

Serverové systémy Microsoft Windows

IW2/XMW2 2012/2013

Jan Fiedor

ifiedor@fit.vutbr.cz

Fakulta Informačních Technologií

Vysoké Učení Technické v Brně

Božetěchova 2, 612 66 Brno

Revize 15. 4. 2013

Active Directory

Údržba, ochrana, Active Directory koš

Údržba Active Directory

- Údržba objektů Active Directory
 - Identit nutných pro autentizaci
 - GPO objektů potřebných pro aplikaci nastavení
 - Objektů míst a propojení míst zajišťujících replikaci
- Údržba služeb (nejen) Active Directory
 - Zajištění přístupu ke službám (DNS, DHCP, ...)
 - Monitorování výkonu serverů poskytujících služby
 - Zabezpečení prostředků i samotných řadičů domény
- ...

Údržba databáze Active Directory

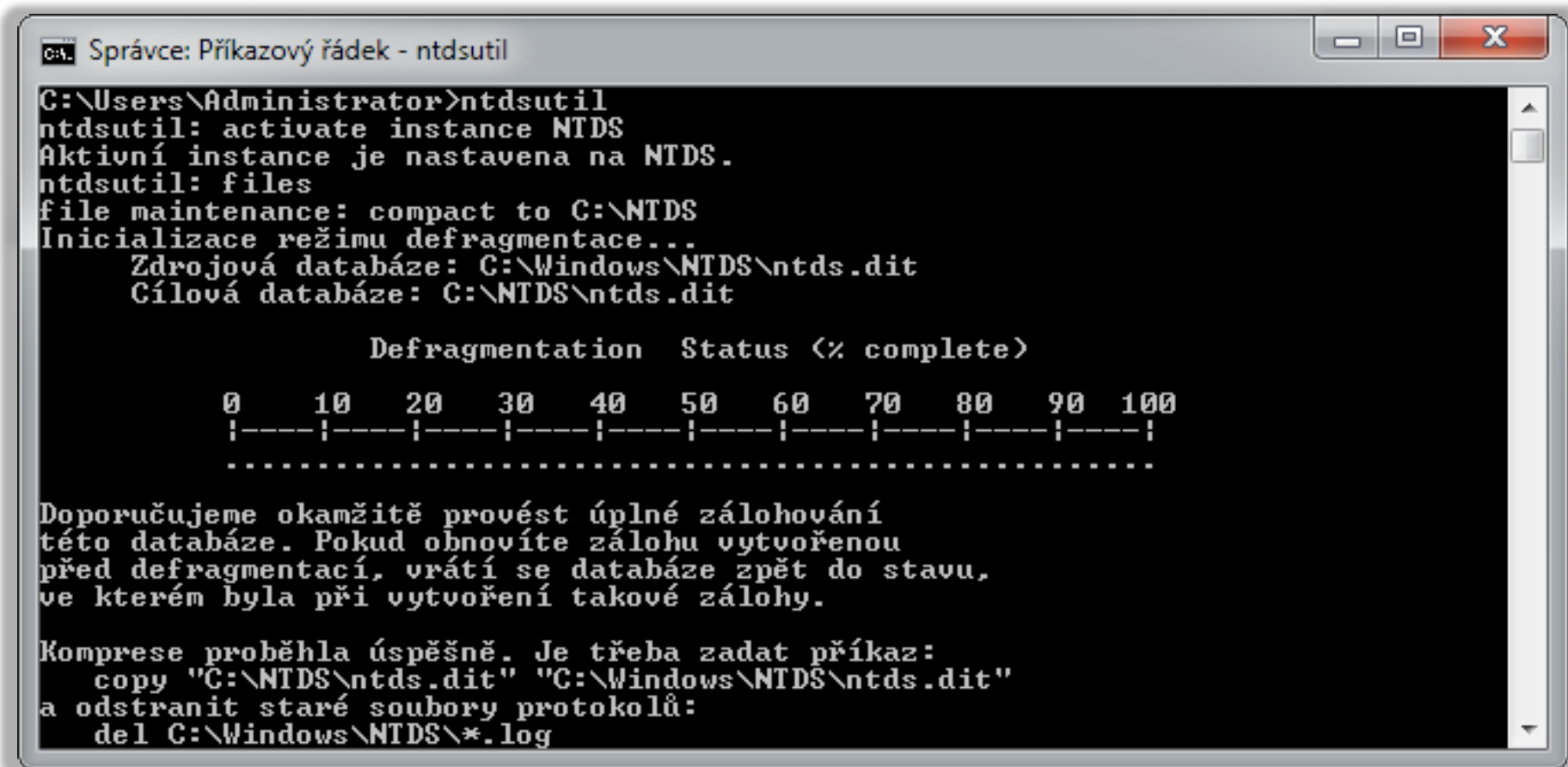
- Role řadiče domény standardní služba systému
 - Může být zastavena, spuštěna nebo restartována
 - Dříve monolitická role
 - Zastavení role vyžadovalo zastavit celý řadič domény
- Vyžaduje zastavení doménových služeb (AD DS)
 - Jdou zastavit pouze pokud je v síti jiný řadič domény
- Proces zkompaktnění databáze Active Directory
 - Defragmentace databáze
 - Minimalizace databáze

