

Wykorzystanie usługi DNS w Active Directory

Konrad Sagała

Wielokrotnie instalując swój pierwszy kontroler domeny, a czasem nawet instalując... dziesiąty zastanawiamy się nad tym, czy dobrze skonfigurowaliśmy DNS, czy stacje będą się logować do domeny i czy nie pojawią się inne problemy z tym związane. Wielu wydawałoby się że doświadczonych administratorów systemów Windows i Active Directory ma mgliste pojęcie o tym, czy jest strefa `_msdcs`, jaka jest rola i czym się różni rekordy SRV. Postaram się rozwiązać kilka wątpliwości na ten temat.

Rekordy SRV

Czym są tajemnicze rekordy SRV?

Przecież DNS istnieje już tak dawno, serwery różnych wersji unixów i linuxów działają tyle lat i nikomu nie były one do niczego potrzebne. Jednak komputery z systemem Windows 2000 i nowszym w celu znalezienia i prawidłowej współpracy z kontrolerami domeny sprawdzają informacje o usługach i serwerach mogących te usługi świadczyć

W jaki sposób te informacje pojawiają się w sieci?

Kiedy kontroler domeny Windows 2003 jest uruchamiany, serwis Net Logon dynamicznie rejestruje odpowiednie rekordy A i SRV w bazie DNS, zgodnie z dokumentem Internet Engineering Task Force (IETF) RFC 2782, [“A DNS RR for specifying the location of services \(DNS SRV\)”](#). Rekordy SRV są używane do mapowania konkretnego serwisu sieciowego do nazwy domenowej komputera, oferują cego tę usługę.

W strukturze domenowej Windows Server 2003, rekordem lokalizującym kontroler domeny jest rekord zasobowy LDAP. Kiedy stacja robocza loguje się w domenę, odpytuje DNS o rekordy SRV w postaci:

`_Serwis._Protokół.NazwaDNSDomeny`

Ponieważ w Active Directory serwery udostępniają usługę LDAP poprzez protokół TCP, zapytanie o serwer udostępniający usługę LDAP (podkreślenia używane są w celu uniknięcia kolizji z mogłymi pojawiającymi się nazwami) wygłąda następująco:

`_ldap.tcp.NazwaDNSDomeny`

Przedstawiona powyżej w opisie rekordu SRV, `NazwaDNSDomeny` odnosi się do nazwy domeny DNS użytej podczas promowania pierwszego kontrolera nowej domeny. Podobnie `NazwaLasuDNS` odnosi się do nazwy DNS głównej domeny lasu Active Directory.

Oczywiście w domenie i lesie Active Directory serwerów świadczących usługę LDAP może być wiele. Oprócz rekordów opisujących usługi LDAP istnieją inne, również ważne w procesie logowania rekordy. Ich opis znajdziecie w dodatku na końcu artykułu.

Oprócz rekordów SRV wymienionych w dodatku, usługa Net Logon rejestruje także rekord aliasu DNS (CNAME) używany w procesie replikacji Active Directory, w formacie: `DsaGuid._msdcs.NazwaLasuDNS`. Ten rekord umożliwia klientowi zlokalizowanie dowolnego kontrolera w całym lesie (poprzez rekord A), dlatego też jego istnienie jest bardzo istotne. Informacja zawiera identyfikator GUID obiektu Directory System Agent (DSA) dla danego kontrolera domeny i nazwę lasu, w którym kontroler się znajduje. Dzięki temu rekordowi możliwa jest lokalizacja kontrolera nawet po zmianie jego nazwy. Znajduje się tu także tajemnicza nazwa `_msdcs`, o której znaczeniu dowiemy się za chwilę

Struktura Active Directory często jest podzielona na lokacje (site'y), odpowiadające fizycznej strukturze czy telekomunikacyjnych. Można się więc domyślać że w DNS powinny znaleźć się także rekordy zasobowe opisujące strukturę lokacji i pozwalające znaleźć kontroler domeny w najbliższej możliwej lokacji, a nie w drugim krańcu Polski. Jak działa mechanizm „namierzania” najbliższego kontrolera, wyjaśnię dokładniej trochę dalej.

