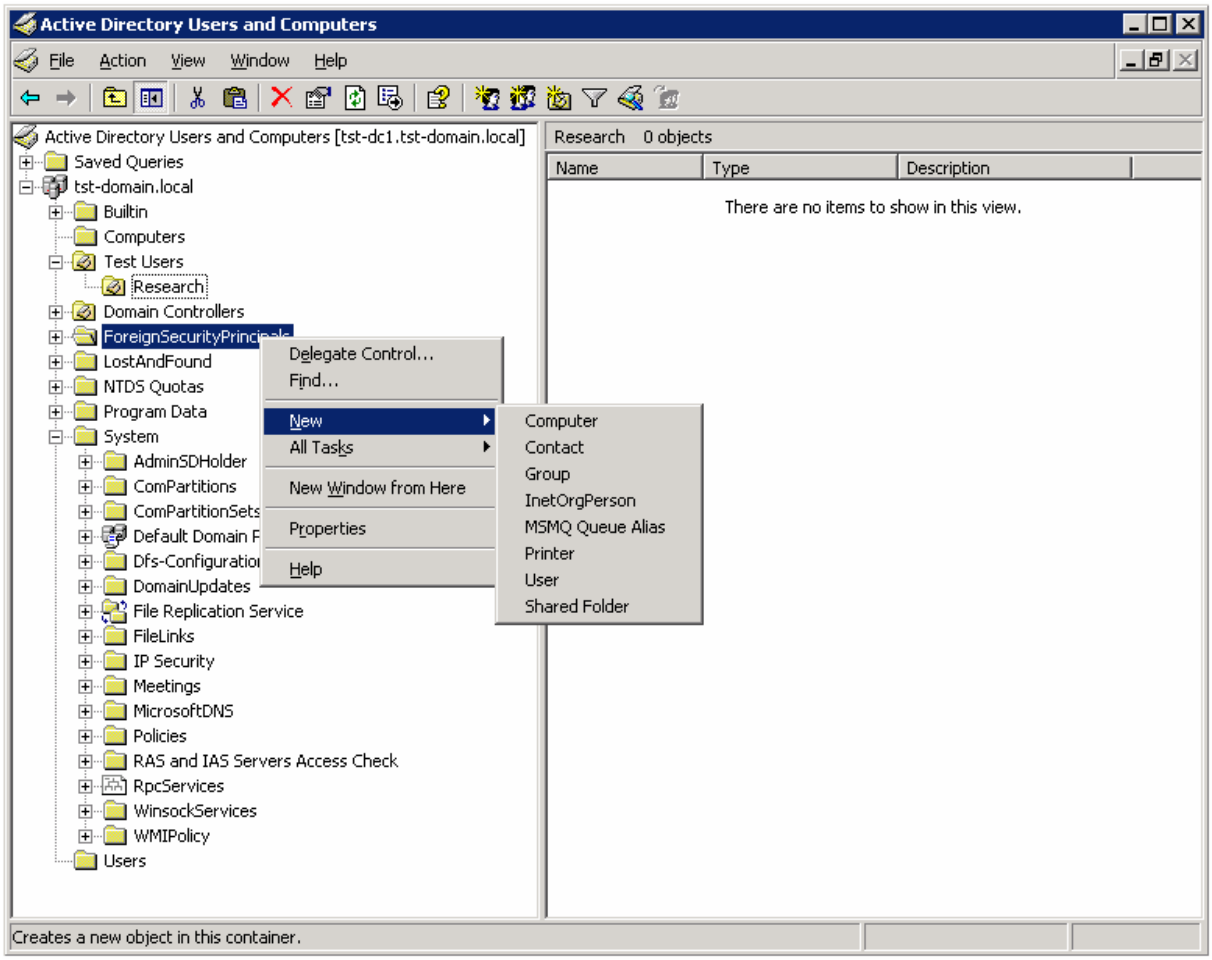
Active Directory –
organizační jednotky, uživatelé a skupiny

V databázi Active Directory jsou uloženy objekty organizačních jednotek, uživatelských účtů a skupin. Organizační jednotka představuje jakýsi kontejner, který může obsahovat další objekty. Dále rozlišujeme uživatelské účty a účty počítačů. Různé druhy skupin byly jmenovány v části Active Directory – Instalace.

Konzole MMC Active Directory Users and Computers

Základní správa objektů ve struktuře Active Directory se provádí pomocí konzole Active Directory Users and Computers.

