Instalace Active Directory

Proces implementace Active Directory se sestává z několika kroků. Před vlastní instalací je zapotřebí zvážit mnoho faktorů. Špatně navržená struktura Active Directory způsobí v budoucnu mnohé problémy. V nejlepším případě dojde pouze ke zbytečným výdajům.

Postup implementace:

- **Návrh –** závisí na potřebách organizace, vychází z její struktury, požadavků na zabezpečení
- **Implementační plán –** zohledňuje technické problémy, výsledkem by měl být detailní plán instalace
- **Instalace –** vytvoření lesa a doménové struktury, vlastní instalace řadičů domény

Během návrhu doménové struktury je zapotřebí získat informace o struktuře organizace. Tyto informace poté musíme zanalyzovat. Příkladem informací důležitých pro návrh struktury Active Directory jsou: geografické členění společnosti, technické možnosti ve společnosti, požadavky na zabezpečení, pravděpodobnost budoucích změn – rozšiřování, Disaster Recovery atd.

Vlastní instalaci Active Directory ze rozdělit do následujících bodů:

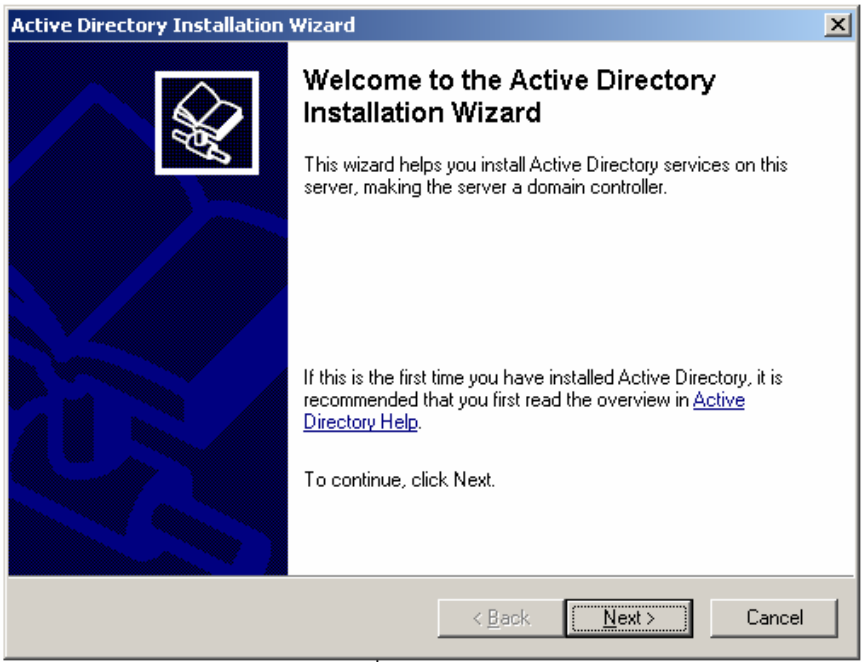
- Implementace lesa, domén a struktury DNS
- Vytvoření organizačních jednotek, skupin
- Vytvoření uživatelů
- Group Policies
- Nastavení lokalit (Sites)