Przykład rejestracji Rekordów przez Net Logon

Kontroler domeny o nazwie Frodo w domenie mojafirma.pl ma adres IP 157.55.81.157.

Rejestruje on następujące rekordy typu A i SRV w DNS:

```
Frodo.mojafirma.pl A 157.55.81.157
_ldap._tcp.mojafirma.pl SRV 0 0 389 Frodo.mojafirma.pl
_ldap._tcp.dc._msdcs.mojafirma.pl SRV 0 0 389 Frodo.mojafirma.pl
_kerberos._tcp.mojafirma.pl SRV 0 0 88 Frodo.mojafirma.pl
_kerberos._tcp.dc._msdcs.mojafirma.pl SRV 0 0 88 Frodo.mojafirma.pl.
```

Na tej podstawie zapytanie DNS `_ldap._tcp.dc._msdcs.mojafirma.pl` zwróci informację o wszystkich kontrolerach w domenie.

Strefa `_msdcs`

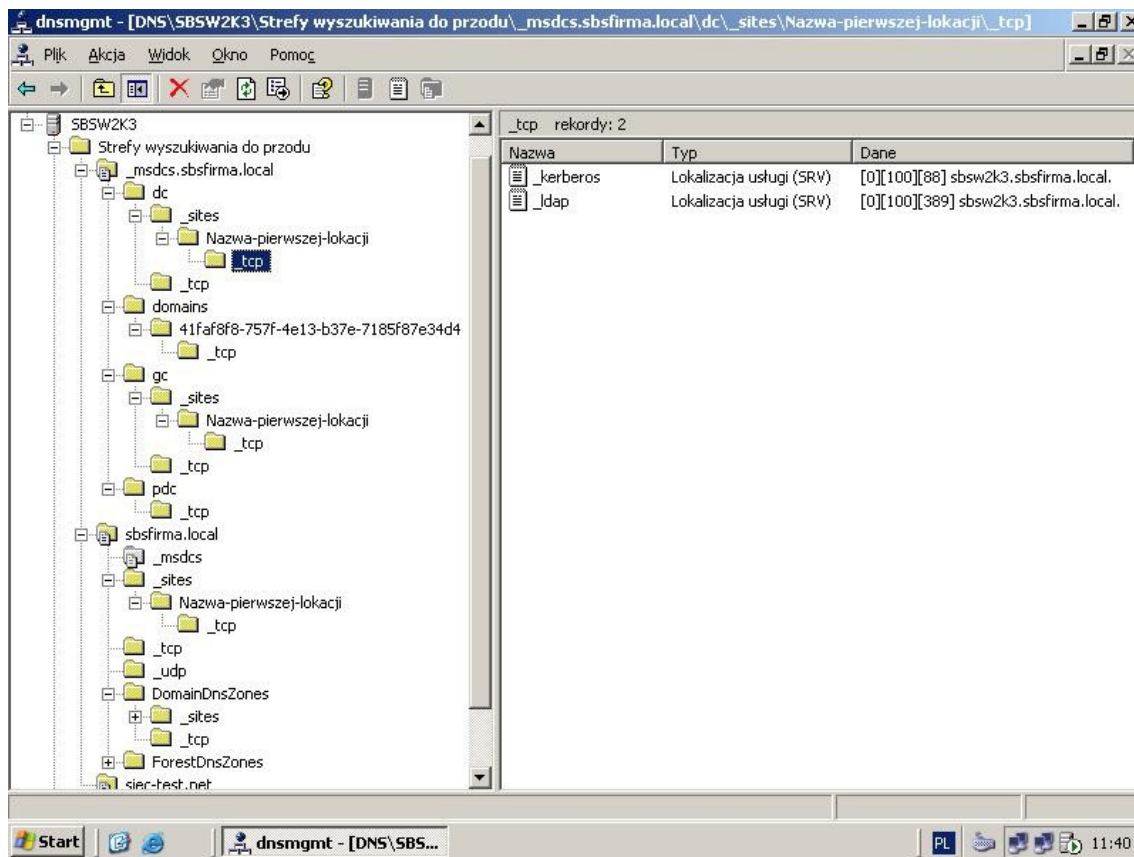
Dodatkowo oprócz standardowych rekordów `_Serwis._Protokół.NazwaDNSDomeny` kontroler domeny Windows Server 2003 rejestruje przy pomocy serwisu Net Logon rekordy SRV identyfikujące dobrze znane administratorom Active Directory skróty “dc” (domain controller), gc (global catalog), pdc (primary domain controller), oraz “domains” (globally unique identifier, czyli GUID, który nie zmienia się nawet w przypadku zmiany nazwy domeny) jako prefiksy w subdomenie `_msdcs`. Ta specyficzna dla usług Microsoft subdomena umożliwia znalezienie kontrolerów, które pełnią specyficzną rolę w danym lesie, bądź tej domenie Active Directory, umożliwia także znalezienie domeny na podstawie jej identyfikatora GUID. Wszystkie tego typu rekordy SRV rejestrowane są w postaci:

`_Serwis._Protokół.DcType._msdcs.NazwaDNSDomeny`

Subdomena `_msdcs.NazwaDNSDomeny` jest wykorzystywana do znajdowania serwerów LDAP, które oprócz obsługi TCP pełnią jakiegokolwiek specyficzną rolę. Nazwa `_msdcs` jest zarezerwowana do wyszukiwania kontrolerów domenowych oraz serwerów Kerberos. Słowo `_msdcs` zostało wybrane w celu uniknięcia niepotrzebnego zaśmiecenia DNS.

Ponieważ strefa zawierająca subdomenę `_msdcs` domeny głównej lasu powinna znajdować się na wszystkich kontrolerach domeny w lesie, a strefa zawierająca domenę główną nie musi, więc Kreator promuje pierwszy kontroler w nowym lesie, ściśle z konfiguracją DNS wydziela automatycznie strefę `_msdcs.NazwaDNSLasu`. W przypadku ręcznej konfiguracji DNS takie rozdzielenie stref jest stanowczo zalecane przez Microsoft.

Strukturę stref dla standardowej instalacji w małej firmie przedstawia poniższy rysunek:



Oczywiście przy strukturze wielodomenowej o wielu lokacjach będzie to wygl¹daćo duż^o bardziej skomplikowanie.

Znajdywanie kontrolera w najbliższej lokacji

Podczas znajdowania kontrolera domeny proces lokalizatora (Locator) używa znalezienia kontrolera znajdując się na najbliższej stacji roboczej. Jak to się odbywa?

Każdy kontroler domeny Windows Server 2003 rejestruje w DNS rekordy SRV opisujące lokalizację, w której kontroler się znajduje. Nazwa lokacji (nazwa widoczna w konsoli Sites and Services) pojawia się w kilku miejscach strefy domenowej i `_msdcs`, opisując różne role, jakie serwer może pełnić (serwer LDAP, Kerberos, Global Catalog), co widać na powyższym rysunku. Lokator najpierw przeszukuje informacje związane z konkretną lokalizacją, a dopiero później bardziej ogólnie.

Komputer przechowuje informację o lokalizacji, w której się znajduje w kluczu rejestru, jednak w procesie logowania informacja ta jest weryfikowana na podstawie aktualnego adresu IP, co jest bardzo istotne dla komputerów mobilnych. W przypadku kiedy komputer mobilny został uruchomiony w innej lokalizacji, spróbuje połączyć się z kontrolerem w swojej macierzystej lokalizacji, a ten porówna adres IP klienta z listą podsieci i przypisaniem ich do odpowiednich lokalizacji i zwróci mu nazwę lokalizacji najbliższej niego. Następnie klient zapisuje sobie w rejestrze.

Lokacja (site) jest zbiorem podsieci, połączonych szybkimi połączeniami. W Active Directory wszystkie lokalizacje z całego lasu są zapisane jako obiekty w partycji Configuration, w kontenerze `cn=Sites,cn=Configuration,dc=DomenaGłówna`. Podsieć z kolei jest zapisywana jako obiekt w kontenerze `cn=Subnets,cn=Sites,cn=Configuration,dc=DomenaGłówna`. Ponieważ partycja Configuration, tak jak i Schema replikowana jest na wszystkie kontrolery

w lesie, więc każdy kontroler domeny może zweryfikować na podstawie adresu IP informację, do jakiej lokacji powinien być przypisany komputer klienta.

