GOC197: Migrace z Windows Serveru 2003

Lukáš Brázda | MCT, MCSA, MCSE | lukas@brazda.org

OBSAH

- Úvod
- Příprava migrace
- Migrační postupy a nástroje

1) Úvod

Windows Server 2003 EOL

Zbývá už jen 98 dní

14. 7. 2015

Co znamená ukončení podpory?

No updates

No compliance

Lack of PCI compliance could mean that Visa and MasterCard will no longer do business with your organization

37 critical updates released in 2013 for Windows Server 2003/R2

KRITICKÉ AKTUALIZACE PRO WS2003

- Listopad 2014
  - Schannel || Remote Code Execution || MS12-049
- Leden 2015
  - Telnet Service || Remote Code Execution || MS15-002
- Únor 2015
  - Group Policy || Remote Code Execution || MS15-011
- Březen 2015
  - Microsoft Windows || Remote Code Execution || MS15-020

- Security Bulletins: https://technet.microsoft.com/en-us/library/security/dn631937.aspx

Migrační proces...

1 Discover Catalog your software and workloads	2 Assess Categorize applications and workloads	3 Target Identify your destination(s)	4 Migrate Make the move
			
System Integrators	Microsoft Server Roles	Microsoft Azure	System Integrators
DIY Tools	Microsoft Applications	Windows Server 2012 R2	DIY Tools
MCS	Custom Applications	Cloud OS Network	MCS
Premier Support	Third Party Applications	Office 365	Premier Support

UPGRADEOVAT A MIGROVAT NA…?

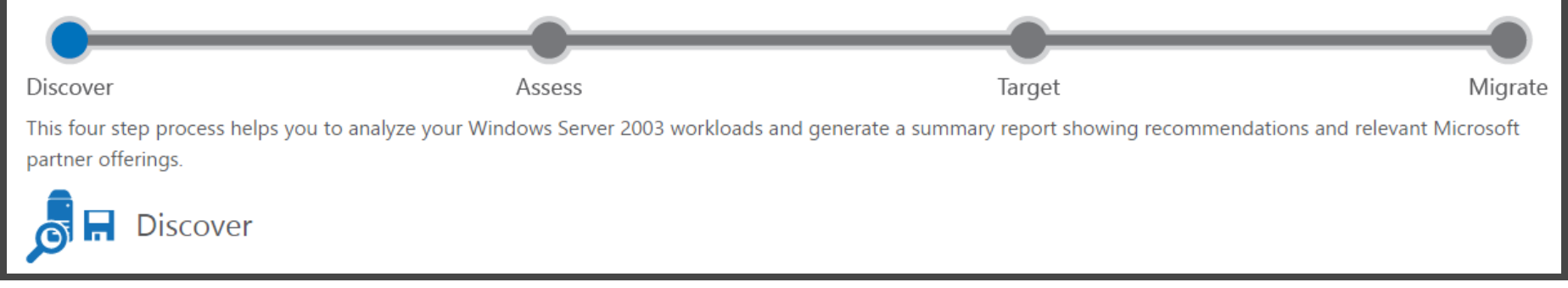
- Windows Server 2008
  - Jak x86 i x64
  - Podpora do 2020
- Windows Server 2008 R2
  - Jen x64
  - Podpora do 2020
- Windows Server 2012
  - Jen x64
  - Podpora do 2023
- Windows Server 2012 R2
  - Jen x64
  - Podpora do 2023

INPLACE UPGRADE

- Jedinou možností je Windows Server 2008 (R1)
- Upgrade paths – http://support.microsoft.com/kb/951041
- Nepodporováno např. cross-platform nebo cross-language
- Důvody pro:
  - Relativní jednoduchost a nenáročnost
- Důvody proti:
  - Přenos chyb do nového systému
  - Není to čistá instalace
  - Upgrade nemusí doběhnout dobře, pak nemám ani původní ani nový systém
  - Atp.

ZDROJE INFORMACÍ K MIGRACI

- http://www.microsoft.com/en-us/server-cloud/products/windows-server-2003/
- Windows Server 2003 Migration Planning Assistant
- Microsoft Assesment and Planning Toolkit
- Microsoft Services JumpStart



OBECNĚ PŘED ZAPOČETÍM MIGRACE

- Záloha existujícího prostředí
- Nainstalované aktualizace
- Dobře fungující prostředí
  - Kontrola logů
  - Kontrola pomocí dostupných nástrojů
  - Možná existence Best Practice Analyzerů

2) Získání informací o prostředí

JAKÉ INFORMACE POTŘEBUJEME?

- Kolik a jaké servery jsou v síti?
- Jaké služby tyto servery dělají?
- Jaké aplikace jsou na nich nainstalované?
- Různé závislosti služeb
- Atp.

DC1	AD, DNS
DC2	AD, DNS
CA1	CA
SRV1	FS, DFS, DHCP, WINS
SRV2	FS, DFS, IAS, PRINT
SRV3	IIS, TS
SRV4	WSUS
CL1	W8 Client, RSAT
CL2	W8 Client, RSAT

DEMO

- Microsoft Assesment and Planning Toolkit

Computer Name	WMI Status	Machine Type	Current Windows Server 2012 Readiness	Installed Roles	Computer Model	Current Operating System
CA1.GOPAS.local	Success	Virtual	Meets minimum requirements. Check CPU to determine if architecture is x64.	Active Directory Certificate Services Web Server	Virtual Machine	Microsoft(R) Windows(R) Server 2003, Enterprise Edition
DC1.GOPAS.local	Success	Virtual	Meets minimum requirements. Check CPU to determine if architecture is x64.	Active Directory DNS Server	Virtual Machine	Microsoft(R) Windows(R) Server 2003, Enterprise Edition
DC2.GOPAS.local	Success	Virtual	Meets minimum requirements. Check CPU to determine if architecture is x64.	Active Directory DNS Server	Virtual Machine	Microsoft(R) Windows(R) Server 2003, Enterprise Edition
SRV1.GOPAS.local	Success	Virtual	Meets minimum requirements. Check CPU to determine if architecture is x64.	DHCP Server WINS Server	Virtual Machine	Microsoft(R) Windows(R) Server 2003, Enterprise Edition
SRV2.GOPAS.local	Success	Virtual	Meets minimum requirements. Check CPU to determine if architecture is x64.		Virtual Machine	Microsoft(R) Windows(R) Server 2003, Enterprise Edition
SRV3.GOPAS.local	Success	Virtual	Meets minimum requirements. Check CPU to determine if architecture is x64.	Web Server	Virtual Machine	Microsoft(R) Windows(R) Server 2003, Enterprise Edition
SRV4.GOPAS.local	Success	Virtual	Meets minimum requirements. Check CPU to determine if architecture is x64.	Web Server Windows Server Update Services	Virtual Machine	Microsoft(R) Windows(R) Server 2003, Enterprise Edition

3) Migrace AD DS

INFORMACE O STÁVAJÍCÍM PROSTŘEDÍ

- Struktura AD domény a forestu?
- Kolik DC, GC, RODC?
- Potřebná oprávnění?
- Jaké operační systémy?
- Jaký je Domain Functional Level a Forest Functional Level?
- Jaké AD site?
- Kdo drží FSMO role?
- Konfigurace DNS, včetně klientů?

POSTUP MIGRACE AD

- Kontrola stávajícího prostředí
- Splnění prerekvizit (DFL, FFL)
- Upgrade AD schema
- Přidání nového DC a GC na Windows Serveru 2012 R2
- Zajištění a ověření správné replikace
- Přesun FSMO rolí
- Překonfigurování DNS serverů, ověření DNS záznamů
- Odstranění původních DC z AD

KONTROLA STÁVAJÍCÍHO PROSTŘEDÍ

- Fungují replikace AD dobře?
- Funguje dobře replikace SYSVOL?
- Existují a aplikují se GPO?

