Serverové systémy Microsoft Windows

IW2/XMW2 2011/2012

Jan Fiedor

ifiedor@fit.vutbr.cz

Fakulta Informačních Technologií

Vysoké Učení Technické v Brně

Božetěchova 2, 612 66 Brno

Revize 11.3.2012

Active Directory

Schéma, Objekty, Operační servery

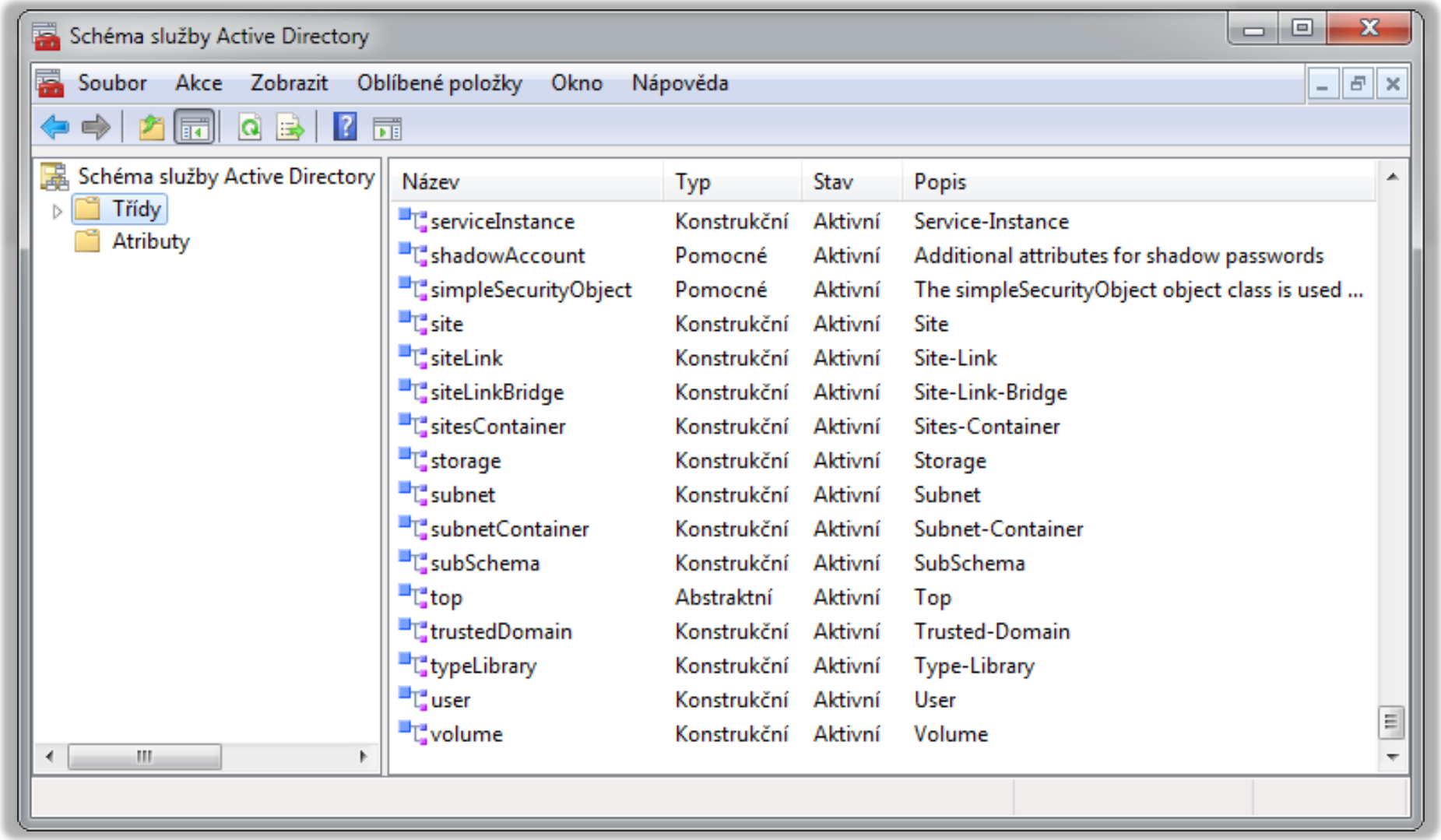
Schéma služby Active Directory

- Formální definice obsahu a struktury adresářové služby Active Directory
  - Stejné pro celý les Active Directory
- Obsahuje
  - Definice tříd Active Directory
  - Definice atributů Active Directory
- Správa pomocí modulu snap-in Schéma adresáře Active Directory
  - Musí být zaregistrován (**regsvr32 schmmgmt.dll**)

