

Desktop systémy Microsoft Windows

IW1/XMW1 2011/2012

Jan Fiedor

ifiedor@fit.vutbr.cz

Fakulta Informačních Technologií

Vysoké Učení Technické v Brně

Božetěchova 2, 612 66 Brno

Revize 4.12.2011

Zálohování a obnova dat

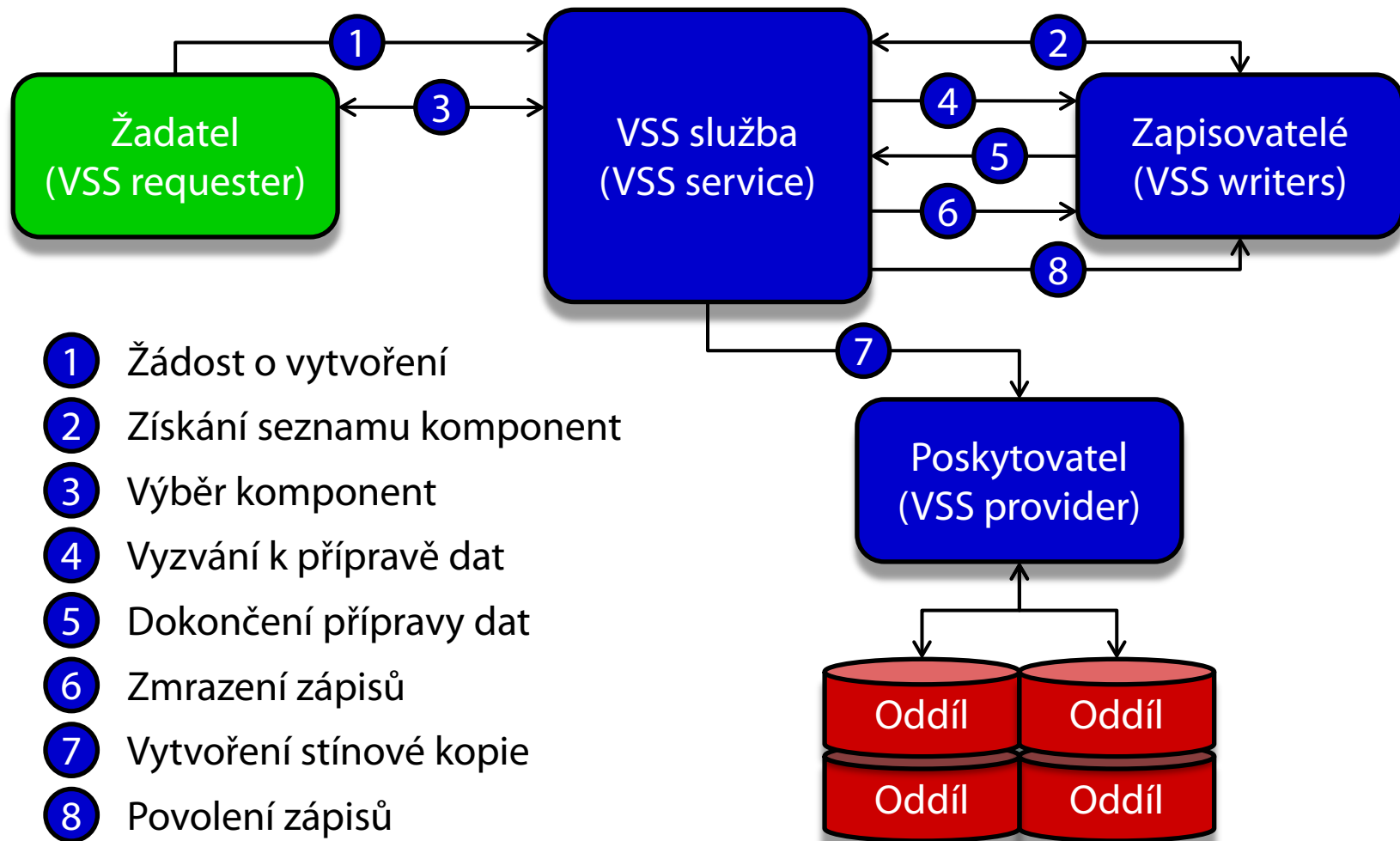
Stínové kopie (Shadow Copies)

- Konzistentní záznamy dat určitých oddílů disků v konkrétních časech (tzv. *point-in-time* kopie dat)
 - Ukládány inkrementálně
- Vytvářeny službou Stínová kopie svazku (*Volume Shadow Copy Service, VSS*)
 - Při vytváření bodů obnovení
 - Při zálohování vybraných adresářů
- Pro uchování vyžadují souborový systém NTFS
 - U jiných souborových systémů vytvořeny jen dočasně

Možnosti a omezení

- Určeny pouze pro čtení (nelze upravovat obsah)
- Každý oddíl disku může obsahovat maximálně 64 stínových kopií
 - Při dosažení limitu je nejstarší stínová kopie smazána
 - Počet uchovaných verzí souborů může být menší
- Povolovány na úrovni oddílů disků
 - Nelze povolit pro konkrétní soubory nebo adresáře
- Nejsou pořizovány stínové kopie souborů offline
- Lze explicitně vyloučit některé soubory a složky

