2. DNS - cz. 1 - Działanie systemu i instalacja usługi w Windows Server 2012

05.12.2012 20:07

W poprzedniej części tej serii opisałem jak szybko zainstalować Windows Server 2012 w maszynie wirtualnej. Teraz chciałbym przedstawić jak działa system DNS oraz pokazać jak zainstalować na naszym serwerze odpowiednią rolę.

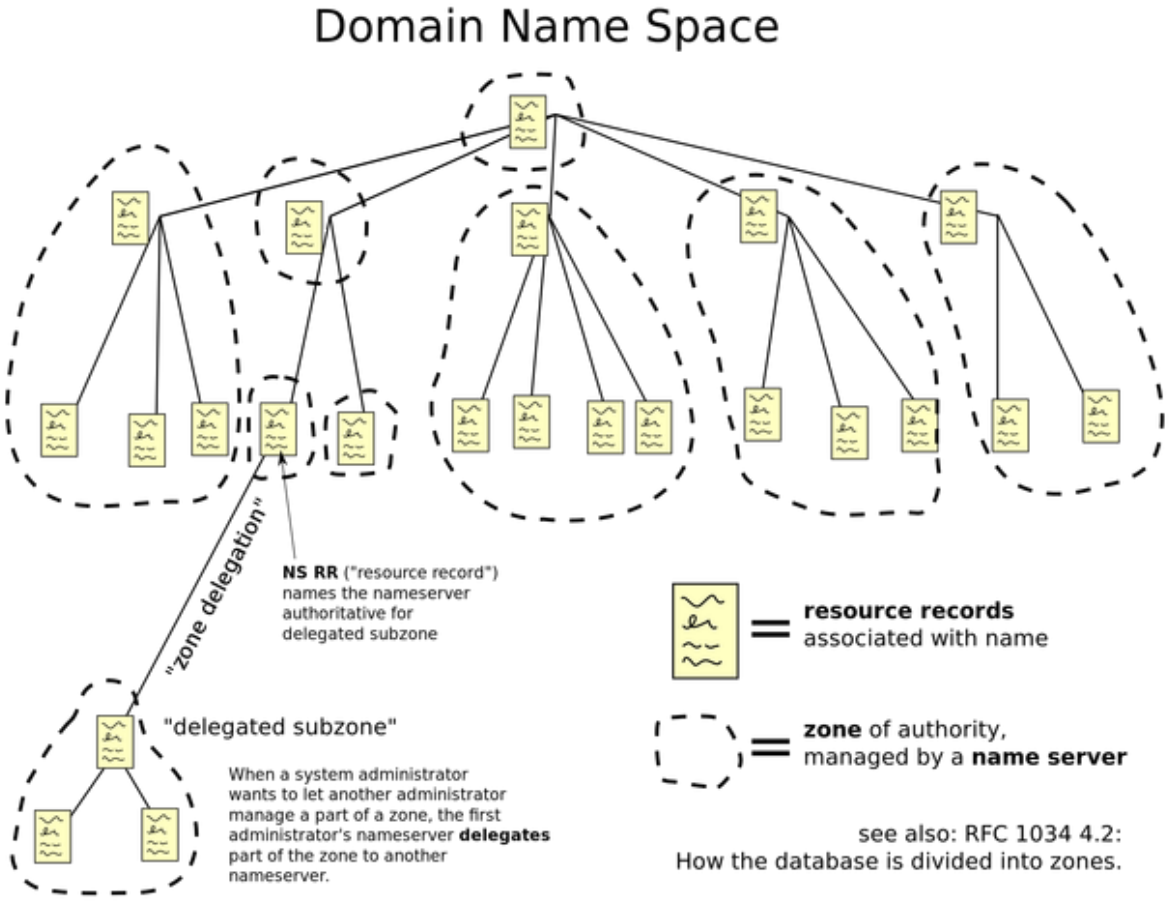
Co to jest DNS?

DNS - Domain Name System, jest wielką rozproszoną bazą danych, umożliwiającą zamianę nazw domen na adresy IP serwerów.