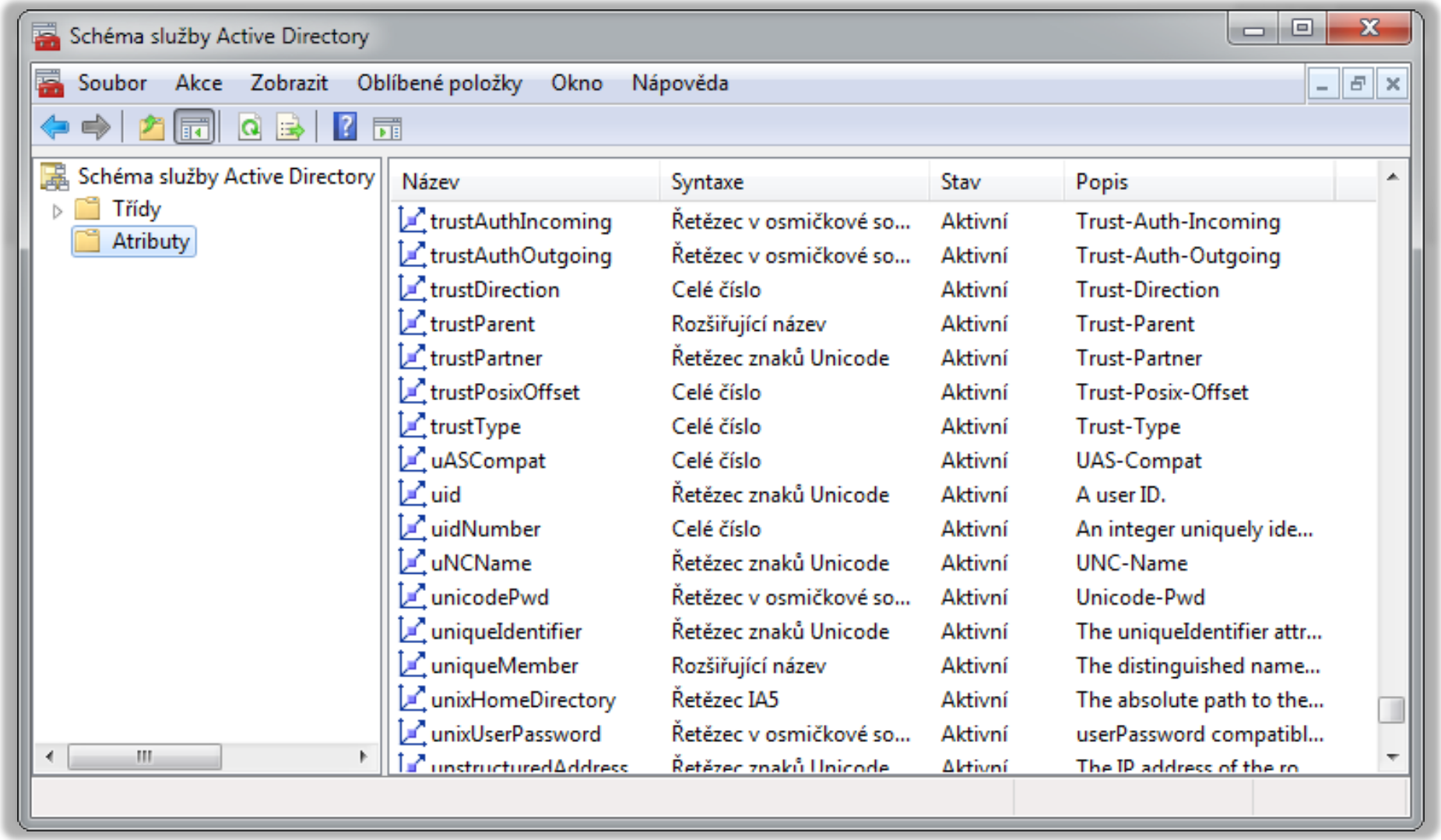
Definice tříd objektů Active Directory

- Každá třída identifikována unikátním OID (*Object Identifier*) identifikátorem
  - Sada čísel oddělených tečkami (stromová hierarchie)
  - Microsoft přidělen prefix 1.2.840
- Každá třída obsahuje definice
  - Možných nadřazených (*parent*) tříd (*poss-superiors*)
  - Vyžadovaných atributů (*must-contain*)
  - Volitelných atributů (*may-contain*)