Zkompaktnění (*compaction*) databáze

- Vliv operací přidávání a mazání na databázi AD
 - Při přidávání nových objektů dochází k alokaci místa pro jejich uložení (většinou na konci databáze)
 - Při mazání objektů není alokované místo uvolněno
- Automatická údržba Active Directory
 - Přesun objektů do neuvolněných (prázdných) míst
- Zkompaktnění databáze Active Directory
 - Přesun dat na začátek databáze (souboru **Ntds.dit**)
 - Ořezání konce databáze (souboru **Ntds.dit**)

Provedení zkompaktnění databáze

- Pomocí nástroje **ntdsutil** (příkaz **compact**)



```
ca: Správce: Příkazový řádek - ntdsutil
C:\Users\Administrator>ntdsutil
ntdsutil: activate instance NTDS
Aktivní instance je nastavena na NTDS.
ntdsutil: files
file maintenance: compact to C:\NTDS
Inicializace režimu defragmentace...
Zdrojová databáze: C:\Windows\NTDS\ntds.dit
Cílová databáze: C:\NTDS\ntds.dit

          Defragmentation Status (<% complete>)
0         10        20        30        40        50        60        70        80        90        100
|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
.....

Doporučujeme okamžitě provést úplné zálohování
této databáze. Pokud obnovíte zálohu vytvořenou
před defragmentací, vrátí se databáze zpět do stavu,
ve kterém byla při vytvoření takové zálohy.

Kompresa proběhla úspěšně. Je třeba zadat příkaz:
copy "C:\NTDS\ntds.dit" "C:\Windows\NTDS\ntds.dit"
a odstranit staré soubory protokolů:
del C:\Windows\NTDS\*.log
```

Ochrana Active Directory

- Primárně se týká ochrany dat (objektů AD)
 - Nejdůležitější ochrana identit
- Možnosti ochrany Active Directory
 - Ochrana objektů před smazáním
 - Auditování změn
 - Obnova objektů
 - Záloha a obnova databáze

Ochrana objektů před smazáním

- Každý objekt Active Directory může být chráněn proti (nechtěnému) smazání
 - Chráněný objekt nemůže být smazán ani přesunut
- Všechny kontejnery jsou po vytvoření chráněny
 - Ochrana interní struktury databáze Active Directory
- Povolení
 - Ve vlastnostech každého objektu (záložka **Objekt**)
 - Odepřením oprávnění **Delete** a **Delete subtree** pro skupinu **Everyone**

Povolení ochrany před smazáním

The image shows the Active Directory console window titled 'Uživatelé a počítače služby Active Directory'. The left pane shows the tree structure with 'Domain Controllers' selected. The right pane shows the 'Vlastnosti' (Properties) dialog box for the 'Domain Controllers' object. The 'Zabezpečení' (Security) tab is active, showing the 'Obecné' (General) section. The 'Chránit objekt před náhodným odstraněním' (Protect object from accidental deletion) checkbox is checked and circled in blue. A blue arrow points from the 'Vlastnosti' option in the console to the dialog box.

