Obnova AD, AD Recycle Bin

Šimon Suchomel

Připojení disku v openstack

- Vypněte dc2
- Vytvořte nový svazek (volume)
  - Výpočty -> Svazky -> + Vytvořit svazek
- Připojte ho k instanci (serveru)
  - Výpočty -> Svazky -> (u vybraného svazku) -> Správa příloh
  - Vyberte instanci k připojení
  - Spusťte instanci
    - Výpočty -> instance -> (u vybrané instance) Spustit instanci

Windows Server Backup

- Feature -> Windows Server Backup
  - Server manager -> Add roles and features (proklikat na features), nevyžaduje restart
  - Využívá Volume Shadow Copy
  - Možnost plánovaných záloh (task scheduler)
  - Typy záloh:
    - Full server (komplet všechny volume)
    - Bare metal recovery (boot + system volume)
    - System State (konfigurační data serveru)
    - Vybrané volume, adresáře či soubory
- `Install-WindowsFeature -Name Windows-Server-Backup -IncludeAllSubfeature –IncludeManagementTools`
- `Get-Command -Module WindowsServerBackup`
- `wbadmin.exe`
- Účet s právem Backup operators

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)

PS module Windows-Server-Backup

- Příklad zálohy system state na disk F:
  - `#create the backup policy`
    `$policy = New-WBPolicy`
  - `#back up the System State`
    `Add-WBSystemState -Policy $policy`
  - `#declare the backup location as my F: volume`
    `$target = New-WBBackupTarget -VolumePath "F:"`
  - `#add the backup location to the policy`
    `Add-WBBackupTarget -Policy $policy -Target $target`
  - `#start the backup`
    `Start-WBBackup -Policy $policy`

Zálohování

- Výpadek dat
  - Přírodní jev
  - Chybné odstranění
  - Nechtěné smazání, selhání na straně lidského faktoru
- Chyba dat
  - Změna chybou aplikace/osoby, útok či náhodné selhání