Hierarchia

System DNS składa się z hierarchii stref. Na szczycie hierarchii znajduje się strefa root - ".". Na mocy umowy CRADA z rządem USA, zarządza nią organizacja IANA. Ze strefy root wydelegowane są strefy niższego poziomu - domen TLD - Top Level Domain, np. "com.", "org.", "net.", "info.", "pl.", "eu.", "ru.", "su.", itp. Domeny TLD dzielą się na domeny funkcjonalne gTLD (np. "com.", "org.", "net." i "info.") i krajowe - ccTLD (np. "pl.", "eu.", "ru." i "su."). Za zarządzanie polską domeną TLD - "pl." odpowiada NASK - Naukowa i Akademicka Sieć Komputerowa. Chociaż w rzeczywistości jest to jedna strefa, w Polskiej domenie również istnieje podział na domeny drugiego poziomu - SLD - Second Level Domain. Są to domeny funkcjonalne (np. "com.pl." i

"edu.pl.") i regionalne (np. "klodzko.pl." i "wroc.pl."). Każdy właściciel domeny może utworzyć w niej wiele delegacji do stref kolejnych niższych poziomów i/lub przypisać subdomeny do poszczególnych hostów/serwerów. Można w ten sposób utworzyć do 128 poziomów zagnieżdżeń.



Rodzaje serwerów

Serwery autorytatywne

- są to serwery utrzymujące domeny/strefy i mające w swojej bazie informacje tylko na temat rekordów znajdujących się w utrzymywanej przez nie strefie.

Istnieją 2 rodzaje serwerów autorytatywnych - główne i zapasowe. Na serwerach głównych można wprowadzać zmiany. Serwery zapasowe, w określonym (w rekordzie SOA) czasie odpytują serwery główne i jeżeli strefa znajdująca się na serwerze głównym ma inny identyfikator niż kopia przechowywana na serwerze zapasowym, za pomocą zapytania AXFR, transferują całą strefę.

Serwery rekursywne

- są to serwery udostępniane najczęściej przez dostawców Internetu. Każdy komputer korzystający z DNS musi korzystać z co najmniej jednego serwera rekursywnego. Taki serwer, początkowo, posiada informacje tylko nt. autorytatywnych serwerów strefy root - root serwerów. Po otrzymaniu zapytania od użytkownika, odpytuje on, zgodnie z hierarchią, serwery autorytatywne kolejnych stref, zapisuje ich adresy w cache, a na końcu, gdy otrzyma już ostateczny adres hosta, odpowiada użytkownikowi jego adresem IP. Następny użytkownik pytający o tą samą domenę dostanie odpowiedź prosto z cache.

Pliki stref i rekordy

Każdy serwer autorytatywny danej strefy musi posiadać "plik strefy" tej strefy. Jego format jest standardem i został zdefiniowany w RFC 1035. Pod Linuksem, gdy korzystamy z ISC Bind (najpopularniejszego serwera od początku istnienia systemu DNS), plik strefy musimy edytować ręcznie (pomijam tutaj DDNS). Pod Windowsem mamy do dyspozycji ładny graficzny manager. Plik strefy, a właściwie to strefa w ogóle, składa się z rekordów. Każdy rekord z kolei składa się z nazwy (sub)domeny której dotyczy ten rekord (np. "przykladowa.pl",

"www.przykladowa.pl" lub "mail.przykladowa.pl"), typu tego rekordu oraz parametrów specyficznych dla danego rekordu. Najpopularniejsze z nich to:

SOA - Start Of Authority

- jest to rekord zawierający "ustawienia domeny". Zawsze musi znajdować się na początku strefy. Przyjmuje 7 parametrów:

- Adres domenowy głównego, autorytatywnego serwera DNS danej strefy (np. "ns1.przykladowa.pl");
- Adres e-mail administratora, z zamienioną małpą na kropkę (np. "admin.przykladowa.pl");
- Numer wersji pliku strefy (zazwyczaj w formie daty i numery poprawki w danym dniu, ale w Windows Server 2012 jest to po prostu numer poprawki);
- Czas który musi upłynąć między kolejnymi transferami strefy na serwery zapasowe;
- Czas po którym serwer zapasowy ma ponowić próbę transferu, w przypadku jego niepowodzenia;
- Czas po upływie którego, serwer zapasowy ma przestać odpowiadać na zapytania, w przypadku niepowodzenia transferu;
- Czas przez jaki serwer rekursywny ma pamiętać że (sub)domena, o którą odpytywał serwer autorytatywny, nie istnieje.