Uživatelé a počítače služby Active Directory

Soubor Akce Zobrazit Nápověda

Uživatelé a počítače služby Active Directory

Uložené dotazy

testing.local

Builtin

Computers

Domain Controllers

Delegovat řízení...

Předem vytvořit účet řadiče domény jen pro čtení...

Najít...

Nová položka

Všechny úkoly

Aktualizovat

Vlastnosti

Nápověda

Otevře dialog vlastností pro aktuální výběr.

Domain Controllers – vlastnosti

Zabezpečení	Model COM+	Editor atributů
Obecné	Správce objektu	Objekt

Kanonický název objektu:
testing.local/Domain Controllers

Třída objektu: Organizační jednotka

Vytvořeno: 21.2.2010 14:07:54

Změněno: 21.2.2010 14:07:54

Čísla pořadí aktualizace (USNs):

Aktuální: 5828

Původní: 5828

Chránit objekt před náhodným odstraněním

OK Storno Použít Nápověda

Auditování změn

- Zaznamenávání přístupů k adresářovým službám
 - Zaznamenávání do **protokolu událostí adresářových služeb** (*Directory Services Event Log*)
 - Celkem 4 kategorie přístupů, z hlediska ochrany dat nejdůležitější auditování **změn v Active Directory**
 - **Změny v Active Directory** (*Directory Service Changes*)
 - Zaznamenávání starých a nových hodnot atributů objektů, které byly vytvořeny, změněny, přesunuty nebo obnoveny
 - Každá změna produkuje 2 události (první obsahuje starou hodnotu atributu a druhá novou)
 - Lze použít pro opravu chybně změněných hodnot atributů

Povolení auditování změn

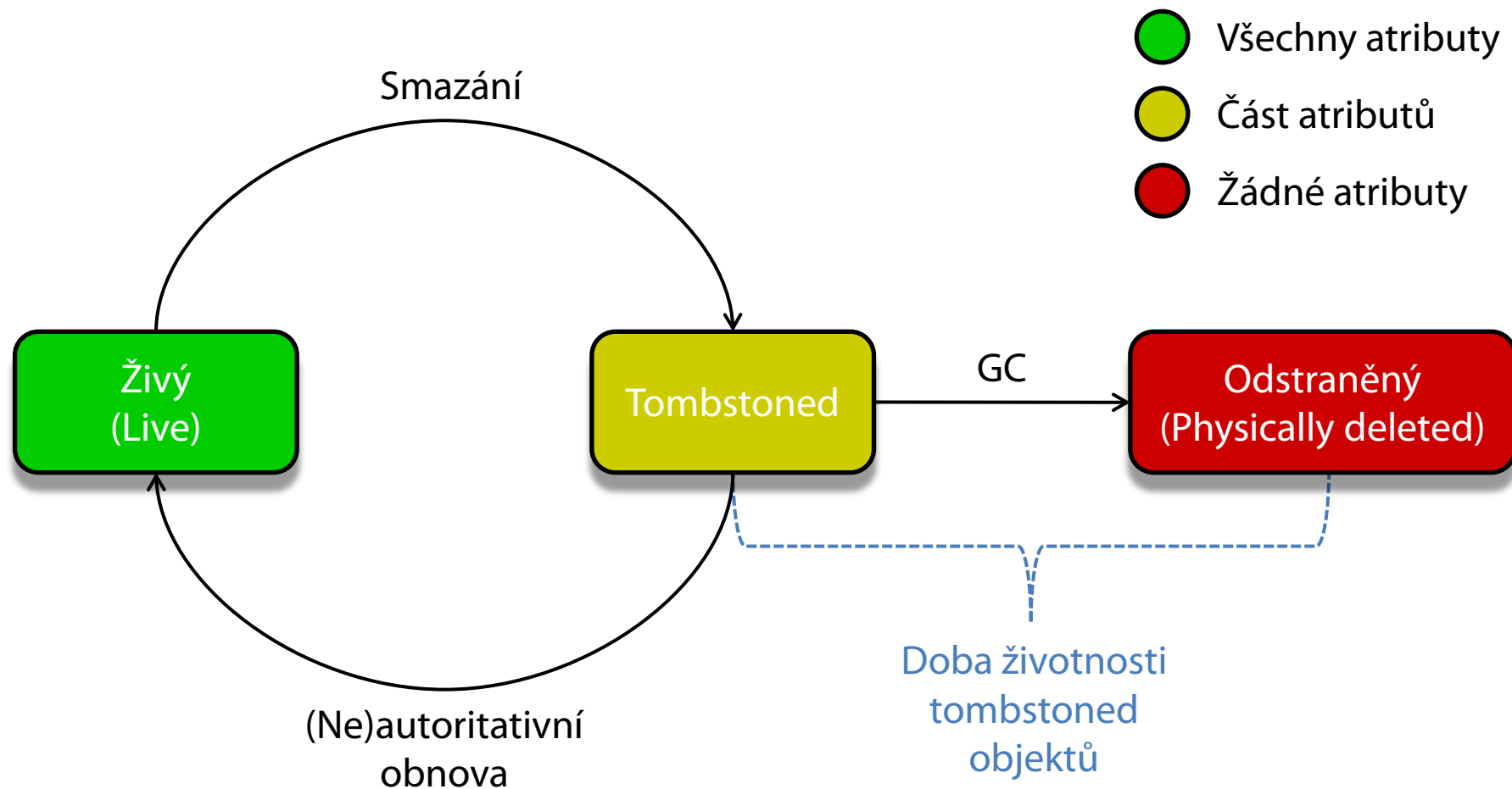
The screenshot shows the Group Policy Editor window. The left pane displays a tree view of policy categories, with 'Upřesnit konfiguraci zásad auditování' expanded to show 'Zásady auditování'. Under 'Zásady auditování', 'Přístup k adresářové službě' is selected. The right pane shows a table of audit events for this category.

