# AD Backup & Restore

Literatura MCTS Exam 70-640: Configuring Windwos Server 2008 Active Directory, Second Edition

# Proč zálohovat

- Ztráta dat vlivem přírodních jevů ale i cílených útoků
- Selhání jednotlivce (smazání objektů v AD)
- Nutnost vrátit se ke starší funkční konfiguraci
- Automatické uchovávání smazaných objektů (tombstone) nemusí stačit
- Uchování více verzí objektu
- Obnova všech atributů objektu

# Windows Server Backup

- Zálohování zajišťuje Windows Server backup (wbadmin.exe)
- Možnost plánovaných záloh (task scheduler)
- Využívá Volume Shadow Copy
- Nutno přidat v Server Manager – Features
- Typy záloh:
  - Full server (komplet všechny volume)
  - Bare metal recovery (boot + system volume)
  - System State (konfigurační data serveru)
  - Vybrané volume, adresáře či soubory
  - Lze kombinovat i použít exclude
- Backup location
  - Nedá se zálohovat na dynamic volume, pásky
  - HDD (dojde k formátu - OS chce výlučný přístup, umožní uložení více záloh)
  - Volume
  - Sdílený adresář (vždy jen jedna záloha)
- Full vs. Incremental backup (sleduje změny na úrovni bloků ne souborů – efektivní, ale výkonnostně náročné)

# AD DS database mounting tool

- Nástroj dostupný od Windows Server 2008 (dsamain.exe)
- Vybranou ntds.dit databázi zpřístupní jako LDAP server, na který je možné se připojit a prohlížet obsah
- Díky tomu můžeme prohlédnout obsah AD databáze ze zálohy ještě před obnovou (dříve bylo nutno nabootovat do DSRM, obnovit data, odpojit síť, restartovat a zkontrolovat co se obnovilo)
- Standardně LDAP běží na portu 389, proto je potřeba při mountu vybrat jiný nekonfliktní port
  - dsamain -dbpath „cesta_k_ntds.dit -ldapport 40000

# Obnova AD objektů

- Obnova
  - Offline = DSRM (Directory Services Restore Mode)
    - Je potřeba heslo pro obnovu AD
    - Př.: System state
  - Online = pod běžícím DC
    - Př.: AD snapshot , AD Recycle Bin, Tombstone
- Obnova z „koše“
  - Tombstone object
  - AD Recycle Bin
- Typy AD obnovy ze zálohy
  - Nonauthoritative
  - Authoritative

# Obnova AD objektů 2.

- **Neautoritativní obnova** se používá k obnovení funkčnosti DC (takové jaká byla v čase vytvoření zálohy). Po jeho zapojení do sítě se provede aktualizace (replikace) dat z ostatních DC (zreplikuje se i informace o smazaných objektech -> neobnoví smazaná data)
  - Provádí se v DSRM režimu
  - Typicky se použije pokud chceme zprovoznit „rozbité" DC
- **Autoritativní obnova** se používá k obnově ztracených či modifikovaných dat. Nastaví u obnoveného objektu atribut Update Sequence Number (verze objektu). Tím, že se nastaví větší USN než má daný objekt na zbylých DC se stane autoritativní a zreplikuje se na všechny zbylé DC
  - Autoritativní obnova se dá dělat bez použití DSRM
  - Spouští se po provedení neautoritativní obnovy s tím, že pro vybrané obnovené objekty nastaví USN (označí je za autoritativní)