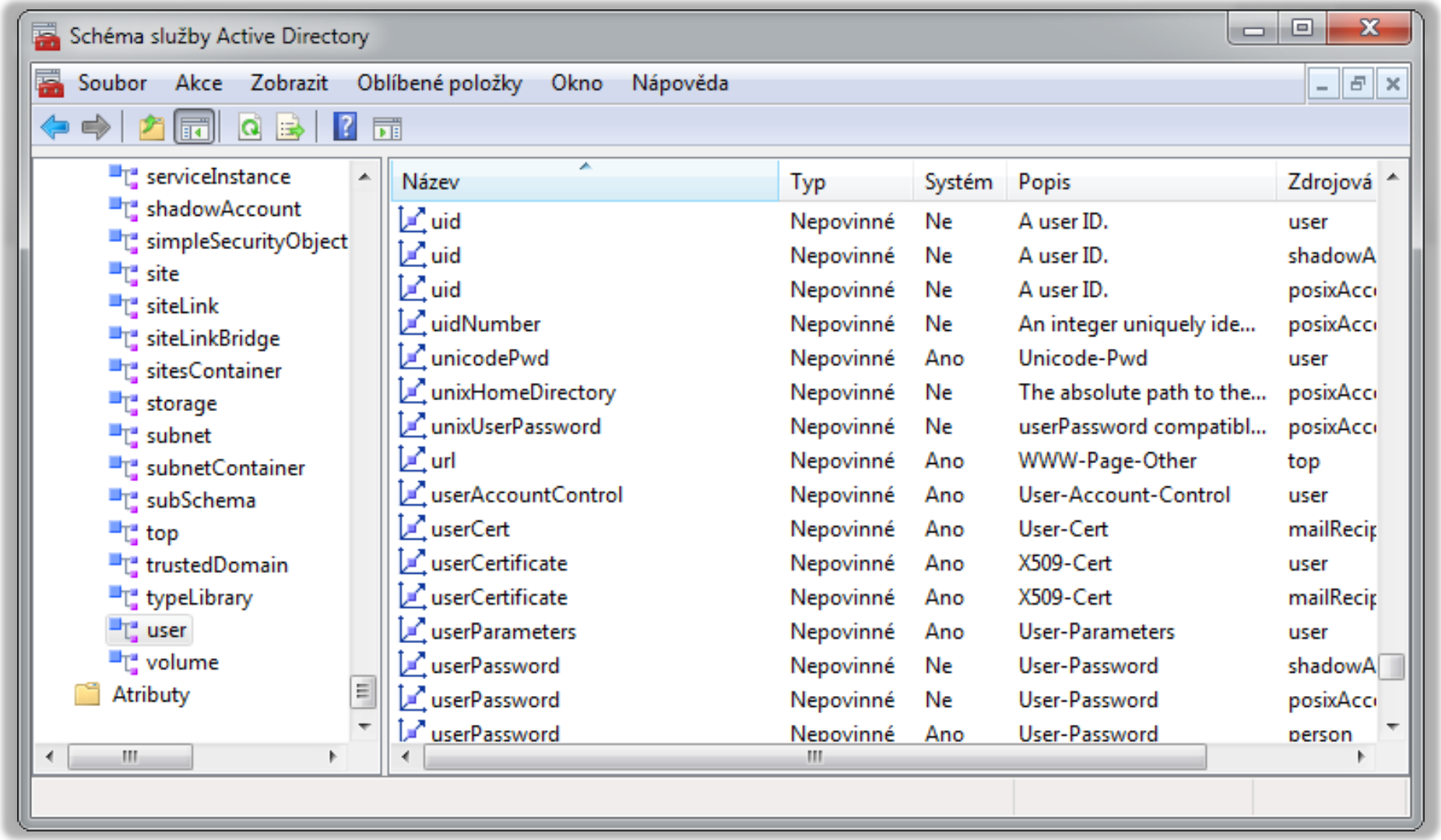
Příklady tříd Active Directory



Příklady atributů Active Directory



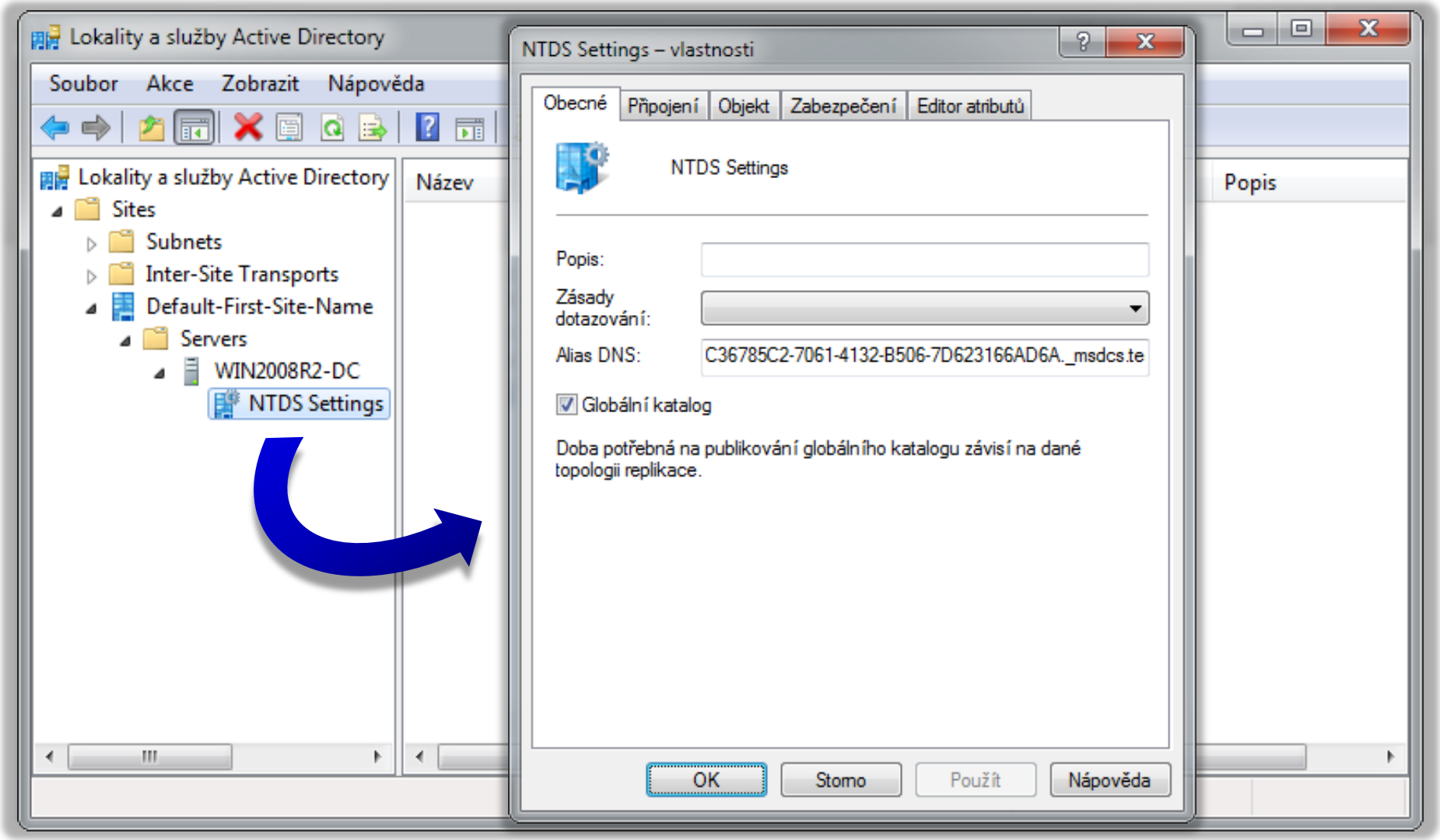
Příklady atributů tříd Active Directory



Globální katalog (Global Catalog)

- Obsahuje částečné informace o všech objektech v lese Active directory (vhodné pro vyhledávání)
  - Lze považovat za index databáze Active Directory
  - Obsahuje informace o univerzálních skupinách
- Obsahuje hodnoty vybraných atributů objektů
  - Výběr těchto atributů ve schématu Active Directory
- Může být přítomen na každém řadiči domény
  - Vhodné mít alespoň 2 v každé doméně (redundance)
  - Povolení přes Lokality a služby Active Directory

Povolení globálního katalogu



Objekty Active Directory

- Identifikace objektů v Active Directory
  - GUID (*Globally Unique Identifier*)
  - SID (*Security Identifier*)
  - DN (*Distinguished Name*)
- Základní objekty Active Directory
  - Uživatelé (*Users*)
  - Skupiny (*Groups*)
  - Počítače (*Computers*)
  - Organizační jednotky (*Organizational Units*)

Identifikace objektů v Active Directory

- GUID (*Globally Unique Identifier*)
  - Interní identifikace objektů Active Directory
  - 128-bitové číslo unikátní v rámci celého světa
  - Nikdy se nemění
  - Atribut **objectGUID**
- SID (*Security Identifier*)
  - Může se měnit (přesuny mezi doménami, lesy, …)
  - Atribut **objectSid**
- DN (*Distinguished Name*)

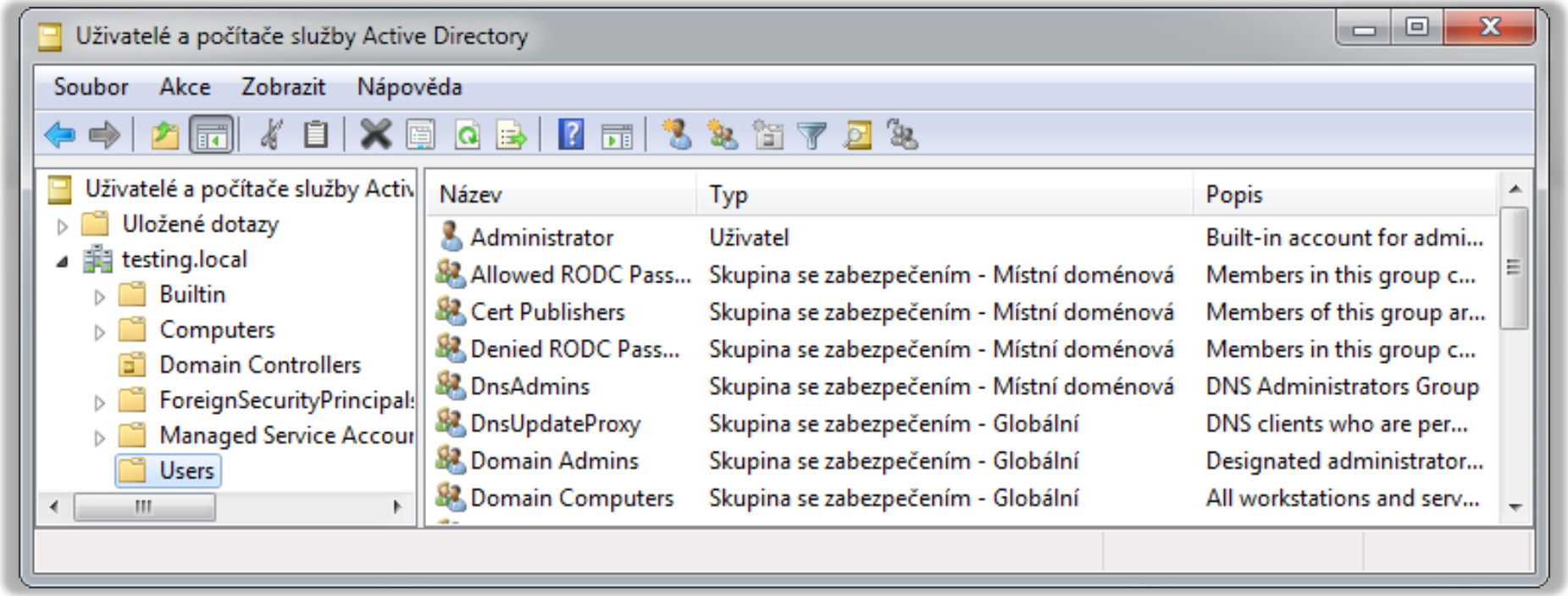
Distinguished Names (DNs)

- Identifikace objektů používaná protokolem LDAP
  - Zachycuje interní i externí strukturu Active Directory
- Sekvence RDN jmen oddělených čárkou na cestě z objektu AD do kořene stromu Active Directory (kořenového uzlu stromu doménových jmen)
- RDN (*Relative Distinguished Name*)
  - Atribut s asociovanou hodnotou
  - UTF-8 řetězec ve formátu ***<atribut>=<hodnota>***

