

Serverové systémy Microsoft Windows

IW2/XMW2 2015/2016

Jan Fiedor

ifiedor@fit.vutbr.cz

Fakulta Informačních Technologií

Vysoké Učení Technické v Brně

Božetěchova 2, 612 66 Brno

Revize 18. 4. 2016

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

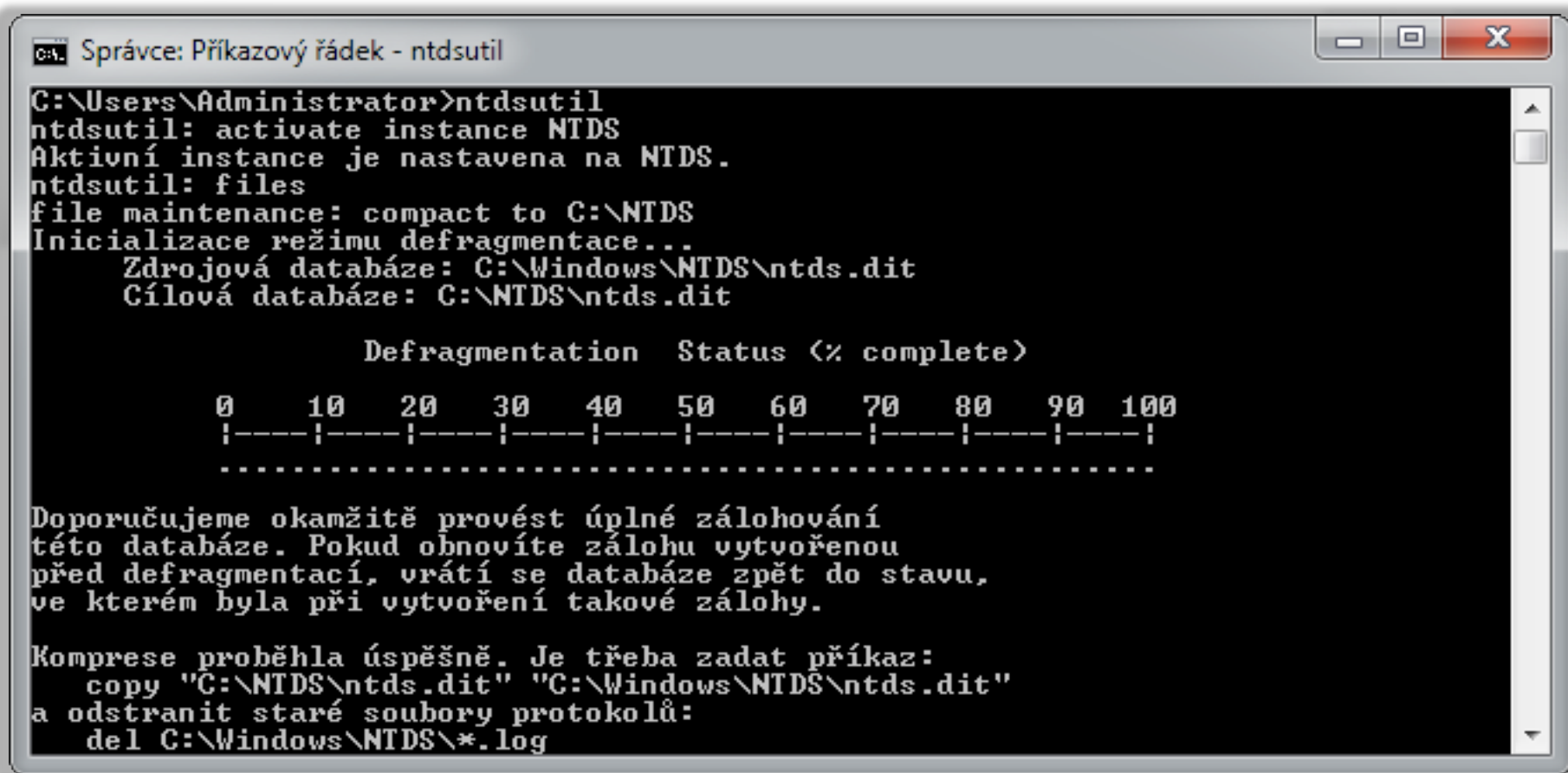
- Role řadiče domény **standardní služba** systému
 - Může být zastavena, spuštěna nebo restartována
 - Před **Windows Server 2008** monolitická role
 - Zastavení role vyžadovalo zastavit celý řadič domény
- Vyžaduje zastavení **doménových služeb** (AD DS)
 - Jdou zastavit pouze pokud je v síti jiný 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.