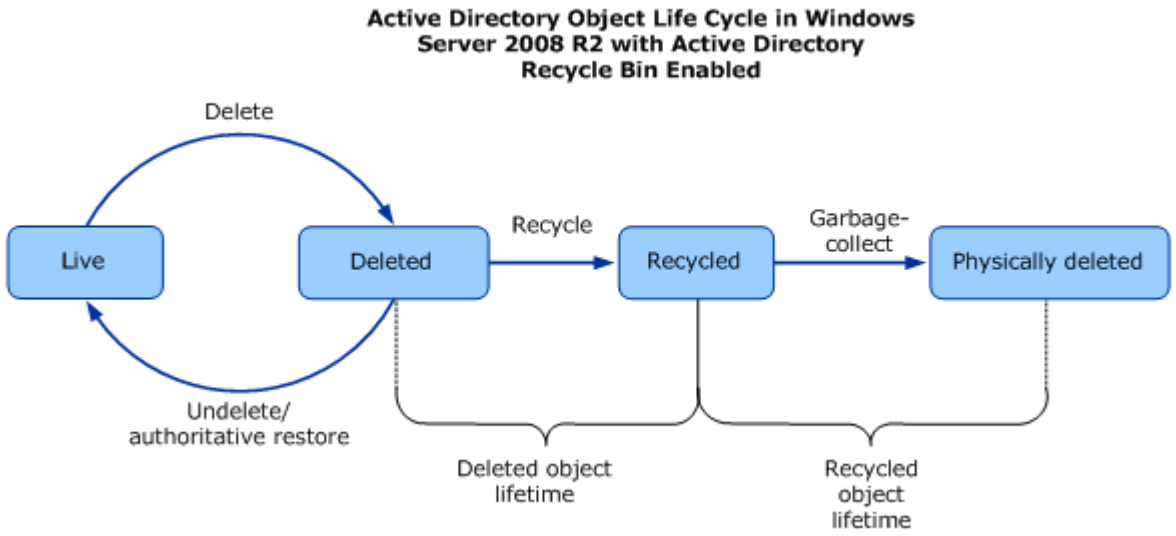
# „Koš“ v AD

- Po smazání objektu v AD nedojde k fyzickému odstranění z ntds databáze
- Smazaný objekt můžeme „obnovit“ ručním vytvořením (jiný SID, GUID,bez atributů) nebo obnovit ze zálohy (v offline režimu DSRM) nebo obnovit z „koše“
- Ne každý objekt v AD se dá obnovit (Configuration NC)
- Před Windows Server 2008 R2 se po smazání objektu:
  - Nastavil atribut isDeleted na TRUE
  - Došlo k **odstranění většiny atributů** (membership,.. – lze upravit ve schématu)
  - Přesunul se do speciálního skrytého kontejneru (cn=deleted objects)
  - Takový objekt je označován jako **Tombstone**
  - Po 180 dnech dojde k trvalému smazání (dříve 60 dnů) díky procesu čištění Garbage collection
  - Kontejner se smazanými objekty není v ADUC konzoli vidět
  - Pro zobrazení/obnovu se používá nástroj ldp.exe (adrestore.exe, ADRecycleBin)

# „Koš“ v AD – AD Recycle Bin

- Od Server 2008 R2 je dostupný AD Recycle Bin
  - Vyžaduje funkční forest level 2008 R2 (všechny DC musí být aspoň Server 2008 R2)
  - Ve výchozím nastavení je vypnut (povolením se smažou všechny tombstone objekty)
  - Smazání zachovává **všechny atributy** objektu
  - Dva stavy
    - Logically deleted object (objekt je přesunut do AD koše, ale zachovávají se všechny atributy)
    - Recycled object (po vypršení deleted lifetime, se jeho stav změní na recycled-nedá se obnovit a ztratí většinu atributů a po uplynutí recycled lifetime je fyzicky smazán)
    - Výchozí čas pro obnovu je 180 dnů, ale dá se měnit modifikací atributů (*msDS-DeletedObjectLifetime* a *TombstoneLifetime*)
  - Pro zobrazení/obnovu se používá nástroj ldp.exe (adrestore.exe, ADRecycleBin)

# Životní cyklus u AD Recycle Bin



# Úkol - obnovení Tombstone objektu

- Vytvořte uživatele xbabel a dejte mu atributy jako adresa, telefon, členství ve skupině administrators. Nyní ho smažte
- Spusťte ldp.exe a připojte se k jednomu z DC (brno.pondeli.local)
- V Connection menu zvolte bind (jako aktuálně přihlášený uživatel)
- V Options menu zvolte Controls – Return deleted objects
- Ve View menu vyberte Tree a napište cn=Deleted Objects,dc=pondeli,dc=local
- Pravým na objekt – modify
  - Napište isDeleted, value nechte prázdné, vyberte operaci Delete a klikněte na Enter
  - Napište distinguishedName, do value dejte DN a vyberte Replace a potvrďte (př. nového DN cn=John Kane,ou=Lide,dc=pondeli,dc=local)
- Zkontrolujte, že je zaškrtnut checkbox Extended a Synchronous a dejte Run
- V ADUC zkontrolujte, že je objekt obnoven (SID je zachován, ale ne členství ve skupinách, je zakázán, bez hesla, ...)
- Vyzkoušejte i nástroje ADRestore (sysinternals) a ADRecycleBin.exe případně Quest Object Restore for Active Directory

# Povolení AD Recycle bin

- Povýšit Forest Functional level na Server 2008 R2 (člen Enterprise Admins)
  - AD Domains and Trusts konzole
  - Set-ADForestMode -Identity pondeli.local -ForestMode Windows2008R2Forest
- Povolení AD Recycle Bin
  - Enable-ADOptionalFeature -Identity „CN=Recycle Bin Feature,CN=Optional Features,CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,DC=pondeli,DC=local“ -Scope ForestOrConfigurationSet -Target pondeli.local
  - Aktivaci provádět na DC které hostuje FSMO role Schema Master a Domain Naming Master
    - netdom query FSMO
  - Zapnout službu AD Web Services!
    - net start adws