FUNGUJÍ REPLIKACE AD DOBŘE?

- Nástroje pro kontrolu:
  - Vytvoření objektu v AD, kontrola replikace na ostatní DC
  - Ruční vynucení replikace v konzole AD Sites and Services
  - Active Directory Replication Status Tool
  - EventLog – Directory Service
  - Repadmin.exe
  - Dcdiag.exe

FUNGUJE DOBŘE REPLIKACE SYSVOL?

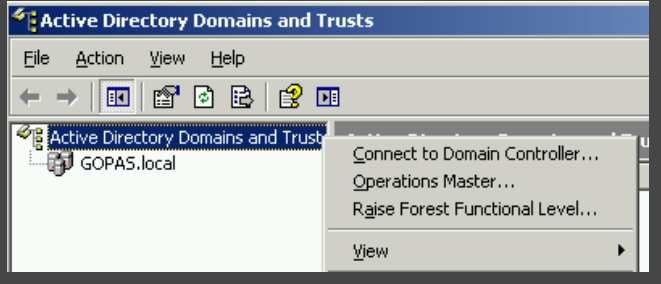
- Windows Server 2003 replikuje SYSVOL pomocí File Replication Service
- Nástroje pro kontrolu:
  - Je SYSVOL vysdílený na všech DC?
  - Je v nich nějaký obsah?
  - Testovací soubor, kontrola zreplikování na ostatní DC
  - EventLog – File Replication Service

EXISTUJÍ A APLIKUJÍ SE GPO?

- Nástroje pro kontrolu:
  - AD Users and Computers
  - Ideálněji ale Group Policy Management Console (do WS2003 se dá doinstalovat)
    - http://www.microsoft.com/en-us/download/details.aspx?id=21895
  - Testovací politika
  - RSOP.msc
  - GPUpdate a GPResult
  - GPOTool.exe (kontrola konzistentnosti GPO)

PREREKVIZITY PRO INSTALACI WS08+

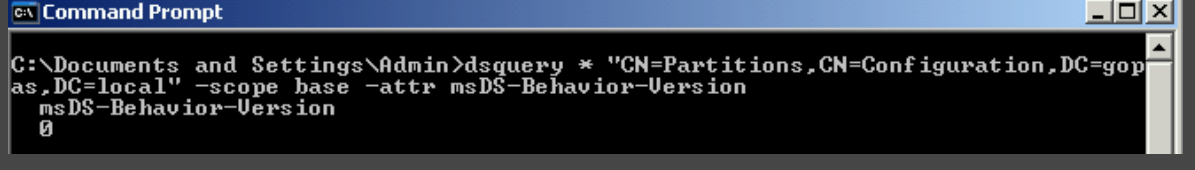
- Hlavní je požadavek na Forest Functional Level
- Musí být Windows Server 2003 a vyšší
- Kde a jak zjistit?
  - Konzola AD Domains and Trusts
  - dsquery * "CN=Partitions,CN=Configuration,DC=domain,DC=com" -scope base -attr msDS-Behavior-Version



0 = Windows 2000

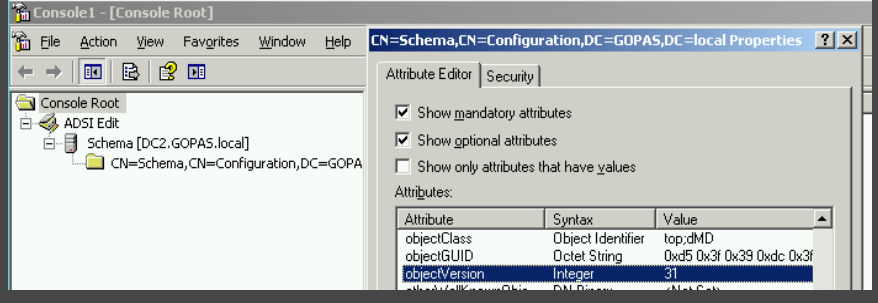
1 = Windows 2003 interim

2 = Windows 2003



UPGRADE SCHEMA AD

- Před přidáním nového DC do stávající AD je třeba povýšit verzi AD Schema
- Nutné oprávnění Schema Admin
- Instalace nového DC to sice dělá „sama“
- Instalační DVD nového serveru, ADPrep
- Příkazy:
  - ADPrep /forestprep
  - ADPrep /domainprep /gpprep
  - ADPrep /rodcprep




```
13 = Windows 2000 Server
30 = Windows Server 2003
31 = Windows Server 2003 R2
44 = Windows Server 2008
47 = Windows Server 2008 R2
56 = Windows Server 2012
69 = Windows Server 2012 R2
```

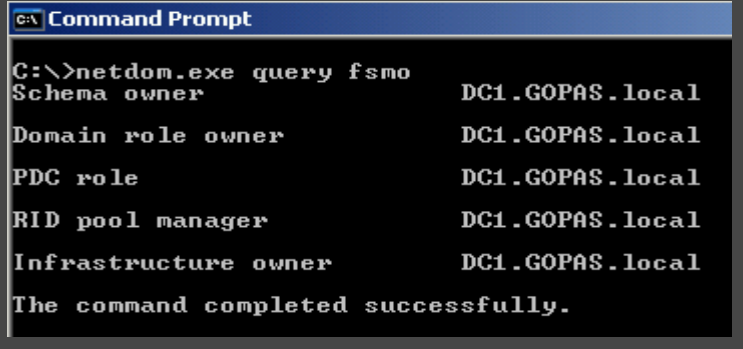
- https://technet.microsoft.com/en-us/library/dd464018%28v=ws.10%29.aspx

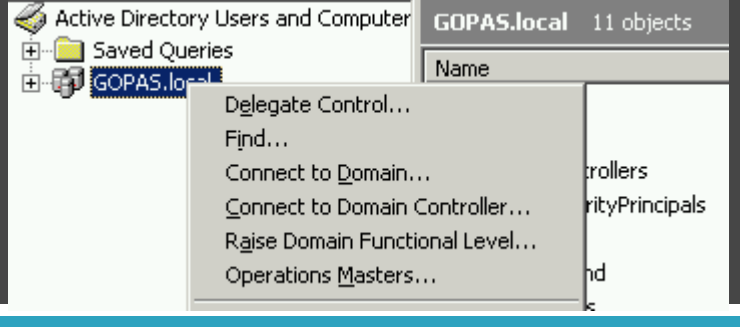
PŘIDÁNÍ NOVÉHO DC DO SÍTĚ

- WS 2012 (R2) již nepoužívá DCPROMO (s výjimkou server core verze)
- Používáme tedy klasického průvodce přidáním role
- Vybíráme AD DS roli
- Po doinstalaci binárek, pouštíme průvodce povýšením na DC
- Tento průvodce už je stejný jako DCPROMO
- Z nových serverů chceme mít i Global Catalogy a DNS servery!
- Restart serveru, kontrola replikací, DNS záznamů, SYSVOLu (FRS)

PŘEVEDENÍ FSMO ROLÍ

- Před odebráním stávajících 2003 serverů musíme převést FSMO role
- Stávající(ho) držitele zjistíme:
  - netdom.exe query FSMO
  - V konzolích ADUC, AD Schema, AD Domains and Trusts
- Převedení rolí provedeme:
  - Ntdsutil.exe
  - V konzolích ADUC, AD Schema, AD Domains and Trusts
- Po každé změně nechat DC poreplikovat
- Kontrola převedení





PŘEKONFIGUROVÁNÍ DNS

- DNS server je pro AD stěžejní funkce!
- Jak jsou nakonfigurovány DC a servery? Pravděpodobně staticky…
- Jak a kdo konfiguruje klienty? Nějaký DHCP server?
- Jaká bude situace po odstranění starých DC?