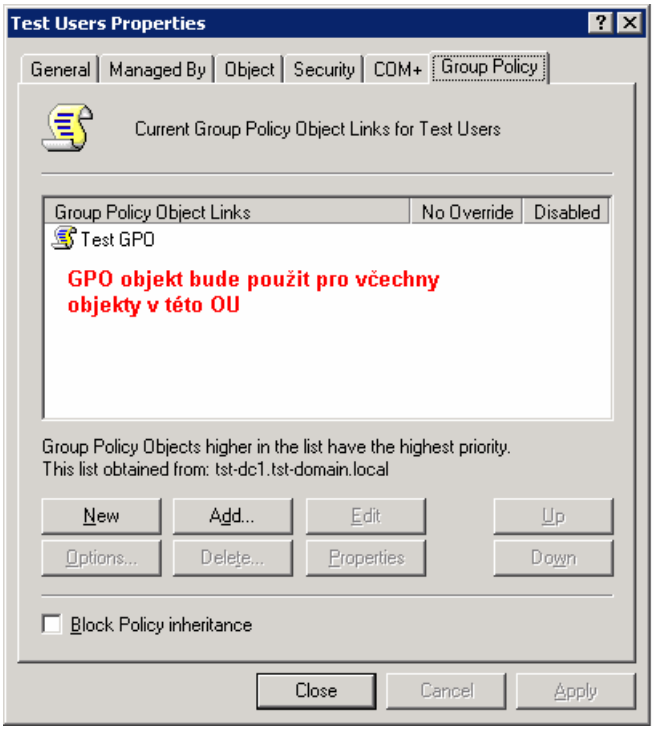


MMC konzole pro správu uživatelů

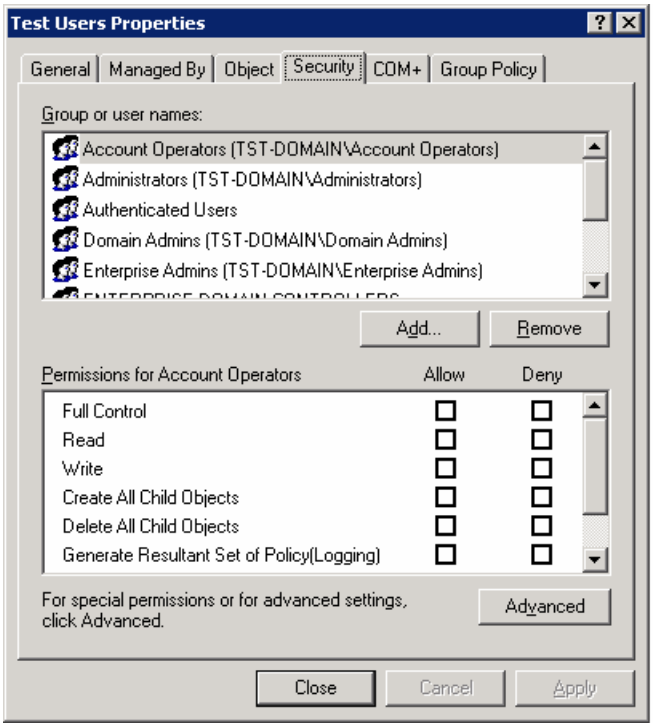
Důležitou volbou této konzole je *View / Advanced Features*. Tato volba zpřístupní záložky zobrazující zabezpečení případně umístění objektu ve struktuře AD. Dále jsou zobrazeny systémové kontejnery, které jsou normálně skryté. Tato konzole je dostupná na všech řadičích domény. Je možné ji nainstalovat i na pracovní stanici. Aplikace je součástí balíku adminpak.msi na instalačním CD Windows 2003. Je možné ji stáhnout i z webu firmy Microsoft.

Organizační jednotky

Základním rozdílem mezi organizační jednotkou a skupinou je v tom, že organizační jednotka nemůže být použita pro přiřazení práv k jinému objektu v síti (sdílená složka, tiskárna apod.). Narozdíl od skupiny je možné k OU přiřadit objekt GPO.