# Obnovení objektu z AD koše

- Proces obnovení objektu je totožný jako v prostředí bez AD Recycle Bin
- Rozdíl je v tom, že nyní se obnoví všechny atributy objektu

- Smažte uživatele jenž byl členem nějakých skupin
- Obnovte a v ADUC zkontrolujte, že je objekt obnoven (včetně SID, membership, hesla, není zakázán,..)
- Vyzkoušejte obnovu pomocí Powershellu
  - Get-ADObject -Filter {deleted –eq “TRUE”} -IncludeDeletedObjects
  - Get-ADObject -Filter {displayName -eq "Mary“} -IncludeDeletedObjects | Restore-ADObject

# AD Snapshots

- AD snapshot slouží k uložení aktuálního stavu domény a všech jejích objektů
- Při vytvoření dalšího snapshotu, se zachycují jen změny oproti předchozí verzi (první snapshot je proto prakticky nulový)
- Pomocí nástrojů jako Directory Service Comparison Tool lze porovnat aktuální databázi s tou ve snapshotu a obnovit vybrané objekty či atributy (pro export / import dat lze použít i ldifde)
- Vytvoření AD snapshotu
  - **Ntdsutil "activate instance NTDS" snapshot create quit quit**
  - Každý snapshot obsahuje všechny volume s AD daty (pokud mám logy či databázi na jiném volume, bude zahrnut)

# Zobrazení obsahu snapshotu

- Získání seznamu všech snapshotů
  - **ntdsutil "activate instance NTDS" snapshot "list all" quit quit**
- Namountování snapshotu:
  - **ntdsutil "activate instance NTDS" Snapshot "mount {guid}" quit quit**
- Použití AD DS database mounting utility pro rozjetí snapshotu jako LDAP serveru
  - **dsamain -dbpath c:\$SNAP_datetime_VOLUMEC$\windows\ntds\ntds.dit -ldapport portnumber** (port použít větší než 40000 kvůli konfliktům)
  - Nezavírat cmd!
- Po použití dsamain můžeme otevřít namountovanou AD databázi pomocí ldp.exe či ADUC konzole
- Otevření pomocí ADUC konzole
  - V ADUC konzoli změňte DC na **JmenoServeru:DriveZadanyPort**
- Zavřením cmd (CTRL+C) dojde k ukončení LDAP serveru
- Unmount snapshotu provedeme:
  - **ntdsutil "activate instance NTDS" snapshot "unmount {*guid*}" quit quit**

# Úkol – obnovení objektu z AD snapshotu

- Vytvořte uživatele xkarel a xbanan v OU Uzivatele
- Uživateli xbanan nastavte i atribut příjmení
- Vytvořte AD snapshot
- Smažte uživatele xkarel
- Změňte příjmení uživatele xbanan
- Otevřete si AD snapshot pomocí ADUC a podívejte se, že xkarel existuje (včetně všech atributů, nastavení, …)
- Všimněte si, že objekty jsou read-only
- Nainstalujte si Directory Service Comparison Tool
- Obnovte ze snapshotu uživatele xkarel (mmc – add snapin)
- Obnovte původní příjmení u uživatele xbanan

# System state

- Záloha pouze vybraných částí systému
- Na DC obsahuje System state záloha:
  - Registry
  - COM+ Class Registration databázi
  - Bootovací soubory (Boot.ini, NDTLDR, NTDetect.com)
  - Chráněné systémové soubory (Windows Resource Protection)
  - AD databázi (ntds.dit)
  - SYSVOL adresář
- Pokud obsahuje jiné role obsahuje první čtyři a:
  - AD CS databázi (u AD certification services role)
  - Cluster service informace (u Failover Cluster feature)
  - IIS konfigurační data (u Web Server role)

# System state - backup

- Backup mohu provést skrze CMD (wbadmin) či GUI (WS backup)
- Pro jednorázovou zálohu system state
  - **wbadmin start systemstatebackup -backupTarget:D: -quiet**
  - **wbadmin start systemstatebackup /?**
- Pro vytvoření plánu zálohování system state
  - **wbadmin enable backup -addtarget:D: -schedule:09:00 -SystemState –quiet**
  - **wbadmin enable backup /?**
- System state data lze obnovit i z Full System zálohy (dostupné módy obnovy jsou fullserver restore, **system state only restore** a individual file or folder restore)

# Úkol

- Vytvořte system state backup

# Full Server Backup

- Kompletní záloha všech volume
- Právo Backup Operators či Administrators
- GUI vs. Cmd (wbadmin.exe)
- Jednorázová záloha
  - wbadmin start backup -allcritical -backuptarget:*location* –quiet
- Vytvoření plánu záloh
  - wbadmin enable backup -addtarget:E: -schedule:21:00,06:00 -include:C:\dir*