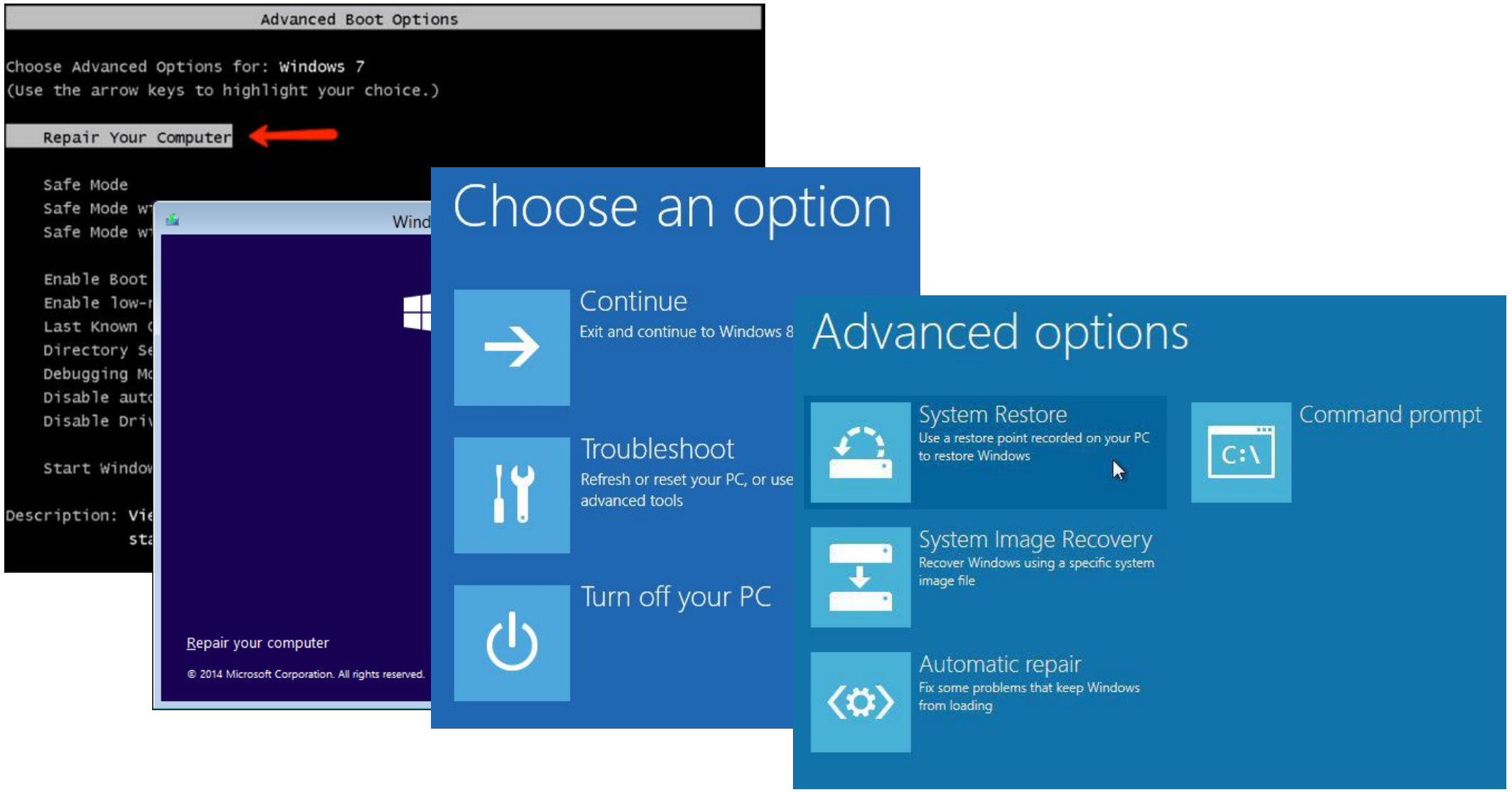
Windows Server Backup

- Jednorázová záloha je typu Full, naplánované zálohy jsou typu Incremental
  - Incremental backup sleduje změny na úrovni bloků ne souborů – efektivní, ale výkonnostně náročnější
- 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)

Directory Service Restore Mode

- Pro obnovení AD
- Boot do SDRM:
  1. F8 při bootu -> repair your computer nebo boot z intalačního média
  2. Msconfig -> Boot options, select Safe boot vybrat Active Directory repair
     - Po obnově před restartem vrátit zpět na normal startup
  3. Bcedit příkaz
     - bcedit /set safeboot dsrepair
     - Po obnově před restartem bcedit /deletevalue safeboot

Repair Your Computer



Obnova AD objektů

- Obnova
  - Offline = DSRM (Directory Services Restore Mode)
    - Je potřeba heslo pro obnovu AD
      - Je k dispozici lokální účet administrator
    - 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 (neautoritativní)
  - Authoritative (autoritativní)

AD Recycle Bin

- Od funkční úrovně Windows Server 2008 R2
- Smazání objektu zachovává **všechny atributy** objektu
- Pokud je zapnut, každý DC je zodpovědný za aktualizaci odkazů objektů jiných domén
  - Infrastucture master nemá žádný význam

Zapnutí AD Recycle Bin

- Server Manager -> Tools -> Active Directory Administrative Center
- Enable-ADOptionalFeature –Identity 'CN=Recycle Bin Feature,CN=Optional Features,CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,DC=ad,DC=local' –Scope ForestOrConfigurationSet –Target 'ad.local'

Obnovení z AD Recycle Bin

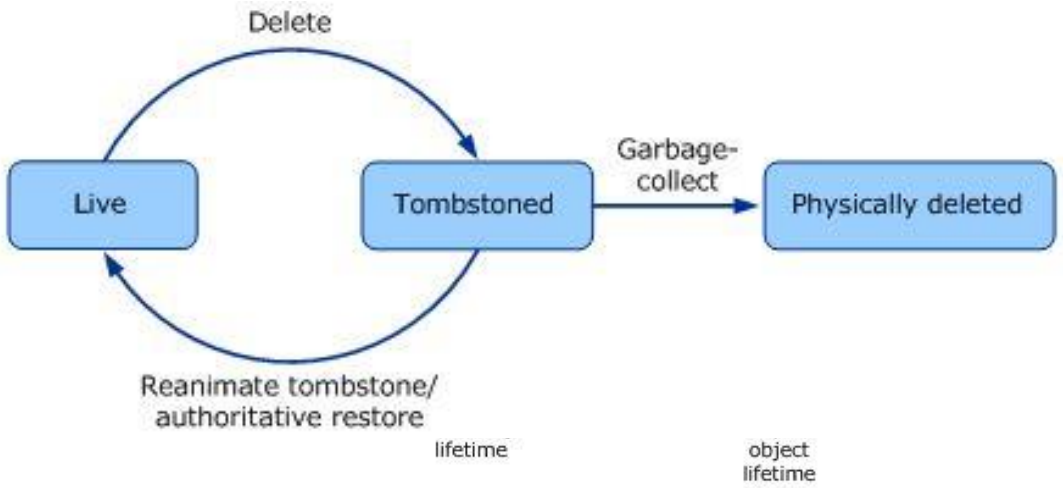
- Ve výchozím nastavení 180 dní
  - Atribut *msDS-DeletedObjectLifetime*
- Get-ADObject -IncludeDeletedObjects -filter {Deleted -eq $true} –property *
  - Vybereme objekt např. filtrem přes jeho display name –filter {DisplayName –eq “Martina Navratilova”} a obnovíme pomocí | Restore-ADObject