- DC musí mít DNS servery buď na sebe nebo „do kříže“ s ostatními DC
- Klienti se také musejí ptát na překlady doménových DNS serverů
- Opětovná kontrola:
  - Nltest /sc_reset:gopas.local

ODSTRANĚNÍ STARÝCH DC

- Pokud jsme se ujistili že:
  - Máme převedené FSMO role
  - Nové DC je zároveň i GC
  - Fungují správně replikace AD i SYSVOL
  - Zreplikovaly se nám všechny GPO
  - Zreplikovaly se nám všechny DNS zóny a záznamy v nich
  - V DNS jsou správné záznamy i nových DC

- …můžeme poslat staré Windows Server 2003 DC do pekla ☺

ODSTRANĚNÍ STARÝCH DC

- Ideálně pomocí DCPROMO
  - Procházíme průvodce
  - Neodstraňujeme poslední DC v doméně
  - Definujeme nové heslo lokálního Administrátora
  - Po restartu je server „obyčejný“ member server (v doméně tedy zůstává…)
  - AD computer account se ale musel přesunout z kontejneru Domain Controllers – kontrola
  - Stejně tak by měly zmizet i záznamy tohoto DC z DNS – kontrola

- Co když ale DC pomocí DCPROMO odstranit nejde?

ODSTRANĚNÍ STARÝCH DC – NÁSILNĚ

- V zásadě jde o vymazání informací o starém DC z AD
- Proces tzv. AD Metadata Cleanup
  - Z GUI
  - Z příkazové řádky
  - Pomocí VBS skriptu
  - Více zde: https://technet.microsoft.com/en-us/library/cc816907%28v=ws.10%29.aspx

KONTROLA FUNKČNOSTI

- EventLogy – Directory Service, File Replication Service
- Repadmin
- AD Sites and Services – ruční vynucení replikací
- Kontrola vytvořením objektu v AD a v SYSVOL
- Nltest /sc_reset:gopas.local
- Vytvoření nového uživatele a přihlášení se na něj (kontrola autentizace)

UPGRADE REPLIKACE SYSVOL NA DFSR

- Doposud se SYSVOL replikoval pomocí File Replication Service
- Od Windows Serveru 2008 můžeme používat novější a robustnější DFSR
- Postup:
  - Upgrade DFL a FFL minimálně na Windows Server 2008
  - DFSRmig /setglobalstate
  - DFSRmig /getmigrationstate
  - Více zde: http://blogs.technet.com/b/askds/archive/2009/01/05/dfsr-sysvol-migration-faq-useful-trivia-that-may-save-your-follicles.aspx

UPGRADE REPLIKACE SYSVOL NA DFSR

- DFSRmig /setglobalstate 1
  - Vytvoří se kopie adresáře SYSVOL (SYSVOL_DFSR), vysdílený do sítě je ale stále původní adresář
  - Původní adresář se replikuje pomocí FRS, nový adresář se replikuje pomocí DFSR
- DFSRmig /getmigrationstate
  - Čekáme až se všechny DC dostanou do stavu 1
- DFSRmig /setglobalstate 2
  - Přesměruje se sdílený adresář a ten je aktuálně sdílen z nového SYSVOL_DFSR
  - Původní SYSVOL se stále replikuje pomocí FRS, nový stále pomocí DFSR
- DFSRmig /getmigrationstate
  - Čekáme až se všechny DC dostanou do stavu 2
- DFSRmig /setglobalstate 3
  - FRS je zastavena, dále se SYSVOL_DFSR replikuje již jen pomocí DFSR
  - Původní adresář SYSVOL zůstává zachován, je možné jej smazat

4) Migrace DNS Serveru

MIGRACE DNS SERVERŮ

- Moment, vždyť DNS servery už jsme odmigrovali spolu s AD, ne?
- A je tomu opravdu tak?
- Nebyly na původních serverech i nějaké zóny do AD neintegrované?
- Tohle bychom také měli mít zkontrolováno dopředu!

JAK NA MIGRACI „FILE“ ZÓN?

- Takovéto zóny se replikují mezi DNS servery pomocí zónových transferů
- V některých situacích lze použít export a následný import zóny
- Mezi 2003 a 2012 R2 serverem nelze export / import použít (nekompatibilita)

JAK NA MIGRACI „FILE“ ZÓN?

- Postup:
  - Na nový DNS server přidáme sekundární (asi neitegrovanou) zónu
  - Pomocí zónového transferu provedeme replikaci obsahu zóny
  - Možná bude třeba povolit zónové transfery i na nové servery
  - Na nových serverech změníme typ zóny ze sekundární na primární
  - Původní držitele primárních zón odstraníme
    - Odstraníme DNS zóny
    - Pravděpodobněji ale odinstalujeme roli, možná odstraníme celý server
  - Ověříme funkčnost překladů z nových DNS serverů
    - Ping
    - Nslookup

5) Migrace AD CS

ZJIŠTĚNÍ INFORMACÍ O STÁVAJÍCÍ CA

- Struktura – jedná se o jedinou Root CA nebo jde o vícevrstvou strukturu?
- Standalone nebo enterprise?
- K čemu se CA používá? A používá se vůbec? ☺
- Jaké certifikáty vystavuje?
- Jakým způsobem? (ruční enrollment, webenrollment, autoenrollment přes GPO, atp.)
- Jaké šablony se používají?
- Stávající konfigurace AIA, CRL

OVĚŘENÍ FUNKČNOSTI STÁVAJÍCÍ CA

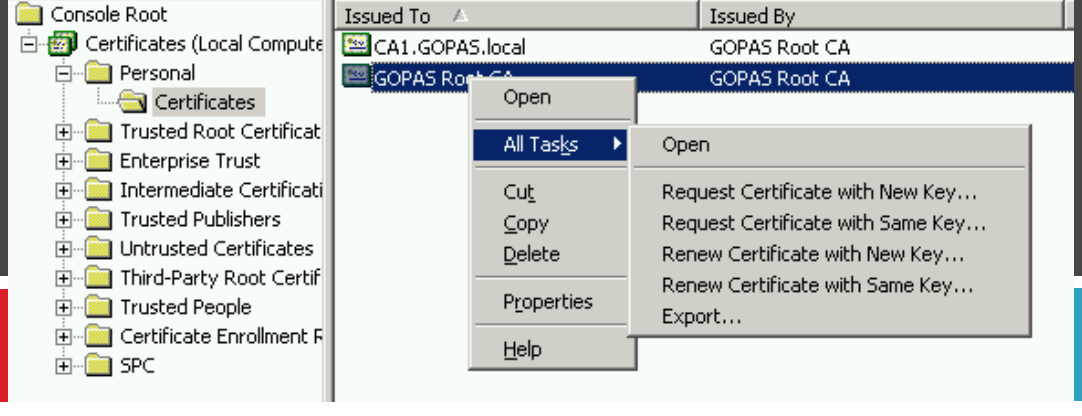
- EventLog – Application log
- Test různých enrollment metod:
  - Ručně z MMC konzole
  - Autoenrollment přes GPO
  - Web enrollment

