

# 3. DNS - cz. 2 - Konfiguracja usługi w Windows Server 2012

[Strona główna](#) > @okokok > 3. DNS - cz. 2 - Konfiguracja usługi w Windows Server 2012  
08.12.2012 14:34

W **poprzedniej części** opisałem jak działa system DNS oraz jak zainstalować rolę serwera DNS w Windows Server 2012. Dzisiaj chciałbym pokazać jak pod Windows Server 2012 dodawać i zarządzać strefami DNS.

## Nasza konfiguracja będzie następująca:

Ponieważ zdobyłem Windows 8 w wersji Enterprise i mam już dostęp do HYPER-V Client., utworzyłem za jego pomocą 2 wirtualne maszyny i zainstalowałem na nich Windows Server 2012 oraz rolę serwera DNS.



Obie maszyny się przyłączone do wirtualnej sieci utworzonej przez HYPER-V. Pierwsza ma IP 192.168.137.101, druga natomiast 192.168.137.102. Przyłączony do niej jest także mój system gospodarza z IP 192.168.137.1, pełniący jednocześnie funkcję bramy domyślnej dla obu maszyn.

Na pierwszej maszynie dodamy, w trybie master, strefę przykładowa.local. Utworzymy w niej:

- 2 rekordy NS, zawierające adresy domenowe serwerów autorytatywnych obsługujących naszą domenę;
- odpowiadające tym adresom domenowym serwerów NS rekordy A, zawierające adres IP (tak zwane glue rekordy);

- rekord MX z adresem domenowy serwera SMTP przyjmującego pocztę dla naszej domeny;
- odpowiedni glue rekord dla rekordu MX;
- oraz 3 osobne rekordy A - dla domeny głównej, dla subdomeny www oraz dla subdomeny ftp.

Na drugiej maszynie dodamy tą samą strefę - przykladowa.local. Będzie one jednak działała w trybie slave.

## **Konfiguracja pierwszego serwera w trybie master:**

1. Uruchamiamy Server Manager i wybieramy z menu Tools -> DNS.

2. W DNS Manager, klikamy 2x na nasz serwer, a następnie na Forward Lookup Zones.

3. Klikamy na ostatni przycisk na pasku - New Zone, a po pojawieniu się okna kreatora, Next >.

4. Wybieramy typ serwera. Primary zone to serwer typu master/główny.

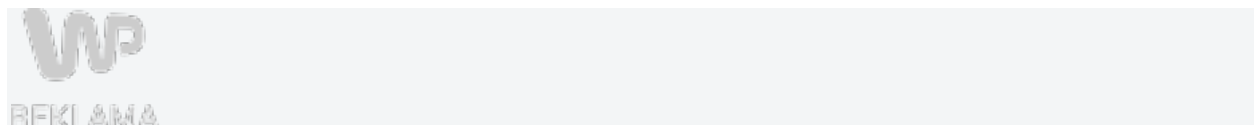
5. Jako nazwę domeny wybieramy przykładowa.local.

6. Nazwę pliku strefy pozostawiamy domyślną.

7. Nie pozwalamy na dynamiczną aktualizację strefy (DDNS).

8. Zatwierdzamy klikając Finish.

9. Klikamy 2x na pozycję Forward Lookup Zones, a następnie na przykladowa.local. w menu po lewej stronie.



Na poniższym screenie widzimy 2 rekordy znajdujące się aktualnie w naszej strefie. Oprócz tego do rekordu NS dołączony jest ukryty rekord glue, typu A, zawierający jego adres IP.

Nie wiem dlaczego (może ktoś wyjaśni to w komentarzach, hostname?), ale Windows użył adresu win-XXXXXXX. jako głównego serwera DNS oraz hostmaster. jako adresu e-mail administratora. Kropka na końcu każdego adresu oznacza że jest to adres FQDN (Fully Qualified Domain Name), a więc

pełny adres. Nie możemy go dopełnić "adresem" strefy. Wypadało by więc że nasz serwer jest bezpośrednio wpięty do strefy root. :)