Snaphosts of AD

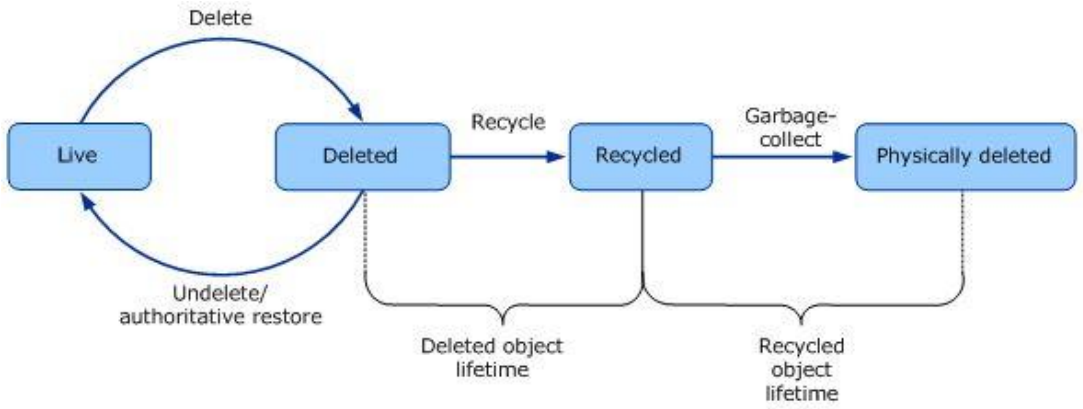
- Volume Shadow Copy snímek disku včetně databáze AD
- Vytvoření AD snapshotu
  - `Ntdsutil`
    - `activate instance NTDS`
    - `snapshot create`
  - Každý snapshot obsahuje všechny volume s AD daty (pokud mám logy či databázi na jiném volume, bude zahrnut)
  - Ukládají se do System Volume Information

Životní cyklus smazaných objektů

Bez AD Recycle Bin



S AD Recycle Bin



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

AD DS database mounting tool

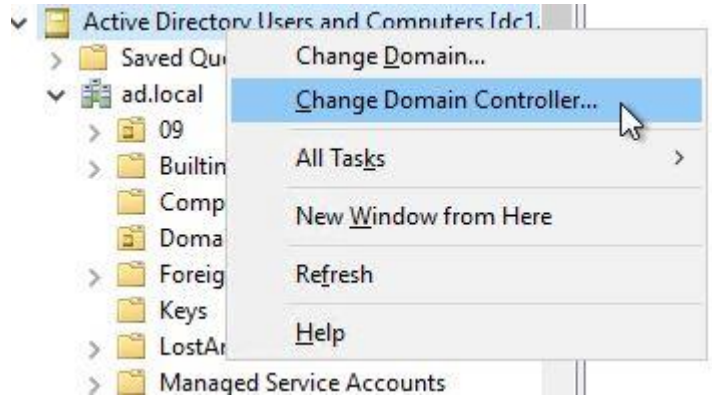
- Spolu se snaphostem
  - Pro zjednodušení obnovy
  - Audit změněných a smazaných objektů
- Nástroj dostupný od Windows Server 2008 (dsamain.exe)
- Vybranou databázi AD (soubor ntds.dit) zpřístupní jako LDAP server, na který je možné se připojit a prohlížet obsah
- Díky tomu si můžeme prohlédnout obsah 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`