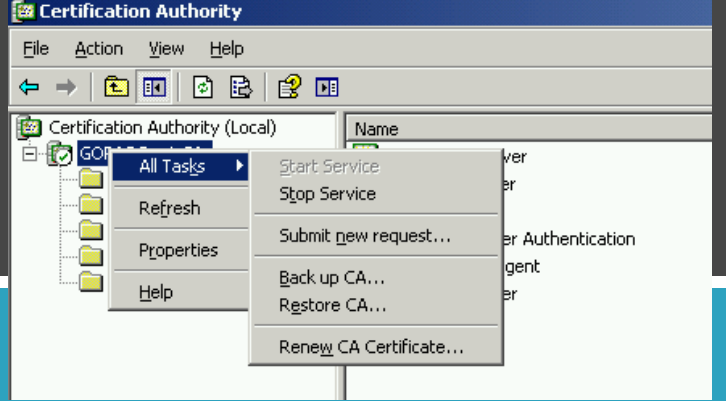
POSTUP MIGRACE AD CS

- Zazálohování CA databáze, certifikátu CA (včetně privátního klíče)
- Zazálohování konfigurace CA v registrech a souboru CAPolicy.inf
- Odinstalace role z původního serveru
- Odstranění původního serveru z domény, včetně computer accountu
- Přidání nového serveru do domény (pod stejným jménem!)
- Instalace a konfigurace role CA
- Obnova databáze CA a konfigurace z registru
- Nastavení oprávnění pro AIA a CRL kontejner
- Ověření funkčnosti
- Více zde: https://technet.microsoft.com/en-us/library/ee126140(v=ws.10).aspx#BKMK_RmvFromDom

ZAZÁLOHOVÁNÍ CA

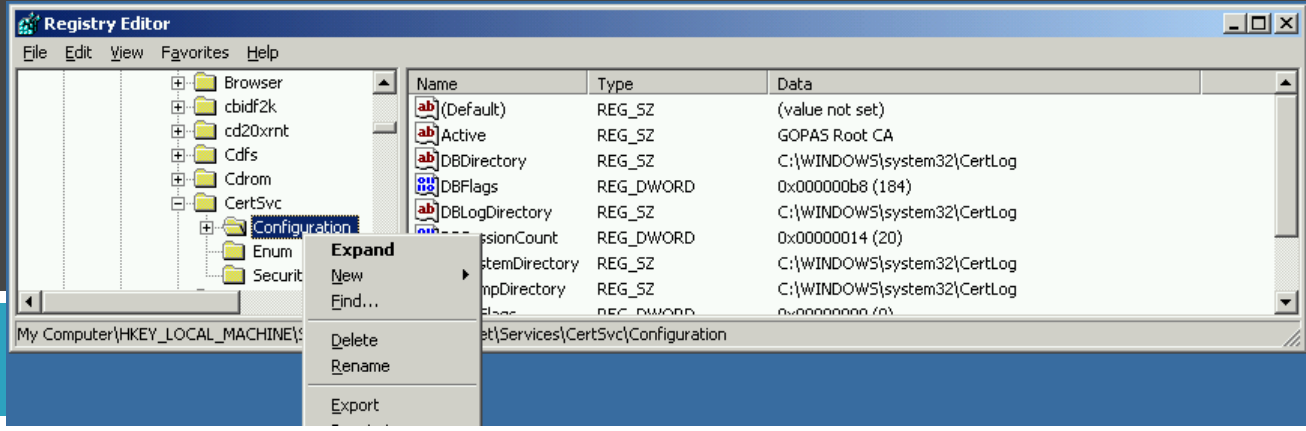
- Zazálohování certifikátu CA (včetně privátního klíče) do souboru:
  - Nejsnadněji pomocí MMC konzoly pro správu computer cerifikátů
  - Soubor by měl být chráněn silným heslem
- Zazálohování CA databáze:
  - Nejsnadněji z MMC konzole Certificate Authority





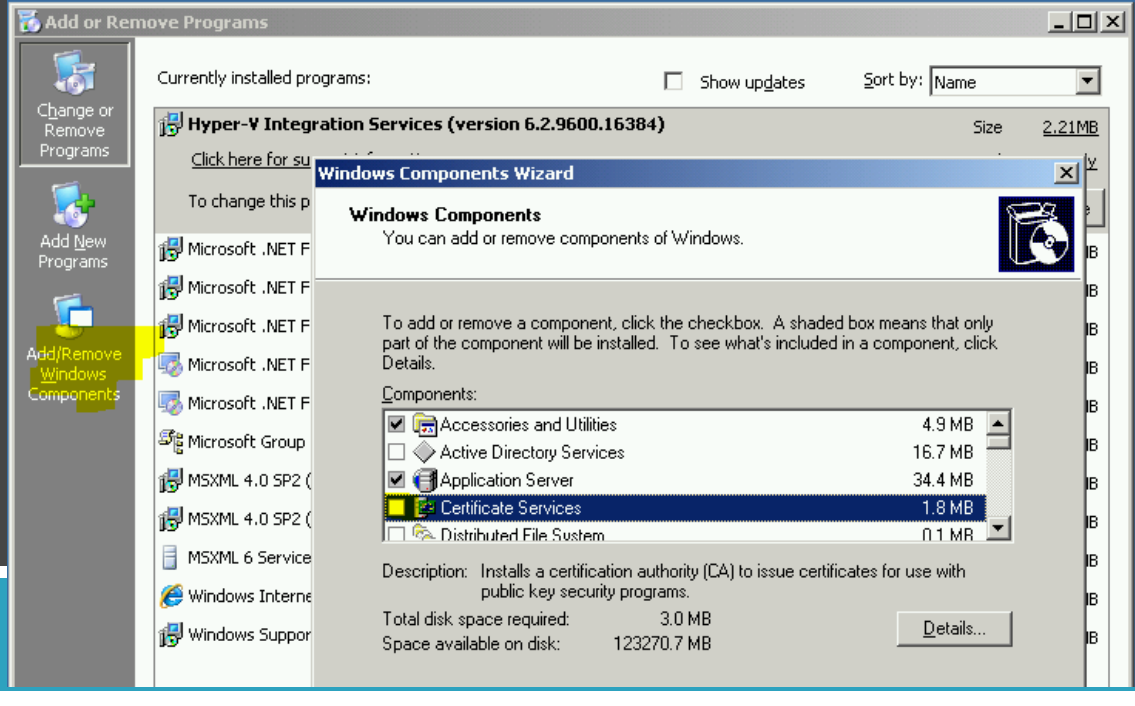
ZAZÁLOHOVÁNÍ CA

- Zazálohování konfigurace CA v registrech
  - Export klíče HKLM\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration
- Zazálohování souboru CAPolicy.inf
  - Manuální zkopírování souboru, pokud existuje
  - Používá se při instalaci CA, kdy může předem konfigurovat některé vlastnosti CA
  - Většinou uložený v adresáři C:\Windows