NS - Name Server

- Adres autorytatywnego serwera nazw danej strefy. Rekordów NS dla danej strefy może być kilka. Każdy z nich przyjmuje tylko 1 parametr i jest nim adres

domenowy serwera. Jeśli adres tego serwera jest wewnątrz strefy, np. "ns1.przykladowa.pl", musi istnieć dla niego dodatkowy rekord A, zawierający adres IP tego serwera, jeśli serwer DNS jest poza naszą strefą, np. "ns1.przykladowa.com", to nie musimy, a nawet nie możemy dodawać takiego rekordu.

Rekordy NS używane są także do delegowania części strefy do strefy niższego poziomu (np. z "przykladowa.pl" do "podstrefa.przykladowa.pl"). Dodaje się wtedy rekordy NS dla każdego serwera nazw obsługującego daną strefę, oraz, podobnie jak wyżej, gdy ich adresy IP znajdują się w delegowanej strefie, odpowiednie rekordy A.

MX - Mail Exchanger

- Adres serwera mailowego, przyjmującego pocztę dla danej domeny. Tak jak w przypadku rekordu NS, rekordów w danej strefie może być kilka i adres serwera mailowego musi być adresem domenowy, więc jeśli znajduje się on w naszej strefie, musi istnieć dodatkowy rekord A zawierający adres IP tego serwera. Rekord ten przyjmuje jeszcze 1 parametr - priorytet. Preferowane są serwery z niższym priorytetem. Te z wyższym są wykorzystywane tylko jeśli te preferowane nie działają.

A - Address

- Jak już wcześniej wspomniałem, rekord A służy do właściwej zamiany adresu domenowego (subdomeny) na adres IP hosta. Rekord A, a właściwie każdy rekord może być dodawany nie tylko do subdomeny, ale także do domeny głównej, np. "www.przykladowa.pl" i "przykladowa.pl".

AAAA - IPv6 Address

- Podobnie jak A, jednak w tym wypadku jest to adres IPv6.

Przykładowy plik strefy

Przykładowy plik strefy bez żadnych ułatwień będzie wyglądał tak:


```
01. przykladowa.pl.                 3600 IN SOA ns1.przykladowa.pl.
admin.przykladowa.pl. 2012120500 86400 900 2592000 3600


02. przykladowa.pl.                 3600 IN NS  ns1.przykladowa.pl.

03. przykladowa.pl.                 3600 IN NS  ns2.przykladowa.pl.


04. ns1.przykladowa.pl.             3600 IN A   10.10.10.10

05. ns2.przykladowa.pl.             3600 IN A   192.168.100.100


06. przykladowa.pl.                 3600 IN MX  10 mx.przykladowa.pl.

07. mx.przykladowa.pl.              3600 IN A   10.222.222.222


08. przykladowa.pl.                 3600 IN A   172.20.40.40
```

```
09. www.przykladowa.pl.             3600 IN A   172.20.40.40

10. ftp.przykladowa.pl.             3600 IN A   172.20.40.40

11. webmail.przykladowa.pl.         3600 IN A   172.20.40.40



12. podstrefa.przykladowa.pl        3600 IN NS  ns1.podstrefa.przykladowa.pl.

13. podstrefa.przykladowa.pl        3600 IN NS  ns2.podstrefa.przykladowa.pl.



14. ns1.podstrefa.przykladowa.pl    3600 IN A   192.168.90.91

15. ns2.podstrefa.przykladowa.pl    3600 IN A   192.168.90.92
```

[list] [item]*01* - Rekord SOA z "ustawieniami domeny":

- "ns1.przykladowa.pl." jest głównym, autorytatywnym serwerem nazw tej domeny;
- "admin.przykladowa.pl." jest adresem e-mail administratora;
- "2012120500" to numer wersji pliku strefy;
- "86400" - 1 dzień, to czas, w sekundach, po upływie którego, serwery zapasowe mają przetransferować strefę (pobrać jej kopię);
- "900" - 15 min, to czas po jakim serwery zapasowe mają powtórzyć próbę transferu strefy, jeśli poprzednia się nie powiedzie;
- Jeśli w ciągu "2592000" - 30 dni serwerom zapasowym nie uda się nawiązać komunikacji z serwerem głównym, muszą przestać odpowiadać na zapytania dotyczące tej strefy;
- "3600", to czas przez jaki serwer rekursywny (dostawcy internetu) ma pamiętać że dana (sub)domena nie istnieje.

