PV176 – FSMO ROLE – AD FUNCTIONAL LEVELS

FSMO ROLE

- Flexible Single Master Operation Role
- AD je multi-master databáze
- Prevence konfliktů
  - Poslední vyhrává X zamykání
- Starší verze AD (≤NT4.0) byly single-master
  - Změny přes Primární DC (PDC)
- Zavedení 5 single-master rolí
  - Forestové X Doménové

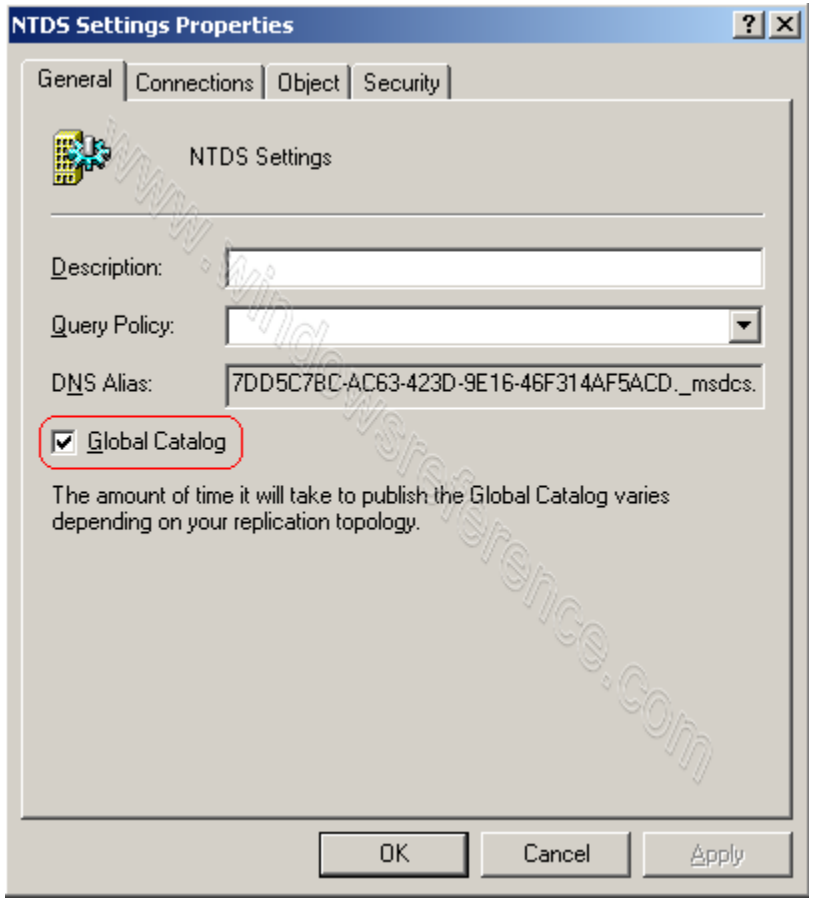
FSMO ROLE

- *Global Catalog*
- Schema Master
- Domain Naming Master
- Infrastructure Master
- Relative Id (RID) Master
- PDC Emulator

GLOBAL CATALOG

- Není FSMO role
- Každý DC udržuje objekty své domény
- GC Obsahuje RO seznam fragmentů každého objektu z celého forestu
- Udržuje se replikací (označením jako Partial Atribute Set)
- Universal Group Membership při přihlašování
- Nepřesouvá se, přiřazuje se
  - Pozor, může to trvat
  - Záznam v logu

