

5. DNS - cz. 4 - Odwrócony DNS w Windows Server 2012

[Strona główna](#) > @okokok > 5. DNS - cz. 4 - Odwrócony DNS w Windows Server 2012

15.12.2012 18:13

Reverse DNS umożliwia zamianę adresów IP na domeny, czyli tak zwaną odwrotną translację. Dzięki temu możliwe jest sprawdzenie czy host o danym adresie IP należy do danej domeny. Dawniej wykorzystywano go do sprawdzenia, czy serwer SMTP wysyłający e-mail faktycznie znajduje się w domenie z której go wysyła. Takie rozwiązanie zakłada że każdy komputer znajdujący się w domenie może wysyłać w jej imieniu pocztę, oraz że serwer SMTP znajduje się w naszej domenie. Z powodu tych ograniczeń, obecnie do celu sprawdzenia nadawcy podczas odbioru wiadomości e-mail wykorzystuje się SPF oraz coraz częściej DKIM. Mimo to revDNS jest nadal wykorzystywany do zamiany adresów IP na hostname. Rekord SPF będzie opisane w dalszej części. Na razie skupmy się jednak na revDNS.

Odwrócony DNS wykorzystuje specjalne domeny - in-addr.arpa, dla adresów IPv4 i ip6.arpa dla IPv6, oraz specjalny typ rekordu - PTR.

W przypadku IPv4, adres revDNS ma format odwróconego adresu IP z końcówką .in-addr.arpa, np. 1.0.168.192.in-addr.arpa, dla adresu 192.168.0.1. Z tego względu teoretycznie wydelegować można tylko fragmenty po 256, 65 536 lub 16 777 216 adresów. W praktyce jednak, dzięki wykorzystaniu aliasów CNAME, możliwa jest delegacja dowolnych fragmentów.



Fragmenty te, lub całe strefy są delegowana przez operatorów udostępniających nam podsieć adresów lub jeśli mamy podsieć niezależną od operatora, od RIPE lub innego rejestratora.

Jak już wspomniałem, w strefie revDNS znajdują się rekordy PTR. Jako jedyny "parametr", przyjmują one po prostu adres domeny, na który chcemy "zamienić" adres IP.

Poniżej przykładowy plik strefy:

Z



```
1. 137.168.192.in-addr.arpa.      3600 IN SOA ns1.przykladowa.local.  
hostmaster.przykladowa.local. 2012120500 86400 900 2592000 3600  
  
2. 137.168.192.in-addr.arpa.      3600 IN NS  ns1.przykladowa.local.  
  
3. 137.168.192.in-addr.arpa.      3600 IN NS  ns2.przykladowa.local.  
  
4. 1.137.168.192.in-addr.arpa.    3600 IN PTR router.przykladowa.local.  
  
5. 101.137.168.192.in-addr.arpa.  3600 IN PTR server1.przykladowa.local.  
  
6. 102.137.168.192.in-addr.arpa.  3600 IN PTR server1.przykladowa.local.
```

```
7. 201.137.168.192.in-addr.arpa. 3600 IN PTR client1.przykladowa.local.
8. 202.137.168.192.in-addr.arpa. 3600 IN PTR client2.przykladowa.local.
9. 203.137.168.192.in-addr.arpa. 3600 IN PTR client3.przykladowa.local.
10. 204.137.168.192.in-addr.arpa. 3600 IN PTR client4.przykladowa.local.
```

- 1. Standardowy rekord z ustawianiami danej strefy. Użyliśmy serwera DNS i adresu e-mail z poza strefy - ns1.przykladowa.local. i hostmaster.przykladowa.local.
- 2 i 3. Adresy serwerów DNS utrzymujących naszą strefę.
- 4. Rekord PTR "zamieniający" adres IP 192.168.137.2 na router.przykladowa.local.
- 5 i 6. Rekordy PTR serwerów.
- 7-10. Rekordy PTR dla innych komputerów w strefie.