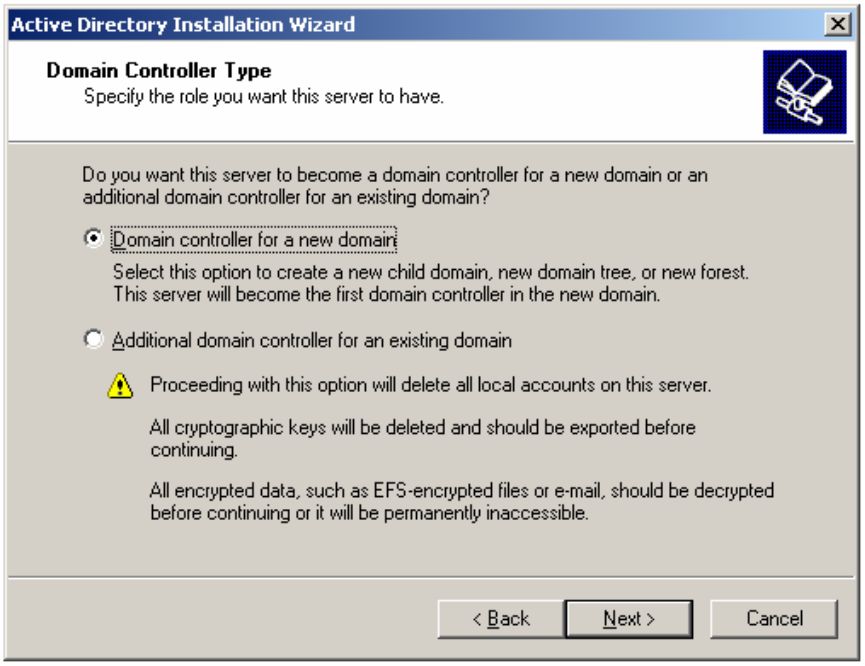
Les domén Active Directory je vytvořen instalací prvního řadiče domény. Abychom mohli instalovat službu Active Directory na počítač musíme splnit následující kritéria:

- Na počítači musí být nainstalován operační systém **Windows Server 2003**
- Musíme mít k dispozici pevný disk **min. 250 MB** volného místa, souborový systém musí být **NTFS**
- Potřebujeme administrátorská oprávnění
- Protokol **TCP/IP**
- Autoritativní server **DNS**, který podporuje záznamy **SRV**

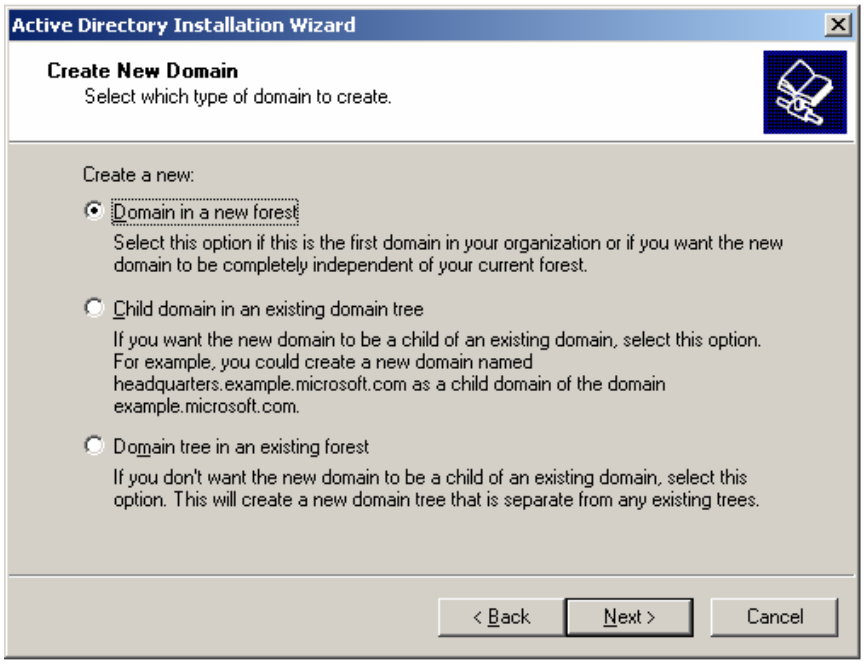
Instalace

Instalace se provádí pomocí Active Directory Installation Wizard. Před začátkem vlastní instalace je nutné zadat několik údajů.