Atributy RDN jmen

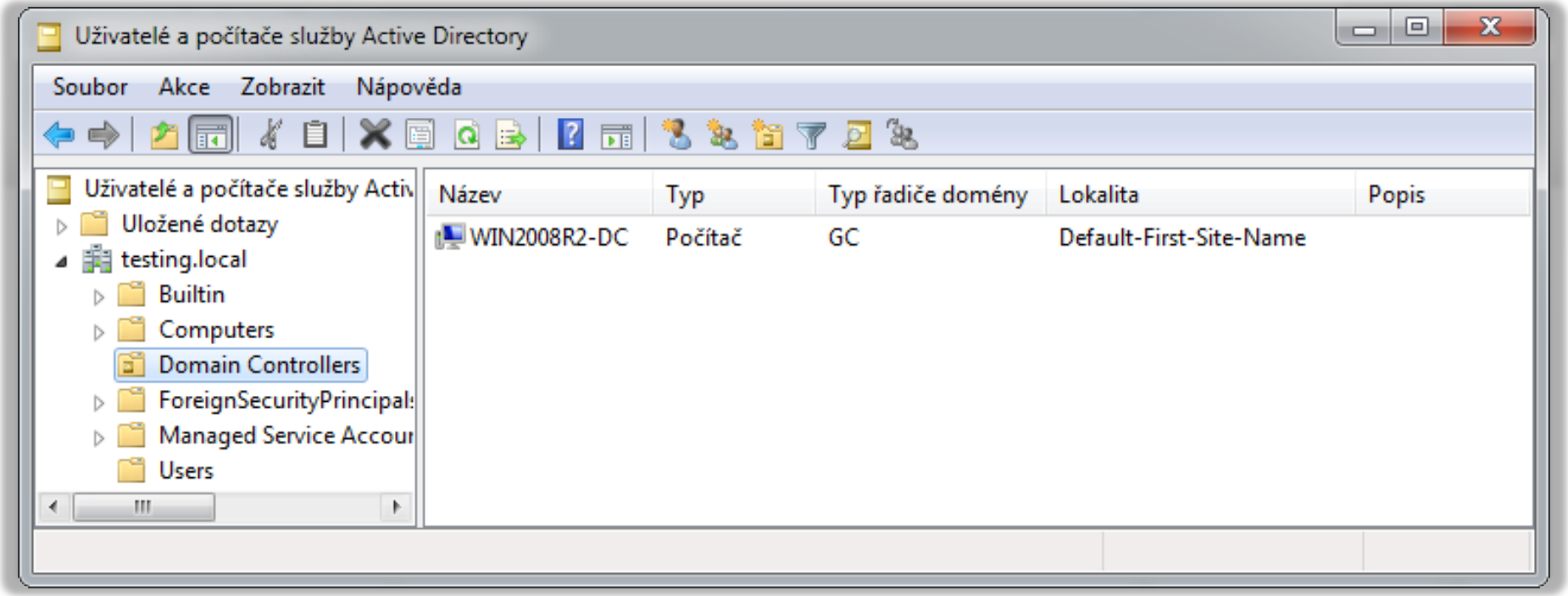
Atribut	Typ	Příklad objektů / atributů
DC	domainComponent	Část názvu domény (uzel v doménovém stromu)
CN	commonName	Uživatel, skupina, počítač, kontejner, …
OU	organizationalUnitName	Organizační jednotka
O	organizationName	Organizace
STREET	streetAddress	Adresa
L	localityName	Město
ST	stateOrProvinceName	Stát
C	countryName	Země
UID	userid	Identifikátor uživatele

Příklady DN jmen uživatelů a skupin



DN jméno pro uživatele **Administrator**
CN=Administrator, CN=Users, DC=testing, DC=local
DN jméno pro skupinu **Domain Admins**
CN=Domain Admins, CN=Users, DC=testing, DC=local

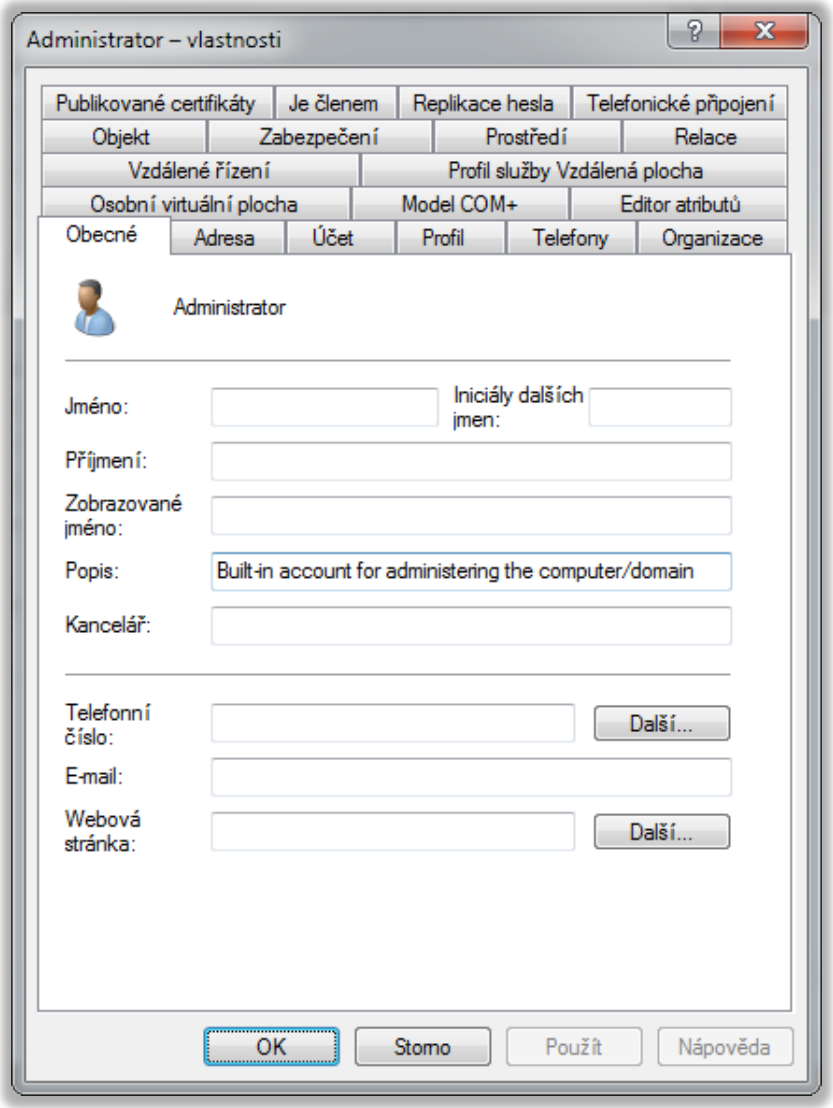
Příklady DN jmen počítačů a OU



DN jméno pro počítač **WIN2008R2-DC**
CN=WIN2008R2-DC, OU=Domain Controllers, DC=testing, DC=local
DN jméno pro organizační jednotku **Domain Controllers**
OU=Domain Controllers, DC=testing, DC=local

Uživatelé (Users)