Podkategorie	Události auditování
Auditovat podrobnou replikaci adresářové služby	Není nakonfigurováno
Auditovat přístup k adresářové službě	Není nakonfigurováno
Auditovat změny adresářové služby	Úspěchy a chyby
Auditovat replikaci adresářové služby	Není nakonfigurováno

Obnova objektů

- Tombstoned objekty
 - Smazané, ale ne odstraněné objekty
 - Uloženy ve skrytém kontejneru **Deleted Objects**
 - Od původních se liší nastaveným atributem **isDeleted**
 - Ve výchozím nastavení uchovávány po dobu 180 dní
- Obnova např. pomocí nástroje **Ldp.exe**
 - Identity si zachovávají původní SID identifikátor
- Obnovou mohou být ztraceny některé informace
 - Např. nemusí být obnoveno členství ve skupinách

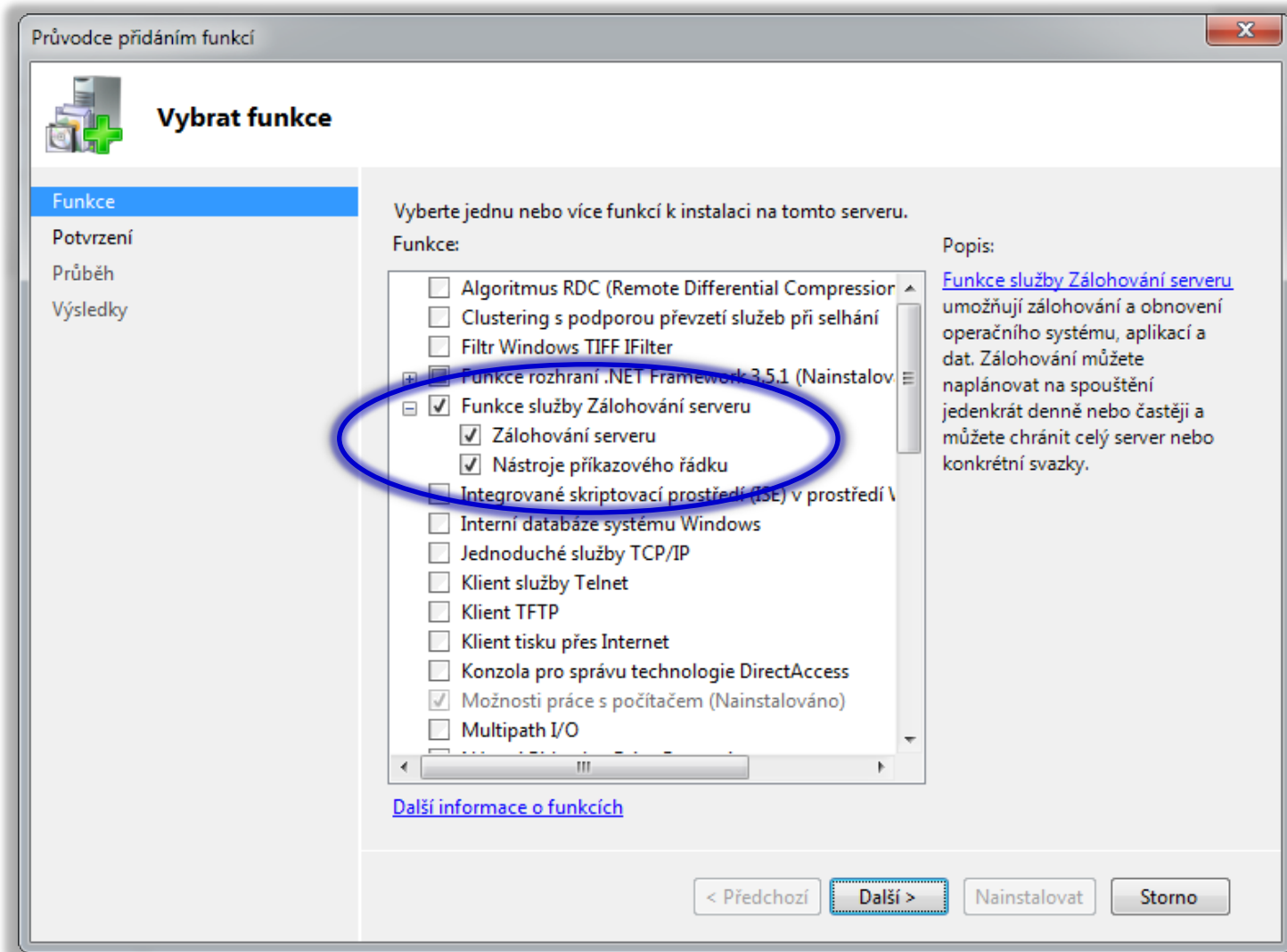
Životní cyklus objektů



Záloha a obnova databáze

- Potřeba přidat **Funkce služby Zálohování serveru**
 - Zahrnuje všechny potřebné nástroje pro zálohování a obnovu databáze Active Directory (i celého serveru)
- Hlavní nástroje pro zálohování a obnovu
 - **Zálohování serveru** (*Windows Server Backup*)
 - **Wbadmin.exe** (*Windows Backup Administration*)

Funkce služby Zálohování serveru



Záloha databáze Active Directory

- Automatické zálohování
 - Zálohování v pravidelných intervalech
 - Mohou nastavovat a provádět pouze správci (členové **Administrators**, u řadičů členové **Domain Admins**)
- Manuální zálohování
 - Mohou provádět i členové **Backup Operators**

Typy záloh

- Záloha celého serveru (*Full Server Backup*)
 - Zálohování veškerých dat všech oddílů disků daného serveru (řadiče domény)
- Záloha kritických oddílů (*Critical Volume Backup*)
- Vlastní záloha (*Custom Backup*)