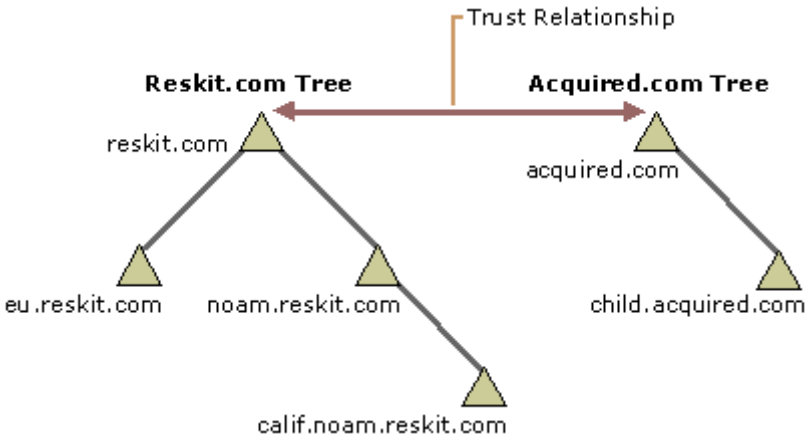




Je zapotřebí určit zda-li chceme instalovat doménový řadič pro zcela novou doménu nebo vytvořit další řadič pro již existující. K vytvoření nové Child domény je nutné být členem skupiny Enterprise Admins. Instalace dalšího řadiče již existující domény vyžaduje členství ve skupině Domain Admins. Pro instalaci první domény je nutné být členem lokální skupiny Administrators.



Dále určíte zda-li chcete založit nový les, novou doménu v existujícím stromu nebo založíte nový strom. Doménové stromy v lese netvoří spojitý jmenný systém. Domény v jednom stromu ano.



Les domén se dvěma stromy

Další důležité nastavení při instalaci Active Directory je heslo pro obnovení adresářových služeb (Directory Services Restore Mode). Což je zvláštní režim serveru, ve kterém je možné obnovit databázi Active Directory ze zálohy.

Umístění jak databáze Active Dierctory tak i sdíleného adresáře SYSVOL je možné nechat na původním místě. Z pohledu zabezpečení je vhodné tyto soubory umístit jinam, jelikož případný útočník je bude nejprve hledat v jejich standardním umístění: %systemroot%NTDS. Dále je možné umístit databázi a logy na 2 různé pevné disky kvůli výkonu.

Před instalací je zobrazeno krátké shrnutí instalačních nastavení.

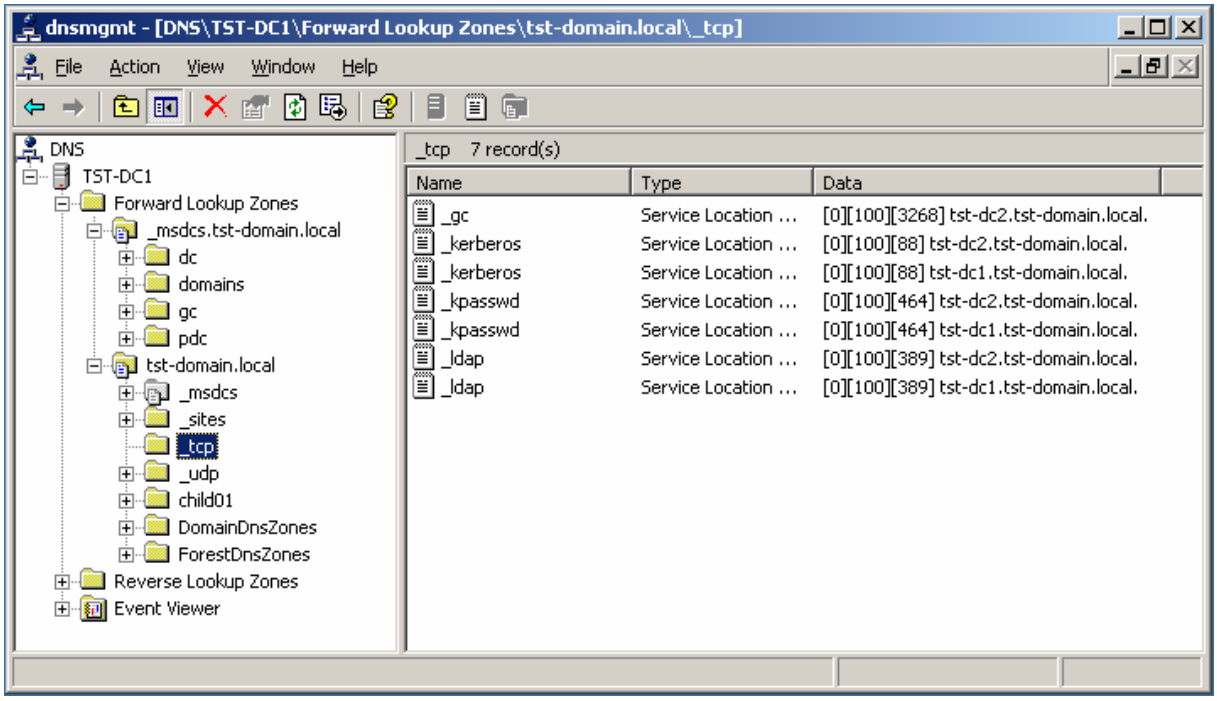
Při instalaci jsou provedeny následující kroky:

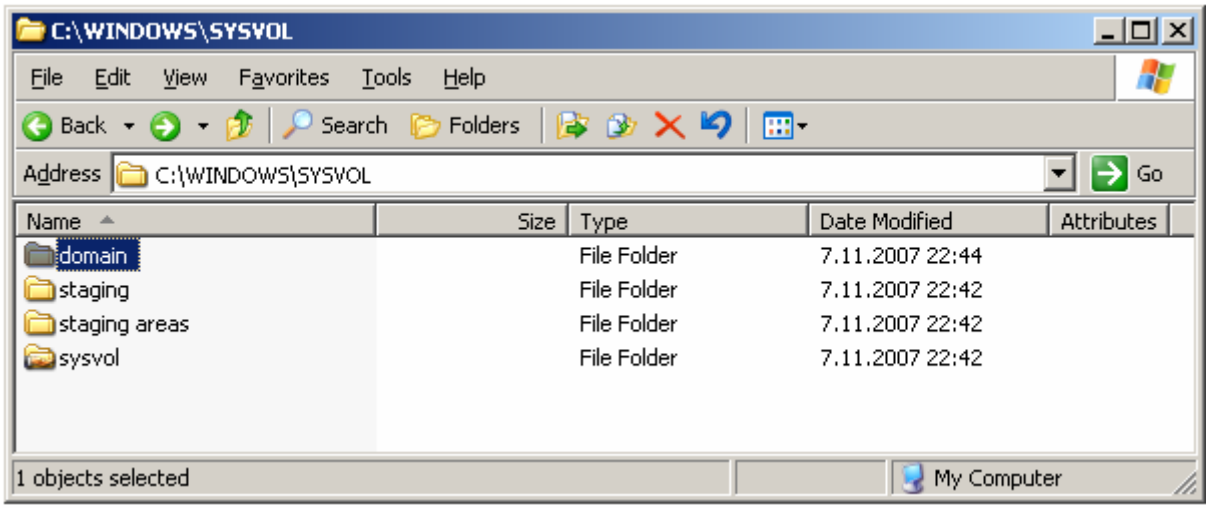
- Aktivuje se ověřovací protokol Kerberos verze 5
- Nastaví se Local Security Authority (LSA Service); tím je počítač označen jako řadič domény
- Vytvoří se oddíly Active Directory
- Vytvoří se Forest DNS zones a Domain DNS zones
- Vytvoří se databáze Active Directory
- Vytvoří se hlavní forest root domain; doménovému řadiči jsou přiřazeny FSMO role
- Vytvoří se sdílená složka SYSVOL
- Nastaví se členství doménového řadiče v Site (první lokalita: Default-First-Site-Name)
- Dojde k nastavení oprávnění na souborovém systému

Všechny doménové řadiče jsou v organizační jednotce Domain Controllers. Pro celou doménu platí Default Domain Policy, pro doménové řadiče pak Default Domain Controllers Policy.

Vytvoření struktury

Po instalaci doménového řadiče je možné zkontrolovat zda instalace proběhla v pořádku. Měly by být vytvořeny všechny SRV záznamy v DNS.