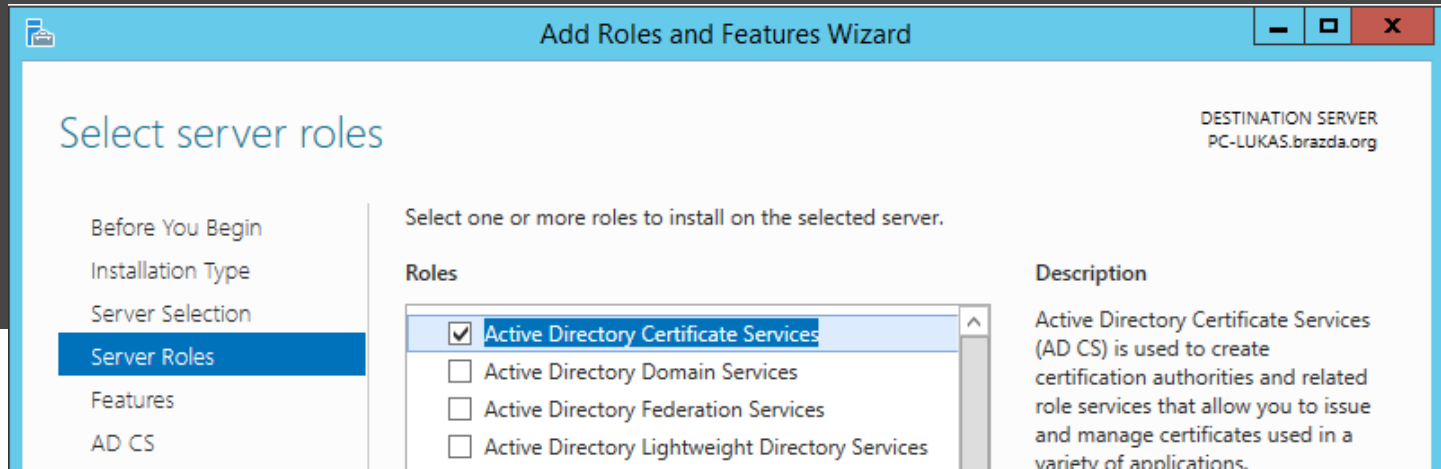
ODINSTALACE ROLE

- Windows Server 2003 nemá instalaci / odinstalaci CA ve správci serveru
- Roli CA musíme odstranit v Control Panelu
- Vykopírování záloh!
- Odebrání serveru z domény
- Smazání computer accountu



PŘIDÁNÍ NOVÉHO SERVERU

- Nový server musí mít stejné jméno, jako původní server s CA
- Přidáme do domény jako klasický member server
- Zkopírujeme si na něj zálohy z původního serveru
- Nainstalujeme roli AD CS se službami (např. web enrollment)
- Po instalaci binárek spustíme průvodce konfigurováním AD CS role



INSTALACE A KONFIGURACE ROLE CA

- Při konfiguraci nově nainstalované role zvolíme:
  - Typ původní CA – např. Root a Enterprise
  - Definujeme použití STÁVAJÍCÍHO certifikátu CA
  - Pokud jsme to ještě neudělali, tak naiportujeme původní certifikát CA (včetně privátního klíče)
  - Definumeme cesty pro uložení databáze a logů
  - Dokončíme průvodce

OBNOVA DB A KONFIGURACE

- V MMC konzoli Certification Authority
- Potvrdit nastartování služeb
- Ve Windows Exploreru potvrdit sloučení *.REG
- Restartování služeb CA
- Přidání potřebných šablon certifikátů
- Doladění konfigurace CA (AIA, CRL, apt.)

NASTAVENÍ OPRÁVNĚNÍ PRO AIA A CRL

- V konzole AD Sites and Services si zobrazit node Services
- Public Key Services → AIA → Název CA → Properties
- Přidat na záložku security computer account aktuálního serveru CA, Full Controll
- Původní computer account můžeme smazat

- Public Key Services → CDP → Název CA → cRLDistributionPoint → Properties
- Přidat na záložku security computer account aktuálního serveru CA, Full Controll
- Původní computer account můžeme smazat
- Opakovat pro každý cRLDistributionPoint

NOVÁ CA – OVĚŘENÍ FUNKČNOSTI

- EventLog – Application log
- Test různých enrollment metod:
  - Ručně z MMC konzole
  - Autoenrollment přes GPO
  - Web enrollment

6) Migrace DHCP Serveru

ZÍSKÁNÍ INFORMACÍ O AKTUÁLNÍM STAVU

- DHCP server je první role, kde využijeme vestavěných migration tools
- U DHCP serveru je vlastně otázka, jestli jej vůbec chceme migrovat
- Například v situaci, kdy máme jeden pool adres, žádné rezervace atp.
- V této situaci bude jistě rychlejší naklikat nový DHCP server a starý odstranit
- V konzoli DHCP serveru tedy zjistíme:
  - Kolik a jakých poolů server rozdává
  - Jestli existují nějaké rezervace
  - Jaké DHCP options má server nakonfigurovany
  - Jak je (pokud vůbec) řešená vysoká dostupnost služby
  - Můžeme prozkoumat logy DHCP serveru (C:\Windows\System32\dhcp)

MIGRATION TOOLS

- Vestavěný nástroj pro migraci některých služeb
- Od Windows Server 2008
- Založený na Windows PowerShell
- Kompatibilní ale i s Windows Server 2003
- Požadavky:
  - Dostatek místa na disku (aspoň 23 MB ☺)
  - Windows PowerShell 1.0 nebo novější
  - Microsoft .NET Framework 2.0 nebo novější

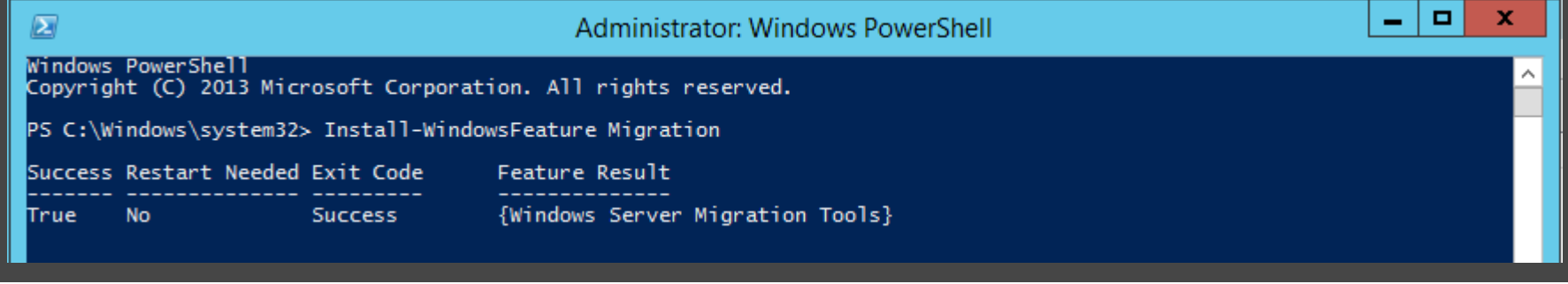
POSTUP MIGRACE

- Instalace Migration Tools na cílový server
- Vytvoření migračního balíčku a jeho zkopírování na zdrojový server
- Export nastavení zdrojového DHCP serveru
- Import nastavení na cílový DHCP server
- Deautorizace a odstranění zdrojového DHCP
- Autorizace a start cílového DHCP serveru

- Více zde: https://technet.microsoft.com/en-us/library/dd379483%28v=ws.10%29.aspx

INSTALACE MIGRATION TOOLS

- Provádíme na cílovém (2008+) serveru
- Buď klasicky přes průvodce přidáním rolí a features
- Nebo PowerShell:
  - Install-WindowsFeature Migration
- Po instalaci dostupné v C:\Windows\System32\ServerMigrationTools



VYTVOŘENÍ MIGRAČNÍHO BALÍČKU

- Opět připravujeme na cílovém serveru
- Migrační balíček vytváříme přesně „na míru“ zdrojovému serveru podle:
  - Bitové platformy (x86 nebo amd64)
  - Verze operačního systému

```
SmigDeploy.exe /package /architecture amd64 /os WS12 /path C:\Migration
SmigDeploy.exe /package /architecture amd64 /os WS08R2 /path C:\Migration
SmigDeploy.exe /package /architecture amd64 /os WS08 /path C:\Migration
SmigDeploy.exe /package /architecture x86 /os WS08 /path C:\Migration
SmigDeploy.exe /package /architecture amd64 /os WS03 /path C:\Migration
SmigDeploy.exe /package /architecture x86 /os WS03 /path C:\Migration
```

