *primary name server* - adres głównego serwera autorytatywnego obsługującego domenę
- *responsible mail addr* - adres e-mail admina (mój)
- *serial* - numer wersji pliku strefy, tym razem w formacie znanym tylko adminom Home.pl.
- *refresh* - czas po jakim serwery zapasowe mają pobrać nową kopię strefy
- *retry* - tyle mają zaczekać jeśli się to nei uda za pierwszym razem
- *expire* - po tym czasie muszą przestać odpowiadać na zapytania dotyczące danej domeny
- *default TTL* - kiedyś to był domyślny czas przez który serwery autorytatywne miały pamiętać rekordy w swoim cache. Obecnie (zgodnie z RFC 2308), jest to czas przez który serwer rekursywny ma pamiętać że dana (sub)domena nie istnieje.

Druga to rekord SPF, który opiszę w kolejnej części.

Zmiana odpytywanego serwera

Za pomocą polecenia server [IP/DOMENA] możemy zmienić odpytywany przez nas serwer. Możemy użyć zarówno serwerów rekursywnych jak i autorytatywnych.




```
> przykladowa.local.

Server:  pdns1.vectranet.pl

Address:  95.160.170.92


*** pdns1.vectranet.pl can't find przykladowa.local.: Non-existent domain
```

Jak widać mój domyślny serwer nazw nie zna domeny przykladowa.local. którą utworzyłem w poprzednim wpisie. Dokładnie tak samo jest w przypadku publicznego serwera nazw udostępnionego przez Google (8.8.8.8 i 8.8.4.4).

```
> server 192.168.137.101

Default Server:  [192.168.137.101]

Address:  192.168.137.101



> przykladowa.local.

Server:  [192.168.137.101]

Address:  192.168.137.101



Name:    przykladowa.local

Address:  192.168.137.101
```

Prawidłową odpowiedź dostajemy po zmianie odpytywanego serwera na ten z poprzedniego wpisu.

dig

Podobnie jak nslookup, dig jest narzędziem konsolowym. Standardowo wchodzi on w skład wielu dystrybucji Linuksa i innych Unix-ów, ale można go także zainstalować pod Windowsem (zaraz to zrobimy). Jest tworzony przez

ISC i dołączany do serwera ISC Bind. Oferuje tylko tryb nie-interaktywny, czyli jedno zapytanie = jedno uruchomienie programu. Ma trochę więcej możliwości niż nslookup.

Instalacja narzędzi z pakietu ISC Bind

1. Pobieramy i rozpakowujemy archiwum zawierające pakiet ISC Bind ze strony https://www.isc.org/software/bind/992-p1/download/bind992-p1zip.

2. Uruchamiamy program BindInstall.exe, zaznaczamy opcje Tools Only, ponieważ potrzebujemy tylko narzędzi, a nie całego serwera i klikamy Install.

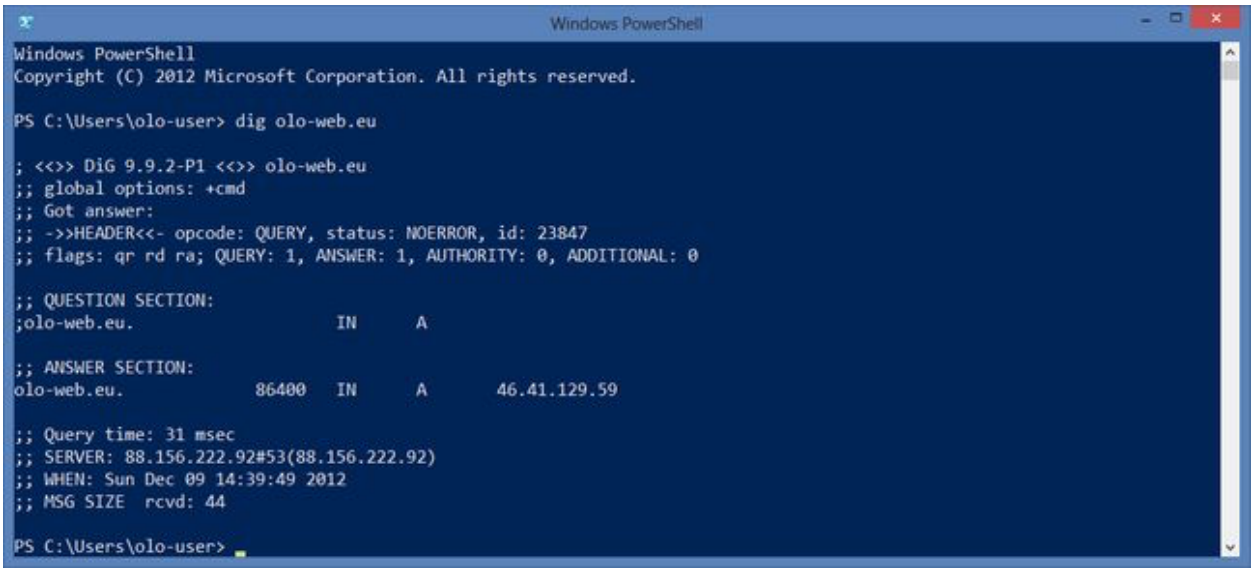
3. Wchodźmy w Panel sterowanie -> System i zabezpieczenia -> System -> Zaawansowane ustawienia systemu -> Zmienne środowiskowe.