Vlastnosti organizační jednotky

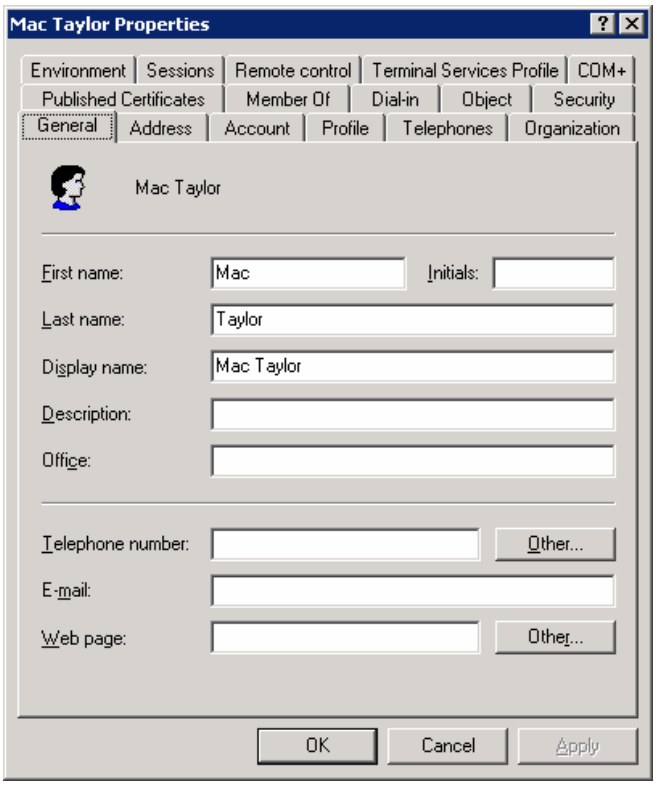


Uživatelům je možné delegovat oprávnění pro správu objektů v OU.

Uživatelé

Účet uživatele je nutný pro přihlášení do domény, přístup k síťovým prostředkům atd. Každý uživatelský účet má rozličné vlastnosti. Tyto vlastnosti je možné nadále rozšiřovat novou definicí ve schématu Active Directory. Přidání vlastností může být provedeno ručně např. pomocí konzole Active Directory Schema nebo je způsobeno instalací některé aplikace. Změny schématu provádí aplikace jako MS Exchange, MS Live Communication Server 2005 apod.

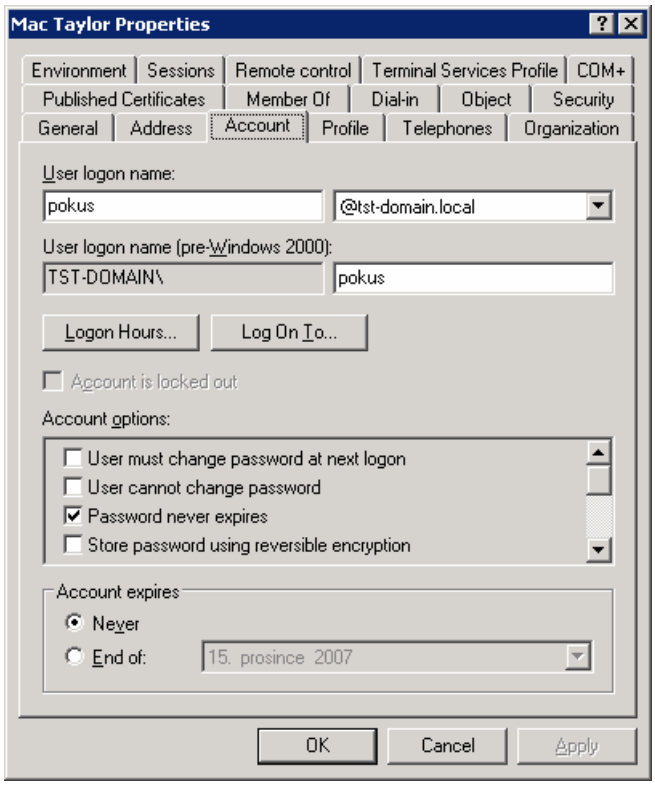
K základním vlastnostem uživatelského účtu patří jméno, adresa, popis.



Zajímavější jsou nastavení týkající se přímo účtu. Pomocí těchto nastavení lze vynutit změny hesla, čas vypršení účtu nebo povolit přihlášení pouze na určité počítače případně v určitou dobu. Heslo je jednocestně šifrováno tzv. hash. Kvůli tomu není možné heslo zjistit ani pokud máte oprávnění administrátora. V případě, že je zapotřebí hesla z nějakého důvodu dekryptovat je nutné použít volbu *Store password using reversible encryption*. Na této záložce je také možné účet uzamknout.