EXPORT NASTAVENÍ ZDROJOVÉHO DHCP

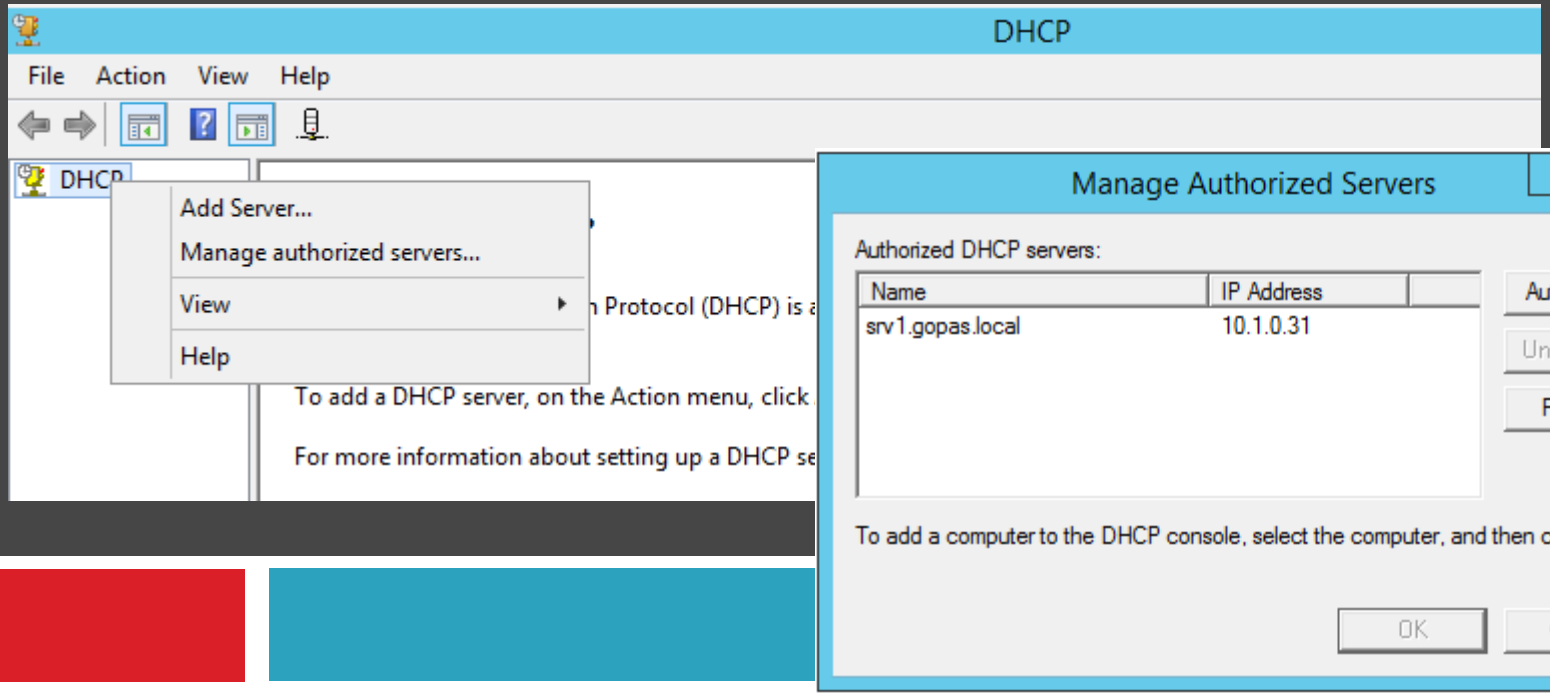
- Na zdrojový server jsme přenesli vytvořený migrační balíček
- V elevované CMD.exe spustíme příkaz SmigDeploy.exe
- To zaregistrovalo migrační nástroje do zdrojového serveru
- Nyní můžeme použít migrační CMDlety:
  - Get-Command *mig*
- Zastavíme službu stávajícího DHCP:
  - Stop-Service DHCPServer
- Vlastní export nastavení:
  - Export-SmigServerSetting -featureID DHCP -path C:\DHCPExport -Verbose

IMPORT NASTAVENÍ NA CÍLOVÝ DHCP

- Zkopírovali jsme si vyexportovanou konfiguraci ze zdrojového serveru:
  - Soubor C:\DHCPExport\svrmig.mig
- Provedeme příkazem v PowerShellu:
  - Import-SmigServerSetting -featureID DHCP -path C:\DHCPExport –Verbose
- Příkaz si i sám nainstaluje roli DHCP, pokud ještě není nainstalována
- Co si bohužel sám nenainstaluje, jsou nástroje pro správu DHCP, na co taky žejo ☺
- Takže ručně:
  - Install-WindowsFeature RSAT-DHCP

(DE)AUTORIZACE SERVERŮ

- Netsh DHCP delete server <Server FQDN> <Server IPAddress>
- Netsh DHCP add server <Server FQDN> <Server IPAddress>
- GUI:



7) Migrace WINS Serveru

WINS: A TO JAKO FAKT?

- WINS server je obdobou DNS serveru, akorát pro NetBios názvy
- NetBios názvy:
  - Max 16 znaků
  - Plochá struktura – tedy žádné suffixy jako např. u FQDN
- WINS umí dvě základní věci:
  - Překládat NetBios jména na IP adresy
  - Umožňuje klientům a serverům na síti dynamické registrace NetBios jmen
- Nejzákladnější otázka – potřebujeme ještě tuhle vykopávku?

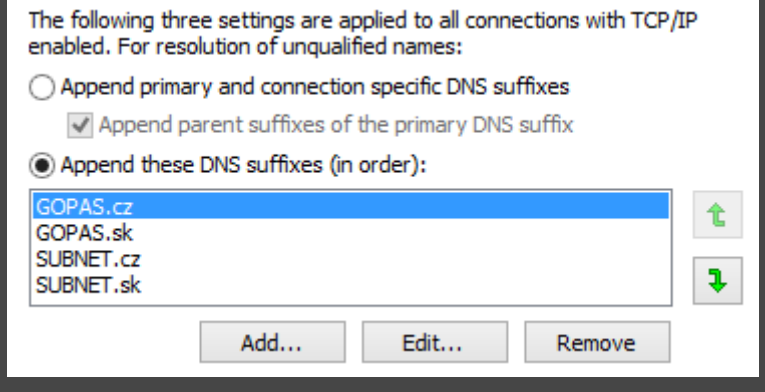
POTŘEBUJEME STÁLE WINS?

- Kdy potřebujeme WINS:
  - V síti se používají krátká jména, která (ne)lze překládat přes DNS
  - Potřebujeme dynamické registrace NetBios jmen
  - Nějaká stará aplikace na NetBios jménech stojí a padá…

- Kdy se můžeme zbavit WINS:
  - Když nepotřebujeme dynamické registrace NetBios jmen
  - Překlady krátkých jmen nám totiž luxusně umí i DNS (od Windows Server 2008)

GLOBAL NAMES DNS ZÓNY

- Speciální typ DNS zóny, která umožňuje překlad i krátkých (jako NetBios) jmen
- Defaultně není v DNS povolená
- Elegantní způsob jak se zbavit:
  - WINS serveru
  - DNS search suffix listu (pokud používáte)

