

# Serverové systémy Microsoft Windows

IW2/XMW2 2015/2016

**Jan Fiedor**

ifiedor@fit.vutbr.cz

Fakulta Informačních Technologií

Vysoké Učení Technické v Brně

Božetěchova 2, 612 66 Brno

Revize 29. 2. 2016

# Active Directory

Schéma, Objekty, Operační servery

# Schéma služby Active Directory

- Formální definice **obsahu** a **struktury** adresářové služby **Active Directory**
  - Stejně 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 má přidělen prefix 1.2.840
- Každá třída obsahuje definice
  - **Pravděpodobných nadřazených tříd** (*poss-superiors*)
    - Třídy, jenž mohou **obsahovat** instance definované třídy
  - **Povinných atributů** (*must-contains*)
    - Musí být nastaveny při **vytváření** objektů dané třídy
  - **Nepovinných atributů** (*may-contains*)

# Příklady tříd Active Directory

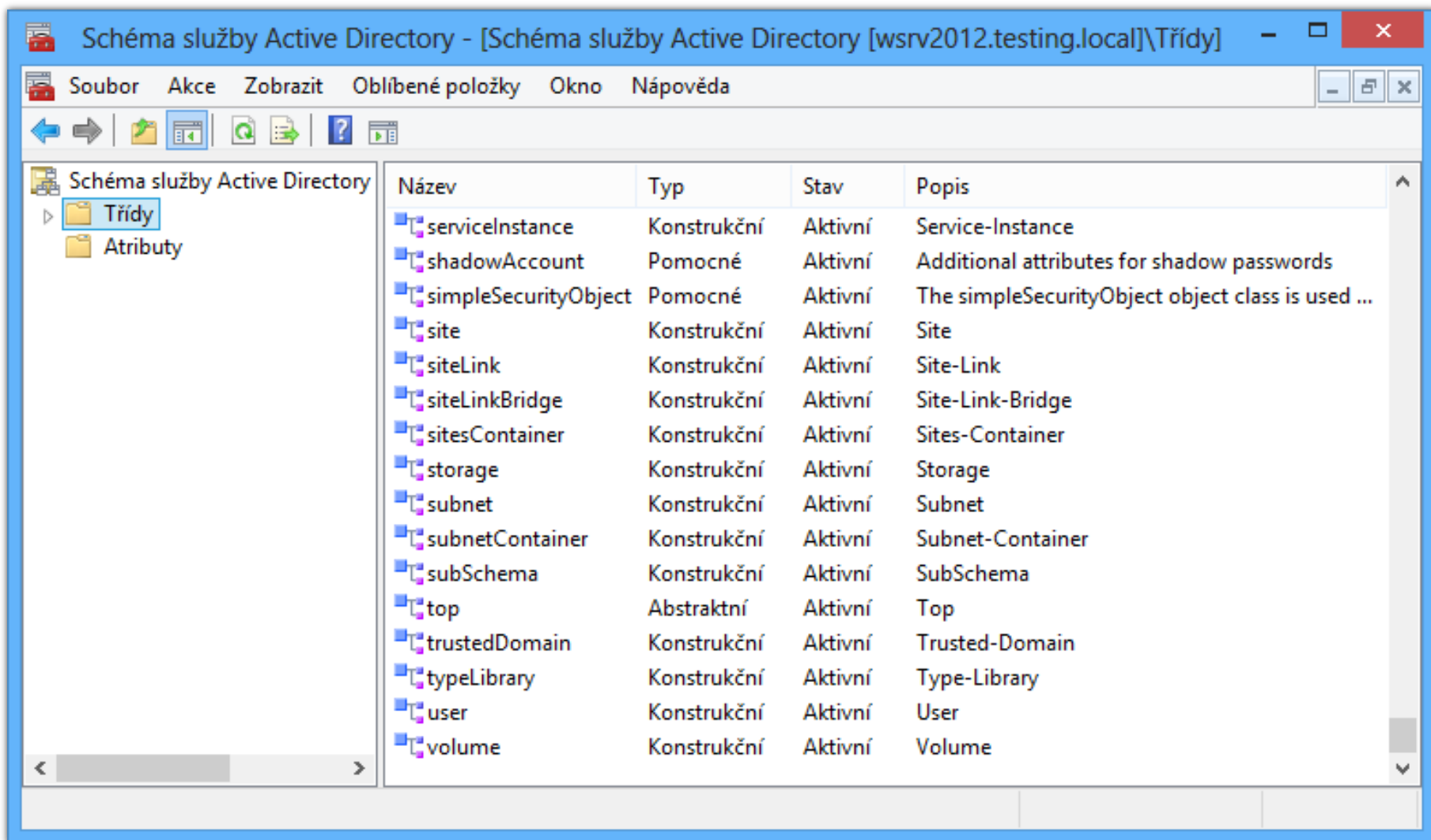


Schéma služby Active Directory - [Schéma služby Active Directory [wsrv2012.testing.local]\Třídy]