Komprese 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 a Windows Active Directory console window titled "Uživatelé a počítače" (Users and Computers). The left pane shows the tree structure: "Uživatelé a počítače služby Active Directory" > "Uložené dotazy" > "testing.local" > "Domain Controllers". The right pane shows a table with columns "Název" and "Typ", containing one entry: "WSRV2012" with type "Počítač". A context menu is open over the "Domain Controllers" folder, with "Vlastnosti" (Properties) selected. A blue arrow points from this menu item to the "Domain Controllers - vlastnosti" dialog box.

The "Domain Controllers - vlastnosti" dialog box has the "Správce objektu" (Object Manager) tab selected. It displays the following information:

- Kanónický název objektu: testing.local/Domain Controllers
- Třída objektu: Organizační jednotka
- Vytvořeno: 24. 2. 2013 21:35:52
- Změněno: 24. 2. 2013 21:35:52
- Čísla pořadí aktualizace (USNs):
 - Aktuální: 5944
 - Původní: 5944

The checkbox "Chránit objekt před náhodným odstraněním" (Protect object from accidental deletion) is checked and highlighted with a blue box.

Auditování změn

- **Zaznamenávání přístupů** k adresářovým službám
 - Informace o zaznamenaných přístupech se ukládají do systémového protokolu **Zabezpečení** (*security*)
 - Celkem 4 kategorie přístupů, z hlediska ochrany dat nejdůležitější auditování **změn adresářové služby**
 - **Změny adresářové služby** (*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