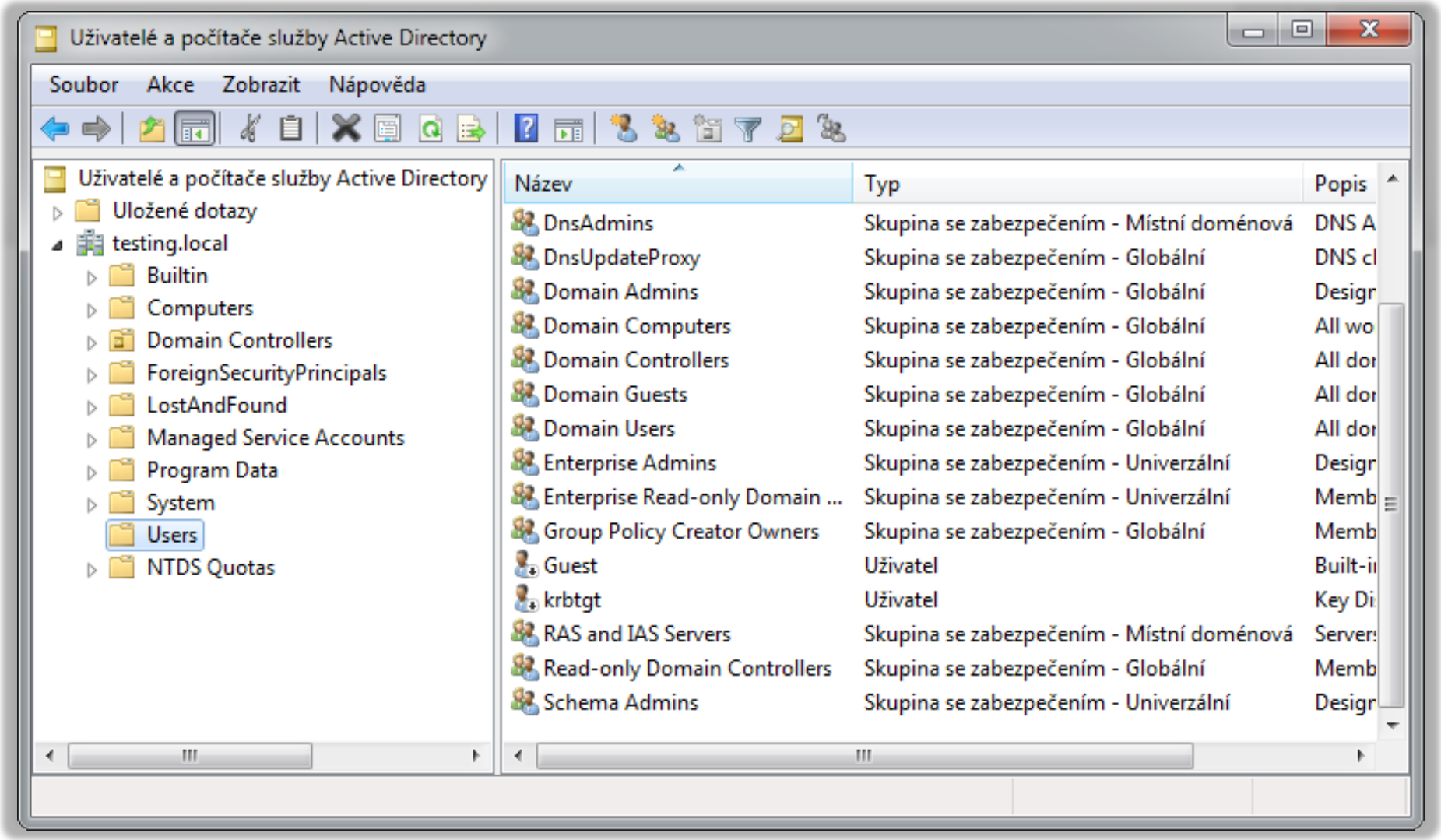
- Jména (objektů) uživatelů
  - **sAMAccountName** (login)
    - Pre-Windows 2000 logon
    - Unikátní v rámci domény
  - **userPrincipalName** (UPN)
    - ***<login>@<doména>***
    - Unikátní v rámci lesa
- Účty nově vytvářených uživatelů ukládány do kontejneru **Users**
  - Lze změnit pomocí příkazu **redirusr *<DN>***



Hromadné vytváření uživatelů

- Použitím šablon účtů (*account templates*)
- Pomocí nástroje **csvde** / **ldifde**
  - Importuje (vytvoří) uživatele z CSV / LDIF souboru
  - Nelze importovat hesla
  - Účty jsou po vytvoření zakázané
- Vytvořením skriptu
  - Pro příkazový řádek
  - Pro Visual Basic (VBScript)
  - Pro Windows PowerShell

Správa uživatelů pomocí ADUC



Správa pomocí příkazové řádky

Příkaz	Popis
dsadd <*typ-objektu*> <*DN*>	Přidání objektu
dsrm <*typ-objektu*> <*DN*>	Smazání objektu
dsmove <*DN*> -newname <*RDN*>	Přejmenování objektu
dsmove <*DN*> -newparent <*DN*>	Přesunutí objektu
dsmod <*typ-objektu*> <*DN*>	Změna hodnot atributů objektu
dsget <*typ-objektu*> <*DN*>	Získání hodnot atributů objektu
dsquery <*typ-objektu*> <*DN*>	Vyhledávání objektů

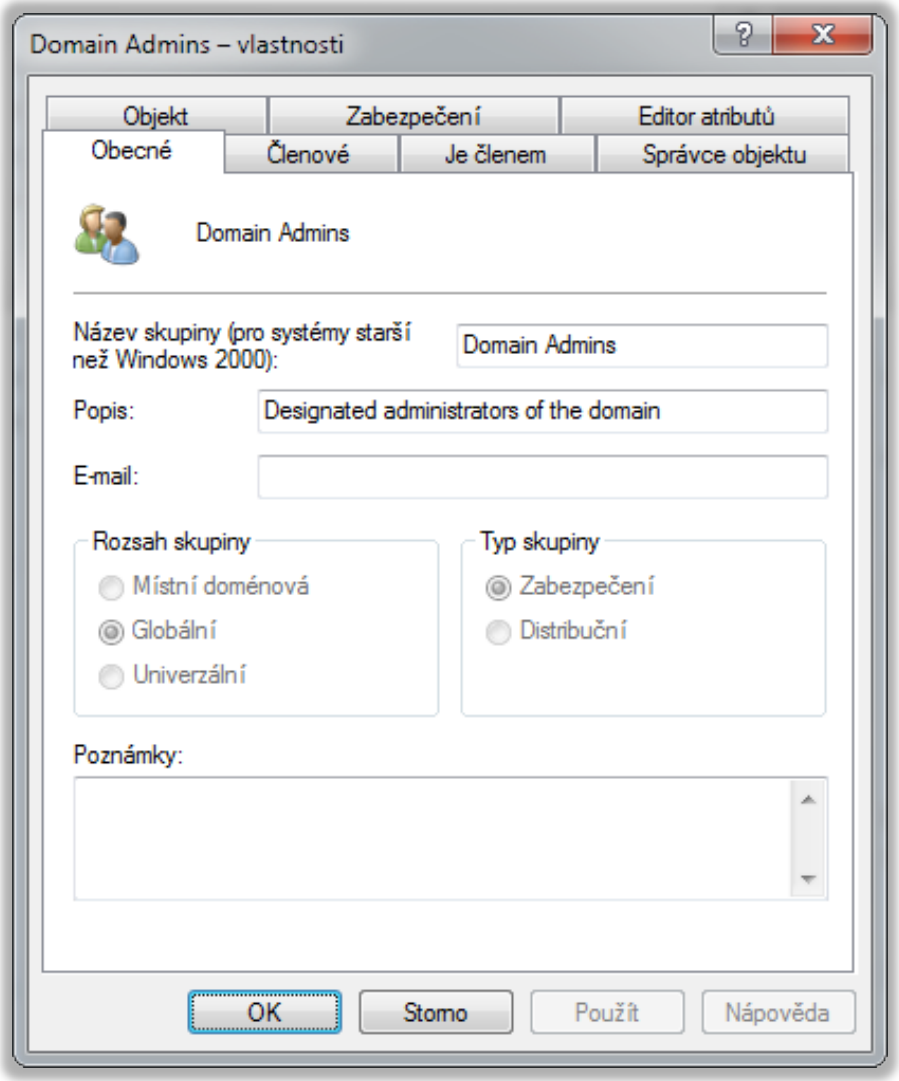
Typ objektu	Popis
user	Uživatelský účet
computer	Účet počítače
group	Skupina
ou	Organizační jednotka