GLOBAL CATALOG

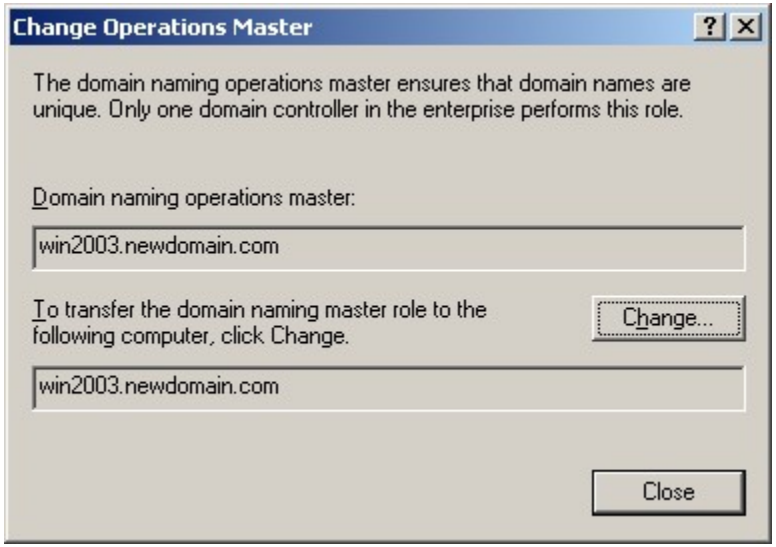


SCHEMA MASTER

- Spravuje modifikace a změny ve schématu
  - Proč změny schématu?
- Jediný DC má R/W kopii schématu
- Pro změnu schématu ve forestu je třeba mít přístup k schema masteru a samozřejmě práva (skupina Schema Admins)
- Forestová role
- Nelze rozšiřovat schéma
  - Nelze instalovat větší SW – Exchange