[/item] [item]*02 i 03* - Rekordy określające serwery nazw obsługujące tą strefę[/item] [item]*04 i 05* - Adres IP serwerów nazw z linii 02 i 03[/item] [item]*06 i 07* - Serwer SMTP przyjmujący maile dla domeny "przykladowa.pl." oraz jego adres IP[/item] [item]*od 08 do 11* - Adresy IP dla domeny głównej i subdomen. Wszystkie wskazują na ten sam serwer.[/item] [item]*12 i 13* - Delegacja fragmentu strefy - subdomeny "podstrefa.przykladowa.pl." na inne serwery nazw[/item] [item]*14 i 15* - Ponieważ serwery nazw delegowanej podstrefy znajdują się w tej strefie, konieczne jest dodanie odpowiednich rekordów A - adresów IP tych serwerów.[/item] [item]"*[...]3600 IN[...]*" - "3600" oznacza że serwer rekursywny ma pamiętać dany rekord przez 3600 sekund, czyli 1 godzinę, natomiast "IN" to domyślna klasa zapytań - Internet.[/item]

Przykładowy plik strefy #2

Naszą przykładową strefę możemy zapisać również w takiej postaci:


```
$ORIGIN         przykladowa.pl.

$TTL            1d



@               SOA ns1 admin 2012120500 1d 15m 30d 1h



                NS  ns1

                NS  ns2
```

```
ns1             A   10.10.10.10
ns2             A   192.168.100.100

@               MX  10 mx
mx              A   10.222.222.222

@               A   172.20.40.40
www             A   172.20.40.40
ftp             A   172.20.40.40
webmail         A   172.20.40.40

podstrefa       NS  ns1.podstrefa
podstrefa       NS  ns2.podstrefa

ns1.podstrefa   A   192.168.90.91
ns2.podstrefa   A   192.168.90.92
```

- *$ORIGIN* - zmienna zawierająca pełny adres domeny. Gdy wewnątrz pliku strefy użyjemy znaku "@", zostanie on zamieniony na zawartość tej zmiennej.

- *$TTL* - domyślny czas przez który serwery rekursywne mają pamiętać rekordy domen. Dzięki tej zmiennej nie musimy przy każdym rekordzie dopisywać jego wartości TTL (3600).
- Gdy nie wpiszemy nazwy (sub)domeny na początku rekordu, zostanie użyta nazwa z poprzedniego rekordu.
- Gdy nie zakończymy adresu domenowego kropką, zostanie on dopełniony zawartością zmiennej $ORIGIN.

Wildcard

Jako nazwy subdomeny możemy również użyć symbolu gwiazdki - "*", będzie to oznaczało każdą subdomenę, jeśli taka nie posiada już swojego osobnego rekordu. Jeśli więc w strefie istnieje rekord A dla subdoemny "*", zawierający adres IP 10.20.30.40, po odpytaniu serwera DNS o subdomenę "foiejwfiqf.przykladowa.pl", zwróci on adres IP 10.20.30.40. Tak samo będzie w przypadku zapytań o "hfoiewi.przykladowa.pl" i "wqeqwer.przykladowa.pl".