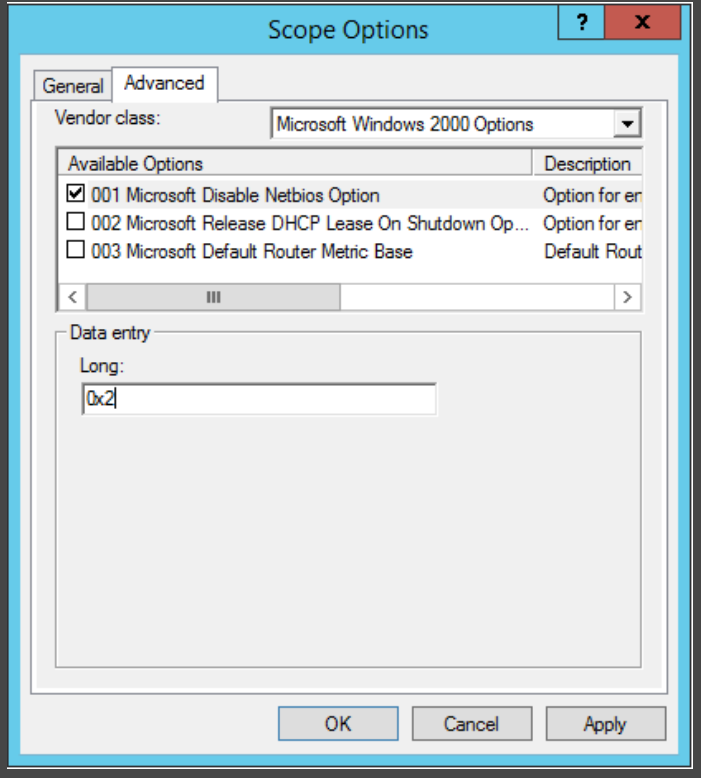


- Elegantnost spočívá hlavně v tom, že na klientech netřeba nic měnit! ;-)

POSTUP VYTVOŘENÍ DNS ZÓN

- Povolení GlobalNames zón v DNS serveru obecně (nutno provést na všech DNS)
  - Dnscmd.exe /Config /EnableGlobalNamesSupport 1
- Na DNS serveru vytvoříme novou zónu:
  - Primární, AD integrovaná
  - Jméno musí být GlobalNames
  - Replikovat ideálně na všechny DNS servery ve forestu (pokud nemáme, stačí doména)
  - Zakázané dynamické updaty (všechny záznamy vytváříme ručně)
  - V zóně tvoříme záznamy typu CNAME
- Ověření funkčnosti (ping, nslookup, atp.)

JAK ZAKÁZAT NETBIOS OVER TCPIP?



8) Migrace File Serveru

MIGRACE FILE SERVERU

- Tuto kapitolu rozdělíme na dvě základní témata:
  - Migrace klasického souborového serveru
  - Migrace Distributed File Systém (DFS)

- Detailně migraci včetně pokročilých scénářů popisuje článek:
  - https://technet.microsoft.com/en-us/library/jj863566.aspx

MIGRACE FILE SERVERU

- Klasický file server pro nás bude reprezentovat:
  - Server s vysdílenými adresáři
  - Nastavená oprávnění ke sdílení
  - Nastavená NTFS oprávnění

- Neuvažujeme např.:
  - Nasazení FSRM (diskové kvóty, file screening atp.)
  - Migraci lokálních uživatelů a skupin
  - GPO nastavení týkající se SMB, offline souborů atp.
  - Nasazení iSCSI Target serveru

POSTUP MIGRACE FILE SERVERU

- Budeme používat migration tools, které umějí migrovat data „za letu“
- Instalace migration tools na cílový server
- Příprava migračního balíčku (podle platformy a OS zdrojového serveru)
- Přenesení migračního balíčku na zdrojový server, spuštění SmigDeploy.exe
- Migrace dat za použití CMDletů:
  - Export-SmigServerSetting
  - Import-SmigServerSetting
  - Get-SmigServerFeature
  - Send-SmigServerData
  - Receive-SmigServerData

VYTVOŘENÍ MIGRAČNÍHO BALÍČKU

- Opět připravujeme na cílovém serveru
- Migrační balíček vytváříme přesně „na míru“ zdrojovému serveru podle:
  - Bitové platformy (x86 nebo amd64)
  - Verze operačního systému

```
SmigDeploy.exe /package /architecture amd64 /os WS12 /path C:\Migration
SmigDeploy.exe /package /architecture amd64 /os WS08R2 /path C:\Migration
SmigDeploy.exe /package /architecture amd64 /os WS08 /path C:\Migration
SmigDeploy.exe /package /architecture x86 /os WS08 /path C:\Migration
SmigDeploy.exe /package /architecture amd64 /os WS03 /path C:\Migration
SmigDeploy.exe /package /architecture x86 /os WS03 /path C:\Migration
```

REQUIREMENTS NA MIGRACI DAT

- Na cílovém serveru musí být dostatečně velký diskový prostor
- Zdrojový i cílový server správně syncovaný čas
- Na cílovém serveru nainstalovat stejné souborové služby, jako na zdrojovém serveru
- Na cílovém i zdrojovém serveru musí být ve firewallu otevřené porty:
  - UDP 7000
  - TCP 7000
  - Ujistěte se, že tyto porty nepoužívá žádná jiná aplikace na cílovém serveru
- Pokud migrace probíhá za provozu, ideální je zajistit neměnnost dat
  - např. nastavením read-only oprávnění pro Everyone skupinu na sdílení

POSTUP VLASTNÍ MIGRACE

- Na zdrojovém serveru máme dostupný migrační balíček
- Na zdrojovém serveru pustíme SmigDeploy.exe
- Na cílovém serveru spusťte příkaz: Receive-SmigServerData
  - Tento příkaz bude nyní čekat 5 minut
  - Během této doby musíme spustit migraci dat ze zdrojového serveru
  - HKEY_LOCAL_MACHINE\Software\Microsoft\ServerMigration\MaxConnectionTime (REG_DWORD): 1 – 3600 s
- Na zdrojovém serveru spustíme příkaz:
  - Send-SmigServerData -ComputerName SRV1 -SourcePath C:\.. -DestinationPath C:\.. -Recurse -Include All -Force
- Data jsou během migrace šifrována (zadáváte heslo)
- Zdrojový a cílový adresář nemusejí být stejné

MIGRACE DFS

- DFS má dvě základní komponenty:
  - DFS Namespaces
  - DFS Replication
- DFS Namespaces je služba „překladače“ virtuální UNC cesty
- DFS Replication je služba, která replikuje data mezi jednotlivými DFS servery

- Pro migraci DFS budeme využívat technologií DFS, nikoli migration tools

POSTUP MIGRACE DFS

- Kontrola a ověření stavu stávajícího prostředí
- Instalace nového serveru, přidání rolí DFS Namespaces, DFS Replication
- Přidání nového serveru jako DFS Namespaces serveru
- Přidání nového serveru do stávající replikační topologie DFS
- Zreplikování obsahu na nový server, kontrola
- Odstranění původních serverů z replikační topologie
- Odstranění původních serverů z DFS Namespaces serverů
- Kontrola funkčnosti nového serveru
- Volitelné přidání dalšího nového serveru (vysoká dostupnost, rozdělení zátěže)