Editor správy zásad skupiny

Soubor Akce Zobrazit Nápověda

← → ↗ ↘ ? ▶

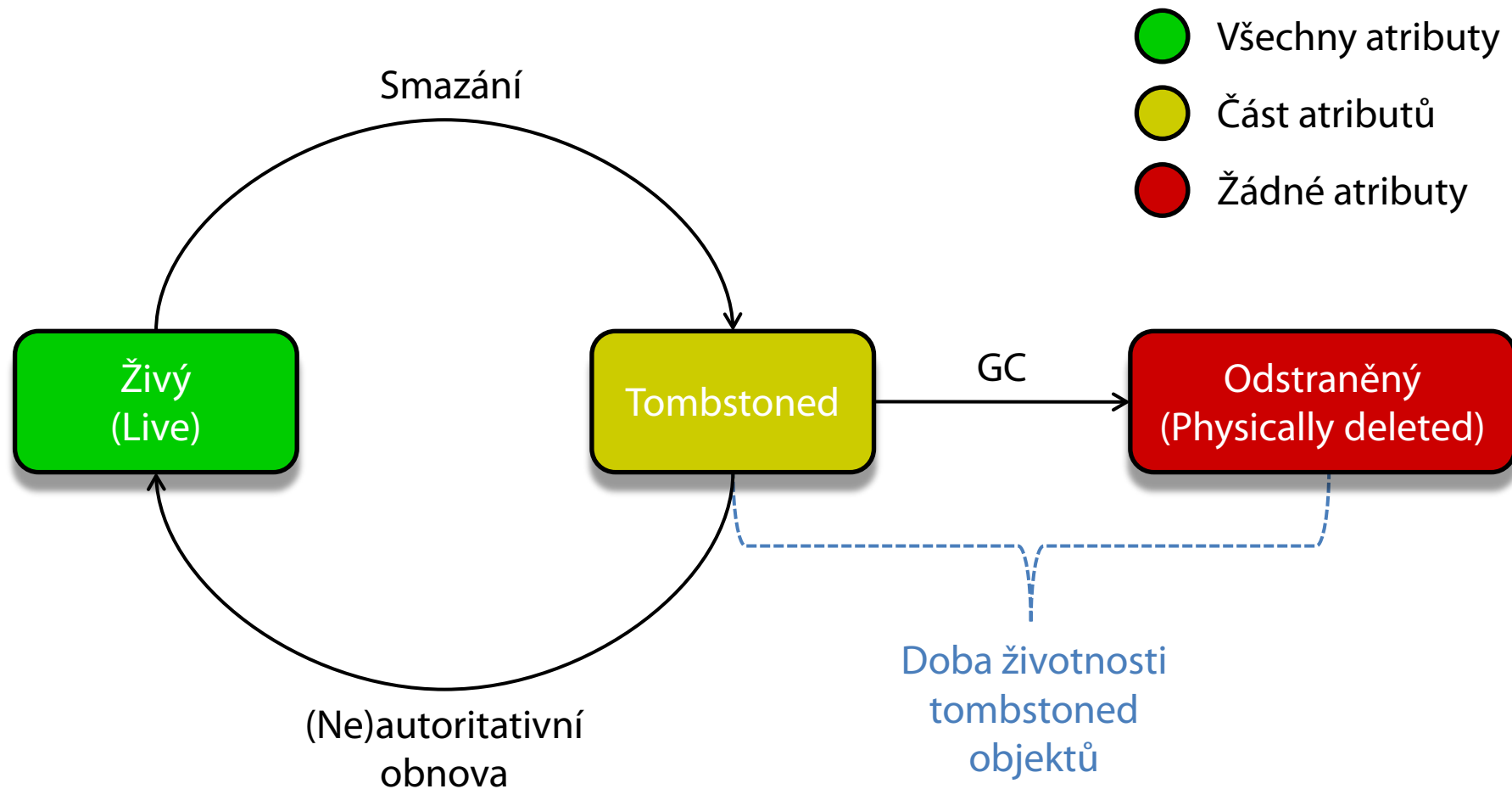
- ▶ Zásady veřejných klíčů
- ▶ Zásady omezení softwaru
- ▶ Architektura NAP (Network Access Protection)
- ▶ Zásady řízení aplikací
- ▶ Zásady zabezpečení protokolu IP - Active Directory
- ▶ **Upřesnit konfiguraci zásad auditování**
 - ▶ **Zásady auditování**
 - ▶ Přihlášení k účtu
 - ▶ Správa účtů
 - ▶ Podrobné sledování
 - ▶ **Přístup k adresářové službě**
 - ▶ Přihlášení či odhlášení
 - ▶ Přístup k objektu
 - ▶ Změna zásady
 - ▶ Oprávněnost použití
 - ▶ Systém
 - ▶ Globální auditování přístupu k objektům
- ▶ Technologie QoS spravovaná pomocí zásad