Oraz w wersji skróconej:

```
@      SOA ns1.przykladowa.local. hostmaster.przykladowa.local. 1d 15m 30d 1h

      NS ns1.przykladowa.local.

      NS ns2.przykladowa.local.

1     PTR router.przykladowa.local.
```


server2.przykladowa.local.. Mają tylko subdomeny dla pełnionych przez nie funkcji - ns1.przykladowa.local., www.przykladowa.local., mx.przykladowa.local. itp. dla pierwszego serwera, oraz ns2.przykladowa.local. dla drugiego serwera. Zanim zajmiemy się domeną reverse lookup, musimy dodać odpowiednie rekordy - router.przykladowa.local., server1.przykladowa.local., server2.przykladowa.local., client1.przykladowa.local., client2.przykladowa.local., client3.przykladowa.local., oraz client4.przykladowa.local, w normalnej strefie. Możemy także ustawić tym komputerom hostname (nazwę komputera), na własnie te adresy.



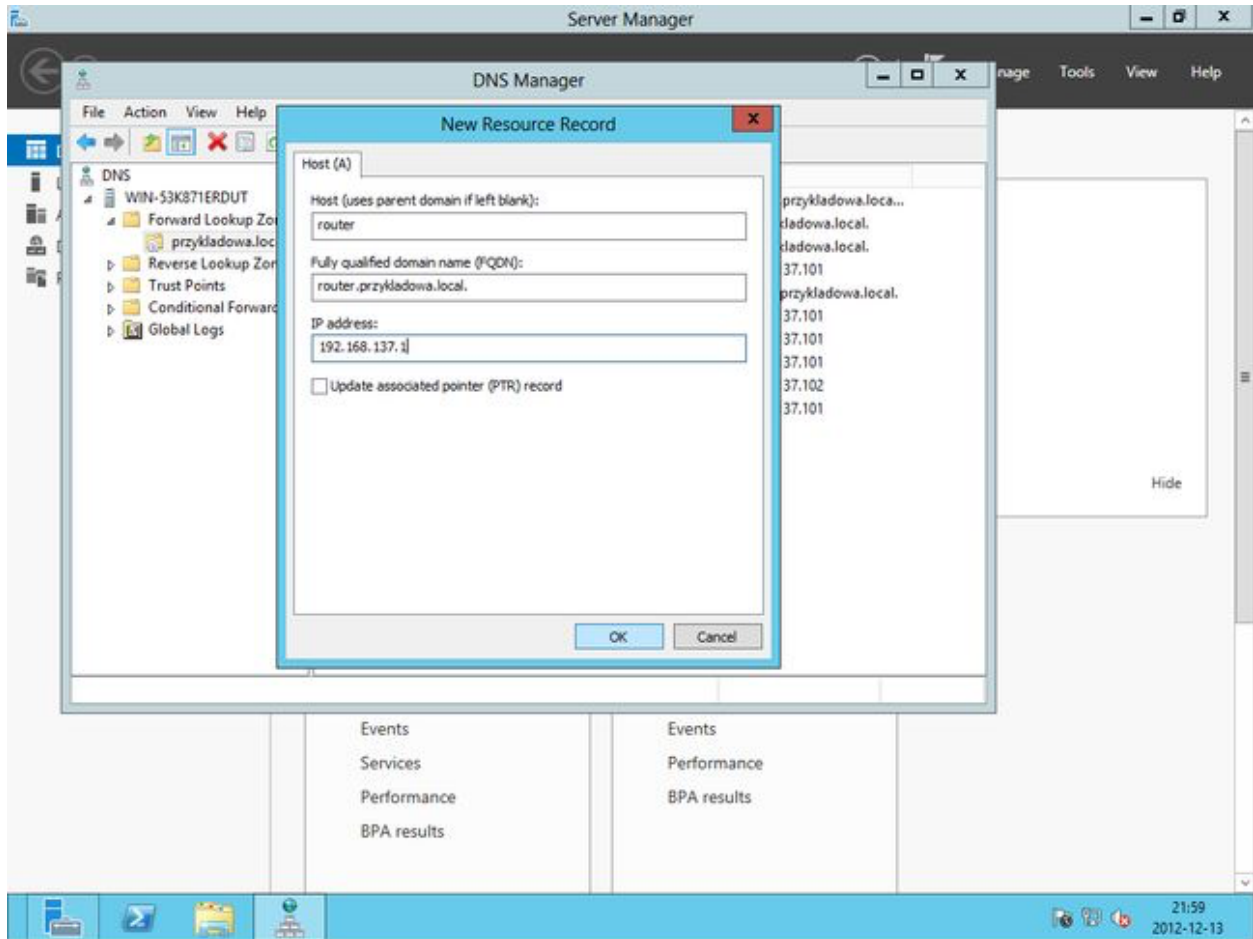
Gdybyśmy korzystali z Active Directory, wpisy te zostały by utworzone automatycznie. Możliwe było by także automatyczne utworzenie strefy revDNS i dodanie odpowiednich rekordów.