Ilustrace vytváření stínových kopií



Postup vytváření stínových kopií

- 1) Žadatel požádá VSS službu o vytvoření stínové kopie
- 2) VSS služba získá od zapisovatelů seznam všech komponent a datových úložišť, jenž mohou být zachycena do stínové kopie
- 3) Žadatel vybere komponenty, jenž mají být zachyceny
- 4) VSS služba vyzve všechny zapisovatele, aby připravili svá data pro zachycení do stínové kopie
- 5) Zapisovatelé oznámí VSS službě dokončení přípravy svých dat
- 6) VSS služba nechá zapisovatele zmrazit požadavky na zápis (na maximálně 60 sekund), vyprázdní vyrovnávací paměti a úplně zmrazí celý souborový systém (pro zajištění konzistence)
- 7) Poskytovatel vytvoří stínovou kopii (za maximálně 10 sekund)
- 8) VSS služba povolí opětovné zpracování požadavků na zápis

Poskytovatelé (Providers)

- Realizují vytváření stínových kopií a jejich správu
- Dva druhy poskytovatelů
 - Hardwaroví (vytváření a správa všech stínových kopií je zajišťována fyzickým úložištěm dat)
 - Softwaroví (vytváření a správu stínových kopií má na starosti speciální ovladač a sada knihoven)
- Systémový poskytovatel (*System Provider*)
 - Softwarový poskytovatel obsažený ve Windows 7
 - Využívá copy-on-write metodu pro vytváření kopií
 - Skládá se z ovladače **volsnap.sys** a knihovny **swprv.dll**

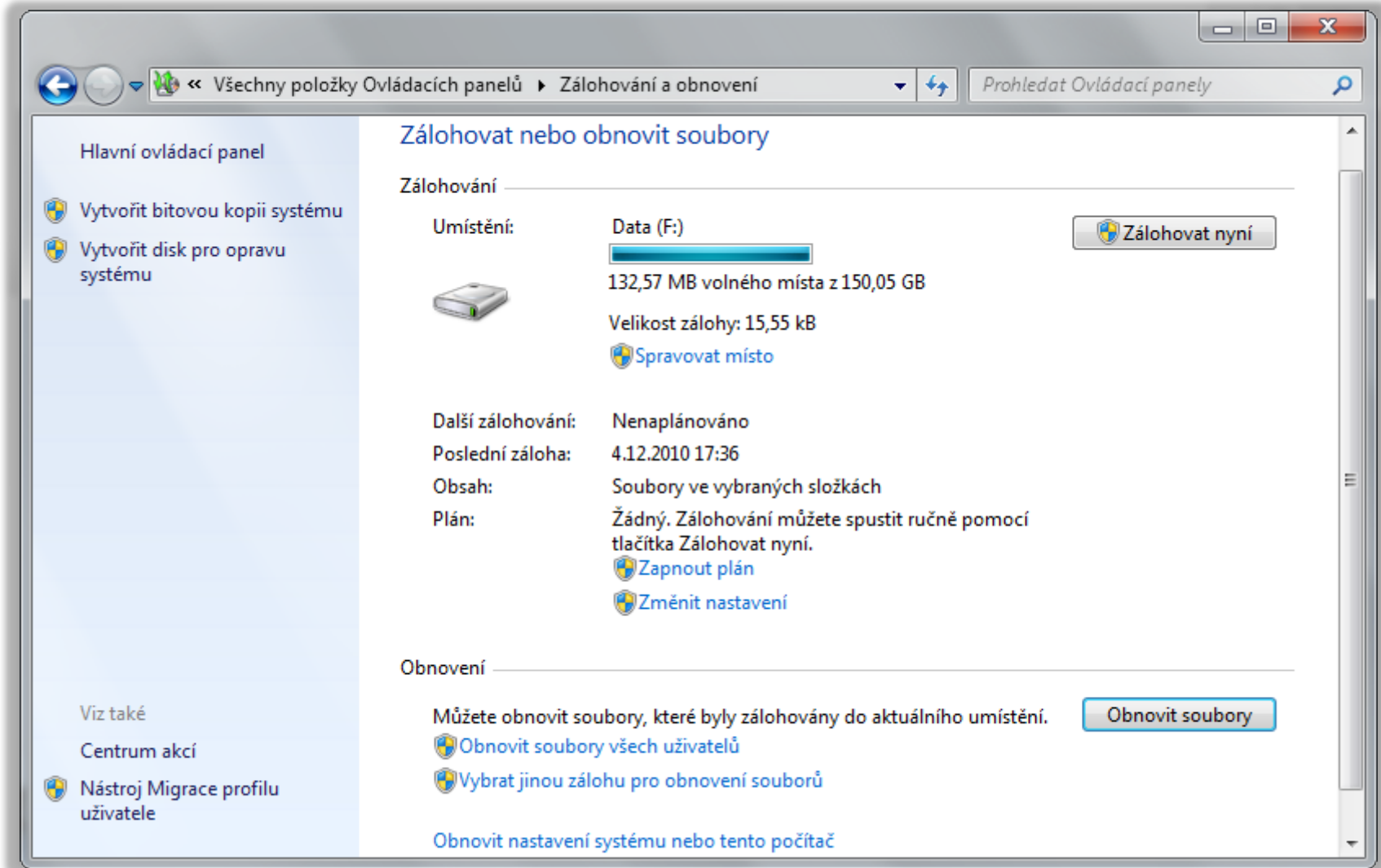
Metody vytváření stínových kopií

- Complete copy
 - Kompletní kopie (klon) dat oddílu disku
 - Časově náročné vytváření
- Copy-on-write
 - Ukládá (kopíruje) data před provedením jejich změny
 - Nevhodné při vysokém počtu operací zápisů
- Redirect-on-write
 - Ukládá (kopíruje) přímo změněná data
 - Nevhodné při vysokém počtu operací čtení