Sdílený adresář SYSVOL

Pokud je vše v pořádku je vhodné nastavit tzv. úroveň funkčnosti domény (Domain Functional Level). Je možné vybrat některou z následujících:

- Windows 2000 Mixed
- Windows 2000 Native
- Windows 2003
- Windows 2003 Interim

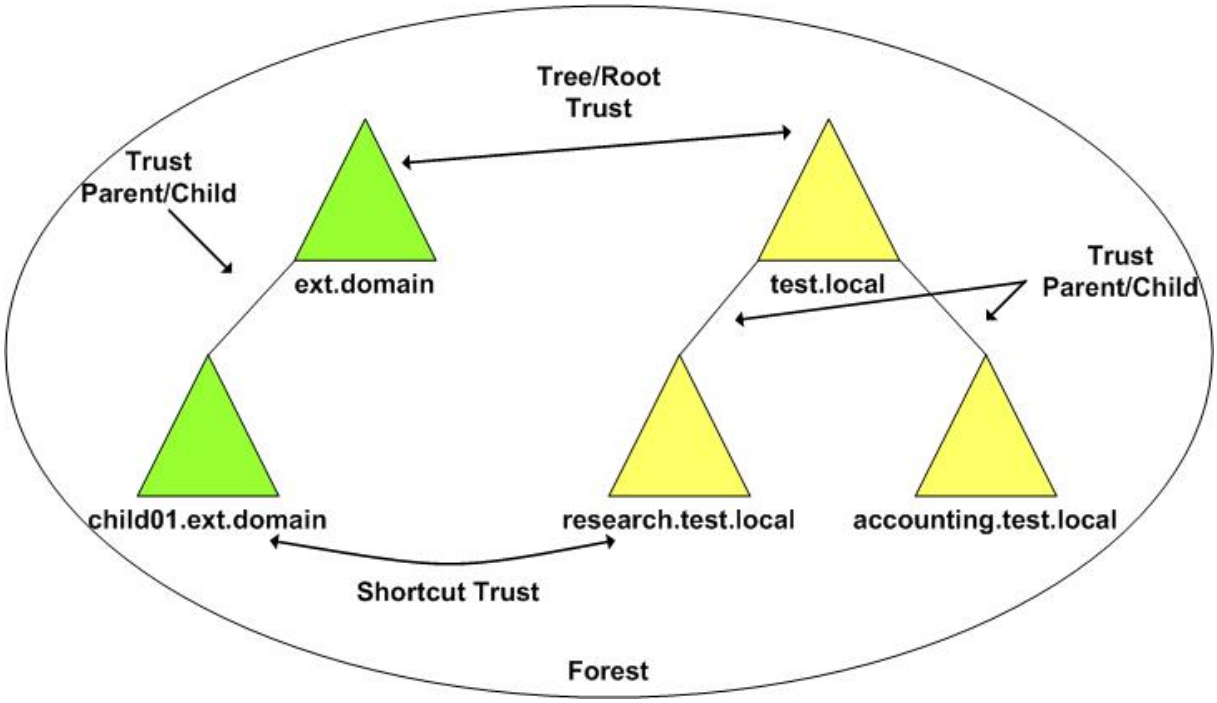
Zároveň je možné změnit úroveň funkčnosti lesa (Forest Functional Level):

- Windows 2000 native
- Windows 2003

V případě, že doménová struktura neobsahuje žádné domény staršího typu Windows NT 4.0 nebo Windows 2000, je doporučená úroveň funkčnosti Windows 2003. Tento režim umožňuje např. používání univerzálních skupin, přejmenovávání domén, inkrementální replikace atd. Provedené změny jsou nevratné. Úroveň funkčnosti lze pouze zvyšovat.

Změna funkční úrovně domény se provádí pomocí konzole Active Directory Users and Computers volbou Raise Domain Functional Level. Zvýšení funkční úrovně lesa je možné v konzole Active Directory Domains and Trusts.

Dalším krokem by mělo být vytvoření vztahů důvěryhodností, pokud je to zapotřebí. Při instalaci child domény jsou automaticky vytvořeny vztahy důvěryhodnosti typu Parent/Child. Vztahy důvěryhodnosti mohou být tranzitivní i netranzitivní. Tranzitivní vztah důvěryhodnosti automaticky přenáší důvěryhodnost i na další domény, kterým důvěřuje doména mezi kterou byl tento vztah vytvořen. Př. **test.local** důvěřuje doméně **ext.domain**, která důvěřuje doméně **child01.ext.domain** automaticky tedy **test.local** důvěřuje i doméně **child01.ext.local**. Tranzitivní vztahy důvěryhodnosti jsou výchozí. Netranzitivní vztahy důvěryhodnosti se používají především mezi doménami v různých lesech.