Soubor Akce Zobrazit Oblíbené položky Okno Nápověda

Schéma služby Active Directory

- Třídy
- Atributy

Název	Typ	Stav	Popis
serviceInstance	Konstrukční	Aktivní	Service-Instance
shadowAccount	Pomocné	Aktivní	Additional attributes for shadow passwords
simpleSecurityObject	Pomocné	Aktivní	The simpleSecurityObject object class is used ...
site	Konstrukční	Aktivní	Site
siteLink	Konstrukční	Aktivní	Site-Link
siteLinkBridge	Konstrukční	Aktivní	Site-Link-Bridge
sitesContainer	Konstrukční	Aktivní	Sites-Container
storage	Konstrukční	Aktivní	Storage
subnet	Konstrukční	Aktivní	Subnet
subnetContainer	Konstrukční	Aktivní	Subnet-Container
subSchema	Konstrukční	Aktivní	SubSchema
top	Abstraktní	Aktivní	Top
trustedDomain	Konstrukční	Aktivní	Trusted-Domain
typeLibrary	Konstrukční	Aktivní	Type-Library
user	Konstrukční	Aktivní	User
volume	Konstrukční	Aktivní	Volume

# Příklady atributů Active Directory

The screenshot shows the Active Directory Schema console window. The title bar reads "Schéma služby Active Directory - [Schéma služby Active Directory [wsrv2012.testing.local]\Atributy]". The menu bar includes "Soubor", "Akce", "Zobrazit", "Oblíbené položky", "Okno", and "Nápověda". The left pane shows a tree view with "Schéma služby Active Directory" expanded to "Třídy" and "Atributy". The main pane displays a table of attributes.

Název	Syntaxe	Stav	Popis
trustAuthIncoming	Řetězec v osmičkové soustavě	Aktivní	Trust-Auth-Incoming
trustAuthOutgoing	Řetězec v osmičkové soustavě	Aktivní	Trust-Auth-Outgoing
trustDirection	Celé číslo	Aktivní	Trust-Direction
trustParent	Rozšiřující název	Aktivní	Trust-Parent
trustPartner	Řetězec znaků Unicode	Aktivní	Trust-Partner
trustPosixOffset	Celé číslo	Aktivní	Trust-Posix-Offset
trustType	Celé číslo	Aktivní	Trust-Type
uASCompat	Celé číslo	Aktivní	UAS-Compat
uid	Řetězec znaků Unicode	Aktivní	A user ID.
uidNumber	Celé číslo	Aktivní	An integer uniquely identifyin...
uNCName	Řetězec znaků Unicode	Aktivní	UNC-Name
unicodePwd	Řetězec v osmičkové soustavě	Aktivní	Unicode-Pwd
uniqueIdentifier	Řetězec znaků Unicode	Aktivní	The uniqueIdentifier attribute t...
uniqueMember	Rozšiřující název	Aktivní	The distinguished name for th...
unixHomeDirectory	Řetězec IA5	Aktivní	The absolute path to the hom...
unixUserPassword	Řetězec v osmičkové soustavě	Aktivní	userPassword compatible with...
unstructuredAddress	Řetězec znaků Unicode	Aktivní	The IP address of the router F...

# Příklady atributů tříd Active Directory

Schéma služby Active Directory - [Schéma služby Active Directory [wsrv2012.testing.local]\Třídy\u... -

Soubor Akce Zobrazit Oblíbené položky Okno Nápověda

servicInstance  
shadowAccount  
simpleSecurityObject  
site  
siteLink  
siteLinkBridge  
sitesContainer  
storage  
subnet  
subnetContainer  
subSchema  
top  
trustedDomain  
typeLibrary  
user  
volume  
Atributy

Název	Typ	Systém	Popis	Zdrojová třída
uid	Nepovinné	Ne	A user ID.	user
uid	Nepovinné	Ne	A user ID.	shadowAccount
uid	Nepovinné	Ne	A user ID.	posixAccount
uidNumber	Nepovinné	Ne	An integer uniquely identifying ...	posixAccount
unicodePwd	Nepovinné	Ano	Unicode-Pwd	user
unixHomeDirectory	Nepovinné	Ne	The absolute path to the home ...	posixAccount
unixUserPassword	Nepovinné	Ne	userPassword compatible with ...	posixAccount
url	Nepovinné	Ano	WWW-Page-Other	top
userAccountControl	Nepovinné	Ano	User-Account-Control	user
userCert	Nepovinné	Ano	User-Cert	mailRecipient
userCertificate	Nepovinné	Ano	X509-Cert	user
userCertificate	Nepovinné	Ano	X509-Cert	mailRecipient
userParameters	Nepovinné	Ano	User-Parameters	user
userPassword	Nepovinné	Ne	User-Password	shadowAccount
userPassword	Nepovinné	Ne	User-Password	posixAccount
userPassword	Nepovinné	Ano	User-Password	person
userPKCS12	Nepovinné	Ne	PKCS #12 PFX PDU for exchange	user

# 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

The image shows the Active Directory Sites and Services console. In the left-hand tree view, the hierarchy is: Sites > Servers > WSRV2012 > NTDS Settings. A blue arrow points from the NTDS Settings icon in the tree to the 'NTDS Settings – vlastnosti' dialog box. The dialog box has several tabs: 'Obecné', 'Připojení', 'Objekt', 'Zabezpečení', and 'Editor atributů'. The 'Obecné' tab is active, showing the following fields and options:

- Popis:** (empty text box)
- Zásady dotazování:** (dropdown menu)
- Alias DNS:** 77DA873B-A7DB-45D0-8220-D7C30C388DD5.\_msdcs:
- Globální katalog**

Below these fields, there is a note: "Doba potřebná na publikování globálního katalogu závisí na dané topologii replikace." At the bottom of the dialog box are buttons for 'OK', 'Storno', 'Použít', and 'Nápověda'.