Zálohování dat

- Využívá stínové kopie (*shadow copies*)
 - Umožňuje zálohování i aktuálně otevřených souborů
 - Vyžaduje souborový systém NTFS
- Nastavení přes nástroj Zálohování a obnovení
 - Vyžaduje oprávnění správce
- Provádění záloh
 - Automaticky (pomocí naplánované úlohy)
 - Manuálně (iniciované správcem)

Nástroj Zálohování a obnovení



Typy úložišť

- Oddíl na pevném disku (interním, externím nebo virtuálním)
 - Nesmí být systémový ani obsahovat zálohovaná data
- Optické médium (CD nebo DVD)
- USB flash disk
 - Musí mít velikost minimálně 1 GB
- Sdílený adresář (nebo síťový disk)
 - Pouze u edicí Professional, Enterprise a Ultimate
 - Nutno zadat účet pro připojení s oprávněním zápisu

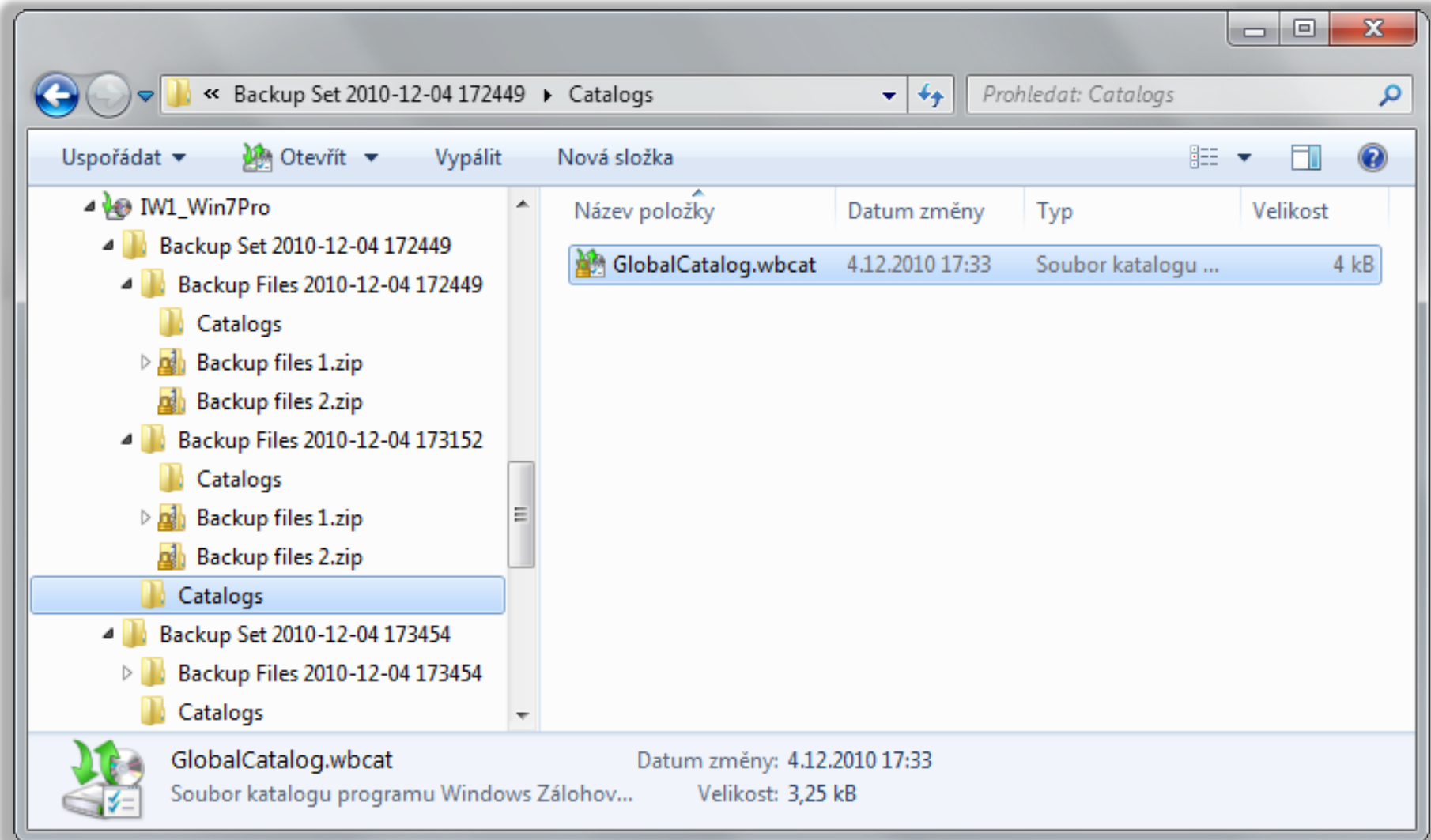
Bitová kopie systému (System Image)

- Obsahuje kopii všech oddílů disků potřebných ke spuštění systému Windows (záloha systému)
 - Obsahuje data systému Windows, programy, všechny ovladače a kompletní nastavení registru
- Lze uložit pouze na interní, externí nebo virtuální disky obsahující souborový systém NTFS nebo do sdíleného adresáře (jen poslední verze)
- Data uložena ve formě **VHD** souboru
 - Lze připojit jako virtuální disk nebo naboťovat (např. ve Virtual PC či přímo u edicí Enterprise a Ultimate)

Záloha souborů ve vybraných složkách

- Data uložena do komprimovaných **ZIP** souborů
 - Lze procházet v jakémkoliv správci souborů
- Inkrementální zálohování dat
 - Ukládají se pouze změny oproti poslední verzi zálohy
- Neukládají se (i když je lze vybrat pro zálohu)
 - Soubory registrované jako součást programů (obecně soubory v adresáři **Program Files**, ale mohou i jiné)
 - Soubory uložené na FAT/FAT32 oddílech disků
 - Soubory v koši a dočasné soubory