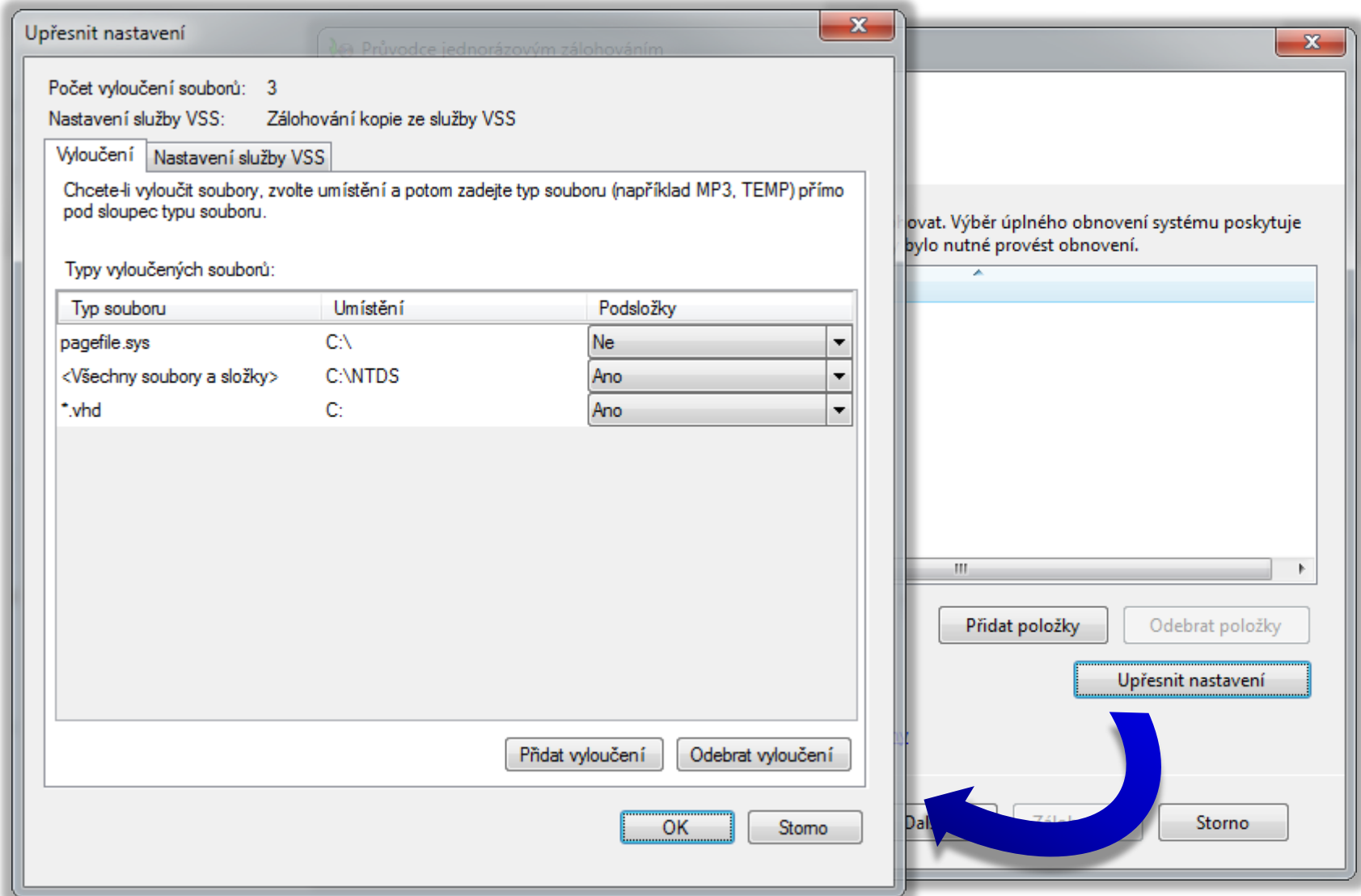
Záloha kritických oddílů

- Obsahuje veškerá data potřebná pro obnovu doménových služeb Active Directory (AD DS)
- Zahrnuje data
 - Bootovacího a systémového oddílu
 - Oddílu, který obsahuje databázi Active Directory
 - Oddílu, který obsahuje protokoly Active Directory
 - Oddílu, který obsahuje adresář SYSVOL
- Pouze u **Windows Server 2008**
 - U **Windows Server 2008 R2** lze použít vlastní zálohu

Vlastní záloha

- Zálohování pouze vybraných souborů a adresářů
 - Lze zahrnout i stav systému a/nebo kritické oddíly
- Možnost vyloučení konkrétních (typů) souborů
 - Specifikace cesty a/nebo přípony souborů, jenž mají být vyloučeny ze zálohy
- Pouze u **Windows Server 2008 R2**