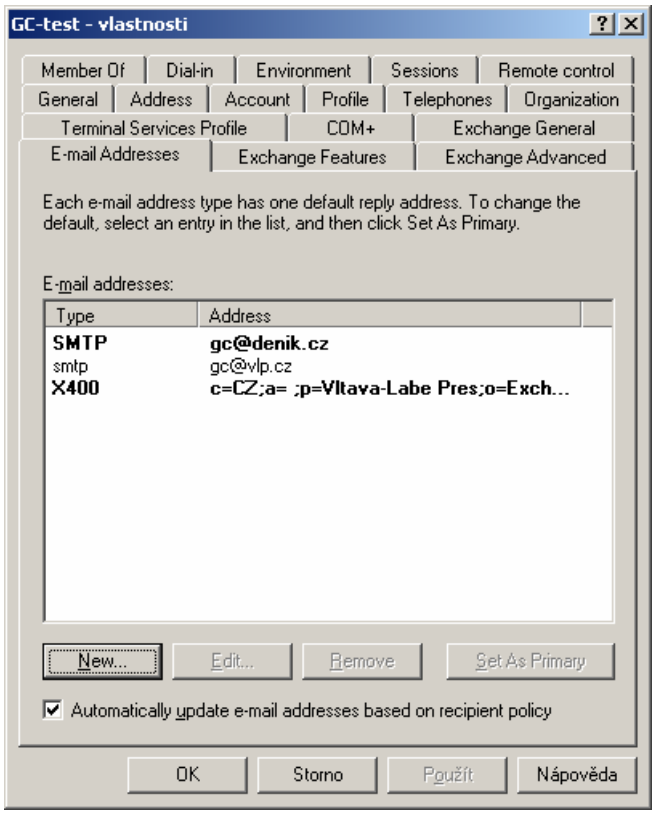
V případě, že je zapnuto zobrazování Advanced Features je na záložce Object vidět umístění objektu v Active Directory ve formátu:

tst-domain.local/Test Users/Mac Taylor



Nastavení účtu uživatele

K dalším vlastnostem uživatelského účtu patří nastavení pravidel pro vzdálené přihlášení. A samozřejmě členství ve skupinách.



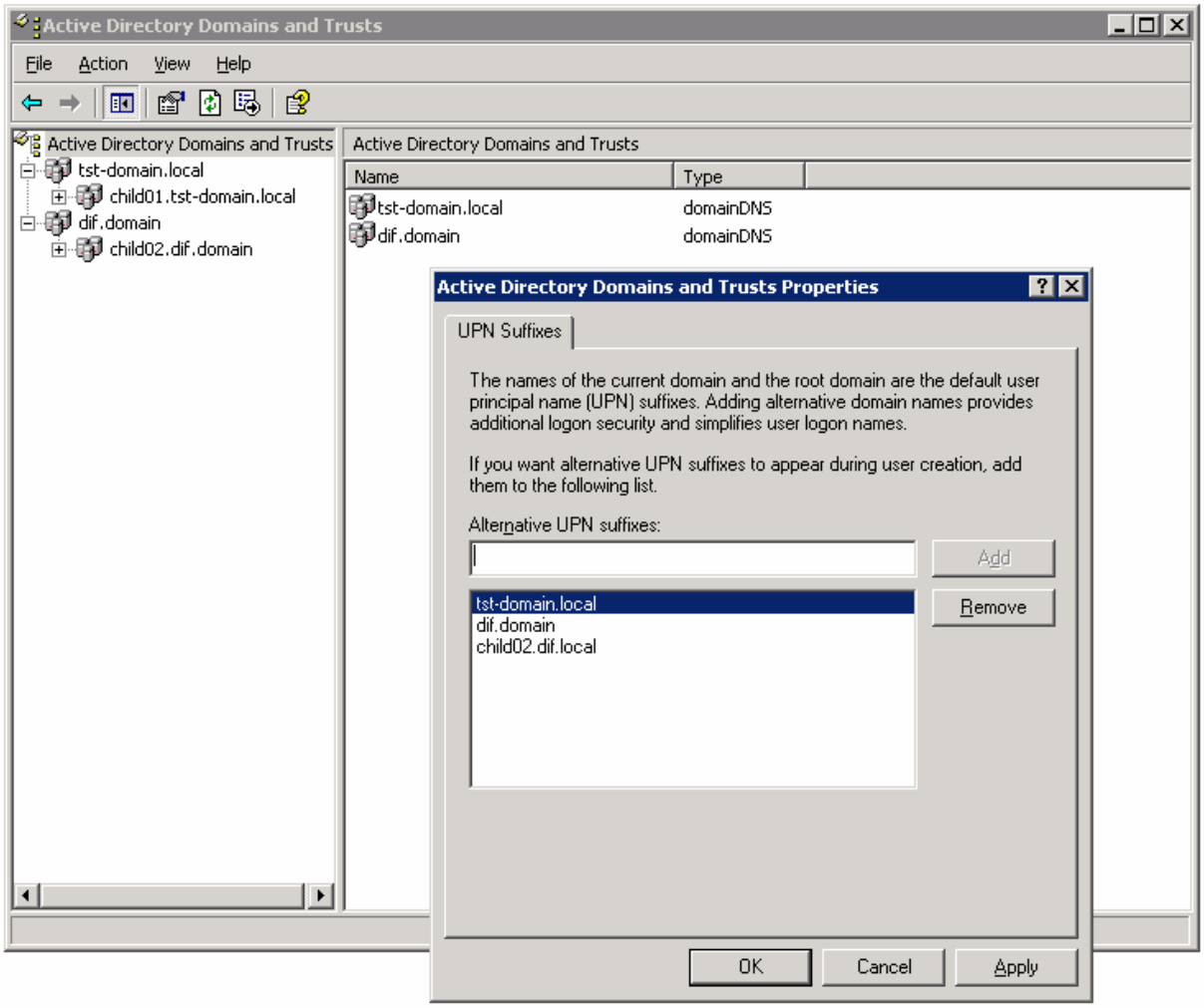
Panel vlastností uživatele v rozšířeném schématu Active Directory