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

# Distinguished Names (DNs)

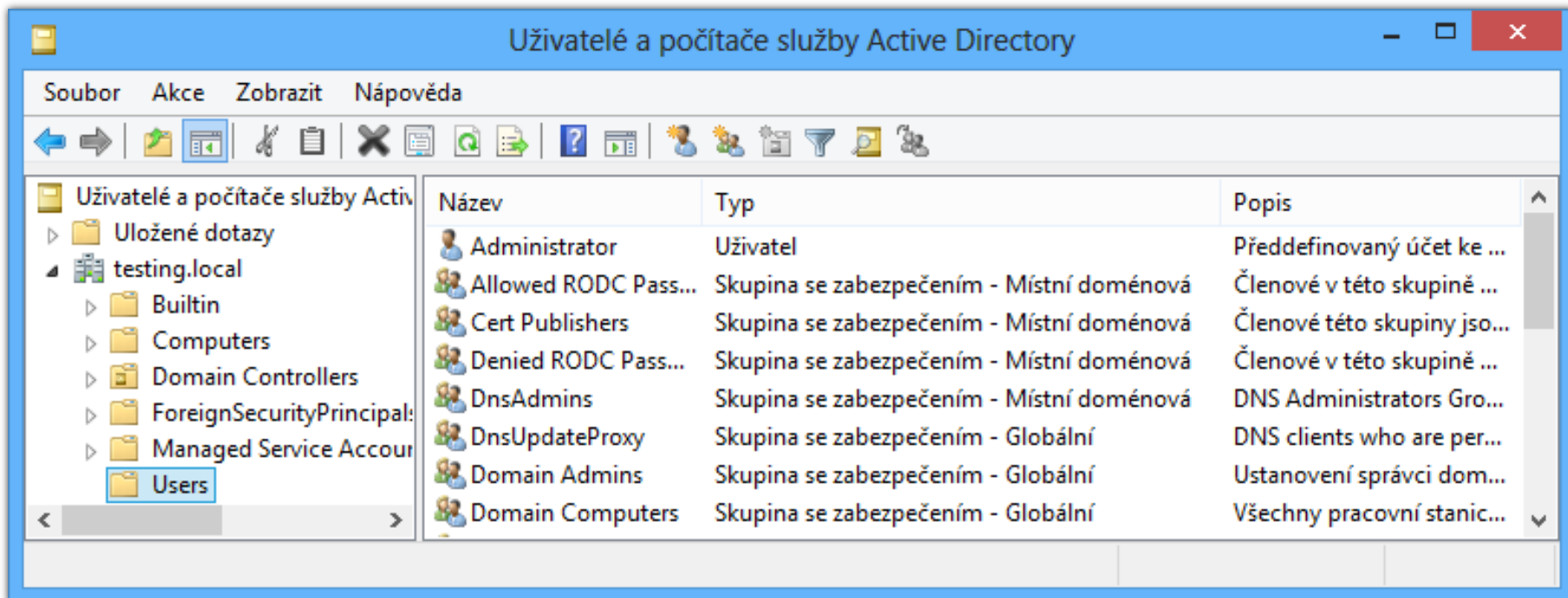
- Identifikace objektů používaná protokolem **LDAP**
  - Zachycuje **interní** i **externí** strukturu Active Directory
- Sekvence **RDN** jmen oddělených čárkou na cestě z **objektu** AD do **kořene** stromu **Active Directory** (kořenového uzlu stromu doménových jmen)
- **RDN** (*Relative Distinguished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

# Atributy RDN jmen

Atribut	Typ	Příklad objektů / atributů
<b>DC</b>	domainComponent	Část názvu domény (uzel v doménovém stromu)
<b>CN</b>	commonName	Uživatel, skupina, počítač, kontejner, ...
<b>OU</b>	organizationalUnitName	Organizační jednotka

Atribut	Typ	Příklad objektů / atributů
<b>O</b>	organizationName	Organizace
<b>STREET</b>	streetAddress	Adresa
<b>L</b>	localityName	Město
<b>ST</b>	stateOrProvinceName	Stát
<b>C</b>	countryName	Země
<b>UID</b>	userid	Identifikátor uživatele

# Příklady DN jmen uživatelů a skupin



Uživatelé a počítače služby Active Directory

Soubor Akce Zobrazit Nápověda

Uživatelé a počítače služby Activ...  
Uložené dotazy  
testing.local  
Builtin  
Computers  
Domain Controllers  
ForeignSecurityPrincipal:  
Managed Service Accour  
Users

Název	Typ	Popis
Administrator	Uživatel	Předdefinovaný účet ke ...
Allowed RODC Pass...	Skupina se zabezpečením - Místní doménová	Členové v této skupině ...
Cert Publishers	Skupina se zabezpečením - Místní doménová	Členové této skupiny jso...
Denied RODC Pass...	Skupina se zabezpečením - Místní doménová	Členové v této skupině ...
DnsAdmins	Skupina se zabezpečením - Místní doménová	DNS Administrators Gro...
DnsUpdateProxy	Skupina se zabezpečením - Globální	DNS clients who are per...
Domain Admins	Skupina se zabezpečením - Globální	Ustanovení správci dom...
Domain Computers	Skupina se zabezpečením - Globální	Všechny pracovní stanic...