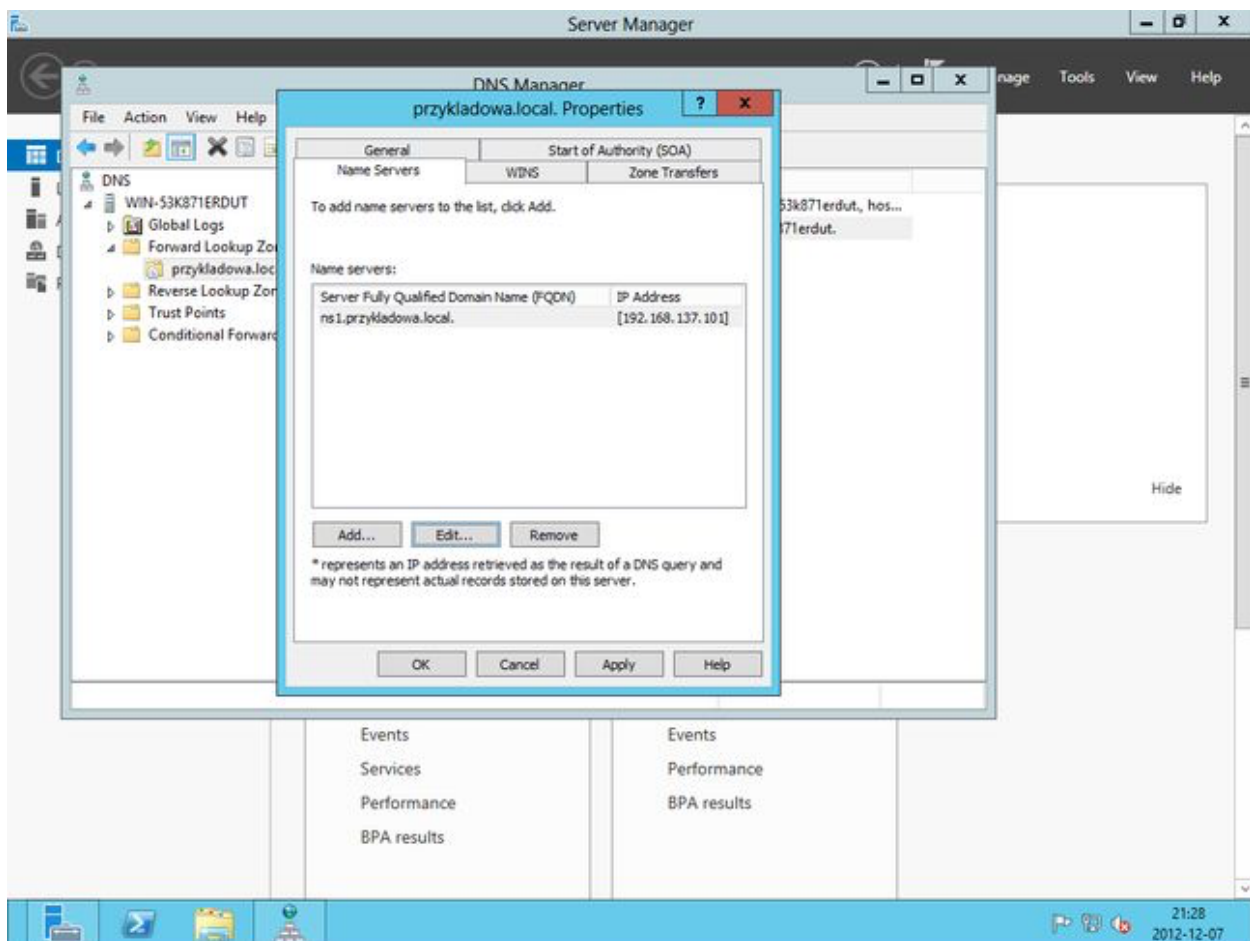
Niestety tak nie jest i musimy to zmienić, przy okazji na coś bardziej przejrzystego.



10. Klikamy 2x na rekord Name Server (NS), a następnie edytujemy jedyny na liście wpis serwera nazw.

11. Wpisujemy ns1.przykladowa.local., a następnie klikamy 2 razy na pole poniżej i wpisujemy adres IP. W moim przypadku jest to adres 192.168.137.101.

