

Active Directory - Windows Server 2003

Położenie: (nie dotyczy)

© Imagine Studio 2005, <http://imagineStudio.of.pl>

Las w *Active Directory* to całość zarządzanych przez nas obiektów połączonych jakąś wspólną konfiguracją: domeny, komputery, użytkownicy, grupy, drukarki, aplikacje, atrybuty i klasy obiektów. Las dzieli się na drzewa (domeny), a te z kolei na liście (obiekty domeny). Wszystkie obiekty określane są za pomocą nazw LDAP. Jeśli tworzymy lokalną domenę, należy nadać jej nazwę z końcówką "local", np. *test.local*.

Działanie Active Directory

Poprawność działania *Active Directory* można sprawdzić za pomocą:

- *Otoczenie sieciowe*
- *Konsola Active Directory Users and Computers*

Tryb domeny

Jeśli w domenie nie występują systemy starsze niż *Windows 2000*, dobrze jest zmienić tryb domeny z mieszanego na macierzysty: *Active Directory Domains and Trusts: Properties/Change Mode*

Poddomeny

Aby utworzyć podrzędne domeny:

Active Directory Users and Computers: Organizational Unit

DNS w Active Directory

Słowniczek DNS:

- **A** - adres, rekord przypisujący nazwę hosta do adresu IP;
- **CNAME** - nazwa kanoniczna, definiuje alias dla nazwy hosta; przy użyciu tego rekordu komputer może być identyfikowany pod inną nazwą, np. *host.alfa.microsoft.com* może posiadać alias *www.microsoft.com*;
- **MX** - usługa wymiany poczty, umożliwia zdefiniowanie serwera wymiany poczty dla domeny; dzięki temu rekordowi poczta elektroniczna będzie dostarczana do właściwego serwera pocztowego w domenie;
- **NS** - serwer nazw, wskazuje na serwer nazw dla domeny, umożliwiając wyszukiwanie nazw DNS w różnych strefach; każdy serwer DNS, zarówno podstawowy, jak i pomocniczy, powinien zostać zadeklarowany przy pomocy tego rekordu;
- **SOA** - adres startowy uwierzytelniania, deklaruje host, który jest najbardziej autorytatywny dla danej strefy i tym samym jest najlepszym źródłem informacji DNS dla tej strefy.

W małych sieciach najczęściej DNS działa w trybie "*Forward Lookup*" (wyszukiwanie do przodu), czyli na podstawie nazwy domeny podaje numer IP. Aby sprawdzić czy serwer DNS poprawnie działa w *Active Directory*, wydajemy polecenia w trybie tekstowym:

- `nslookup`
- `set type=srv`
- `ldap.tcp.nazwaDomeny`

Jako wynik poleceń, system wypisuje nazwę serwera i jego adres IP. Serwer można skonfigurować w taki sposób, aby zapytania DNS przekazywał innemu serwerowi DNS, np. wszystkie zapytania dotyczące *.com przesyła na adres 123.456.2.1. Przy włączonej w systemie usłudze udostępniania połączenia (ICS) mogą nastąpić problemy podczas uruchamiania serwera DNS.

Serwer DNS może również wysyłać zapytania (w przypadku, gdy nie znajdzie numeru IP) do lokalnego serwera WINS: *Właściwości DNS/WINS*.

Zabezpieczenia serwera DNS ("Właściwości"):

- Zakładka "**Interfejsy**" - wprowadzić adresy tylko naszego LAN;
- Zakładka "**Zaawansowane**" - zabezpiecz pamięć podręczną przed zanieczyszczeniem; wyłącz rekursję (obsługa zapytań przekazywanych przez inne zewnętrzne serwery DNS, ale także obsługa wysyłania takich zapytań przez nasz serwer);

Na klientach można dodać IP trzech serwerów DNS (jako pierwszy będzie adres lokalnego serwera DNS). Jeśli pierwszy serwer nie

jest w stanie odnaleźć adresu IP na podstawie nazwy, klient próbuje dwóch pozostałych. W przypadku gdy klient poda tylko samą nazwę *NetBIOS* (bez kropek), nazwa ta będzie domyślnie uzupełniana przez sufiksy naszej sieci od najbardziej szczegółowych do najbardziej ogólnych, np. na zapytanie "komp1" będzie sprawdzany najpierw *komp1.warszawa.firma.com*, potem *komp1.firma.com* i wreszcie *komp1.com*. Odpowiada za to opcja "Append parent suffixes of the primary DNS suffix". Jeśli wszystkie próby zawiodą, zostanie sprawdzony sufiks podany w "DNS suffix for this connection".