4. W zmiennych systemowych odnajdujemy zmienną Path, klikamy Edytuj i na końcu wartości zmiennej dopisujemy ";C:\Windows\SysWOW64\dns\bin".

Teraz już możemy korzystać z polecenia dig w wierszu polecenia i PowerShellu.

Resolvowanie rekordu A

```
dig olo-web.eu.
```



Jak widać na screenie, output diga bardziej przypomina format wiadomości DNS i jest przy tym zgodny z formatem pliku strefy. Czasami jest to bardzo przydatne.

Nas najbardziej będzie interesowała sekcja odpowiedzi:

```
;; ANSWER SECTION:

olo-web.eu.             86400   IN      A       46.41.129.59
```

Inne typy rekordów

```
dig olo-web.eu IN [TYP]
```

np.

```
dig olo-web.eu IN NS
```

Właściwie to nie zawsze musimy wpisywać IN. Jest to wymagane tylko w przypadku zapytań o rekordy typu ANY. IN oznacza klasę Internet, w przypadku gdybyśmy wpisali tylko dig olo-web.eu. ANY, odpytamy serwer o rekord A dla domeny olo-web.eu, w dowolnej klasie, zamiast dowolnego typu rekordu w klasie IN.

Tutaj interesuje nas sekcja odpowiedzi oraz sekcja dodatkowa, zawierająca glue rekordy.

```
;; ANSWER SECTION:
olo-web.eu.             86400   IN      NS      ns1.cloudservice.pl.
olo-web.eu.             86400   IN      NS      ns8.cloudservice.pl.
olo-web.eu.             86400   IN      NS      ns6.cloudservice.pl.
```

```
;; ADDITIONAL SECTION:

ns6.cloudservice.pl.    3600    IN      A       62.129.250.8

ns8.cloudservice.pl.    2209    IN      A       62.129.250.9

ns1.cloudservice.pl.    3220    IN      A       62.129.250.7
```

Zmiana odpytywanego serwera

```
dig @[IP/DOMENA SERWERA] olo-web.eu.
```

np.

```
dig @ns1.cloudservice.pl olo-web.eu.
```

lub

```
@8.8.8.8 olo-web.eu.
```

PowerShell ma z tym problemy:

Ale w cmd wszystko działa OK:

Jak pisze Docet, możemy zacytować odpowiedni fragment polecenia, aby zadziałało w PowerShellu:

```
dig '@8.8.8.8' olo-web.eu.
```

Tutaj pojawia się także AUTHORITY SECTION, w której znajdują się serwery autorytatywne obsługujące domenę. Ta sekcja jest dołączana tylko przez serwery autorytatywne.

Inne zapytania

Napisałem że dig oferuje więcej możliwości niż nslookup, więc poniżej przedstawiam przykłady innych zapytań:

- *dig olo-web.eu. +short* - pokaże tylko adres IP. przydatne przy programowaniu w bashu.
- *dig olo-web.eu. +trace* - odpyta wszystkie serwery w dół hierarchii, aż dojdzie do serwera obsługującego moją domenę i wyświetli wszystkie te odpowiedzi. przydatne do sprawdzania delegacji, gdy zmiany w cache jeszcze nie nastąpią (to może potrwać nawet 24 h, a według protokołu 68 lat).
- *dig olo-web.eu. IN AXFR* - przetransferuje i wyświetli cały plik strefy (jeśli nie zablokowane na serwerze)

- *dig olo-web.eu. IN IXFR=[SERIAL*] - przetransferuje i wyświetli zmiany w strefie od określonego numeru SERIAL - numeru wersji pliku strefy.
- *dig -x 46.41.129.59* - zamieni adres IP na domenę. więcej o tym w następnej części.
- *dig -f plik.txt* - wykona zapytania z pliku txt
- *dig* - wyświetli adresy root serverów
- *dig -help* - wyświetli wszystkie możliwe opcje