Co zrobić jednak, kiedy w danej lokacji nie ma kontrolera domeny?

Z różnych przyczyn w niektórych lokacjach może nie być zainstalowanego kontrolera domeny. Kontroler domeny bada wszystkie lokacje w lesie i przypisuje się sam (poprzez ogłoszenie odpowiedniego rekordu SRV) do tych lokacji, w których nie ma przypisanego żadnego kontrolera jego domeny i koszt połączenia jest dla niego najniższy. Dzięki temu w każdej domenie lasu każda z lokacji ma automatycznie przypisany kontroler domeny. Jest to kontroler znajdujący się w najbliższej połączonej lokacji, co jest wyliczane na podstawie topologii replikacji. Proces ten nazywany jest automatycznym pokryciem lokacji (automatic site coverage).

Sposób wyliczania pokrycia lokacji na podstawie kosztów ³¹czy lokacji

Pokrycie lokacji jest określone na podstawie kosztów przypisanych do ³¹czy lokacji (site links), a także zarejestrowanych rekordów poszczególnych kontrolerów. Wyobraźmy sobie, że mamy naszą domenę oraz lokacje Lublin, Katowice i Olsztyn. W lokacji Lublin nie mamy żadnego kontrolera naszej domeny. W momencie, kiedy klient w lokacji Lublin próbuje zlokalizować kontroler domeny, pojawia się pytanie, który kontroler powinien zostać wybrany? Odpowiedź została zainicjowana przez strukturę ³¹czy.

Zauważmy, że lokacja Lublin ma zdefiniowane ³¹czy lokacji zarówno z lokacją Katowice jak i Olsztyn, przy czym z Katowicami ³¹czy ma przepustowość 2MB, a do Olsztyna tylko 256kB. W związku z powyższym dla obu ³¹czy lokacji są zdefiniowane inne koszty, odpowiadające prędkościom ³¹czy. Replikacja odbywa się na podstawie wyliczenia minimalnych kosztów, więc jeżeli na podstawie tych wyliczeń ³¹czy pomiędzy Lublinem i Olsztynem ma o wiele wyższy koszt niż pomiędzy Lublinem i Katowicami. Algorytm pokrycia lokacji sprawdza, czy kontroler domeny z lokacji Katowice zarejestrował się w lokacji Lublin. W przeciwnym wypadku klient musi szukać kontrolera domeny w lokacji Olsztyn.

Jak działa algorytm pokrycia lokacji?

Podczas rejestrowania rekordów SRV w DNS następuje sprawdzenie, czy kontroler domeny powinien zarejestrować rekordy związane z lokacjami, opisując ten serwer jako preferowany kontroler dla danej lokacji. Procedura odbywa się w następujący sposób:

- Tworzona jest lista możliwych lokacji (lokacji pozbawionych kontrolerów domeny macierzystej dla kontrolera, na którym uruchamiany jest proces),
- Tworzona jest lista lokacji posiadających odpowiednie kontrolery domeny,
- Dla każdej lokacji przeprowadzane są odpowiednie kroki:
 1. Budowana jest pełna lista lokacji,
 2. Budowana jest lista lokacji, które mają najniższy koszt ³¹czy lokacji dla docelowej lokacji,
 3. W przypadku, kiedy takich lokacji jest kilka wybierana jest jedna z największej liczby kontrolerów domenowych,
 4. Jeżeli nadal pozostaje kilka lokacji wybór jednej dokonywany jest alfabetycznie,
 5. Rejestrowane są rekordy SRV związane z docelową lokacją dla wybranych w powyższych krokach kontrolerów domeny.