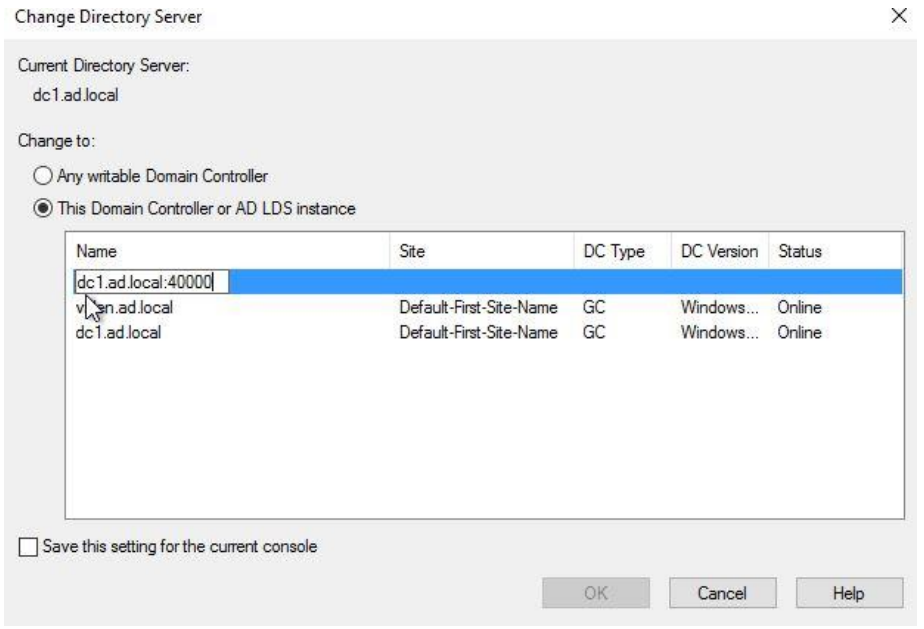
Prohlídka snímku ze zálohy

- Záloha Windows Backup používá také Volume Shadow Copy
- Seznam snímků
  - `ntdsutil „activate instance NTDS“ snapshot „list all“`
- Připojení snímku na lokální disk
  - `ntdsutil "activate instance NTDS" Snapshot "mount {guid}„`
- Lokace databáze
  - Pokud jsme si připojili snímek zálohy z Windows backup, vidíme její soubory, data která jsou přímo na disku jsou ale obsažena ve vhd souboru (read only)
  - Připojení vhd v mmc nástroji disk management
  - Přístup na svazek pomocí cesty s ID
    - get-volume | format-list
    - Cesta s ID lze zadat do příkazu run
      - nebo např. `start \\?\Volume{f89b2150-4a7a-48b1-a78a-0f5a0b9681cd}\`

Prohlídka snímku ze zálohy

- Máme-li přístup k databázi (NTDS.dit), lze ho připojit jako funkční LDAP server, na který se již můžeme dotazovat standardním způsobem, např. v Active Directory Users and Computers
  - dsamain -dbpath „cesta_k_ntds.dit -ldapport 40000
  - LDAP ukončíme později zavřením otevřeného okna nebo ctrl+c





Odpojení snímku

- Zavřeme LDAP server, který jsme spustili přes dsamain
- Provedem `unmount {guid}` v ntdsutil

Autoritativní obnova – vybraných objektů

- Restarovat DC do DSRM
- Obnovit objekty ze zálohy (neautoritativně)
- Označit konkrétní objekt jako autoritativní
- Restartovat DC do normálního módu
  - Replikace již zajistí zbytek

Označení objektu jako autoritativní

- `ntdsutil`
  - `activate instance ntds`
  - `authoritative restore`
- Vybrat například celou OU, pak se autoritativně obnoví všechny objekty v ní obsažené
  - `restore subtree <distinguishedName>`
  - Př. `restore subtree “OU=Zamestnanci,OU=Uzivatele,DC=ad,DC=local”`
- Nebo vybrat konkrétní objekt
  - `restore object <distinguishedName>`
- Je potřeba zadat správně DN objektu, možná chyba, je že objekt byl smazán až po záloze a proto neexistuje ani v restore