Vyloučení vybraných (typů) souborů



Možnosti umístění (uložení) záloh

- Nelze zálohovat na USB Flash disky
- U **Windows Server 2008**
 - Síťové (*network*) a odnímatelné (*removable*) disky
 - CD a DVD média
- U **Windows Server 2008 R2** navíc také
 - Interní disky (oddíly neobsahující zálohovaná data)
 - Sdílené adresáře (udržována jediná verze zálohy)
 - Před každým zálohováním je stará záloha smazána
 - Virtuální a dynamické disky

Zálohování u Windows Server 2008 R2

- Inkrementální zálohy se chovají jako úplné
 - Všechna data lze obnovit z jediné zálohy
- Automatické mazání starých záloh
 - Uživatel nemusí mazat zálohy při nedostatku místa
- Rozšířená podpora nástrojů
 - **Wbadmin.exe** poskytuje stejné možnosti jako nástroj **Zálohování serveru** (vše lze naskriptovat)
 - Nové příkazy (*cmdlety*) pro Windows PowerShell
 - **Start-WBBackup** pro spuštění zálohování, **Set-WBPolicy** pro výběr položek, **Get-WBBackupSet** pro zjištění záloh

Záloha stavu systému

- Stav systému (*System State*)
 - Sada dat potřebná pro chod systému Windows a pro plnění některých rolí
- Obsahuje bootovací a systémové soubory, registr a databázi registrovaných COM+ tříd
- V případě řadiče domény zahrnuje navíc
 - Databázi AD (soubor **Ntds.dit**) a adresář SYSVOL
- V případě jiných rolí může zahrnovat například
 - Databázi AD CS, konfigurační soubory IIS, ...

Zálohování stavu systému

- Windows Server 2008
 - Pouze pomocí nástroje **Wbadmin.exe**
 - **Wbadmin { start | delete } systemstatebackup**
- Windows Server 2008 R2
 - Lze použít i **Zálohování serveru**
 - Možnost přidat ke stavu systému i další data
 - Podpora inkrementálního zálohování (stavu systému)
 - Využívá stínové kopie (*shadow copies*) pro verzování

Připojení databáze Active Directory

- Umožňuje zobrazit obsah zálohy databáze Active Directory před provedením obnovy
 - Možnost ověření, zda záloha obsahuje objekty, které je potřeba obnovit
- Sada nástrojů AD DS Database mounting tool
 - **ntdsutil (snapshot mount)** pro připojení snímku (zálohy) obsahujícího databázi Active Directory
 - **dsamain** pro vytvoření a spuštění LDAP serveru obsahujícího databázi z připojeného snímku
 - Konzole (ADUC, ...) pro připojení k LDAP serveru

Připojení zálohované databáze AD

- Pomocí nástrojů **ntdsutil** a **dsamain**

C:\> Správce: Příkazový řádek - ntdsutil

```
Microsoft Windows [Verze 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. Všechna práva vyhrazena.

C:\Users\Administrator>ntdsutil
ntdsutil: snapshot
snímek: list all
 1: 2011/04/10:22:11 <f90ac439-4601-430e-b1e8-aa3dd277687d>
 2: C: <1d074ff8-5986-4b15-af06-3313cddb4a4c>

snímek: mount 1
Snímek <1d074ff8-5986-4b15-af06-3313cddb4a4c> byl připojen jako C:\$SNAP_201104102211_VOLUMEC$\
snímek: _
```

C:\> Správce: Příkazový řádek - dsamain -dbpath C:\\$SNAP_201104102211_VOLUMEC\$\Windows\NTD...

```
C:\Users\Administrator>dsamain -dbpath C:\$SNAP_201104102211_VOLUMEC$\Windows\NTD
DS\ntds.dit -ldapport 55000
EVENTLOG (Informational): NTDS General / Řízení služby : 1000
Spuštění služby Microsoft Active Directory Domain Services dokončeno, verze 6.1.
7600.16385
```

Obnova databáze Active Directory

- Režim obnovení adresářových služeb
(DSRM, *Directory Services Restore Mode*)
 - Umožňuje obnovu pouze databáze Active Directory
 - Přístupný v pokročilých možnostech bootování (**F8**)
 - Vyžaduje heslo pro DSRM režim (zadáno při instalaci)
- Prostředí pro obnovu systému Windows
(WinRE, *Windows Recovery Environment*)
 - Umožňuje obnovu celého systému (včetně databáze)
 - Součást instalačního média (lze nainstalovat lokálně)