Kluczowe w powyższym procesie jest zdefiniowanie wszystkich podsieci i przypisanie ich do odpowiednich lokacji. Jeżeli adres IP klienta nie zostanie znaleziony i przypisany do żadnej z lokacji, opisane powyżej mechanizmy nie zadziałają i klient nie będzie potrafił zlokalizować najbliższego kontrolera domenowego, co w rozbudowanej strukturze lasu może uniemożliwić lub co najmniej znacznie utrudnić zalogowanie do domeny.

Podsumowanie

Oczywiście przedstawione powyżej informacje to tylko krótki skrót informacji o rekordach SRV i ich wykorzystaniu w procesie logowania do domeny. Mam nadzieję, że uda się mi się tym artykułem odpowiedzieć na kilka pytań związanych z DNS w Active Directory, co w połączeniu z odpowiednimi narzędziami (takimi jak dcdiag, dnslint, nslookup), może trochę uprościć zarządzanie domenami Windows.

Dodatek

Rekordy SRV rejestrowane przez usługę Net Logon

Rekord SRV	Opis
<code>_ldap._tcp.NazwaDNSDomeny.</code>	Pozwala klientowi zlokalizować serwer obsługujący usługę LDAP w domenie <i>NazwaDNSDomeny</i> . Serwer nie musi być kontrolerem domeny, ale musi wspierać API usługi LDAP. Wszystkie kontrolery Windows Server 2003 rejestrują ten rekord SRV (np. <code>_ldap._tcp.mojafirma.pl.</code>).
<code>_ldap._tcp.NazwaLokacji._sites.NazwaDNSDomeny.</code>	Pozwala klientowi zlokalizować serwer obsługujący usługę LDAP w domenie <i>NazwaDNSDomeny</i> w lokalizacji <i>NazwaLokacji</i> . <i>NazwaLokacji</i> jest względnie nazwą obiektu lokalizacji przechowywaną w kontenerze Configuration Active Directory. Wszystkie kontrolery Windows Server 2003 rejestrują ten rekord SRV (np. <code>_ldap._tcp.krakow._sites.mojafirma.pl.</code>).
<code>_ldap._tcp.dc._msdcs.NazwaDNSDomeny.</code>	Pozwala klientowi zlokalizować kontroler domeny (dc) <i>NazwaDNSDomeny</i> . Wszystkie kontrolery Windows Server 2003 rejestrują ten rekord SRV.
<code>_ldap._tcp.NazwaLokacji._sites.dc._msdcs.NazwaDNSDomeny.</code>	Pozwala klientowi zlokalizować kontroler domeny <i>NazwaDNSDomeny</i> w lokalizacji <i>NazwaLokacji</i> . Wszystkie kontrolery Windows Server 2003 rejestrują ten rekord SRV.
<code>_ldap._tcp.pdc._msdcs.NazwaDNSDomeny.</code>	Pozwala klientowi zlokalizować serwer, który pełni rolę podstawowego kontrolera domeny (PDC) w domenie trybu mixed-mode <i>NazwaDNSDomeny</i> . Tylko kontroler pełniący rolę PDC emulatora w domenie rejestruje ten rekord SRV.
<code>_ldap._tcp.gc._msdcs.NazwaDNSLasu.</code>	Pozwala klientowi zlokalizować serwer globalnego katalogu (gc) w ramach lasu. Tylko kontrolery, pełniące rolę globalnego katalogu <i>NazwaDNSLasu</i> rejestrują ten rekord SRV (np. <code>_ldap._tcp.gc._msdcs.mojafirma.pl.</code>).
<code>_ldap._tcp.NazwaLokacji._sites.gc._msdcs.NazwaDNSLasu.</code>	Pozwala klientowi zlokalizować serwer globalnego katalogu (gc) w lokalizacji o nazwie <i>NazwaLokacji</i> . Tylko kontrolery domenowe, pełniące rolę globalnego katalogu w lesie <i>NazwaDNSLasu</i> rejestrują rekord SRV (np. <code>_ldap._tcp.krakow._sites.gc._msdcs.mojafirma.pl.</code>).
<code>_gc._tcp.NazwaDNSLasu.</code>	Pozwala klientowi zlokalizować serwer globalnego katalogu (gc) w domenie. Co ciekawe serwer nie musi być kontrolerem domeny (w innych niż Windows implementacjach usług katalogowych). Tylko serwery udostępniające usługę LDAP i funkcjonujące jako serwer GC w lesie <i>NazwaDNSLasu</i> rejestruje ten rekord SRV (np. <code>_gc._tcp.mojafirma.pl.</code>).
<code>_gc._tcp.NazwaLokacji._sites.NazwaDNSLasu.</code>	Pozwala klientowi zlokalizować serwer globalnego katalogu (gc) w lokalizacji o nazwie <i>NazwaLokacji</i> (np. <code>_gc._tcp.krakow._sites.mojafirma.pl.</code>).
<code>_ldap._tcp.GuidDomeny.domains._msdcs.NazwaDNSLasu.</code>	Pozwala klientowi zlokalizować kontroler domeny poprzez jego GUID, który jest 128-bitowym numerem, tworzonym automatycznie dla odpowiedniego obiektu w