SCHEMA MASTER

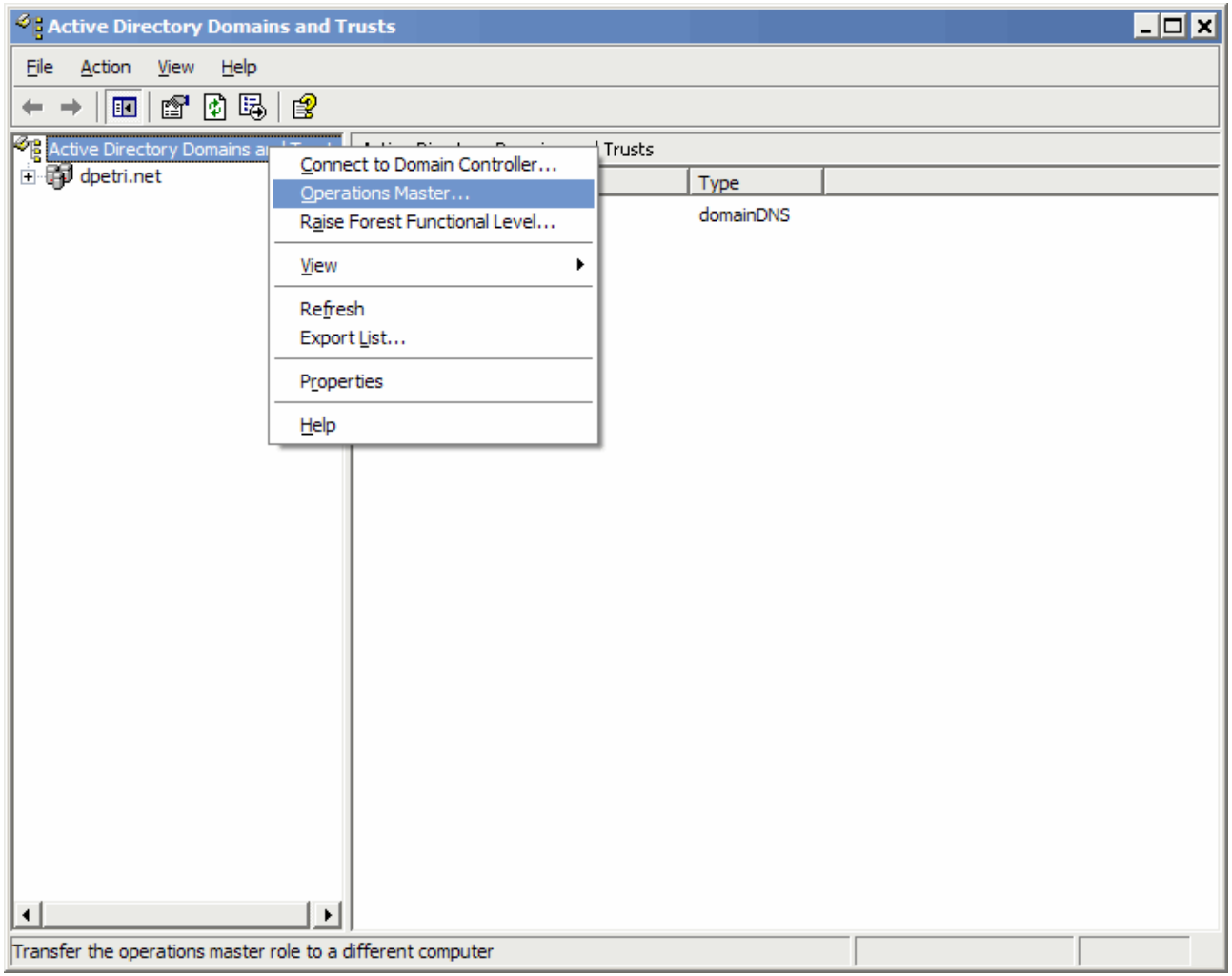
regsvr32 schmmgmt.dll



DOMAIN NAMING MASTER

- Kontroluje přidávání/odebírání domén ve forestu
- Lze provádět z libovolného DC, ale Domain Naming Master musí být k dispozici
- Forestová role
- Nelze instalovat nové childdomény