Struktura záloh vybraných adresářů



Katalogy

- Globální katalog (**GlobalCatalog.wbcats**)
 - Obsahuje index všech zálohovaných souborů spolu s informacemi, ve kterých ZIP souborech jsou uloženy
 - U bitových kopií systému obsahuje informace o verzi zachycené bitové kopie systému (*system image*)
- Souborové katalogy (**.wbcat** soubory)
 - Obsahují seznam oprávnění (ACL seznam) pro každý zálohovaný soubor
 - Při manuálním obnovení souborů (extrakci souborů ze ZIP souboru) nejsou obnovena jejich oprávnění

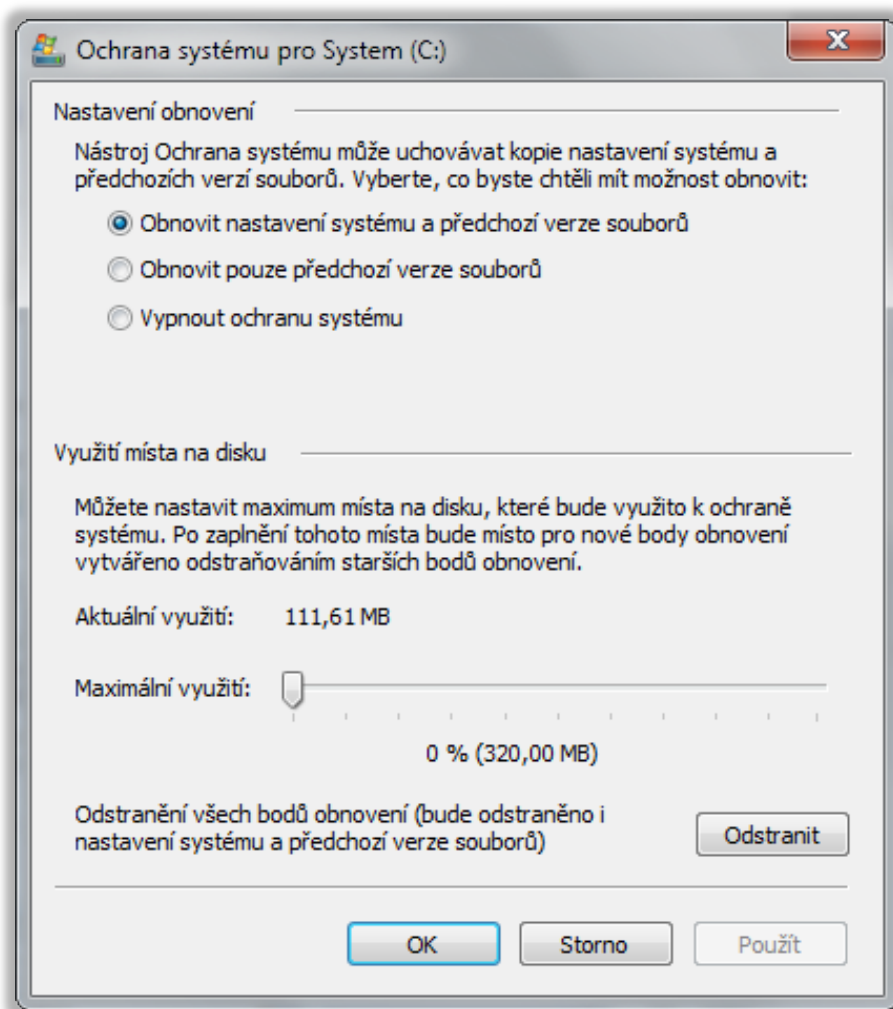
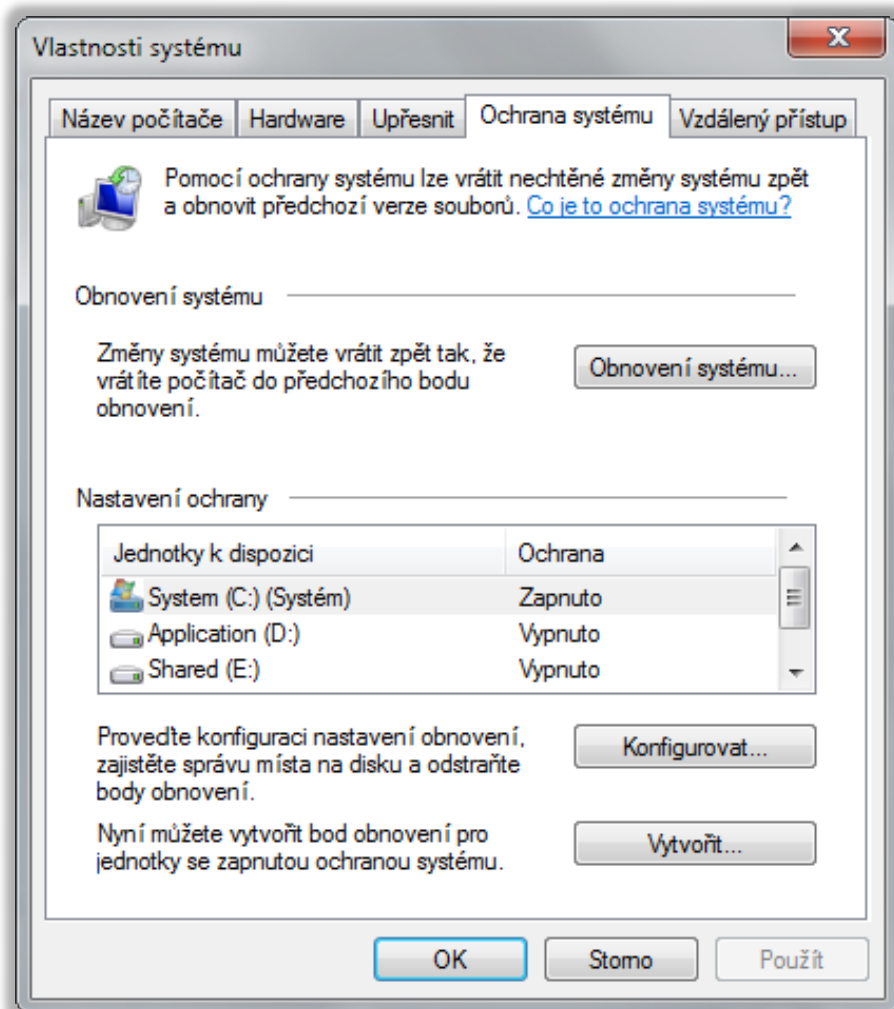
Zálohování přes příkazový řádek