DFS w Active Directory

DFS (*Distributed File System*) to rozproszony system plików, od *Samby* (*Otoczenia sieciowego*) różni się tym, że udostępnione przez klientów zasoby znajdują się (logicznie) w jednym miejscu, choć faktycznie mogą znajdować się na kilku komputerach. Klientami DFS może być system *Windows 98* i wyższe wersje.

Serwer czasu

Windows Server 2003 odwołuje się przy starcie do serwera czasu *time.windows.com*. Niestety, serwer ten bywa czasami przeciążony, i wtedy start naszego systemu przedłuża się znacznie. Aby zmienić serwer czasu (np. na *vega.cbk.poznan.pl*) należy zmienić ustawienia w rejestrze:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters: NtpServer (typ: REG_SZ) serwer.czasu.com, inny.serwer.com
```

Tę samą operację można przeprowadzić za pomocą polecenia **w32tm**.

Aby nasz komputer pełnił rolę serwera czasu dla innych maszyn z LAN, należy wyedytować klucz:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters
```

Tworzymy w nim wartość typu **DWORD** o nazwie **LocalNTP** i ustawiamy ją na **1**. W przypadku posiadania firewalla należy jeszcze pamiętać o otwarciu na nim odpowiedniego portu dla usługi *Network Time Protocol* (jest to 123/udp).

Drukarki

Obsługa uniksowego polecenia lpr:

Panel sterowania/Network and Dial-Up Connections/Advanced/Optional Networking Components

Dodając w systemie *Windows* drukarkę sieciową pracującą pod uniksową kontrolą CUPS, można ją dodać jako lokalną tworząc nowy port LPR, który będzie odnośnikiem do drukarki sieciowej. W takiej sytuacji (podobno) nie jest wymagana lokalna instalacja sterowników.

Udostępnianie połączenia

We właściwościach protokołu TCP/IP karty sieciowej zewnętrznej LAN klikamy na zakładkę "Zaawansowane" oraz "Udostępnianie połączenia internetowego". Przekierowanie połączeń zewnętrznych do komputerów wewnątrz sieci: na tej samej zakładce "Zaawansowane" należy kliknąć w "Ustawienia". Bardziej rozbudowana wersja translacji adresów to usługa *Routing and Remote Access*.

IP z podsieci 169.254.0.0

Powodem, dla którego komputer posiada adres z tej podsieci jest fakt, że został on skonfigurowany do uzyskania adresu IP z serwera DHCP i nie może się z nim skontaktować. W takim przypadku na komputerze klienckim zostaje uruchomiony mechanizm APIPA (*Automatic Private IP Addressing*), który przydziela do interfejsu unikatowy adres z zakresu 169.254.0.1 do 169.254.255.254. Istnieje możliwość wyłączenia mechanizmu APIPA i aby to uczynić należy dodać w rejestrze wpis **IPAutoconfigurationEnabled** o wartości **0x0** (typ danych **REG_DWORD**) i umieścić go w kluczu `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\adapter`.

Zdalne uruchamianie programów

Budujemy skrypt:

```
strComputer = "zdalnyKomputer"  
Set objWMIService = GetObject _  
    ("winmgmts:\\\" & strComputer & "\root\cimv2:Win32_Process")  
errReturn = objWMIService.Create _  
    ("calc.exe", Null, Null, intProcessID)
```

Skrypt uruchamia program *calc.exe* na komputerze "zdalnyKomputer" przy pomocy WMI. Jeśli zdalny komputer pracuje pod kontrolą

Windows 2000, użytkownikowi na pulpicie uruchomi się kalkulator. W przypadku systemów *XP/2003*, ze względów bezpieczeństwa użytkownik nie zobaczy niczego na ekranie, niemniej kalkulator zostanie uruchomiony - jego proces można będzie bez problemu podejrzeć np. pod *Task Managerem*.

Pomoc

- www.windows2003.pl

Ostatnia aktualizacja: 4 czerwiec 2005.