Správa pomocí Windows PowerShell

Akce	Příkaz
Získání reference na objekt	**<*objekt*> = [ADSI]"LDAP://<*DN*>"**
Přidání objektu	**<*kontejner*>.Create("<*typ-objektu*>", "<*RDN*>")**
Smazání objektu	**<*kontejner*>.Delete("<*typ-objektu*>", "<*RDN*>")**
Smazání všech objektů v kontejneru	**<*kontejner*>.DeleteTree()**
Přejmenování / přesunutí objektu	**<*objekt*>.MoveTo("<*kontejner*>", "<*RDN*>")**
Změna hodnot atributů objektu	**<*objekt*>.<*set-metoda*>("<*hodnota*>")** **<*objekt*>.put("<*atribut*>", "<*hodnota*>")** **<*objekt*>.InvokeSet("<*atribut*>", "<*hodnota*>")**
Získání hodnot atributů objektu	**<*objekt*> | Format-List *** **<*objekt*> | Format-List -property <*atribut*>**
Vyhledávání objektů	Třída **DirectoryServices.DirectorySearcher**
Potvrzení akcí nad objektem	**<*objekt*>.SetInfo()**

Skupiny (Groups)

- Hlavní identity pro řízení přístupu ke zdrojům
- Mohou ovlivňovat rozsah aplikace zásad skupiny
- Stínové (*shadow*) skupiny
  - Obsahují stejné uživatele jako organizační jednotky



Typy skupin

- Distribuční skupiny (*Distribution Groups*)
  - Nemají SID identifikátor
    - Nelze jim nastavovat oprávnění pro přístup ke zdrojům
  - Primárně určeny pro rozesílání elektronické pošty
- Bezpečnostní skupiny (*Security Groups*)
  - Mají vlastní SID identifikátor
    - Reprezentuje identitu
  - Lze je použít i jako distribuční skupiny
    - Nedoporučuje se (nárůst počtu SID v přístupovém tokenu)

Rozsahy skupin (group scopes)

- Lokální (*Local*)
- Doménově lokální (*Domain Local*)
- Globální (*Global*)
- Univerzální (*Universal*)

Lokální skupiny

- Primárně používány pro
  - Správu přístupů ke zdrojům v pracovních skupinách (minimální využití v doménovém prostředí)
- Definovány v SAM (*Security Accounts Manager*) databázi jednotlivých počítačů
  - Nejsou replikovány na jiné počítače
- Dostupné
  - Pouze na počítači, na kterém byly definovány

Členství

- Mohou obsahovat
  - Uživatele, počítače, globální skupiny nebo doménově lokální skupiny z domény daného počítače
  - Uživatele, počítače a globální skupiny
    - Z jakékoliv domény v daném lese
    - Z jakékoliv důvěryhodné domény
  - Univerzální skupiny z jakékoliv domény daného lesa
- Mohou být členy
  - Lokálních skupin na daném počítači

Doménově lokální skupiny

- Primárně používány pro
  - Správu přístupů ke zdrojům v doméně
- Definovány v jedné konkrétní doméně
  - Replikovány na všechny řadiče domény této domény
- Dostupné
  - Pouze v doméně, ve které byly definovány

Členství

- Mohou obsahovat
  - Uživatele, počítače, globální skupiny nebo doménově lokální skupiny z domény daného počítače
  - Uživatele, počítače a globální skupiny
    - Z jakékoliv domény v daném lese
    - Z jakékoliv důvěryhodné domény
  - Univerzální skupiny z jakékoliv domény daného lesa
- Mohou být členy
  - Lokálních skupin na všech počítačích v dané doméně
  - Doménově lokálních skupin v dané doméně

Globální skupiny

- Primárně používány pro
  - Definici rolí v rámci domény
  - Vytváření kolekcí doménových objektů (uživatelů, …)
- Definovány v jedné konkrétní doméně
  - Replikovány na všechny řadiče domény této domény
- Dostupné
  - Ve všech doménách v daném lese
  - Ve všech důvěryhodných doménách

Členství

- Mohou obsahovat
  - Uživatele, počítače a globální skupiny z dané domény
- Mohou být členy
  - Doménově lokálních a univerzálních skupin ze všech domén v daném lese
  - Doménově lokálních skupin z důvěryhodných domén

Univerzální skupiny

- Primárně používány pro
  - Definici rolí rozprostřených přes více domén
  - Správu zdrojů rozprostřených přes více domén
- Definovány v jedné konkrétní doméně
  - Replikovány na všechny řadiče domény v daném lese, které obsahují globální katalog
- Dostupné
  - Ve všech doménách v daném lese

Členství

- Mohou obsahovat
  - Uživatele, globální skupiny a univerzální skupiny z kterékoliv domény v daném lese
- Mohou být členy
  - Doménově lokálních a univerzálních skupin ze všech domén v daném lese

Shrnutí možných členství ve skupinách

Možná členství ve skupinách		Členská skupina (může být členem)			
		Lokální	**Doménově lokální**	**Globální**	**Univerzální**
Cílová skupina (může obsahovat)	**Lokální**	Počítač	Doména	Les, důvěryhodná doména	Les
	Doménově lokální		Doména	Les, důvěryhodná doména	Les
	Globální			Doména	
	Univerzální			Les	Les

Vestavěné skupiny (built-in groups)