- Umožňuje automatizaci vytváření bitových kopií systému (s pomocí naplánovaných úloh)
- Vytvoření bitové kopie oddílů
 - **wbadmin start backup -backupTarget:{<oddíl> | <sdílený-adresář>} -include:<oddíl> [,<oddíl> ...]**
- Vypsání informací o bitových kopiích oddílů
 - **wbadmin get versions [-backupTarget:<oddíl/adr>]**
- Vypsání obsahu určité verze bitové kopie oddílů
 - **wbadmin get items -version:<identifikátor>**

Ochrana a obnovení systému

- Ochrana systému (System Protection)
 - Zajišťuje vytváření bodů obnovení (*restore points*)
 - Umožňuje přístup k předchozím verzím souborů
 - Využívá stínové kopie (*shadow copies*)
- Obnovení systému (System Restore)
 - Navrací systém do dříve uloženého stavu (vybraného bodu obnovení)
 - Spuštění buď ze systému Windows nebo z prostředí Windows RE (*Windows Recovery Environment*)

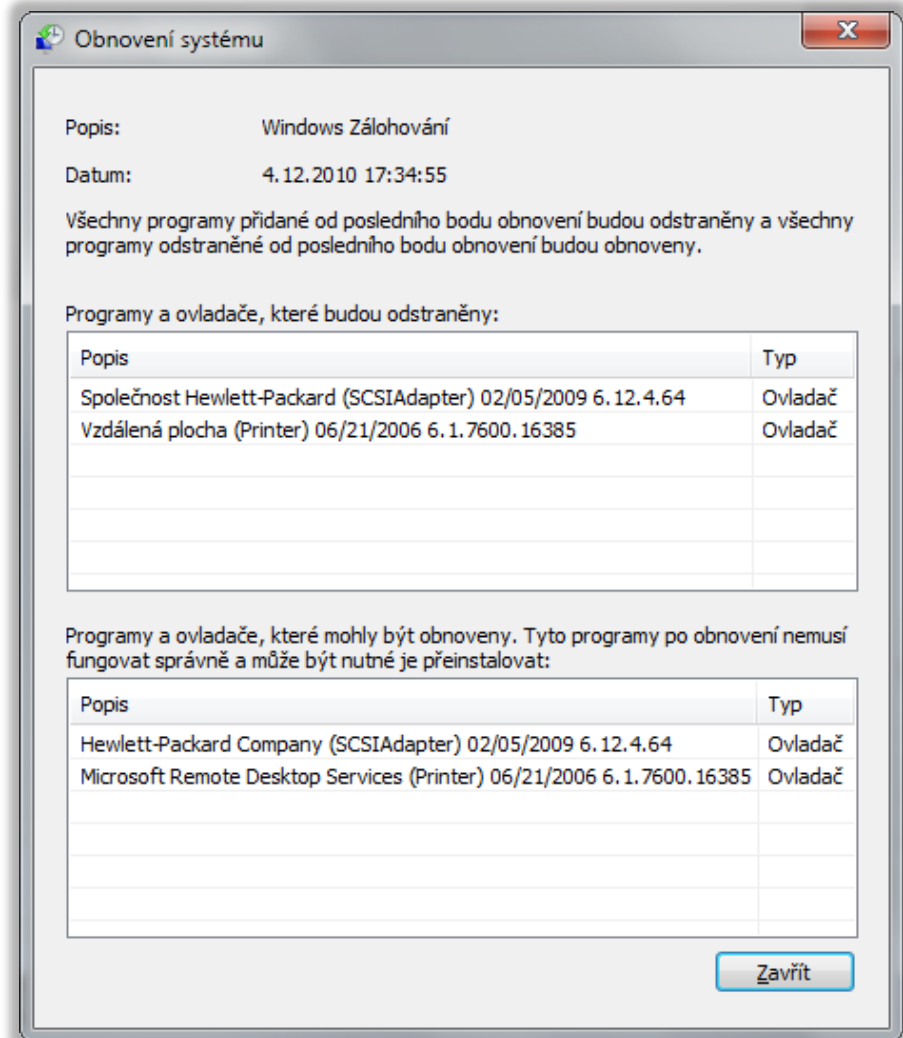
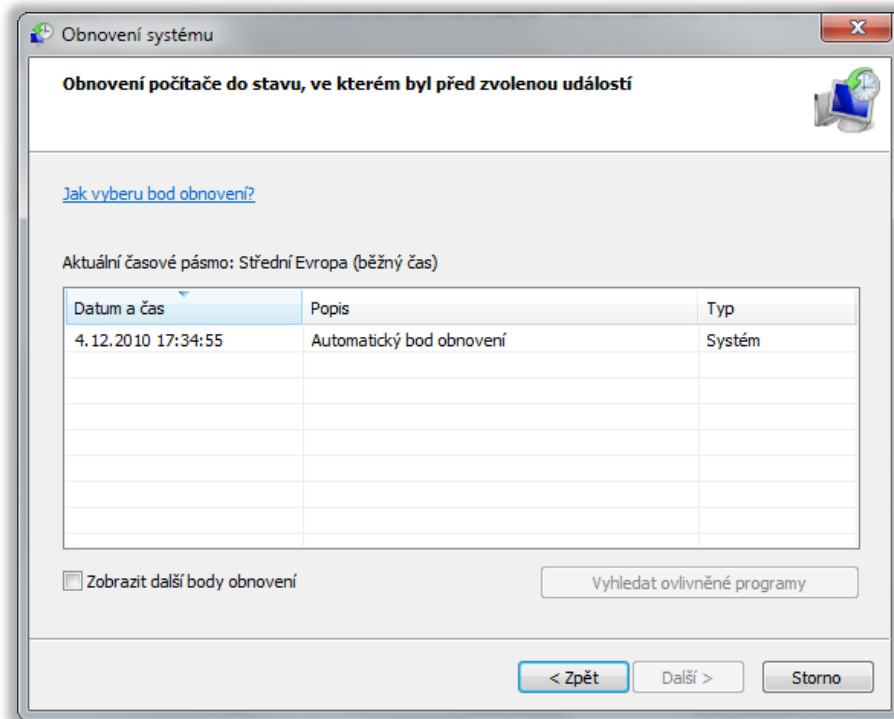
Nastavení ochrany systému