1. Uruchamiamy Server Manage i z menu Tools wybieramy DNS.
2. Przechodzimy do strefy przykladowa.local. i klikamy Add Record.
3. Jako typ rekordu wybieramy Host (A or AAAA) i klikamy Create Record...

4. Dodajemy rekordy i wracamy do DNS Managera.



- router.przykladowa.local. - 192.168.137.1
- server1.przykladowa.local. - 192.168.137.101
- server2.przykladowa.local. - 192.168.137.102
- client1.przykladowa.local. - 192.168.137.201
- client2.przykladowa.local. - 192.168.137.202
- client3.przykladowa.local. - 192.168.137.203
- client4.przykladowa.local. - 192.168.137.204



5. Obecnie nasza strefa wygląda tak:

Tworzenie strefy revDNS

1. 2x klikamy na Reverse Lookup Zones, a następnie wybieramy New Zone.

2. Klikamy Next >, wybieramy Primary zone i znów klikamy Next >.

3. Wybieramy IPv4 Reverse Lookup Zone i podajemy prefix sieci. Może się on składać z 1, 2 lub 3 oktetów. Najczęściej jest to część sieci adresu IP. W moim przypadku: 192.168.137.

4. Pozostawiamy domyślną nazwę pliku strefy oraz, również domyślnie, nie pozwalamy na dynamiczne aktualizacja strefy.

5. Zamykamy kreator

Zmiana NS-ów

1. 2x klikamy na rekord NS, a następnie Edit...

2. Wpisujemy adres domenalny serwera DNS - ns1.przykladowa.local. i podajemy jego adres IP, w moim przypadku jest to 192.168.137.101.

3. Klikamy Add i dodajemy rekord kolejnego serwera - ns2.przykladowa.local. U mnie ma on IP 192.168.137.102. Tym razem wyświetli się błąd, bo serwer nie jest jeszcze skonfigurowany do obsługi tej domeny.

4. Przechodzimy do zakładki Start of Authority (SOA) i zmieniamy wartość pola Primary server na ns1.przykladowa.local.

Dodawanie rekordów PTR

1. Klikamy PPM na puste miejsce na liście i z menu kontekstowego wybieramy New Pointer (PTR)...

2. Dodajemy rekordy dla kolejnych adresów:

- 192.168.137.1 - router.przykladowa.local.
- 192.168.137.101 - server1.przykladowa.local.
- 192.168.137.102 - server2.przykladowa.local.
- 192.168.137.201 - client1.przykladowa.local.
- 192.168.137.202 - client2.przykladowa.local.
- 192.168.137.203 - client3.przykladowa.local.
- 192.168.137.204 - client4.przykladowa.local.

Dodawanie domeny do drugiego serwera

1. Wchodzimy w Server manager na drugim serwerze i z menu Tools, wybieramy DNS.

2. Z menu po lewej stronie wybieramy Reverse Lookup Zones i klikamy na New Zone.

3. Klikamy Next >, Secondary zone i ponownie Next >.

4. Wybieramy IPv4 Reverse Lookup Zone i podajemy prefix sieci - 192.168.137.

5. Wpisujemy adres IP pierwszego serwera. U mnie jest to 192.168.137.101.

6. Zamykamy kreator

Testujemy