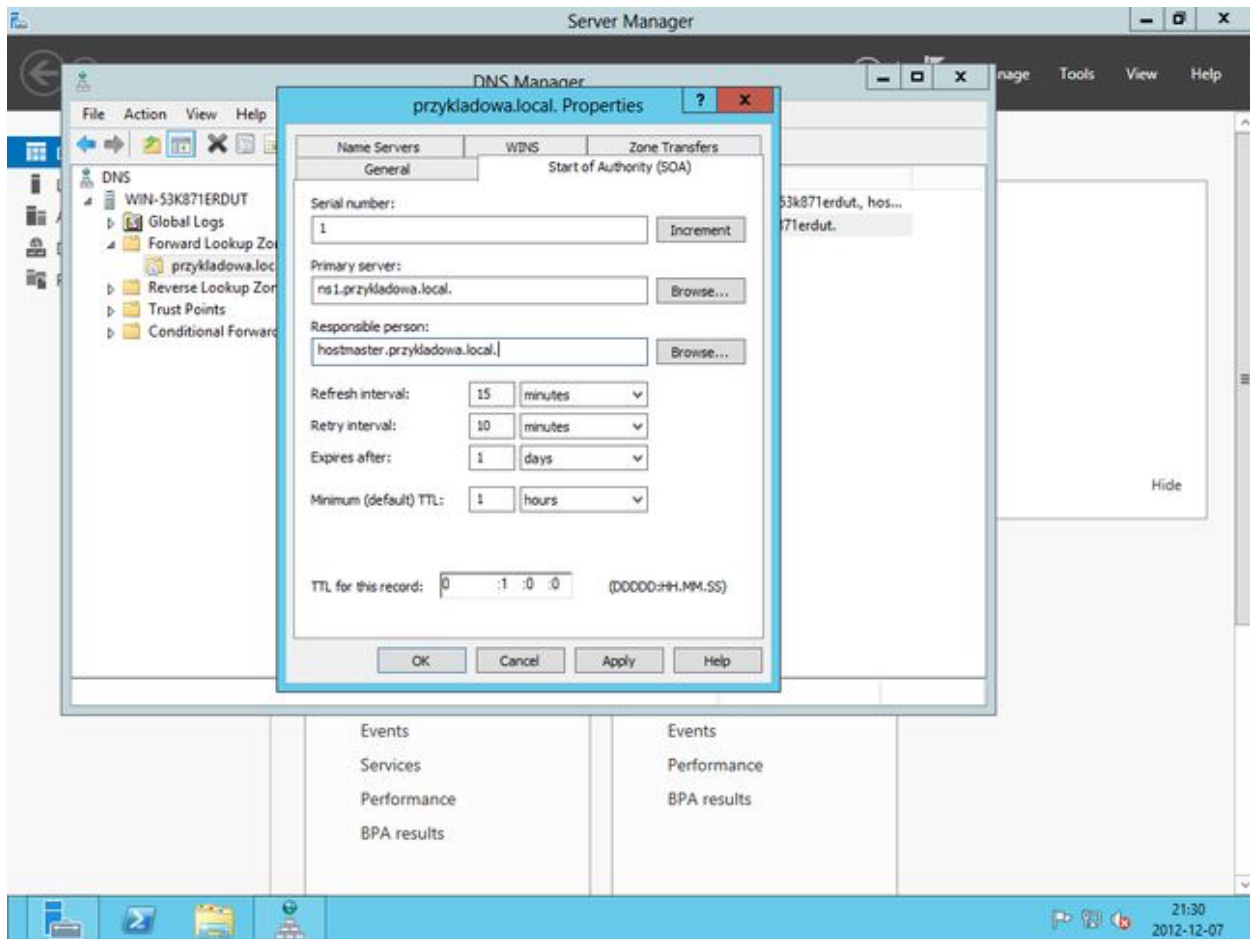
Teraz nasza lista serwerów DNS wygląda tak:



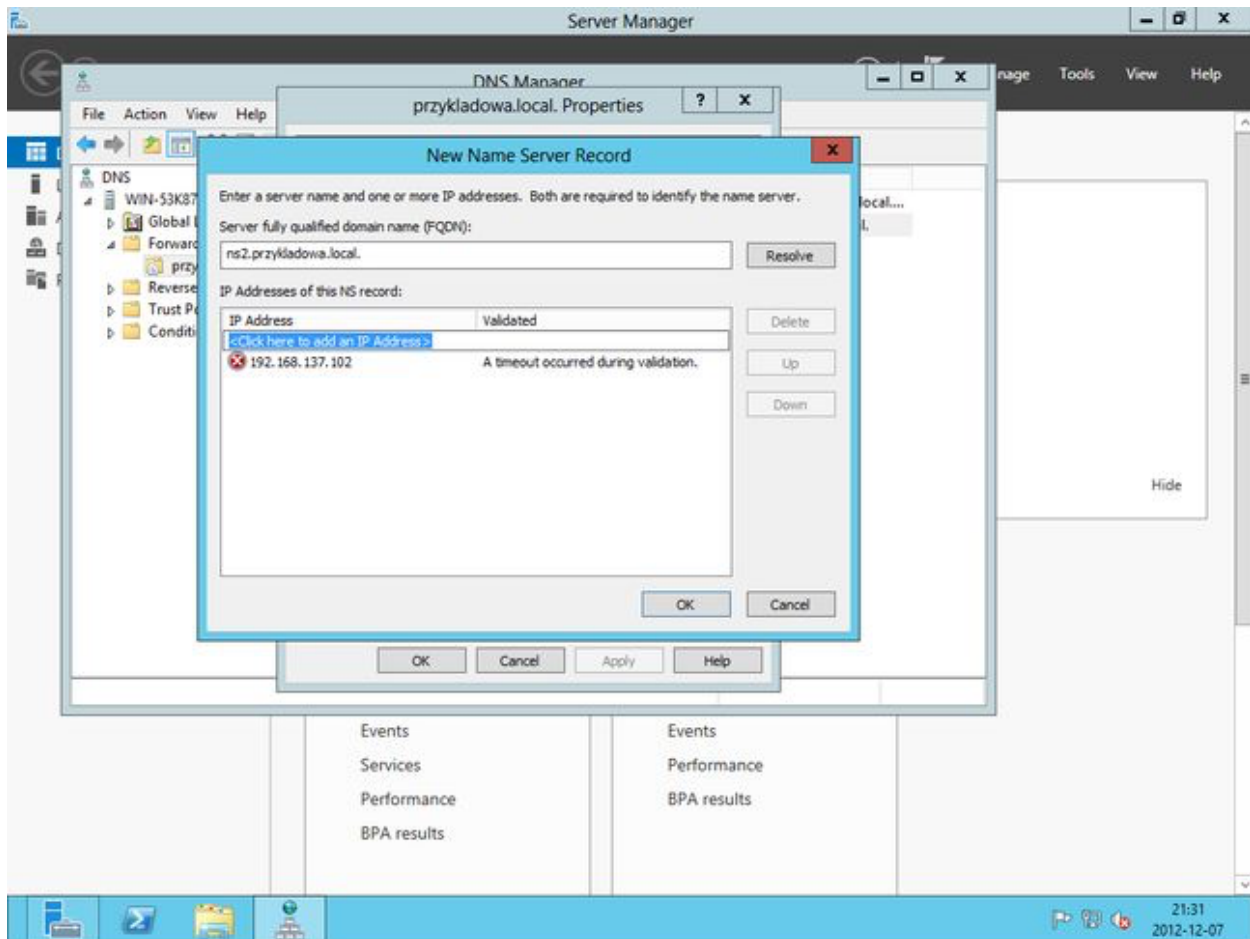
Za chwilę dopiszemy do niej serwer zapasowy.



12. Po zatwierdzeniu zmian w rekordzie NS, nie zamykamy głównego okna ustawień strefy, tylko przechodzimy do zakładki Start of Authority (SOA) i zamieniamy zawartość pola Primary server, wpisując adres naszego głównego serwera nazw - ns1.przykladowa.local. oraz zmieniamy adres e-mail administratora na hostmaster.przykladowa.local. Możemy tam właściwie wpisać jakikolwiek adres e-mail, pamiętając tylko żeby małpę zamienić na kropkę. Jeśli w części nazwy użytkownika, adresu e-mail, występuje kropka, należy ją poprzedzić znakiem "\" np. aleksander\kurczyk@olo-web.eu.



13. Wracamy do zakładki Name Servers i dodajemy kolejny rekord - ns2.przykladowa.local. W polu IP Address wpisujemy adres naszego drugiego name servera. W moim przypadku jest to 192.168.137.102. W chwili wykonywania tego screena, druga maszyna wirtualna była wyłączona, a Windows to wykrył. Jeśli była by włączona, i tak wyświetlał by się błąd, ponieważ maszyna nie była by skonfigurowana do obsługi domeny przykladowa.local.



Teraz mamy już oba serwery nazw na liście:

Lista wszystkich rekordów w strefie wygląda tak:

Nie są wyświetlane tutaj odpowiednie rekordy glue zawierające adresy IP naszych serwerów. W rzeczywistości są 2.