Body obnovení (Restore Points)

- Obsahují soubory a nastavení systému Windows, soubory programů a různé spustitelné soubory
 - Uloženy na stejném oddílu jako zálohovaná data
- Vytvářeny inkrementálně
 - Automaticky v pravidelných intervalech
 - Automaticky vždy před důležitými změnami systému (instalace aplikací, ovladačů, aktualizací, ...)
 - Manuálně uživatelem
- Neovlivňují uživatelská data (v profilech i mimo)

Nástroj Obnovení systému



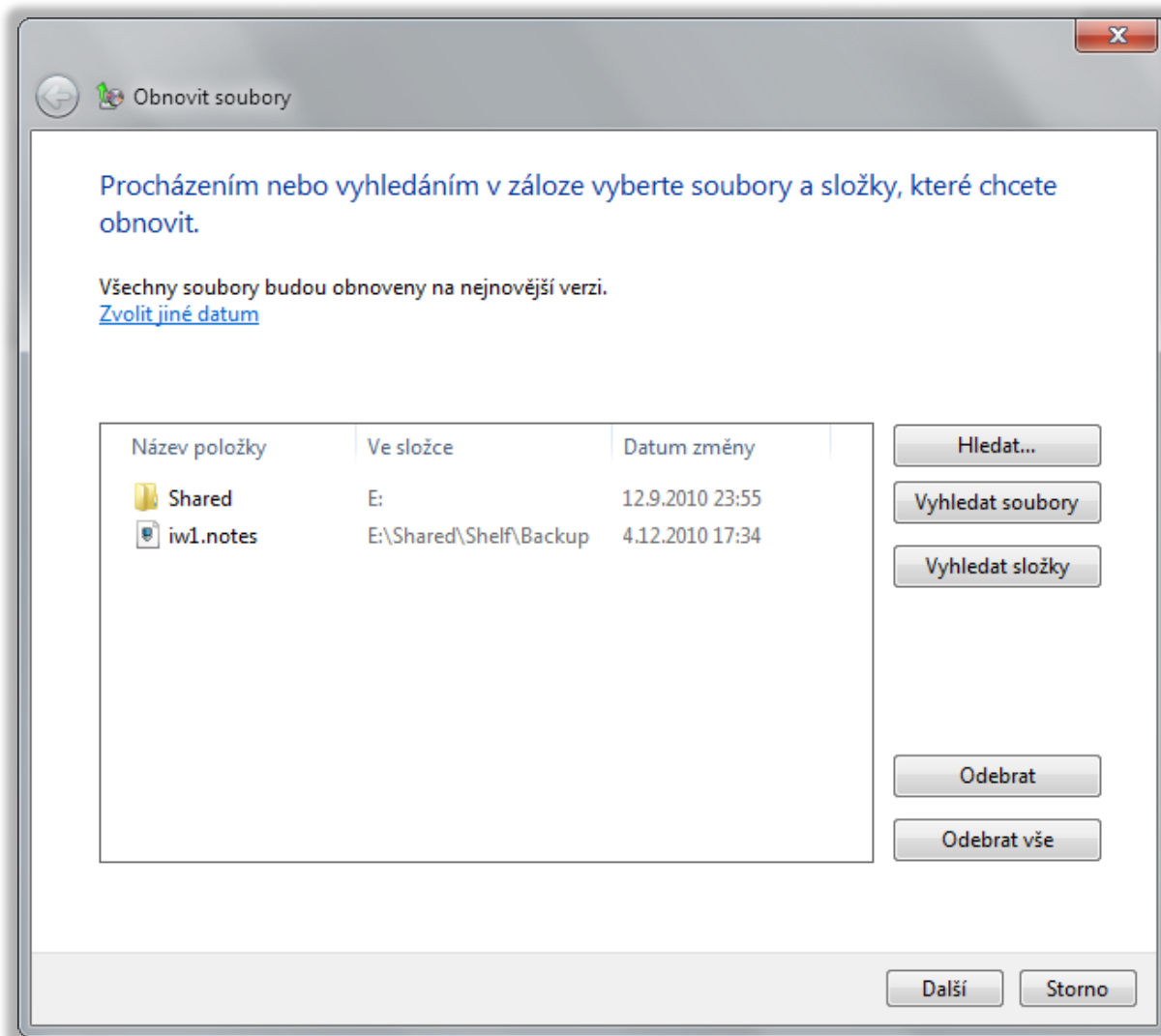
Obnovení bitové kopie systému

- Obnovení systému a veškerých uživatelských dat obsažených na systémovém (i jiných) oddílech
 - Přepisuje veškerý obsah cílových oddílů
- Nástroje pro obnovení jsou obsaženy v prostředí *Windows RE (Windows Recovery Environment)*
 - Lze spustit z bootovací nabídky (režim ladění) nebo z instalačního média systému Windows

Obnova souborů a složek

- Realizace přes nástroj Zálohování a obnovení
 - Umožňuje obnovit všechny soubory, k nimž má daný uživatel oprávnění pro čtení