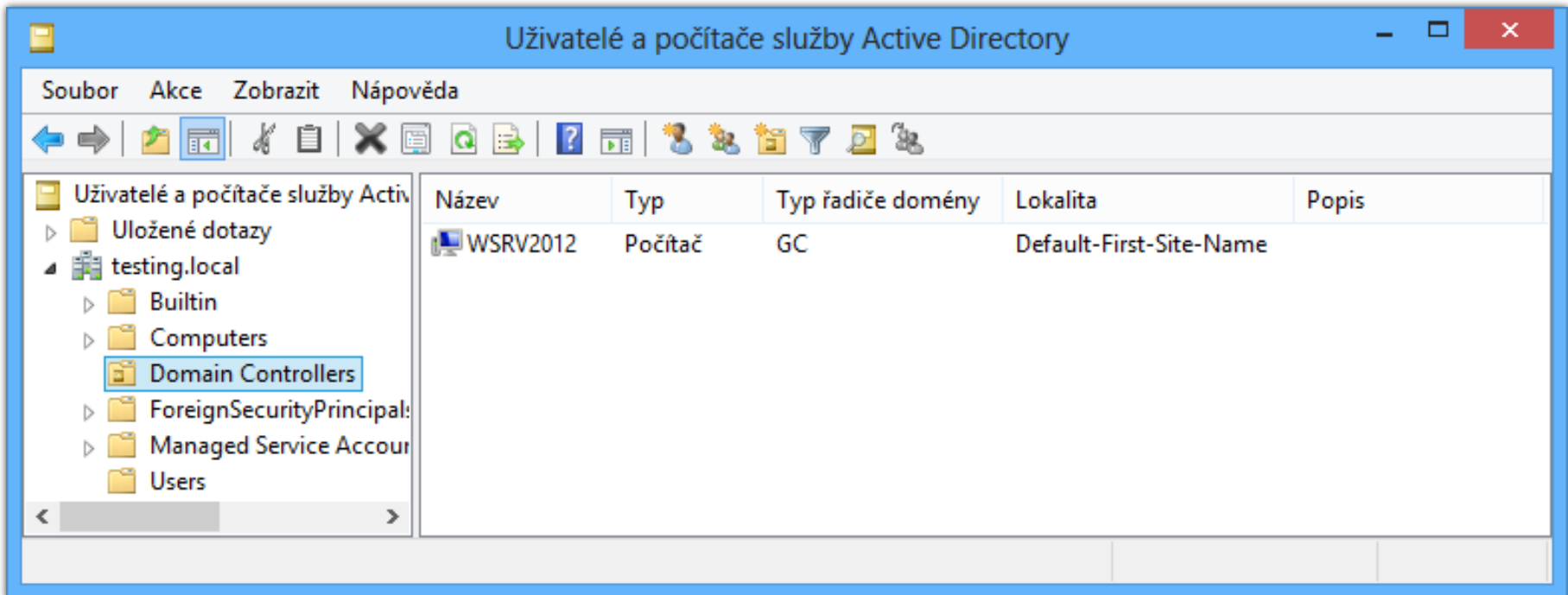
DN jméno pro uživatele **Administrator**

**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



Uživatelé a počítače služby Active Directory

Soubor Akce Zobrazit Nápověda

Uživatelé a počítače služby Activ  
Uložené dotazy  
testing.local  
Builtin  
Computers  
Domain Controllers  
ForeignSecurityPrincipal:  
Managed Service Accour  
Users

Název	Typ	Typ řadiče domény	Lokalita	Popis
WSRV2012	Počítač	GC	Default-First-Site-Name	

DN jméno pro počítač **WSRV2012**

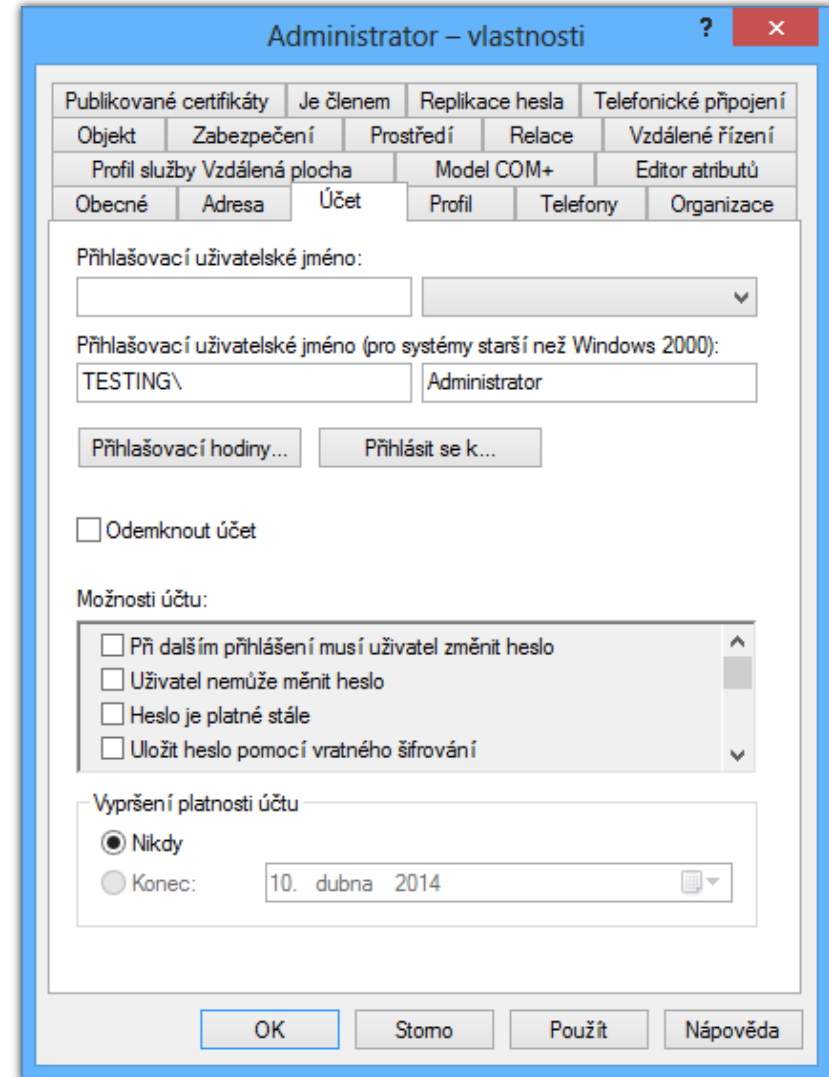
**CN=WSRV2012, OU=Domain Controllers, DC=testing, DC=local**