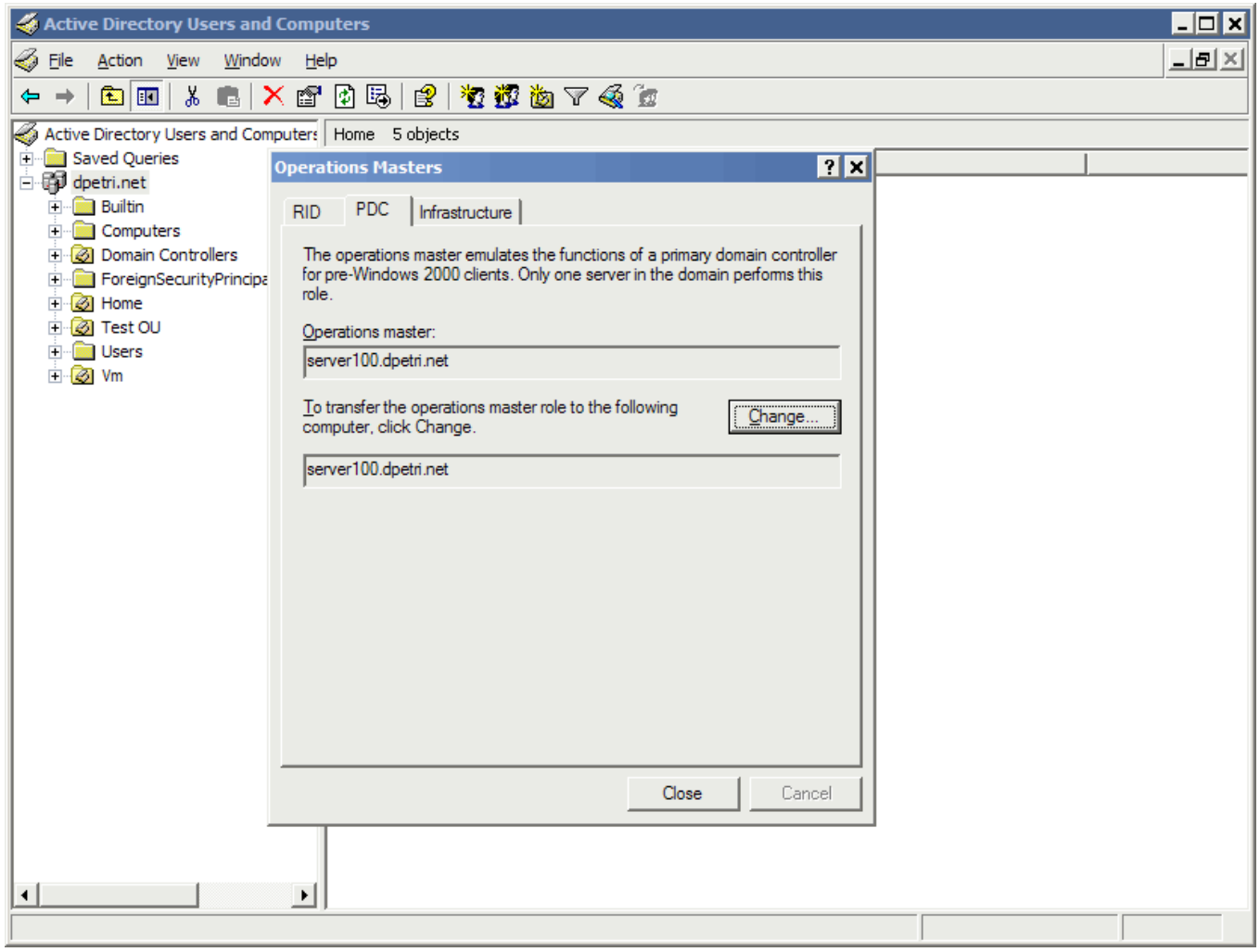
DOMAIN NAMING MASTER



INFRASTRUCTURE MASTER

- Objekt z cizí domény je referencován
  - GUID
  - SID
  - DN
- Infrastructure master drží informace pro cross-domain reference (SID a DN)
- Neměl by být na stejném DC jako GC
  - IM role je vypnuta, neboť DC neupdatuje objekty, které nezná (zná všechny, je GC)
  - Pokud všechny DC jsou i GC, pak IM pozbývá smysl
- Ve vícedoménovém prostředí může být nekonzistentní group membership

INFRASTRUCTURE MASTER



RID MASTER

- Security principal object má unikátní SID
- Skládá se z
  - Domain SID
  - Relative ID
- Každému DC je přidělena zásoba (pool) jeho relativních ID pro vytváření SID
  - Defaulní velikost poolu je 500, renew při 50%
- Nelze po nějaké době vytvářet další objekty (uživatele a počítače)

PDC EMULATOR

- Hierarchická synchronizace času
  - Kerberos snese rozdíl 5min
- Replikace hesel přes PDC
- Přeposílání bad-loginů a uzamykání účtů
- Defaultně se v jeho SYSVOL share vytvářejí politiky
- Nesynchronizuje čas, problémy s GP a hesly

FSMO ROLE

- Schema Master
  - Forest – první DC v forest root doméně
- Domain Naming Master
  - Forest - první DC v forest root doméně
- RID Master
  - Domain – první DC v každé doméně
- Infrastructure Master
  - Domain – první DC v každé doméně
- PDC Emulator
  - Domain – první DC v každé doméně

FSMO SEIZING

- Násilné přesunutí role v případě pádu konkrétní role
- Pomocí ntdsutil
- Po seiznutí se již nesmí objevit původní
  - Schema Master
  - Domain Naming Master
  - RID Master

AD FUNCTIONAL LEVELS

- Úroveň funkcionality AD
- Soubor nových vlastností pro každou úroveň
- Při povyšování úrovně změna schématu
- Domain level X Forest level

AD FUNCTIONAL LEVELS

- Domain
  - Windows 2000 mixed (default w2k3)
  - Windows 2000 native
  - Windows Server 2003 interim
  - Windows Server 2003
  - Windows Server 2008
  - Windows Server 2008 R2

AD FUNCTIONAL LEVELS

- Forest
  - Windows 2000 (default w2k3 a w2k8)
  - Windows Server 2003 interim
  - Windows Server 2003 (default w2k8 R2)
  - Windows Server 2008
  - Windows Server 2008 R2

AD FUNCTIONAL LEVELS

- V každé úrovni mohou být jako DC pouze korespondující OS nebo vyšší
  - Pro mixed je korespondující a o jedna nižší
- Rollback?
  - Pouze 2008 R2 → 2008