 - Správce může obnovit veškerá zálohovaná data

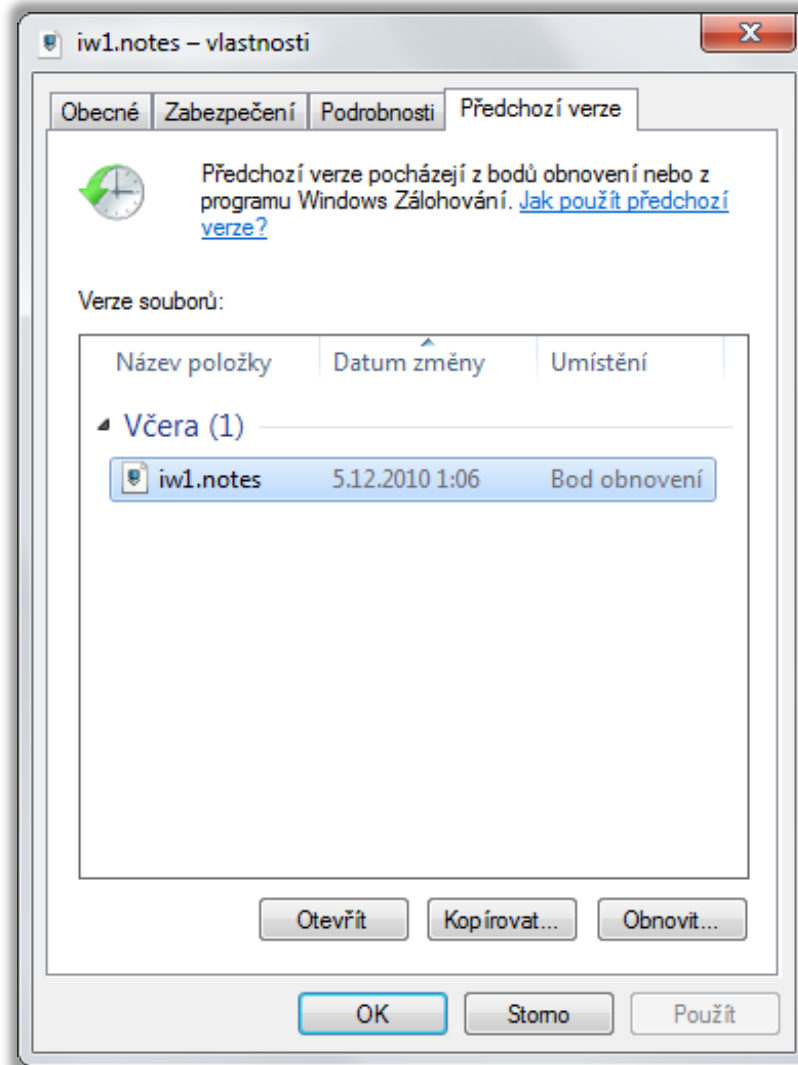
Obnovení souborů a složek



Předchozí verze (Previous Versions)

- Umožňují přístup k stínovým kopiím jednotlivých souborů i celých adresářů
 - Možnost návratu k předchozím verzím souborů
- Je možné obnovovat i přejmenované a smazané soubory (včetně souborů vymazaných z koše)
 - Potřeba znát adresář, kde byly původně uloženy
 - Obnovení přes předchozí verze tohoto adresáře

Obnovení předchozí verze souboru



Windows Recovery Environment

- Rozšíření prostředí Windows PE o sadu nástrojů pro obnovu systému Windows
 - Obnova systému (System Restore)
 - Obnovení bitové kopie systému (System Image)
 - Oprava spouštění systému (Startup Repair)
- Součást instalační bitové kopie systému Windows
 - Soubor **winre.wim** (umístěn v **install.wim** v adresáři **windows\system32\recovery**)
 - Vytvoření bootovatelné bitové kopie postupem jako u Windows PE, jen s **winre.wim** namísto **boot.wim**