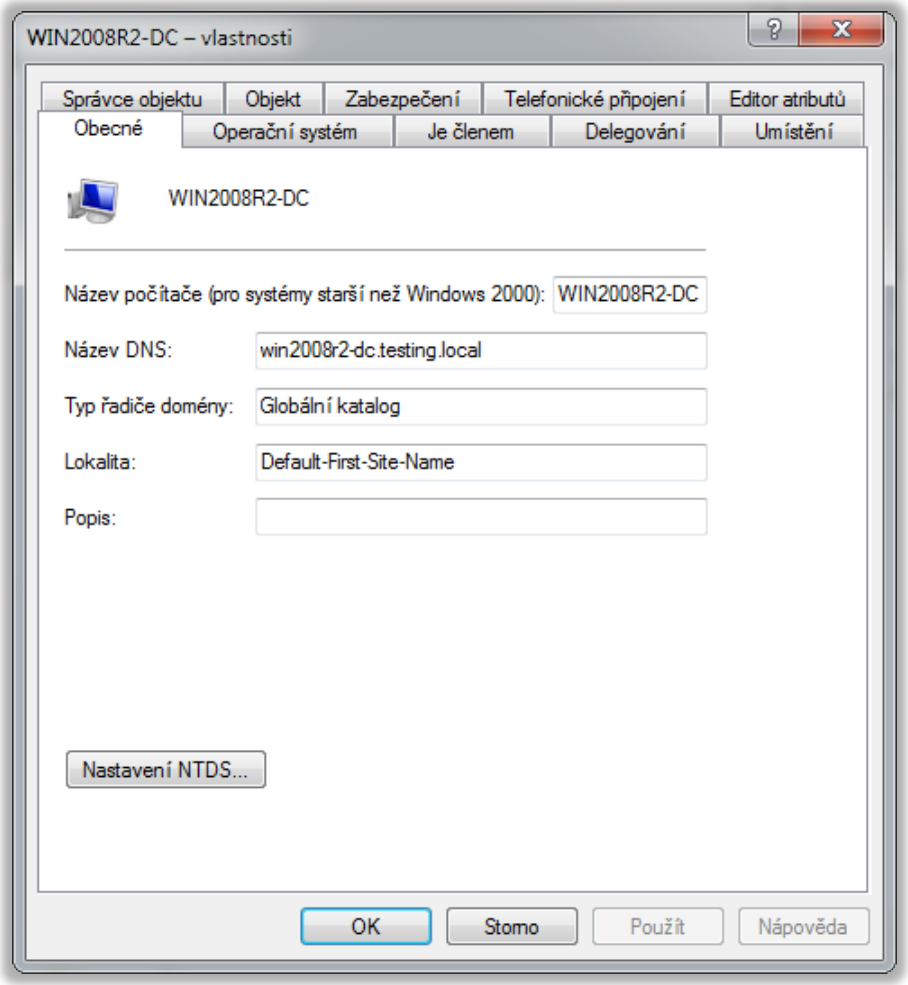
Skupina	Popis
Administrators	Správci všech řadičů domén (změny členství ve všech skupinách, plná kontrola nad oddílem domény, …)
Enterprise Admins	Správci lesa (přidávání a odebírání domén, autorizace DHCP serveru, …), vlastní oddíl konfigurace AD
Schema Admins	Správci schématu (změny definic tříd, atributů, …)
Domain Admins	Správci domény (správa objektů, nastavení, …)
Domain Users	Všichni uživatelé v doméně
Domain Computers	Všechny počítače v doméně
Domain Controllers	Všechny řadiče domény v doméně
Read-only Domain Controllers	Všechny read-only řadiče domény v doméně
Group Policy Creator Owners	Uživatelé, jenž mohou vytvářet objekty zásad skupiny
Server Operators	Uživatelé, jenž mohou provádět údržbu řadičů domén
Account Operators	Uživatelé, jenž mohou spravovat účty uživatelů, …

Speciální skupiny (special identities)

Skupina	Popis
Anonymous Logon	Spojení bez poskytnutí pověření (jména a hesla)
Authenticated Users	Identity, jenž byly ověřeny řadičem domény
Everyone	Zahrnuje všechny ověřené uživatele a uživatele **Guest**
Interactive	Obsahuje uživatele, jenž přistupují ke zdroji, který je umístěn na stejném počítači na kterém je daný uživatel přihlášen (zahrnuje také uživatele připojené přes vzdálenou plochu)
Network	Obsahuje uživatele, jenž přistupují ke zdroji přes síť (na počítači, na kterém nejsou sami přihlášeni)

Počítače (Computers)

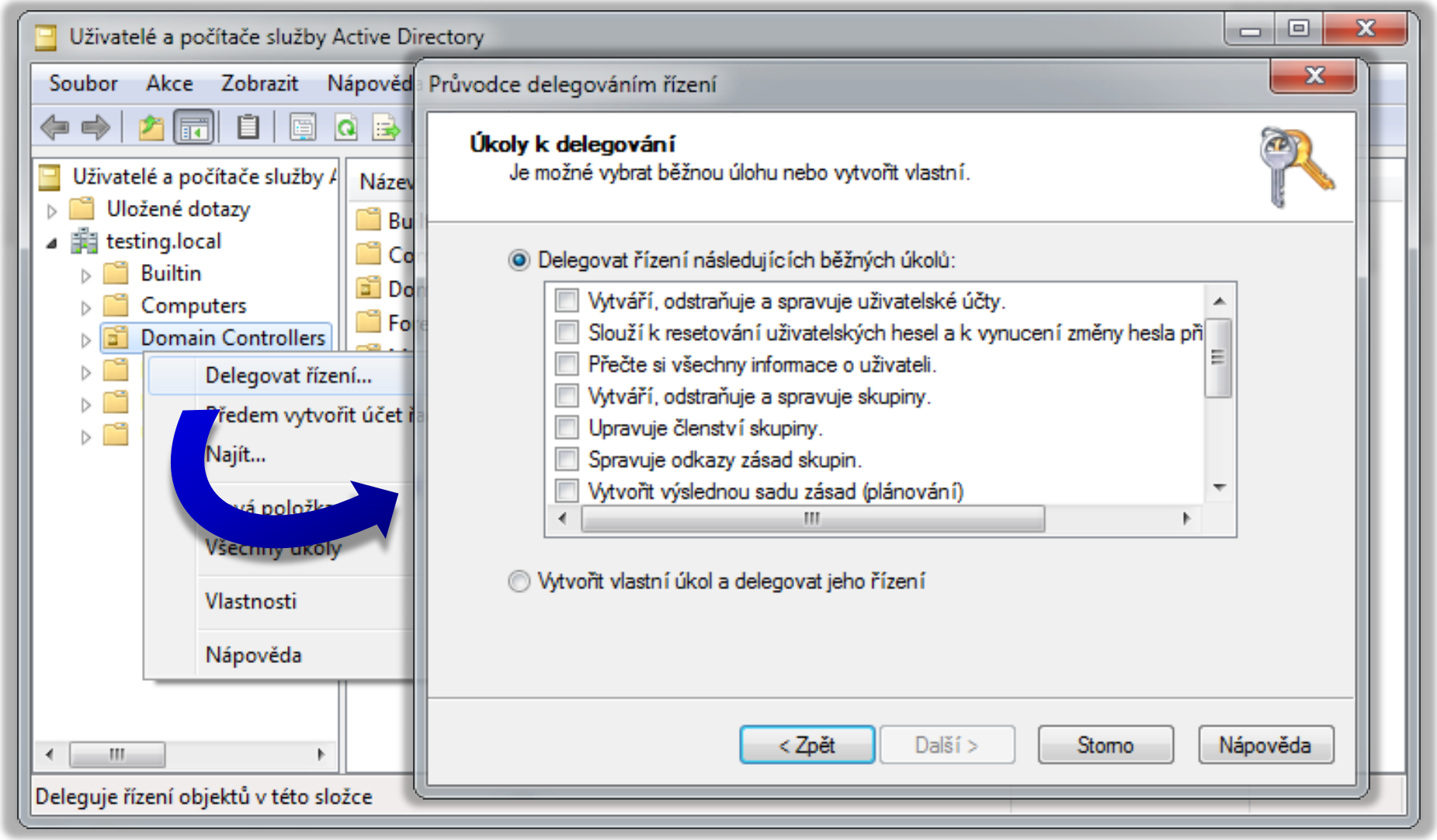
- Účty vytvářeny systémem při připojení do domény
  - Hesla měněna co 30 dní
  - Lze předpřipravit dopředu
- Účty nově vytvářených počítačů ukládány do kontejneru **Computers**
  - Lze změnit pomocí příkazu **redircmp *<DN>***