Dodajmy teraz trochę innych rekordów - serwer pocztowy oraz kilka zwykłych adresów - dla domeny głównej i subdomen www oraz ftp.

13. W tym celu klikamy na przedostatnią pozycję w menu - New Record i wybieramy pozycję Max Exchanger (MX).

14. Pierwsze pole - Host or child domain pozostawiamy puste. W końcu chcemy dodać serwer mailowy dla całej domeny a nie tylko dla jednej subdomeny. W drugim podajemy adres naszego mail servera - mx.przykladowa.local. Pole priorytetu pozostawiamy bez zmian i klikamy OK.

W kolejnej części artykułu opiszę reverse DNS i rekordy PTR, bez których maile w obecnych czasach będą odrzucane przez filtry antyspamowe.

15. Tym razem z listy wybieramy rekord typu Host (A or AAAA) i podobnie jak poprzednio pole "subdomeny" pozostawiamy puste i tylko wpisujemy IP.

16. Analogicznie robimy w przypadku subdomen www i ftp.

Teraz nasza strefa wygląda tak:

Musimy jeszcze ją przeładować - zapisać zmiany.

17. Klikamy PPM w puste miejsce na liście rekordów i wybieramy z menu Reload, a następnie zatwierdzamy OK.

18. Za pomocą narzędzia nslookup (opiszę je dokładniej później) testujemy czy wszystko jest OK.

## **Konfiguracja drugiego serwera w trybie slave:**

1. Na drugim serwerze włączamy Server Manager, klikamy Tools, a następnie DNS, aby uruchomić DNS Manager.

2. Klikamy 2x na nasz jedyny na liście serwer, następnie na Forward Lookup Zones i klikamy New Zone.

3. Klikamy Next > i wybieramy Secondary zone.

4. Wpisujemy jej nazwę - przykladowa.local.

5. Dodajemy adres IP serwera głównego.

6. Klikamy Next > oraz Finish.

7. Wybieramy Forward Lookup Zones, a następnie przykładowa.local.

8. Jeśli coś by nie zadziało i zamiast listy rekordów wyświetlił się błąd, musimy tylko "odświeżyć" strefę, klikając PPM na jej nazwę, w menu po lewej stronie i wybierając Refresh.

9. Sprawdzamy czy wszystko jest OK.

### **Zmiany w strefie i czas propagacji:**

Podczas tworzenia strefy zrobiłem błąd - nie dodałem odpowiedniego "glue" rekordu dla serwera mailowego - mx.przykladowa.local. Dodamy go teraz i przy okazji zobaczymy jak szybko propagują się zmiany.

Jak widać subdomena mx.przykladowa.local. nie istnieje, a wersja strefy (pole serial w rekordzie SOA) to 12.

Dodamy teraz odpowiedni rekord A dla subdomeny mx.przykladowa.local.

1. Na pierwszym serwerze wchodzimy w Server Manager -> Tools -> DNS.

2. Wybieramy z menu Forward Lookup Zones -> przykladowa.local.

3. Klikamy przycisk New Record.

4. W pole subdomeny, wpisujemy mx oraz podajemy IP naszego serwera mailowego.

Na poniższym screenie widać że zmiany w strefie nastąpiły od razu. Automatycznie został także wykonany transfer strefy, najprawdopodobniej za pomocą mechanizmu Notify.

Uległ zmianie numer wersji strefy - serial w rekordzie SOA. Gdyby tak się nie stało, drugi serwer nie pobrał by kopii myśląc że nic się nie zmieniło.

## Delegacja domeny od rejestratora

@krendzeL w komentarzach pod [poprzednim wpisem](#), zapytał jak wydelegować na taki serwer domenę od dostawcy.

Gdybyśmy zamiast domeny przykładowa.local. użyli jakiejś z publicznego systemu DNS, a serwery miały by publiczne adresy IP, moglibyśmy wydelegować tą domenę na nasze serwery i wtedy była by ona dostępna dla każdego. Teraz można o nią odpytywać tylko 2 serwery z prywatnymi adresami IP.

Delegacja na zewnętrzne serwery w przypadku panelu Home.pl wygląda tak:

W następnych częściach chciałbym opisać: narzędzie nslookup i dig (z pakietu ISC Bind), rekordy PTR i TXT oraz łączenie serwerów i zdalną konsolę MMC, aby zarządzać nimi z jednego miejsca.