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>**

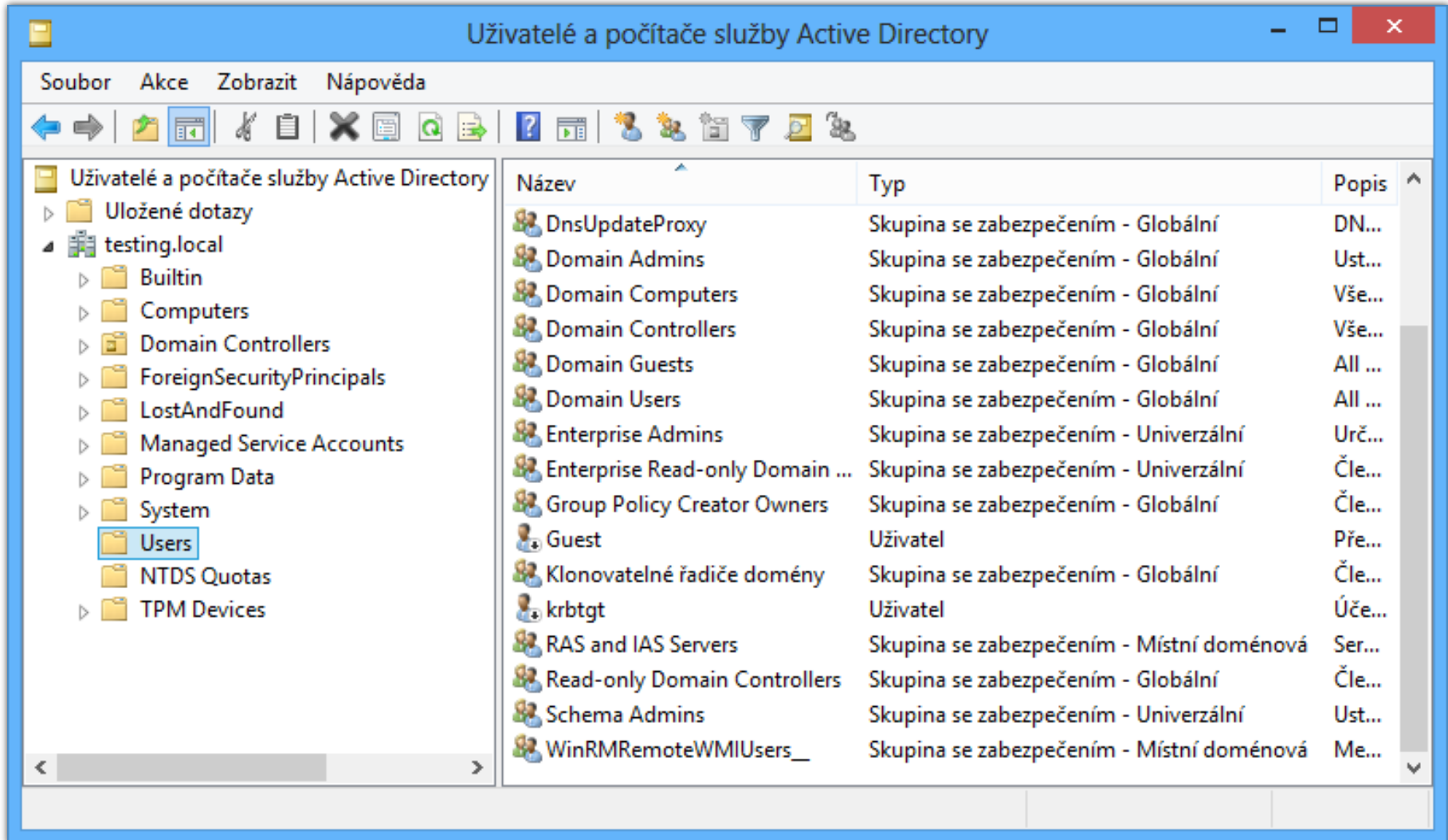




# Hromadné vytváření uživatelů

- 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



Uživatelé a počítače služby Active Directory

Soubor Akce Zobrazit Nápověda

Uživatelé a počítače služby Active Directory

- Uložené dotazy
- testing.local
  - Builtin
  - Computers
  - Domain Controllers
  - ForeignSecurityPrincipals
  - LostAndFound
  - Managed Service Accounts
  - Program Data
  - System
  - Users**
  - NTDS Quotas
  - TPM Devices