Rekord SRV	Opis
	Active Directory — w tym przypadku domeny (np. <code>_ldap._tcp.4f904480-7c78-11cf-b057-00aa006b4f8f.domains</code> . <code>_msdcs.mojafirma.pl.</code>). Wszystkie kontrolery rejestrują ten rekord SRV.
<code>_kerberos._tcp.NazwaDNSDomeny.</code>	Pozwala klientowi zlokalizować serwer obsługujący usługę Kerberos KDC w domenie <i>NazwaDNSDomeny</i> . Serwer nie musi być kontrolerem domeny. Wszystkie serwery Windows 2003, obsługujące usługę Kerberos KDC zgodnie z RFC 1510 rejestrują ten rekord SRV.
<code>_kerberos._udp.NazwaDNSDomeny.</code>	Podobnie <code>_kerberos._tcp.NazwaDNSDomeny.</code> , ale dla protokołu UDP.
<code>_kerberos._tcp.NazwaLokacji.</code> <code>_sites.NazwaDNSDomeny.</code>	Pozwala klientowi zlokalizować serwer obsługujący usługę Kerberos KDC w domenie <i>NazwaDNSDomeny</i> i znajdujący się w lokalacji <i>NazwaLokacji</i> . Serwer nie musi być kontrolerem domeny. Wszystkie kontrolery Windows 2003, obsługujące usługę Kerberos KDC zgodnie z RFC 1510 rejestrują ten rekord SRV.
<code>_kerberos._tcp.dc._msdcs.NazwaDNSDomeny.</code>	Pozwala klientowi zlokalizować kontroler domeny Windows 2003 obsługujący usługę Kerberos KDC w domenie <i>NazwaDNSDomeny</i> . Wszystkie kontrolery, które obsługują usługę KDC rejestrują ten rekord SRV.
<code>_kerberos.tcp.NazwaLokacji.</code> <code>_sites.dc._msdcs.NazwaDNSDomeny.</code>	Pozwala klientowi zlokalizować kontroler domeny, z działający w wersji Windows Server 2003 implementacji serwisu Kerberos KDC dla domeny <i>NazwaDNSDomeny</i> w lokalacji o nazwie <i>NazwaLokacji</i> . Wszystkie kontrolery, które obsługują usługę KDC rejestrują ten rekord SRV.
<code>_kpasswd._tcp.NazwaDNSDomeny.</code>	Pozwala klientowi zlokalizować serwer usługi Kerberos Password Change w domenie. Wszystkie serwery usługi Kerberos Password Change (wszystkie kontrolery domeny Windows Server 2003) rejestrują ten rekord. Serwer nie musi być kontrolerem domeny. Wszystkie serwery Windows 2003, obsługujące usługę Kerberos KDC zgodnie z RFC 1510 rejestrują ten rekord SRV..
<code>_kpasswd._udp.NazwaDNSDomeny.</code>	Podobnie jak <code>_kpasswd._tcp.NazwaDNSDomeny.</code> , ale dla protokołu UDP.

Literatura:

- [How DNS Support for Active Directory Works](#)
- [DNS Support for Active Directory Tools and Settings](#)
- [How DNS Works](#)