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

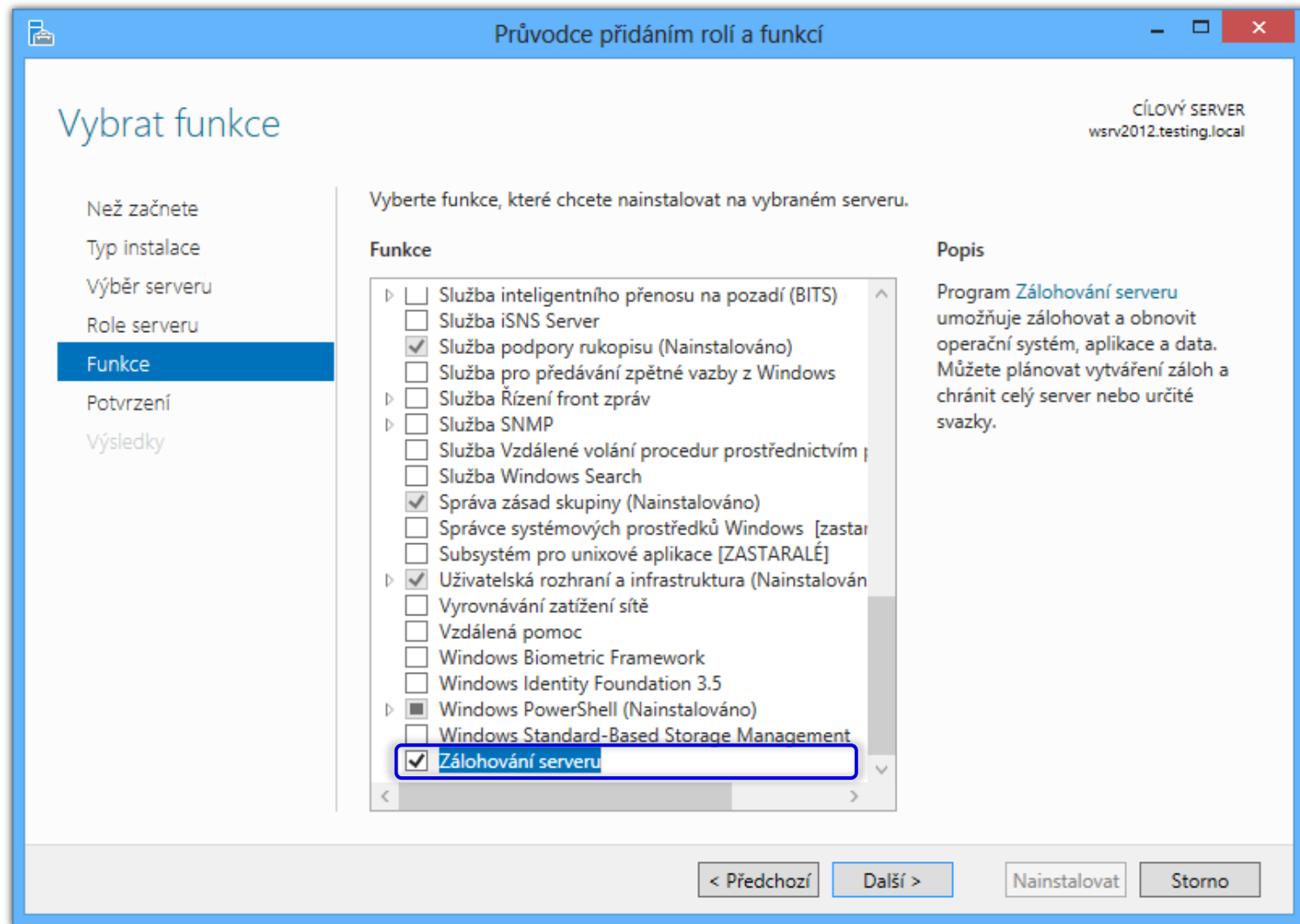
Životní cyklus objektů



Záloha a obnova databáze

- Provádí se **standardními nástroji** pro zálohování
 - Mohou provádět **správci** počítače (u řadičů členové **Domain Admins**) nebo členové **Backup Operators**
 - K dispozici po instalaci funkce **Zálohování serveru**
 - Databáze Active Directory je součástí **Stavu systému**
- **Nástroje** pro zálohování a obnovu **Stavu systému**
 - **Zálohování serveru** (*Windows Server Backup*)
 - **Wbadmin.exe** (*Windows Backup Administration*)
 - Nástroje pro **Windows PowerShell** (*cmdlety*)