Název	Typ	Popis
DnsUpdateProxy	Skupina se zabezpečením - Globální	DN...
Domain Admins	Skupina se zabezpečením - Globální	Ust...
Domain Computers	Skupina se zabezpečením - Globální	Vše...
Domain Controllers	Skupina se zabezpečením - Globální	Vše...
Domain Guests	Skupina se zabezpečením - Globální	All ...
Domain Users	Skupina se zabezpečením - Globální	All ...
Enterprise Admins	Skupina se zabezpečením - Univerzální	Urč...
Enterprise Read-only Domain ...	Skupina se zabezpečením - Univerzální	Čle...
Group Policy Creator Owners	Skupina se zabezpečením - Globální	Čle...
Guest	Uživatel	Pře...
Klonovatelné řadiče domény	Skupina se zabezpečením - Globální	Čle...
krbtgt	Uživatel	Úče...
RAS and IAS Servers	Skupina se zabezpečením - Místní doménová	Ser...
Read-only Domain Controllers	Skupina se zabezpečením - Globální	Čle...
Schema Admins	Skupina se zabezpečením - Univerzální	Ust...
WinRMRemoteWMIUsers_	Skupina se zabezpečením - Místní doménová	Me...

# Správa pomocí příkazové řádky

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

Typ objektu	Popis
<b>user</b>	Uživatelský účet
<b>computer</b>	Účet počítače
<b>group</b>	Skupina
<b>ou</b>	Organizační jednotka

# Správa pomocí Windows PowerShell

Příkaz	Popis
<b>New-AD</b> <typ-objektu> <jméno> [-Path <DN>]	Přidání objektu
<b>Remove-AD</b> <typ-objektu> <DN>	Smazání objektu
<b>Rename-ADObject</b> <DN> -NewName <jméno>	Přejmenování objektu
<b>Move-ADObject</b> <DN> -TargetPath <DN>	Přesunutí objektu
<b>Set-AD</b> <typ-objektu> <DN>	Změna hodnot atributů objektu
<b>Get-AD</b> <typ-objektu> <DN>	Získání hodnot atributů objektu
Třída <b>DirectoryServices.DirectorySearcher</b>	Vyhledávání objektů

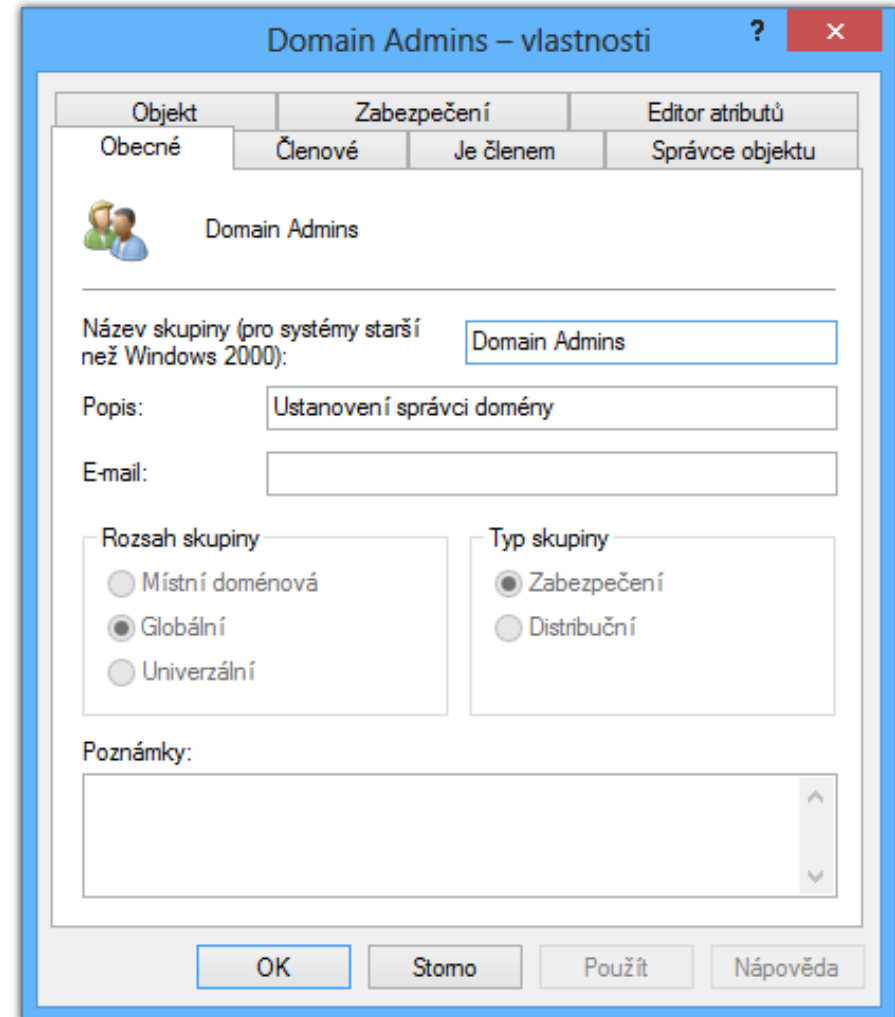
Typ objektu	Popis
<b>User</b>	Uživatelský účet
<b>Computer</b>	Účet počítače
<b>Group</b>	Skupina
<b>OrganizationalUnit</b>	Organizační jednotka