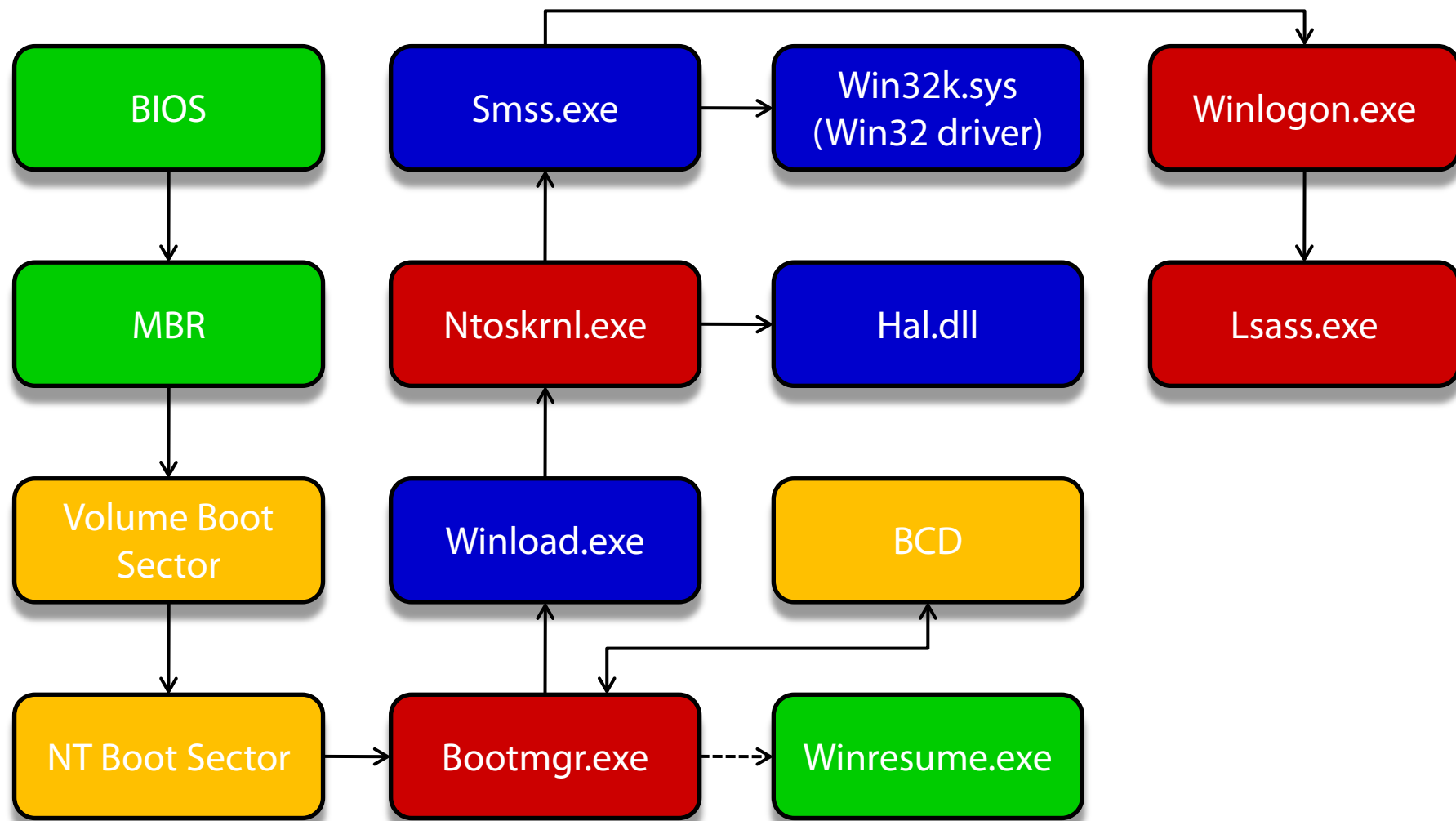
Oprava spouštění systému

- Automatická analýza a oprava
 - Chyb v MBR, zaváděcím sektoru nebo tabulce oddílů
 - Poškozených dat v BCD (Boot Configuration Data)
 - Chybějících nebo poškozených systémových souborů nebo souborů ovladačů
 - Problematických nebo nekompatibilních ovladačů
 - Nekompatibilních servisních balíků nebo aktualizací
 - Poškozených klíčů registru
 - Chyb v metadatech souborového systému

Nástroj Bootrec

- Kompatibilní jen s Windows Vista a Windows 7
- Nalezení všech nainstalovaných systémů
 - **Bootrec /ScanOs**
- Přidání vybraných systémů do úložiště BCD
 - **Bootrec /RebuildBcd**
- Oprava MBR (*Master Boot Record*)
 - **Bootrec /FixMbr**
- Oprava zaváděcího sektoru systémového oddílu
 - **Bootrec /FixBoot**

Ilustrace bootování systému Windows



Postup bootování systému Windows 7

- 1) MBR najde a načte Volume a NT Boot Sector (umí číst z FAT a NTFS)
- 2) NT Boot Sector lokalizuje a načte bootmgr.exe (obvykle v **C:\Boot**)
- 3) Bootmgr.exe spustí winresume.exe pokud existují data hibernace
- 4) Bootmgr.exe načte informace z BCD a nechá uživatele vybrat systém
- 5) Bootmgr.exe spustí winload.exe (zavaděč systému Windows)
- 6) Winload.exe načte ntoskrnl.exe, hal.dll, ostatní vyžadované soubory, bootovací ovladače a větev registru **SYSTEM**
- 7) Winload.exe spustí ntoskrnl.exe (jádro systému Windows)
- 8) Ntoskrnl.exe inicializuje jádro, ovladač zobrazení a spustí debugger
- 9) Ntoskrnl.exe ukončí debugger a spustí smss.exe (správce sezení)
- 10) Smss.exe načte zbytek registru a nastaví prostředí (**Win32k.sys**)
- 11) Smss.exe spustí winlogon.exe pro vytvoření sezení uživatele, služby, zbylé ovladače zařízení a lsass.exe (bezpečnostní podsystém)