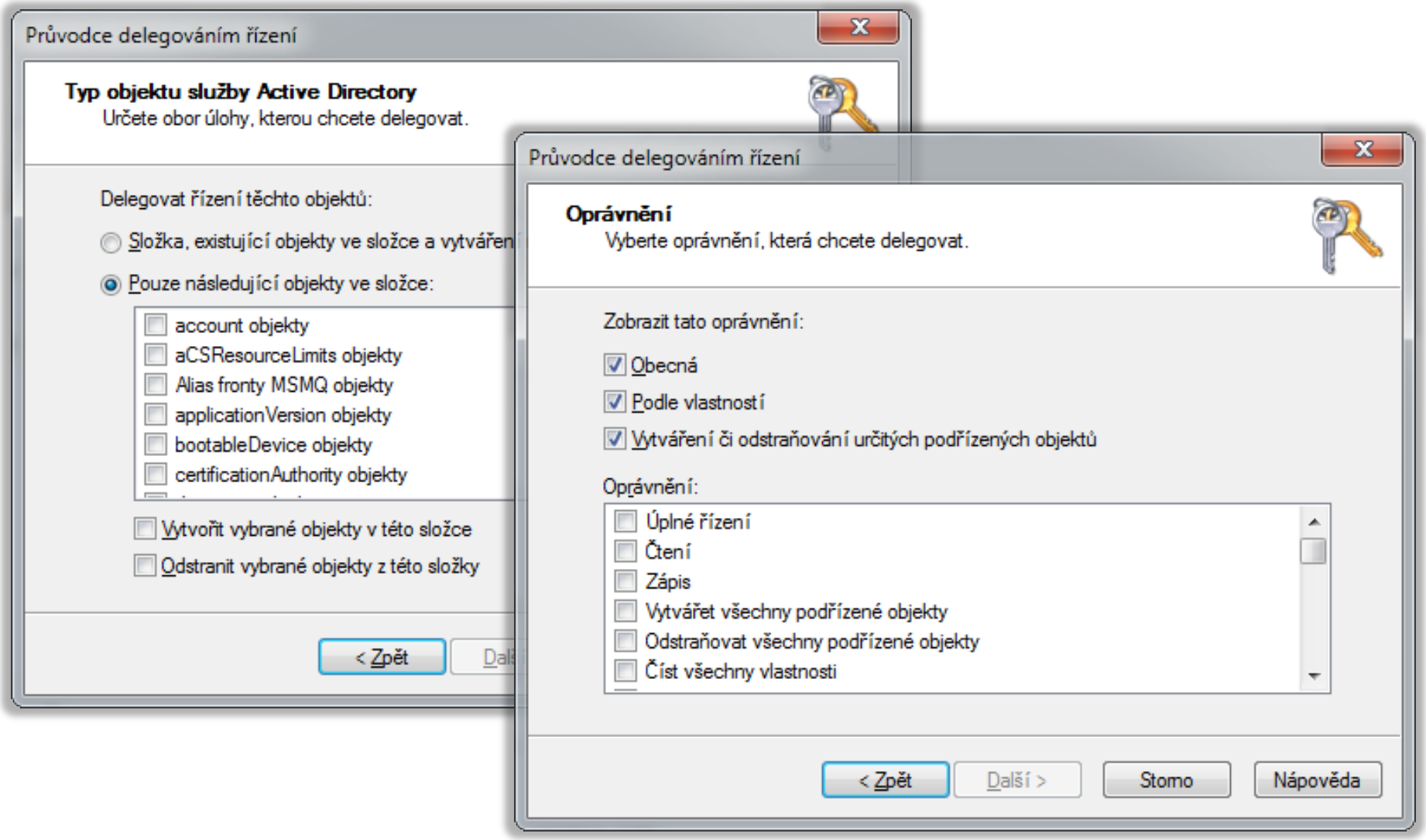
Delegace řízení (delegation of control)

- Určení uživatelů nebo skupin, jenž budou moci provádět určité akce s objekty Active Directory
  - Přiřazení oprávnění, jenž spravují přístup k objektům Active Directory a jejich atributům
  - Vztahuje se na vybrané objekty v konkrétní doméně, kontejneru nebo organizační jednotce
    - Delegovaná oprávnění se dědí do podřízených kontejnerů
- Lze realizovat
  - Nastavením příslušných oprávnění v ACL seznamech
  - Pomocí Průvodce delegováním řízení

Průvodce delegováním řízení



Výběr cílových objektů a oprávnění



Operační servery (Operations Masters)

- Řadiče domény zajišťující realizaci FSMO operací (*Flexible Single-Master Operations*)
  - Operace, které musí provádět vždy pouze jediný člen domény nebo lesa Active Directory
  - Zabraňují konfliktním aktualizacím dat, kde by řešení těchto konfliktů bylo nevhodné (nebo nemožné)
- Dvě kategorie FSMO operací
  - Operace prováděné na úrovni lesa (*forest-wide*)
  - Operace prováděné na úrovni domény (*domain-wide*)
    - Změna přes Uživatele a počítače služby Active Directory

FSMO operace na úrovni lesa

- Pojmenování domén (*Domain Naming*)
  - Zajišťuje přidávání a odebírání domén v lese
  - Změna přes Domény a vztahy důvěryhodnosti služby Active Directory
- Schéma (*Schema*)
  - Umožňuje modifikace schématu Active Directory
  - Ostatní řadiče domény obsahují *read-only* kopii
  - Změna přes Schéma adresáře Active Directory

FSMO operace na úrovni domény

- RID (*Relative Identifier*)
  - Přiděluje rozsahy RID identifikátorů řadičům domény
  - SID identifikátory objektů vytvářeny připojením RID identifikátoru k SID identifikátoru domény
- Infrastruktura (*Infrastructure*)
  - Aktualizuje reference na objekty z jiných domén při jejich přejmenování nebo přesunutí
- Primární řadič domény (*PDC Emulator*)

Primární řadič domény (1)

- Emuluje funkci PDC (*Primary Domain Controller*)
  - Umožňuje starším aplikacím provádět změny v Active Directory databázi
- Umožňuje ověřování aktuálnosti hesel
  - Obsahuje aktuální hesla uživatelů (replikovány ihned po jejich změně nebo resetování)
- Zajišťuje centralizovanou správu zásad skupiny
  - Provádí všechny změny v zásadách skupiny
  - Zabraňuje konfliktům při aktualizaci zásad skupiny

Primární řadič domény (2)

- Poskytuje hlavní zdroj času pro doménu
  - PDC emulátor v kořenové doméně lesa je hlavní zdroj času pro celý les Active Directory
  - PDC emulátory v jiných doménách synchronizovány s PDC emulátorem v kořenové doméně lesa
  - Ostatní řadiče domény v jednotlivých doménách jsou pak synchronizovány s PDC emulátory z jejich domén
- Působí jako doménový prohlížeč
  - Vytváří tzv. *browse listy*, jenž obsahují okolní domény a počítače a slučuje je do jediného, jenž vidí klienti

Zrušení (seize) operačního serveru

- Odebrání realizace FSMO operace řadiči domény
  - Probíhá bez vědomí stávajícího operačního serveru
  - Lze použít v případě selhání operačního serveru
- Zrušení pomocí nástroje **ntdsutil roles**
  - Připojení k řadiči domény, který se má stát novým operačním serverem
  - Zrušení a přesun příkazem **seize *<fsmo-operace>***
- Některé typy operačních serverů nelze, po jejich zrušení, již připojit zpět

Rušení operačních serverů a omezení

FSMO operace	Opětovné připojení do AD	Potřebná oprávnění
Schéma	Musí být přeinstalován	Schema Admins
Pojmenování domén	Musí být přeinstalován	Enterprise Admins
RID	Musí být přeinstalován	Domain Admins
Primární řadič domény	Může být připojen zpět	Domain Admins
Infrastruktura	Může být připojen zpět	Domain Admins