Typy obnovy databáze AD

- **Autoritativní obnova**
 - Při připojení řadiče domény do sítě aktualizuje tento řadič data na všech ostatních řadičích domény
 - Použití pro opravu chyb v databázi Active Directory
- **Neautoritativní obnova**
 - Při připojení řadiče domény do sítě budou jeho data aktualizována replikací z ostatních řadičů domény
 - Použití při obnově řadičů domény pro snížení zátěže sítě (snížení objemu dat, jenž musí být replikována)

Instalace z média (*Install From Media*)

- Speciální kopie databáze Active Directory, která může být použita při instalaci řadiče domény
 - Alternativní zdroj dat (namísto replikace)
 - Snížení množství replikovaných dat při instalaci
- Vytvoření média IFM pomocí **ntdsutil (ifm)**

Příkaz	Popis
Create Full	Vytvoří médium IFM pro úplný řadič domény
Create RODC	Vytvoří médium IFM pro RODC řadič
Create SYSVOL Full	Vytvoří médium IFM s oddílem SYSVOL pro úplný řadič domény
Create SYSVOL RODC	Vytvoří médium IFM s oddílem SYSVOL pro RODC řadič

Ochrana řadičů domény virtualizací

- Jednoduché zálohování
 - Zachycení (*capture*) snímku virtuálního stroje
 - Zálohování disku (VHD souboru) virtuálního stroje
 - Lze využít službu VSS (*Volume Shadow Copy Service*)
 - Možnost vytváření záloh v pravidelných intervalech
 - Nevyžaduje zastavení virtuálního stroje
- Rychlá obnova
 - Obnovení dříve zachyceného snímku
 - Obnovení předchozí verze VHD souboru
 - Při použití služby VSS přes záložku **Předchozí verze**

Active Directory koš (*recycle bin*)

- Umožňuje obnovit smazané objekty AD do stavu ve kterém byly těsně přes svým smazáním
 - Neplatí pro GPO objekty a Exchange objekty
- Povolení pomocí **Enable-ADOptionalFeature**
 - Vyžaduje funkční úroveň lesa [Windows Server 2008 R2](#) a aktualizované schéma Active Directory
 - Nevratný proces (po povolení nelze již zpět zakázat)
- Lze použít i pro adresářové služby AD (AD LDS)
 - Nutná aktualizace konfigurace pomocí **Ldifde.exe**

Obnova objektů Active Directory

- Obnovují se přímé i nepřímé atributy
- Přímé (*non-link-valued*) atributy
 - Atributy uložené přímo v objektech
- Nepřímé (*link-valued*) atributy
 - Atributy, jenž se vážou k objektům, ale nejsou v nich přímo uloženy (např. členství ve skupinách)
- Obnovení objektů Active Directory
 - Pomocí **Ldp.exe** (jako u obnovy tombstoned objektů)
 - Pomocí PowerShell příkazu **Restore-ADObject**

Rozlišované typy objektů (1)

- Živý objekt (*Live Object*)
 - Nesmazaný objekt Active Directory
- Smazaný objekt (*Deleted Object*)
 - Živý objekt, který byl smazán
 - Je přesunut do kontejneru **Deleted Objects** na dobu životnosti smazaných objektů (standardně 180 dnů)
 - Má zachovány všechny přímé i nepřímé atributy
 - Lze obnovit (autoritativně i neautoritativně)

Rozlišované typy objektů (2)

- Recyklovaný objekt (*Recycled Object*)
 - Smazaný objekt po vypršení jeho doby životnosti
 - Zůstává umístěn v kontejneru **Delete Objects** na dobu životnosti recyklovaných objektů (180 dní)
 - Většina atributů je odstraněna
 - Které mají být ponechány lze specifikovat ve schématu AD
 - Není viditelný, ale pořád lze obnovit
- Odstraněný objekt (*Physically Deleted Object*)
 - Objekt fyzicky smazaný z databáze Active Directory
 - Odstraňuje pravidelně GC (*Garbage Collector*)

Životní cyklus objektů (s AD košem)