User Principal Name

Pro přihlášení do domény Active Directory je možné použít několik formátů přihlašovacího jména.

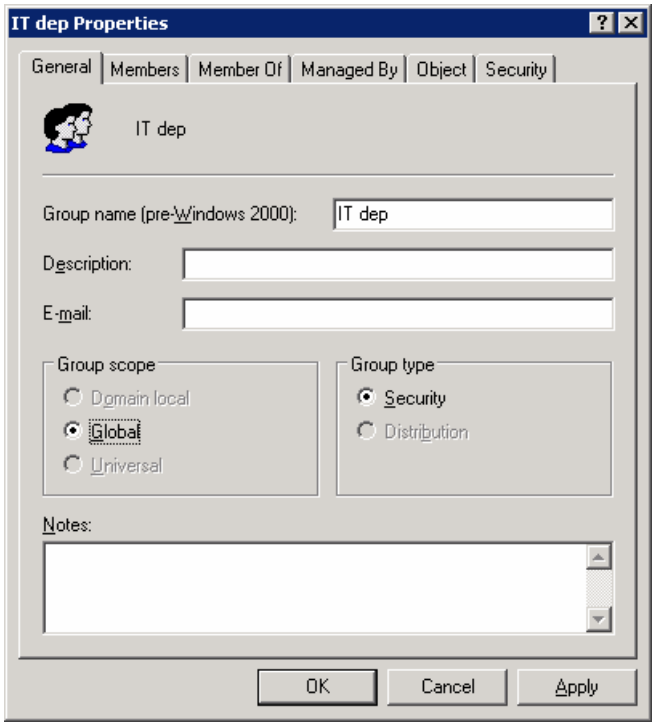
- Domain Name \ User Name (MOJE\Filip)
- Doted Domain Name \ User Name (moje.local\Filip)
- User Principal Name (Filip@moje.local)

Poslední zmiňovaný formát přihlašovacího jména vychází z RFC 822. Je ve formátu e-mailové adresy. V případě, že máme v rámci domén, které si navzájem důvěřují zaveden systém unikátních uživatelských jmen, je možné definovat, které přípony má systém vyzkoušet při přihlašování. To usnadní uživatelům přihlašování do domény.



Výběr UPN suffixes v rámci lesa AD

Skupiny



Vlastnosti skupiny uživatelů

Pro přístup k síťovým prostředkům by měli sloužit skupiny, nikoliv přímo uživatelé. Skupina obsahuje členy *Members*, ale zároveň může být členem jedné nebo více skupin *Member Of*.

Použití univerzálních skupin: univerzální skupiny by měli obsahovat globální skupiny. Mohou být použity pro nastavení oprávnění k prostředkům v různých doménách. Univerzální skupiny pro zabezpečí je možné používat od funkční úrovně Windows 2000 Native.