# Pokročilé metody správy objektů AD

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

# Skupiny (Groups)

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

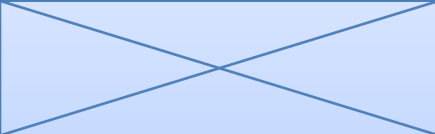
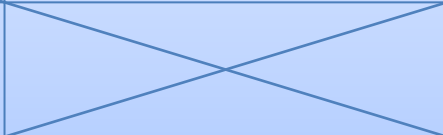
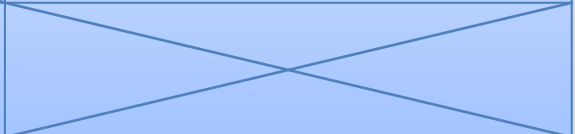


# Typy skupin

- **Distribuční skupiny** (*Distribution Groups*)
  - **Nemají** SID identifikátor
    - Nelze jim nastavovat oprávnění pro přístup k prostředkům
  - Primárně určeny pro rozesílání elektronické pošty
- **Bezpečnostní skupiny** (*Security Groups*)
  - **Mají** vlastní SID identifikátor
    - Reprezentují **identity** (lze používat v ACL seznamech)
  - 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*)

Možné konverze rozsahů skupin		Konverze na		
		Doménově lokální	Globální	Univerzální
Konverze z	Doménově lokální		Nelze	Nesmí obsahovat žádné doménově lokální skupiny
	Globální	Nelze		Není členem žádné globální skupiny
	Univerzální	Žádná omezení	Nesmí obsahovat univerzální skupiny	



# Lokální skupiny

- Primárně používány pro
  - Správu přístupů k prostředkům v **pracovní skupině** (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 a **globální** skupiny
    - Z jakékoliv domény **lesa**
    - Z jakékoliv **důvěryhodné domény**
  - **Univerzální** skupiny z jakékoliv domény **lesa**
  - **Doménově lokální** skupiny z **domény** počítače
  - Lokální skupiny z daného počítače
- Mohou být členy
  - Lokálních skupin na daném počítači

# Doménově lokální skupiny

- Primárně používány pro
  - Správu přístupů k prostředkům v doméně
- Definovány v jedné **konkrétní** doméně
  - Replikovány na všechny řadiče domény v doméně
- Dostupné
  - Pouze v rámci domény, ve které byly definovány

# Členství

- Mohou obsahovat
  - Uživatele, počítače a **globální** skupiny
    - Z jakékoliv domény **lesa**
    - Z jakékoliv **důvěryhodné domény**
  - **Univerzální** skupiny z jakékoliv domény **lesa**
  - **Doménově lokální** skupiny ze stejné **domény**
- Mohou být členy
  - **Doménově lokálních** (a lokálních) skupin
    - Ze stejné **domény**

# 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** v **doméně**
- Dostupné
  - Ve všech **doménách lesa**
  - Ve všech **důvěryhodných doménách**

# Členství

- Mohou obsahovat
  - Uživatele, počítače a **globální** skupiny
    - Ze stejné **domény**
- Mohou být členy
  - **Doménově lokálních** (a lokálních) skupin
    - Ze všech domén **lesa**
    - Z **důvěryhodných domén**
  - **Univerzálních** skupin ze všech domén **lesa**
  - **Globálních** skupin ze stejné **domény**

# Univerzální skupiny

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

# Členství

- Mohou obsahovat
  - Uživatele, počítače a **globální** skupiny
    - Z jakékoliv domény **lesa**
  - **Univerzální** skupiny
    - Z jakékoliv domény **lesa**
- Mohou být členy
  - **Doménově lokálních** (a lokálních) skupin
    - Ze všech domén **lesa**
  - **Univerzálních** skupin
    - Ze všech domén **lesa**



