Operations Masters

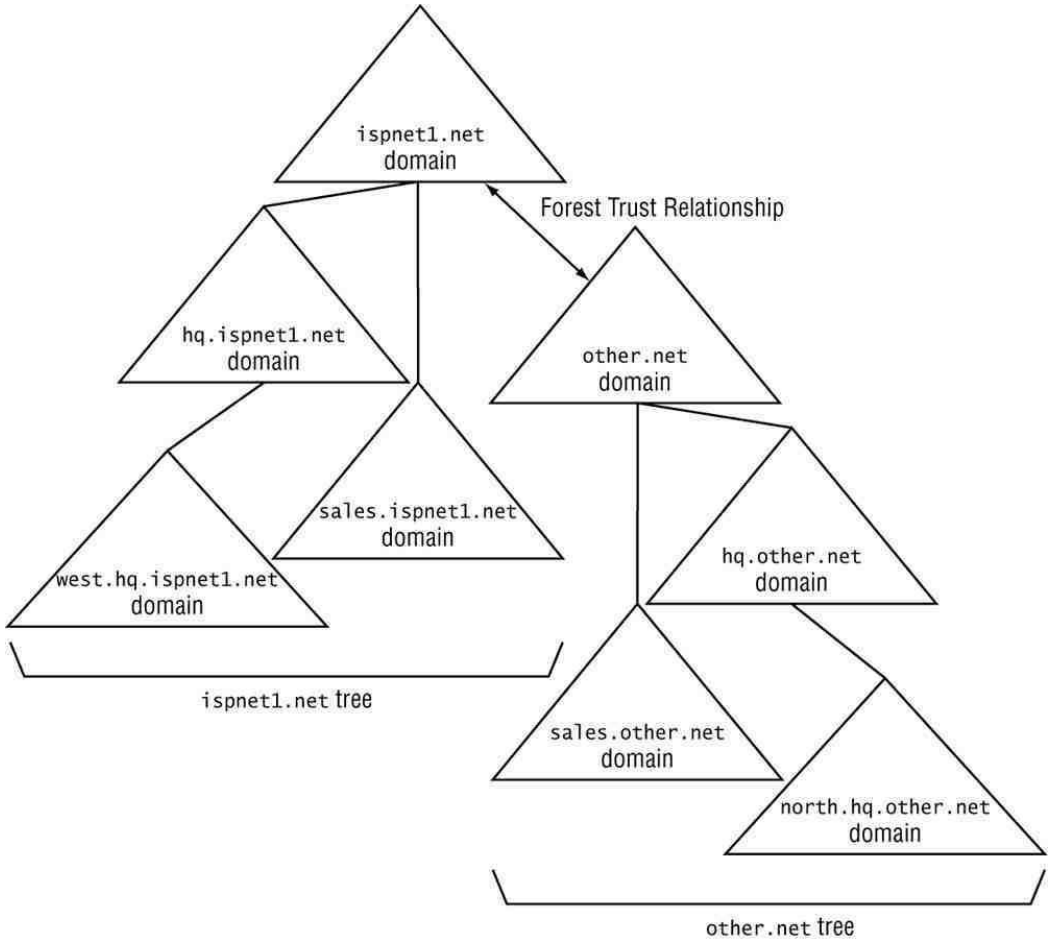
Šimon Suchomel

Flexible Single Master Operations [FSMO]

- Forest wide
  - Domain Naming
  - Schema
- Domain wide
  - Relative identifier (RID)
  - Infrastructure
  - PDC Emulator

Kontrolní otázka

- Kolik celkově FSMO rolí je v tomto prostředí?



Domain Naming Master

- Jeden v celém lese
- Přidávání / odebírání
  - domén
  - Application Directory Partitions

- Instalaci domény můžeme provést odkudkoliv, ale musí být k dispozici
- Výpadek: Nelze přidávat a odebírat domény
- Právo Change Domain Master: Enterprise Administrators

Schema master

- Jeden v celém lese
- Obsahuje R/W kopii schématu, ostatní mají pouze pro čtení
- Modifikace schématu databáze
- Výpadek: Nelze editovat schéma databáze
- Právo Change Schema Master: Schema Administrators

RID master

- Jeden pro celou doménu
- Generování SIDU na každém řadiči musí být unikátní v celém prostředí
- Výpadek: Po čase nelze vytvářet objekty
- Právo Change RID Master: Domain Admins

Infrastructure master

- Jeden pro celou doménu
- Udržuje konzistentní odkazy na objekty z jiných domén ve skupinách
- Výpadek: Možné nekonzistentní zobrazení členů z jiných domén ve skupinách

- Výlučné s globálním katalogem
- Postrádá význam pokud:
  - všechny servery v doméně jsou GC
  - prostředí obsahuje pouze jednu doménu
  - je aktivován AD Recycle Bin
- Právo Change Infrastructure Master: Domain Admins

PDC emulator

- Jeden pro celou doménu
- Emuluje primární DC pro zpětnou kompatibilitu
- Zpracovává změnu hesel
- Defaultně zajišťuje úpravu politik
- Synchronizace času
  - Kerberos – rozdíl víc jak 5 minut je fatální
- Výpadek: problém se synchronizací času, problémy s GPO a hesly
- Právo Change PDC: Domain Admins

Best practice

- Prvně je všech 5 rolí na 1. DC
  - Schema master a Domain Naming master spolu na jeden GC v kořenové doméně lesa
  - PDC Emulator a RID master na jeden DC
  - Infrastructure master na DC, který není GC
  - Identifikovat záložní servery pro všechny FMSO role („standby servers“)
    - zajistit, aby záložní server pro FSMO roli byl přímý replikační partner původního serveru (viz. příště)

Správa rolí (GUI)

- AD Users and Computers
  - PDC emulator, RID master, Infrastructure master
  - Domain wide role
- AD domains and Trusts
  - Domain naming master
- AD Schema
  - Schema master
  - *regsvr32 schmmgmt.dll*

Přemístění rolí

- Transfer
  - Přesunutí rolí, servery se „domluví“
  - Přesun v GUI nástroji, záleží kam jste připojení, nezáleží na jakém serveru jste přihlášení
  - ntdsutil
  - Move-ADDirectoryServerOperationMasterRole
- Seize
  - Násilné převzetí role
  - Původní hostitel již nesmí být nikdy online
    - PDC emulator a Infrastructure master to “přežijí”, můžeme je zpátky přesunout
  - ntdsutil použít seize místo transfer
  - Move-ADDirectoryServerOperationMasterRole -Force
  - Provedu až když to vyžadují okolnosti

Úkoly

- Identifikujte umístění rolí
  - pomocí GUI
  - netdom query fsmo
  - Get-ADDomain, Get-ADForest
- Přesuňte RID Master pomocí GUI na server 2
- Přesuňte PDC emulátor na server 2 pomocí ntdsutil
  - ntdsutil:
    - roles
    - connections
    - connect to server *_hostname_*
    - quit
    - transfer …
- Přesuňte Infrastructure Master na server 2 pomocí PowerShellu
  - Move-ADDirectoryServerOperationMasterRole -identity “jmenoDC" -OperationMasterRole InfrastructureMaster

Funkční úrovně

- http://technet.microsoft.com/library/understanding-active-directory-functional-levels

- Lze jen povyšovat
  - Výjimka W. Server 2008 < – > W. Server 2008 R2
- Domény – AD Users and Computers
- Lesa – AD Domains and Trusts

- Úkol: Povýšit na maximální úroveň