Použití globálních skupin: globální skupiny jsou viditelné v celém lese. Není proto vhodné je používat pro nastavení oprávnění v rámci jedné domény. Globální skupiny je vhodné používat jako kontejnery pro organizaci uživatelů a skupin.

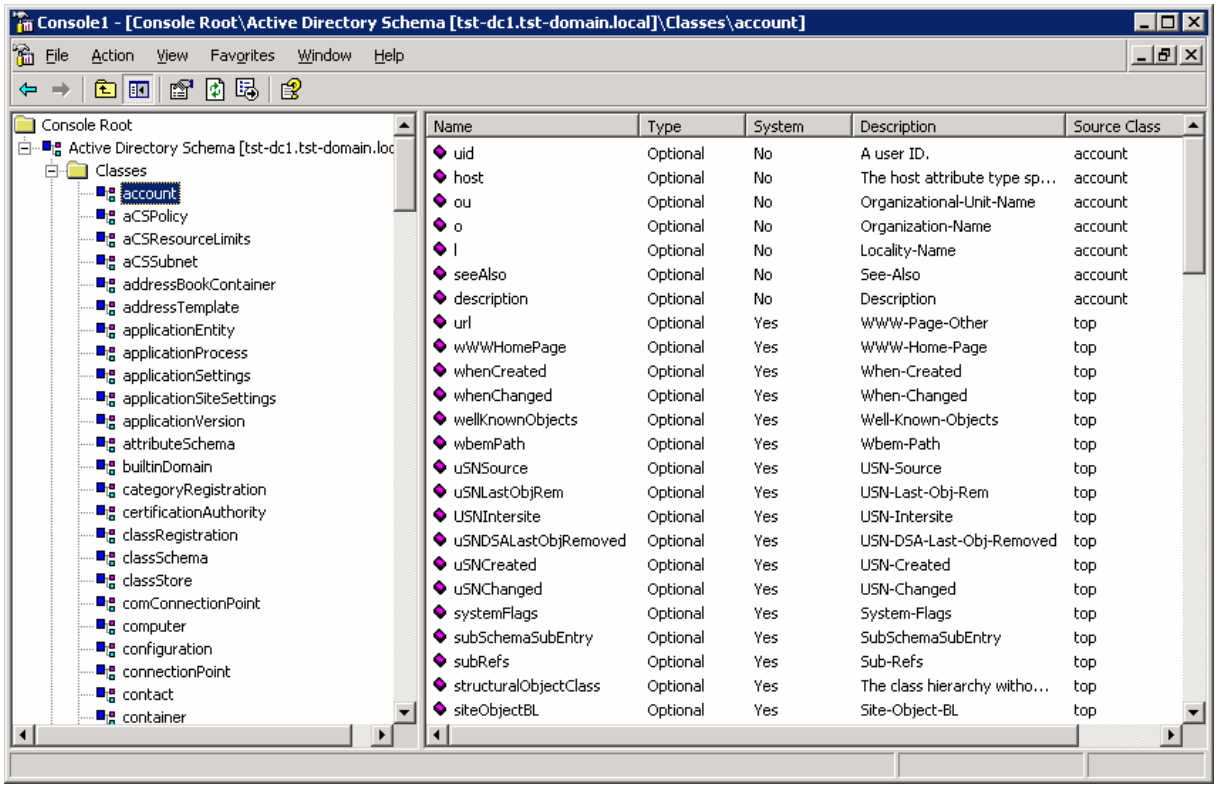
Použití doménových lokální skupin: tyto skupiny jsou vhodné pro přiřazení oprávnění v rámci domény, kde byly vytvořeny. Lokální skupiny mohou obsahovat všechny ostatní typy skupin i uživatelské účty ze všech domén v lese.

Schema Active Directory

V případě, že je zapotřebí přidávat atributy k objektům v AD slouží k tomu konzole Active Directory Schema. K modifikacím schématu je zapotřebí být členem skupiny Schema Admins. Konzole je ve výchozím stavu nepřístupná a je zapotřebí ji aktivovat. Nejprve je nutné registrovat knihovnu schmmgmt.dll:

regsvr32 schmmgmt.dll

Poté již je možné přidat do konzole MMC snap-in Active Directory Schema:



Konzole MMC pro správu schématu Active Directory

Pomocí této konzole je také možné přesunout roli Schema Master na jiný doménový řadič.