9) Migrace IAS/NPS Serveru

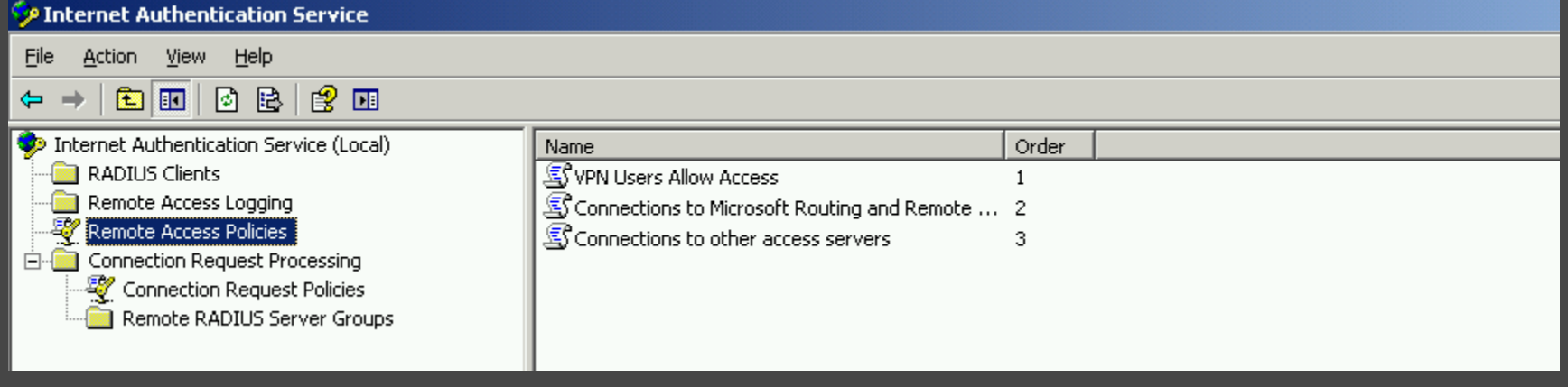
IAS/NPS SERVER

- Jedná se o stejnou funkcionalitu:
  - Na Window Serveru 2003 byl IAS server
  - Od Windows Serveru 2008+ role přejmenována na NPS
- Je to RADIUS server
- Slouží k řízení přístupu do sítě přes nejrůznější přístupové prvky:
  - Switche, WiFi AP, VPN servery, RDSGW, DirectAccess atp.

- Detailněji zde: https://technet.microsoft.com/en-us/library/hh831346

CO CHCEME MIGROVAT Z IAS?

- Z původního IAS serveru chceme do NPS migrovat:
  - Informace o případných RADIUS klientech
  - Existující network policy
  - Existující connection request policy



POSTUP MIGRACE

- Na cílový server nainstalujeme NPS roli, zaregistrujeme do AD
- Z cílového serveru překopírujeme na zdrojový soubor IASMigReader.exe
- Dostupný je:
  - C:\Windows\Syswow64
  - Na instalačním DVD: \sources\dlmanifests\microsoft-windows-iasserver-migplugin\
- Na zdrojovém serveru spustíme z příkazové řádky IASMigReader.exe
- Tento vyexportuje nastavení z IAS do TXT souboru, ten zkopírujeme na cílový server
- IASImport TXT souboru do NPS:
  - netsh nps import filename=„C:\IAS.txt„
  - Import-NpsConfiguration

NÁSLEDNÉ KROKY PO MIGRACI

- Kontrola importu v konzoli NPS
- Kontrola autentizačních metod (hlavně těch certifikátových)
- Volitelně:
  - Přejmenování serveru
  - Změna IP adresy
- Pokud tyto změny neprovedete, je potřeba překonfigurovat stávající RADIUS klienty

10) Migrace Print Serveru

MIGRACE PRINT SERVERU

- Podobná otázka jako u DHCP – je třeba ji vůbec nějak migrovat?
- Pokud máte hodně driverů, tiskáren atp. tak asi ano
- V opačném případě bude možná snazší tiskárny zmigrovat ručně…
- Migrace print serveru opět nepoužívá migration tools
- Celá migrace se dá provést buď:
  - Konzole Print Management (je dostupná i na klientských systémech)
  - Příkaz Printbrm.exe
- Alfou a omegou je mít už na zdrojovém serveru správné ovladače pro cílový server!

- Podrobněji zde: https://technet.microsoft.com/en-us/library/jj134150

POSTUP MIGRACE

- V rámci přípravy je vhodné stávající server „vyčistit“ od nepotřebných:
  - tiskáren
  - portů
  - ovladačů
- Na zdrojový server doinstalujeme ovladače všech tiskáren (pro cílovou platformu)
- Na cílovém serveru nainstalujeme roli Print Serveru, spustíme Print Management
- Provedeme export / import z průvodce
- Kontrola Application EventLogu
- Následné přemapování tiskáren klientům nebo alias v DNS (jiné jméno)

11) Migrace Terminal Services

MIGRACE TERMINAL SERVICES

- Zde pravděpodobně není co migrovat
- Licenční server s 2003 RDS CAL? Ten už asi nevyužijeme…
- Vlastní Terminal Server?
  - Aplikace, které na něm jsou, stejně musíme nainstalovat na nový RD Server

12) Migrace IIS

MIGRACE IIS

- Při migraci IIS musíme vzít v potaz následující faktory:
  - Existující Sites
  - Existující App Pools a jejich konfigurace
  - Komponenty a závislosti nainstalované na stávajícím serveru
  - SSL/TLS certifikáty
  - Vlastní obsah IIS
  - Atp.
- V případě existence např. jediné Site, můžeme klidně migrovat ručně
- V opačném případě můžeme využít některých toolů:
  - MS Web Deploy - http://www.microsoft.com/cs-cz/download/details.aspx?id=39277
  - IIS Easy Migration Tool (není od MS) http://www.iis.net/downloads/community/2013/04/iis-easy-migration-tool-%28iemt%29

POSTUP MIGRACE IIS

- Na zdrojový i cílový server instalujeme Web Deployment Tool (podle bitové verze!)
- Na zdrojovém serveru zjistíme případné závislosti“
  - msdeploy -verb:getDependencies -source:metakey=lm/w3svc/1
  - Tyto případně doinstalujeme na cílovém serveru
- Na zdrojovém serveru vyexportujeme obsah IIS
  - msdeploy.exe -verb:sync -source:metakey=lm/w3svc/1 -dest:package=C:\IISBack.zip, encryptPassword=Pa$$w0rd -enableLink:AppPoolExtension
- Na cílovém serveru obnovíme obsah balíčku IISBack.zip do IIS
  - msdeploy.exe -verb:sync -source:package=C:\IISBack.zip, encryptPassword=Pa$$w0rd -dest:metakey=lm/w3svc/1 -whatif > msdeploysync.log -enableLink:AppPoolExtension

13) Migrace WSUS

MIGRACE WSUS

- Jediný pro nás podporovaný scénář je migrace z WS2003 SP2 + WSUS 3.0 SP2!
- Podporované jsou i scénáře migrace z SQL2005 na SQL2008 R2 SP1
- Lze migrovat i ze zdrojové WID do cílového SQL2008 R2 SP1
- Lze migrovat mezi WRKGRP i doménou, i mezi jazykovými verzemi

- Více zde: https://technet.microsoft.com/en-us/library/hh852352.aspx

PŘÍPRAVA MIGRACE WSUS

- Odinstalujte WSUS ze zdrojového serveru
- Na zdrojový server nainstalujte SQL Management Studio Express
- Pokud na cílovém serveru budete používat SQL, nainstalujte ho
- Pomocí server manageru nainstalujte na cílový server WSUS, wizarda neprocházejte
- Pokud na cílovém serveru používáte WID, nainstalujte SQL Management Studio

POSTUP VLASTNÍ MIGRACE WSUS

- Migrace vlastních aktualizací (souborů) ze zdrojového serveru na cílový
- Migrace případných WSUS security skupin (např. pomocí WSMT nebo ručně)
- Zazálohování WSUS databáze ze zdrojového serveru
- Obnovení WSUS databáze na cílovém serveru
- Změna WSUS server identity
- Změna konfigurace klientů (např. konfigurací WSUS v GPO)

- Detailní postup: https://technet.microsoft.com/en-us/library/hh852349.aspx

GOC197: Migrace z Windows Serveru 2003

Lukáš Brázda | MCT, MCSA, MCSE| lukas@brazda.org