# Kompletní obnova systému ze zálohy

- Pokud dojde k selhání DC a je potřeba provést kompletní obnovu z WinRE (lokálně (WAIK), instalační CD)
- GUI
  - Rozjeďte Repair my Computer z instalačního média
  - Recovery Tool - System Image Recovery
  - Aby nedošlo ke smazání volume, které nejsou obsaženy v záloze použijte Exclude Disks
- CMD
  - Rozjeďte Repair my Computer z instalačního média
  - Recovery Tool – Command Prompt
  - Diskpart – list vol (zjistěte na kterém volume je záloha) – exit
  - wbadmin get versions -backuptarget:drive-machine:servername
  - wbadmin start sysrecovery -version:datetime -backuptarget:drive -machine:servername –quiet
  - restart

# Srovnání jednotlivých variant

| Tombstone object | AD Recycle Bin | Backup |
|---|---|---|
| Obnovuji z běžícího DC | Obnovuji z běžícího DC | Obnovuji pomocí DSRM (offline) |
| Obnovím jen některé atributy objektu | Obnovím všechny atributy objektu | Obnovím všechny atributy objektu |
| Obsahuje jen smazanou verzi objektu | Obsahuje jen smazanou verzi objektu | Každá záloha obsahuje jednu verzi objektu |

# Neautoritativní obnova

- Skrze F8 se dostaňte do DSRM (u virtuálu nejdřív F5)
- Vyberte Directory Services Restore Mode
- Pro přihlášení použijte heslo pro obnovu AD, které jste zadali při vytváření prvního DC

(Pokud chcete obnovit jen AD data (System State) musíte použít cmd jinak GUI Windows Server Backup)

- Pro získání seznamu záloh na disku F pro stroj brno1
  - **wbadmin get versions -backuptarget:F: -machine:brno1**
- Pro obnovu System State
  - **wbadmin start systemstaterecovery -version:02/15/2012-19:38 -backuptarget:C: -machine:brno1 –quiet**
  - U lesa s Server 2008 R2 f.l. a DFS replikací tento postup vytvoří neautoritativní obnovu SYSVOLu, přepínač –authsysvol tomu zabrání
- Po provedení obnovy a restartu dojde ke kontrole integrity AD

# Autoritativní obnova - online

- Je možno provádět na běžícím DC (pod doménovým adminem)
- Zastavte službu Active Directory Domain Services
- Do příkazové řádky zadejte:
  - **ntdsutil „activate instance NTDS“ „authoritative restore“ „restore object database“ quit quit**
- Pro obnovení jen části AD použijte
  - **ntdsutil “activate instance NTDS“ “authoritative restore“ “restore subtree ou=pc,dc=test,dc=local“ quit quit**
- “Zavřete cmd a restartujte ADDS službu
- Data označená jako autoritativní budou zreplikována na ostatní DC

# Autoritativní obnova - offline

1. Provedeme zálohu System state
   - **wbadmin start systemstatebackup -backupTarget:D:**
2. Smažeme OU ou=test1,dc=pondeli,dc=local s uživateli
3. V msconfig vyberu safe-boot-active directory repair
4. Restart
5. Provedeme neautoritativní obnovu System state
   - **wbadmin get versions (opsat version identifier:)**
   - **wbadmin start systemstaterecovery -version:04/04/2009-20:16 –quiet**
6. Provedeme autoritativní obnovu vybrané OU
   - **ntdsutil "activate instance NTDS" "Authoritative restore" "restore subtree" "ou=test1,dc=pondeli,dc=local" q q**
7. Upravit msconfig aby naběhlo do klasického režimu
8. Restart

# Úkol – autoritativní obnova

- (Ukazuje učitel)
- Vytvořte system state zálohu na serveru1
- Smažte nějakou OU (s objekty), nějaký klíč v registru
- Přejděte do DSRM a obnovte system state
- Autoritativně obnovte dříve smazanou OU
- Restartujte a zkontrolujte

# Ochrana objektů

- Ochrana před náhodným smazaním (přesunem)
  - Přiřadí 2 deny oprávnění pro Everyone na delete a delete subtree
- Auditování změn v AD (event log)

# GPO backup

- GPO backup
- GPO restore
- Import Settings

# Best pratice

- Každý DC by měl sloužit jen k jednomu účelu, nepřidávejte žádné další role (kromě DNS)
- Virtualizujte DC (skrze Hyper-V)
- Na DC neukládejte žádná další data
- Mějte na Hyper-V serveru pro virtuály k dispozici instalační ISO pro obnovu DC nebo na virtuálních DC nainstalujte WinRE (součást WAIK)
- Provádějte pravidelné automatické zálohy (AD snapshot, System state a občas i full systém backup)
- Chraňte heslo pro obnovu DC (Directory Service Restore Mode password)