Jednotlivé druhy vztahů důvěryhodnosti

Dalším krokem je vytvoření struktury organizačních jednotek. Ty by měly sloužit k zpřehlednění struktury Active Directory. Organizačním jednotkám jsou přiřazeny jednotlivé Group Policy, takže můžeme členstvím v organizační jednotce spouštět různé login sktripty, instalovat software nebo vynutit určité nastavení uživatelům nebo počítačům v nich obsažených. Vybraným uživatelům je možné delegovat oprávnění k administraci objektů v OU.

Po vytvoření základní struktury OU je nutné vytvořit bezpečnostní skupiny a uživatele. Zde platí pravidlo, že pro přístup k síťovým prostředkům je vhodnější používat skupiny na místo uživatelů.

Skupiny uživatelů se rozdělují dle účelu na:

- **Distribuční (Distribution Groups) –** slouží k posílání e-mailů skupinám uživatelů
- **Bezpečnostní (Security Groups) –** je možné je použít pro přístup k síťovým prostředkům i pro posílání e-mailů

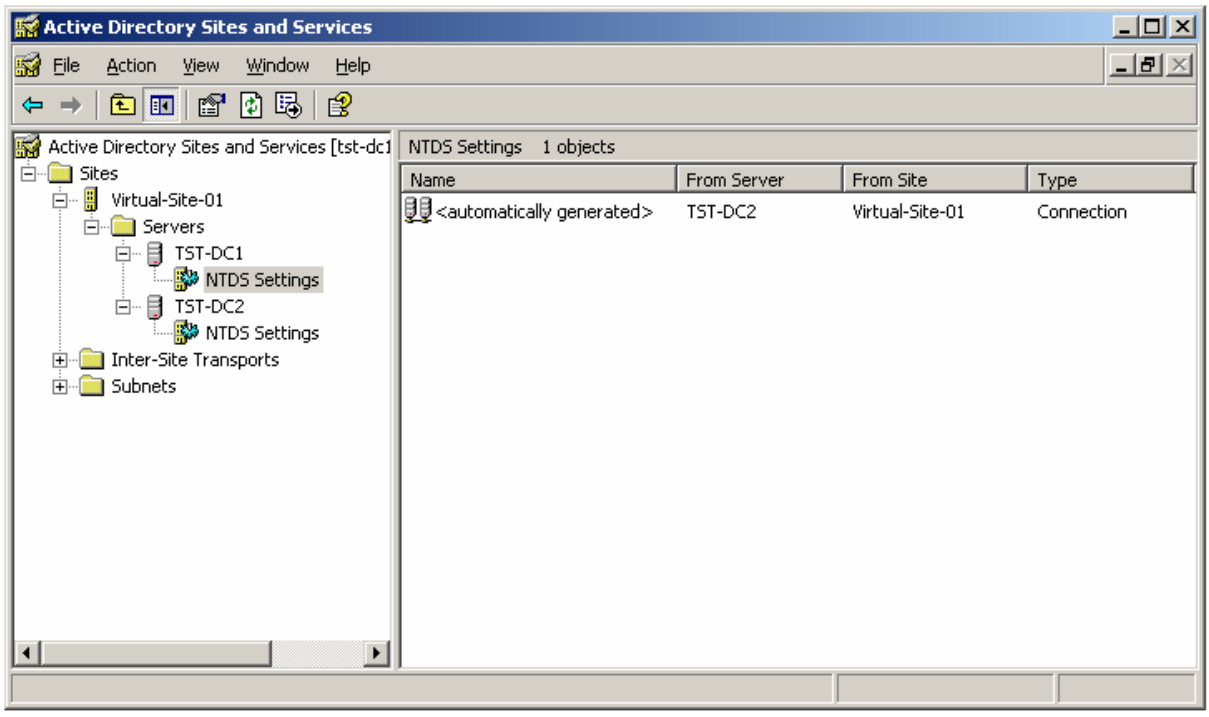
Dle platnosti:

- **Místní doménové (Domain Local Groups) –** mohou obsahovat uživatele i skupiny ze všech domén, kterým doména důvěřuje. Místní doménové skupiny nemohou být členy žádné skupiny. Tato skupina je viditelná pouze v dané doméně.