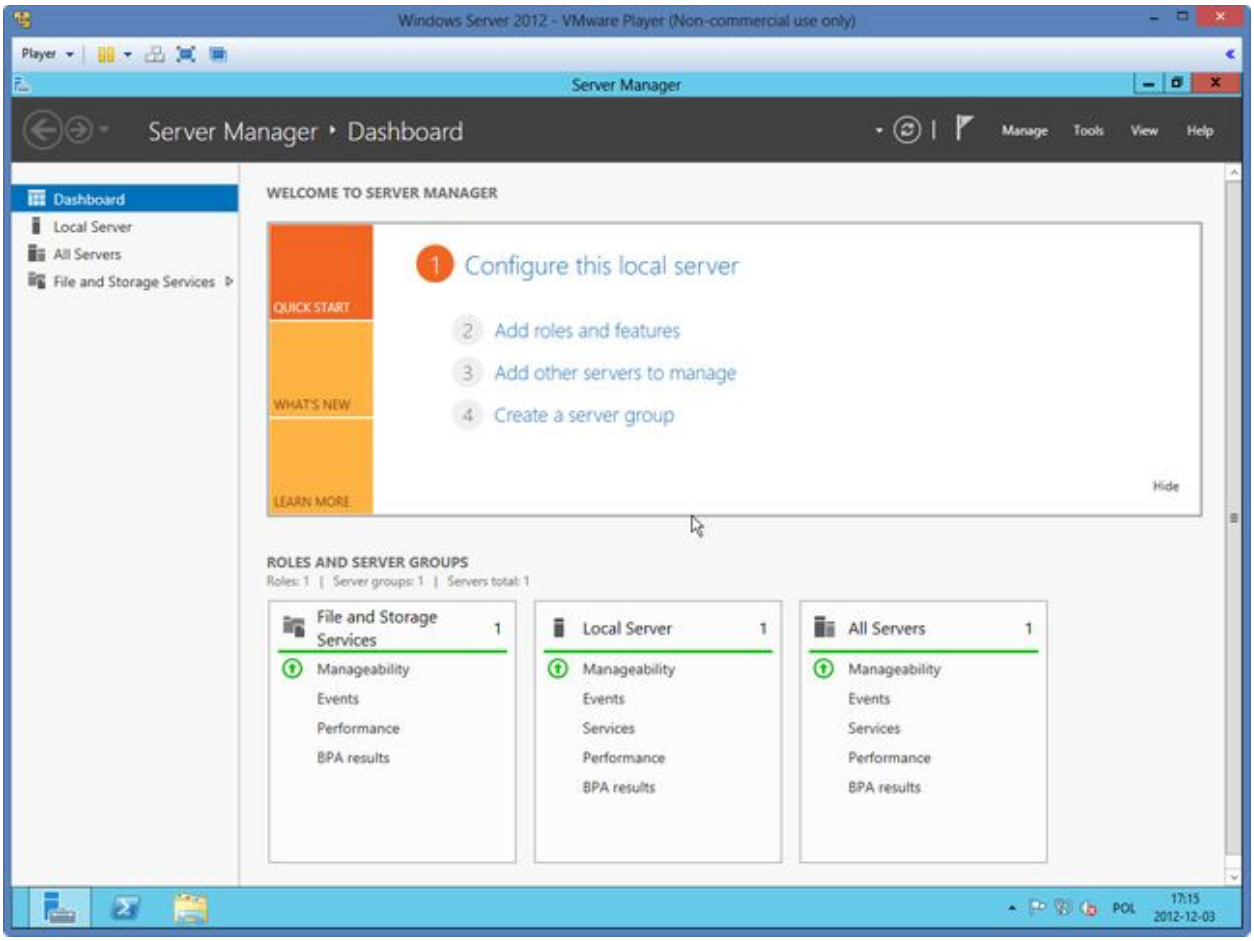
Z wykorzystaniem wildcard-u, nasza przykładowa strefa może wyglądać tak:

```
$ORIGIN         przykladowa.pl.

$TTL            1d



@               SOA ns1 admin 2012120500 1d 15m 30d 1h
```

```
                NS  ns1
                NS  ns2


ns1             A   10.10.10.10
ns2             A   192.168.100.100


@               MX  10 mx
mx              A   10.222.222.222


*               A   172.20.40.40


podstrefa       NS  ns1.podstrefa
podstrefa       NS  ns2.podstrefa


ns1.podstrefa   A   192.168.90.91
ns2.podstrefa   A   192.168.90.92
```

Instalacja roli serwera DNS

1. Włączamy Server Manager i klikamy Add roles and features.



2. Klikamy Next >, a na drugim ekranie kreatora wybieramy Role-based or feature-based installation.

3. Wybieramy nasz jedyny serwer, a następnie DNS Server.

4. Po zaznaczeniu DNS Server, Windows odrazy zaproponuje dodanie dodatkowej funkcji - narządzi do zarządzania serwerem DNS, klikamy Add Features oraz Continue. Windows wykrył błąd - nasza maszyna ma adres IP przydzielony przez serwer DHCP - w przypadku VMWare i pierwszej utworzonej maszyny będzie to adres 192.168.137.128.

5. Nie dodajemy żadnych dodatkowych funkcji, tylko 2x klikamy przycisk Next >.

6. Potwierdzamy chęć instalacji wybranych składników, klikając Install i czekamy na zakończenie instalacji. Okno instalatora możemy już teraz zamknąć.

Po zainstalowaniu usługi, domyślnie serwer jest skonfigurowany do pracy jako serwer rekursywny (odpytujący inne).

W następnych częściach chciałbym pokazać jak dodawać strefy do serwera DNS w Windows Server 2012, jak debugować DNS za pomocą narzędzi nslookup i dig oraz jak ustawić odwrócony DNS i rekord SPF, aby umożliwić prawidłowe działanie mailowi.