Přidání funkce Zálohování serveru



Stav systému (*system state*)

- Sada dat potřebná pro **běh serveru** a pro **plnění** nainstalovaných **rolí**
- Zahrnuje
 - Bootovací a systémové soubory
 - Registr a databázi registrovaných COM+ tříd
 - V případě řadiče domény zahrnuje navíc
 - Databázi AD (soubor **Ntds.dit**), **protokoly** a adresář **SYSVOL**
 - V případě jiných rolí může zahrnovat například
 - Databázi certifikátů AD CS, konfigurační soubory IIS, ...

Záloha databáze Active Directory

- Pomocí nástroje **Zálohování serveru**
 - Automatické zálohování v pravidelných intervalech
 - Manuální (jednorázové) zálohování
- Pomocí nástroje **Wbadmin.exe**
 - **Wbadmin { start | delete } systemstatebackup**
- Pomocí nástrojů pro **Windows PowerShell**
 - 1) Vytvoření konfigurace zálohování (**New-WBPolicy**)
 - 2) Přidání stavu systému (**Add-WBSystemState**)
 - 3) Spuštění zálohování (**Start-WBBackup**)

Typy konfigurací zálohování

- Záloha celého serveru (*full server backup*)
 - Zálohování **všech oddílů** disků daného serveru
 - Zahrnuje také **Stav systému**
- Vlastní záloha (*custom backup*)
 - Zálohování vybraných **souborů** a **adresářů**
 - Lze zahrnout **Stav systému** nebo **Úplné obnovení systému** (*bare metal recovery*, obsahuje **oddíly** disku potřebné pro **běh serveru**, tedy oddíly obsahující data **Stavu systému**)
 - Možnost **vyloučení** konkrétních (typů) souborů
 - Specifikace na základě cesty a/nebo přípony souborů

Vyloučení vybraných (typů) souborů

Upřesnit nastavení

Počet vyloučení souborů: 3
Nastavení služby VSS: Zálohování kopie ze služby VSS

Vyloučení **Nastavení služby VSS**

Chcete-li vyloučit soubory, zvolte umístění a potom zadejte typ souboru (například MP3, TEMP) přímo pod sloupec typu souboru.

Typy vyloučených souborů:

Typ souboru	Umístění	Podsloužky
pagefile.sys	C:\	Ne
<Všechny soubory a složky>	C:\NTDS	Ano
*.vhd	C:	Ano

Přidat vyloučení Odebrat vyloučení

OK Storno

Zálohování

ovát. Výběr úplného obnovení systému poskytuje bylo nutné provést obnovení.

Přidat položky Odebrat položky

Upřesnit nastavení

Storno

Možnosti umístění (uložení) záloh

- Optická média (CD, DVD, BD)
 - Zálohy ukládány v **komprimované** formě
- Disky (musí obsahovat souborový systém **NTFS**)
 - Interní disky (oddíly **neobsahující** zálohovaná data)
 - Síťové (*network*) a odnímatelné (*removable*) disky
- Sdílené adresáře (udržována **jediná verze** zálohy)
 - Před každým zálohováním je stará záloha **smazána**
- Virtuální a dynamické disky, **prostory úložišť**
 - Nemusí být podporovány všemi nástroji pro obnovu