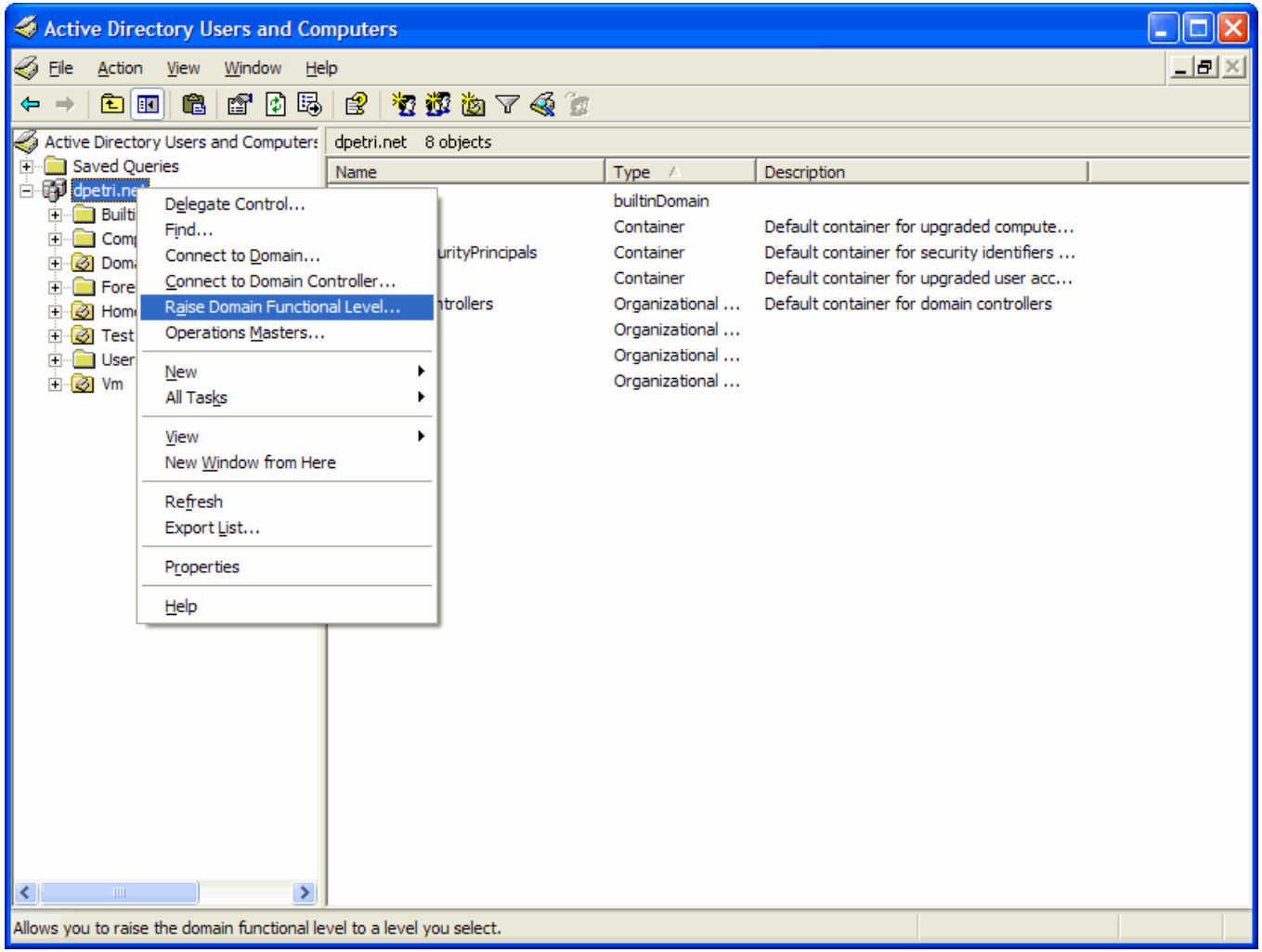
DOMAIN FUNCTIONAL LEVELS

- W2k native
  - universal groups, group nesting, SID history
- WS2k3
  - přejmenování domén, lastLogonTS,…
- WS2k8
  - SYSVOL DFS, AES KRB, PASSW policies
- WS2k8 R2
  - menší změny v KRB, Service Accounts

FOREST FUNCTIONAL LEVELS

- WS2k3
  - Forest trust, lepší replikace skupin, RODC, …
- WS2k8
  - Nic nového, nové domény jsou defaultně v WS2k8
- WS2k8 R2
  - Active Directory Recycle Bin

RAISING DOMAIN FUNCTIONAL LVL



RAISING FOREST FUNCTIONAL LVL