# 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)

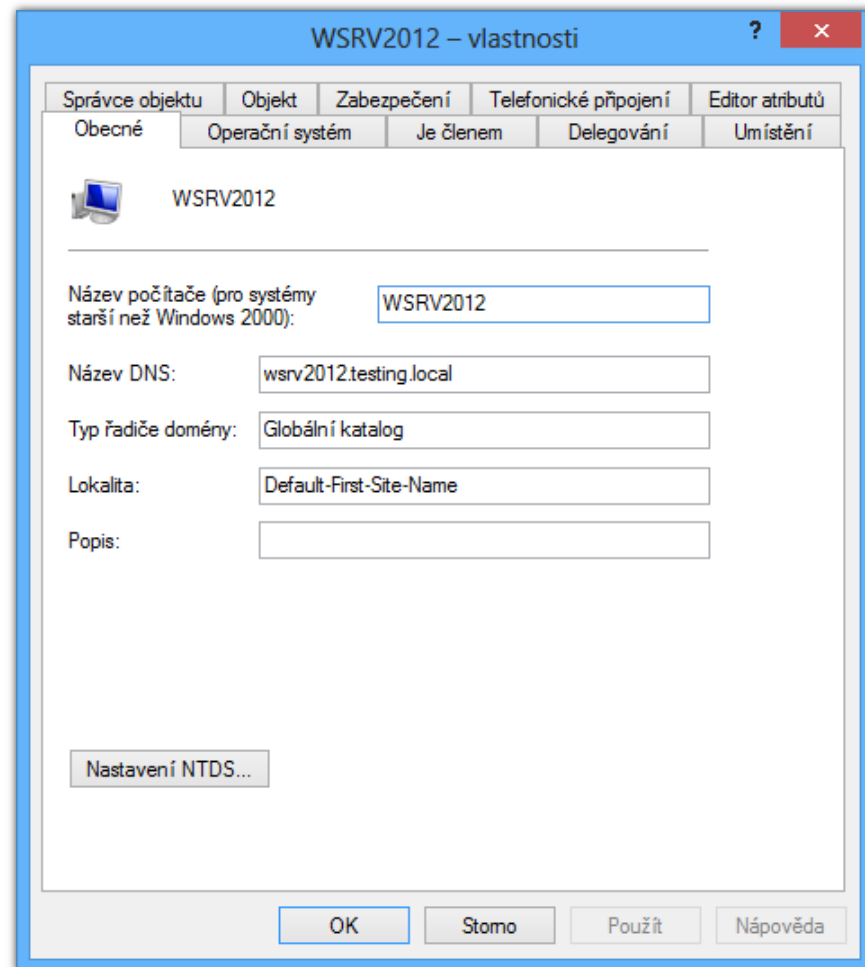
Skupina	Popis
<b>Administrators</b>	Správci všech řadičů domén (změny členství ve všech skupinách, plná kontrola nad oddílem domény, ...)
<b>Enterprise Admins</b>	Správci lesa (přidávání a odebrání domén, autorizace DHCP serveru, ...), vlastní oddíl konfigurace AD
<b>Schema Admins</b>	Správci schématu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

# Speciální skupiny (special identities)

Skupina	Popis
<b>Anonymous Logon</b>	Spojení bez poskytnutí pověření (jména a hesla)
<b>Authenticated Users</b>	Identity, jenž byly ověřeny řadičem domény
<b>Everyone</b>	Zahrnuje všechny ověřené uživatele a uživatele <b>Guest</b>
<b>Interactive</b>	Obsahuje uživatele, jenž přistupují k prostředkům umístěným na stejném počítači na kterém jsou daní uživatelé přihlášení (zahrnuje také uživatele připojené přes vzdálenou plochu)
<b>Network</b>	Obsahuje uživatele, jenž přistupují k prostředkům přes síť (na počítači, na kterém nejsou sami přihlášení)

# Počítače (Computers)

- Účty vytvářeny **systemem** při **připojení** do domény
  - Hesla měněna co 30 dní
  - Lze **předpřipravít** 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

Uživatelé a počítače služby Active Directory

Průvodce delegováním řízení

**Úkoly k delegování**  
Je možné vybrat běžnou úlohu nebo vytvořit vlastní.

Delegovat řízení následujících běžných úkolů:

- Vytváří, odstraňuje a spravuje uživatelské účty.
- Slouží k resetování uživatelských hesel a k vynucení změny hesla při
- Přečte si všechny informace o uživateli.
- Vytváří, odstraňuje a spravuje skupiny.
- Upravuje členství skupiny.
- Spravuje odkazy zásad skupin.
- Vytvořit výslednou sadu zásad (plánování)

Vytvořit vlastní úkol a delegovat jeho řízení

< Zpět   Další >   Storno   Nápověda

Deleguje řízení objektů v této složce

# Výběr cílových objektů a oprávnění

**Průvodce delegováním řízení**

**Typ objektu služby Active Directory**  
Určete obor úlohy, kterou chcete delegovat.

Delegovat řízení těchto objektů:

Složka, existující objekty ve složce a vytváření nových objektů

Pouze následující objekty ve složce:

- account objekty
- aCSResourceLimits objekty
- Alias fronty MSMQ objekty
- applicationVersion objekty
- bootableDevice objekty
- certificationAuthority objekty

Vytvořit vybrané objekty v této složce

Odstranit vybrané objekty z této složky

< Zpět

**Průvodce delegováním řízení**

**Oprávnění**  
Vyberte oprávnění, která chcete delegovat.

Zobrazit tato oprávnění:

- Obecná
- Podle vlastností
- Vytváření či odstraňování určitých podřízených objektů

Oprávnění:

- Úplné řízení
- Čtení
- Zápis
- Vytvářet všechny podřízené objekty
- Odstraňovat všechny podřízené objekty
- Čist všechny vlastnosti

< Zpět

Další >

Storno

Nápověda

# 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 (prefixu) **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
<b>Schéma</b>	Musí být přeinstalován	Schema Admins
<b>Pojmenování domén</b>	Musí být přeinstalován	Enterprise Admins
<b>RID</b>	Musí být přeinstalován	Domain Admins
<b>Primární řadič domény</b>	Může být připojen zpět	Domain Admins
<b>Infrastruktura</b>	Může být připojen zpět	Domain Admins

```

C:\Users\Administrator>ntdsutil roles
ntdsutil: roles
fsmo maintenance: connections
server connections: connect to server win2008r2-dc
Uytváření vazby na win2008r2-dc...
Připojen k win2008r2-dc s využitím pověření místně přihlášeného uživatele
server connections: quit
fsmo maintenance: seize <fsmo-operace>
  
```