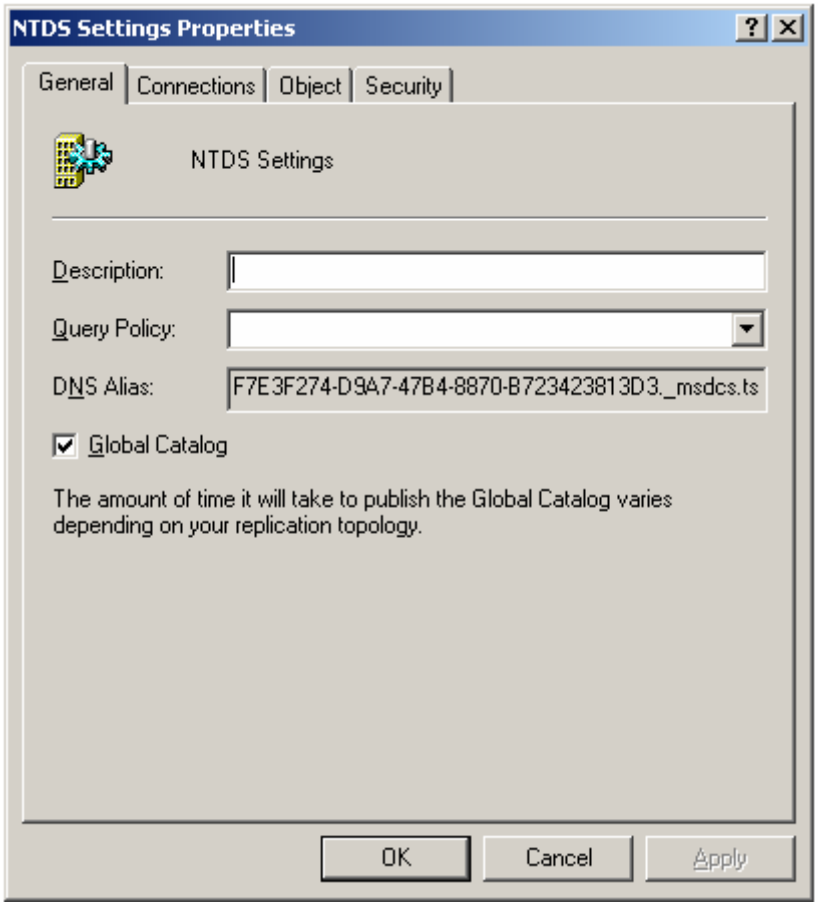
- **Globální skupiny (Global Groups) –** mohou obsahovat uživatele a jiné globální skupiny z domény, ve které je vytvořena. Globální skupina může být členem jak místní doménové nebo univerzální skupiny v kterékoliv doméně, které důvěřuje tak i členem globální skupiny v dané doméně. Globální skupina je viditelná ve všech doménách v lese.

- **Univerzální skupiny (Universal groups) –** může obsahovat uživatele, univerzální a globální skupiny ze všech domén v lese. Univerzální skupina může být členem místní doménové nebo univerzální skupiny ze všech domén v lese. Jsou viditelné ve všech doménách v daném lese. Fungují pokud je úroveň funkčnosti domény Windows 2000 native a vyšší.

Nakonec je vhodné upravit nastavení lokalit a upřesnit umístění Globálního katalogu. K tomu slouží MMC konzole Active Directory Site and Services. Zde je možné změnit replikační topologii nebo vynutit okamžitou replikaci Active Directory.



Konzole Active Directory Site and Services



Konfigurace Globálního katalogu