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$\.
```

```
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

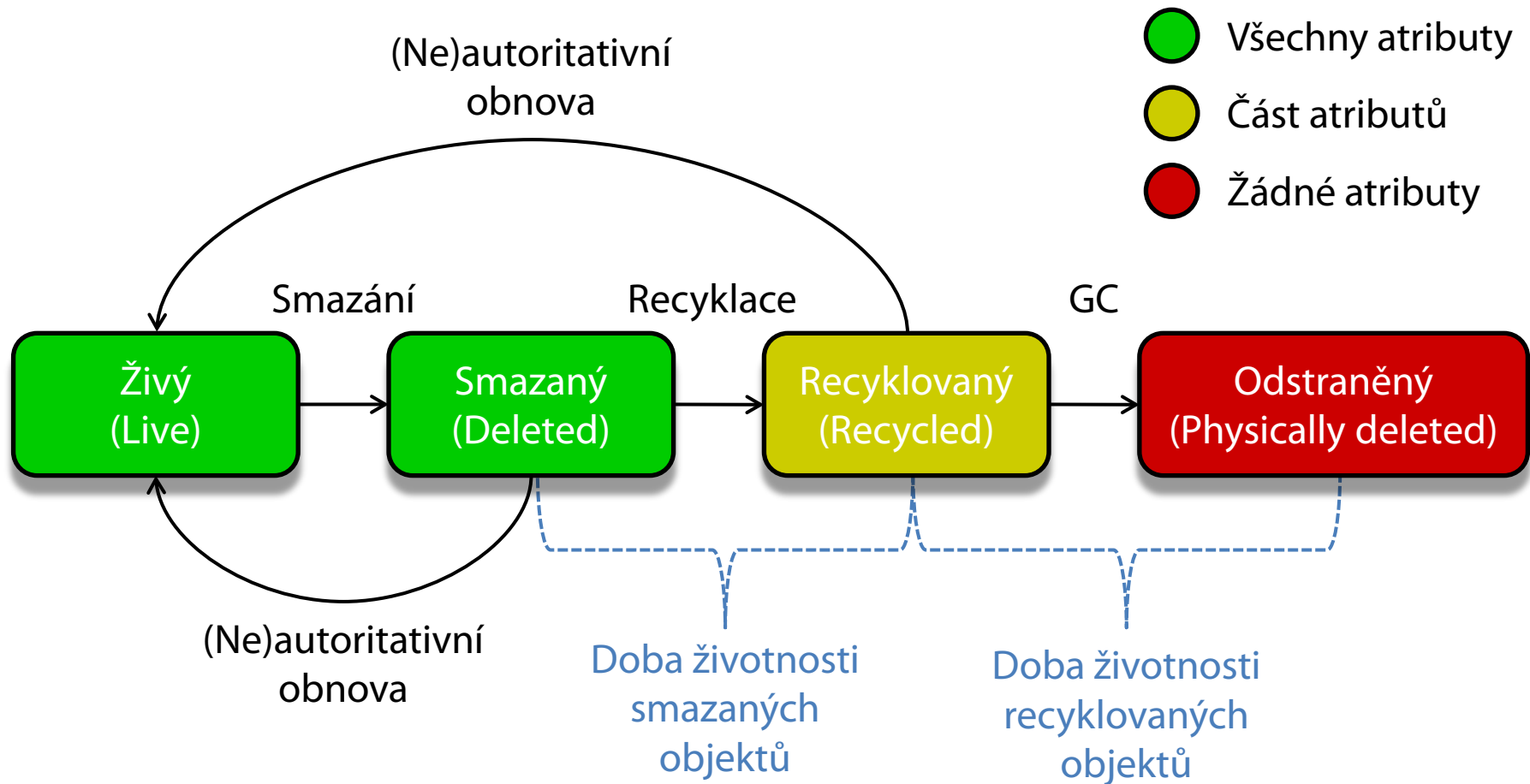
Active Directory koš (*recycle bin*)

- Umožňuje **obnovit** smazané objekty AD do stavu ve kterém byly těsně **před** svým **smazáním**
 - Neplatí pro GPO objekty a Exchange objekty
- **Povolení** v konzoli **Centrum správy služby Active Directory**, příkazem **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** (členství ve skupinách, oprávnění, ...)
- Obnovení objektů Active Directory
 - Pomocí **Centra správy služby Active Directory**
 - Pomocí PowerShell příkazu **Restore-ADObject**

Životní cyklus objektů (s AD košem)



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*)