

# Desktop systémy Microsoft Windows

IW1/XMW1 2015/2016

**Jan Fiedor**

ifiedor@fit.vutbr.cz

Fakulta Informačních Technologií

Vysoké Učení Technické v Brně

Božetěchova 2, 612 66 Brno

Revize 2. 11. 2015

# Sdílení a zabezpečení prostředků

# Sdílení prostředků

- Domácí skupiny
- Sdílení souborů
  - Sdílené adresáře
  - Knihovny
- Sdílení tiskáren
- Soubory offline

# Povolení sdílení prostředků

- Na úrovni **síťových profilů** (v části pokročilých nastavení sdílení)
  - Povolit **Sdílení souborů a tiskáren**
- Na úrovni **síťových rozhraní** (ve vlastnostech jednotlivých síťových rozhraní)
  - Povolit **Sdílení souborů a tiskáren v síti Microsoft**
  - Povolit **Klient sítě Microsoft**

# Nastavení sdílení pro profil a adaptér

The image shows two overlapping Windows windows. The background window is 'Pokročilé nastavení sdílení' (Advanced Sharing Settings), and the foreground window is 'Ethernet - vlastnosti' (Ethernet - Properties).

**Pokročilé nastavení sdílení**

Centrum síťových připojení a sdílení > Pokročilé nastavení sdílení

Soubor Upravit Zobrazit Nástroje Nápověda

### Změnit možnosti sdílení pro různé síťové profily

Systém Windows vytvoří samostatný síťový profil pro každou používanou síť. Každý profil má specifické možnosti.

Privátní \_\_\_\_\_

Host nebo veřejný (aktuální profil) \_\_\_\_\_

Zjišťování sítě \_\_\_\_\_

Pokud je zapnuto zjišťování sítě, bude možné z tohoto počítače vidět tento počítač také bude viditelný pro jiné počítače v síti.

Zapnout zjišťování sítě  
 Vypnout zjišťování sítě

**Sdílení souborů a tiskáren**

Je-li zapnuto sdílení souborů a tiskáren, mohou mít uživatelé v síti přístup ke sdíleným z tohoto počítače.

Zapnout sdílení souborů a tiskáren  
 Vypnout sdílení souborů a tiskáren

Všechny sítě \_\_\_\_\_

Uložit změny Storno

**Ethernet - vlastnosti**

Sítě Ověřování Sdílení

Připojit pomocí:

Killer e2200 Gigabit Ethernet Controller (NDIS 6.30)

Konfigurovat...

Toto připojení používá následující položky:

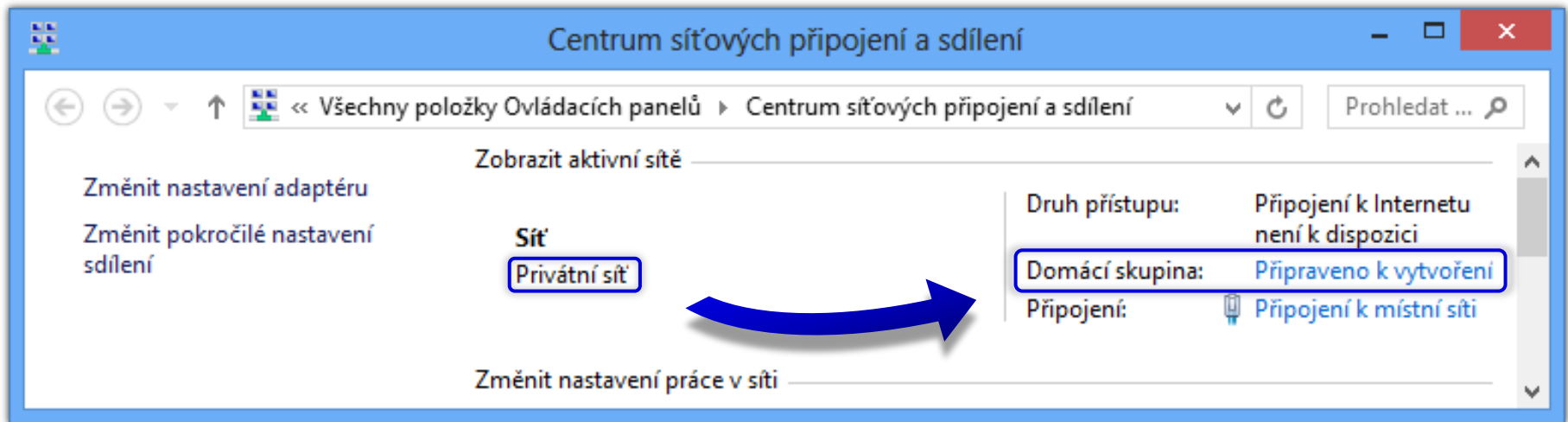
- Klient sítě Microsoft
- Qualcomm Atheros Bandwidth Control
- COMODO Internet Security Firewall Driver
- Plánovač paketů technologie QoS
- Sdílení souborů a tiskáren v sítích Microsoft
- Rozšiřitelný virtuální přepínač technologie Hyper-V
- Protokol multiplexoru pro síťový adaptér od společnosti

Nainstalovat... Odinstalovat Vlastnosti

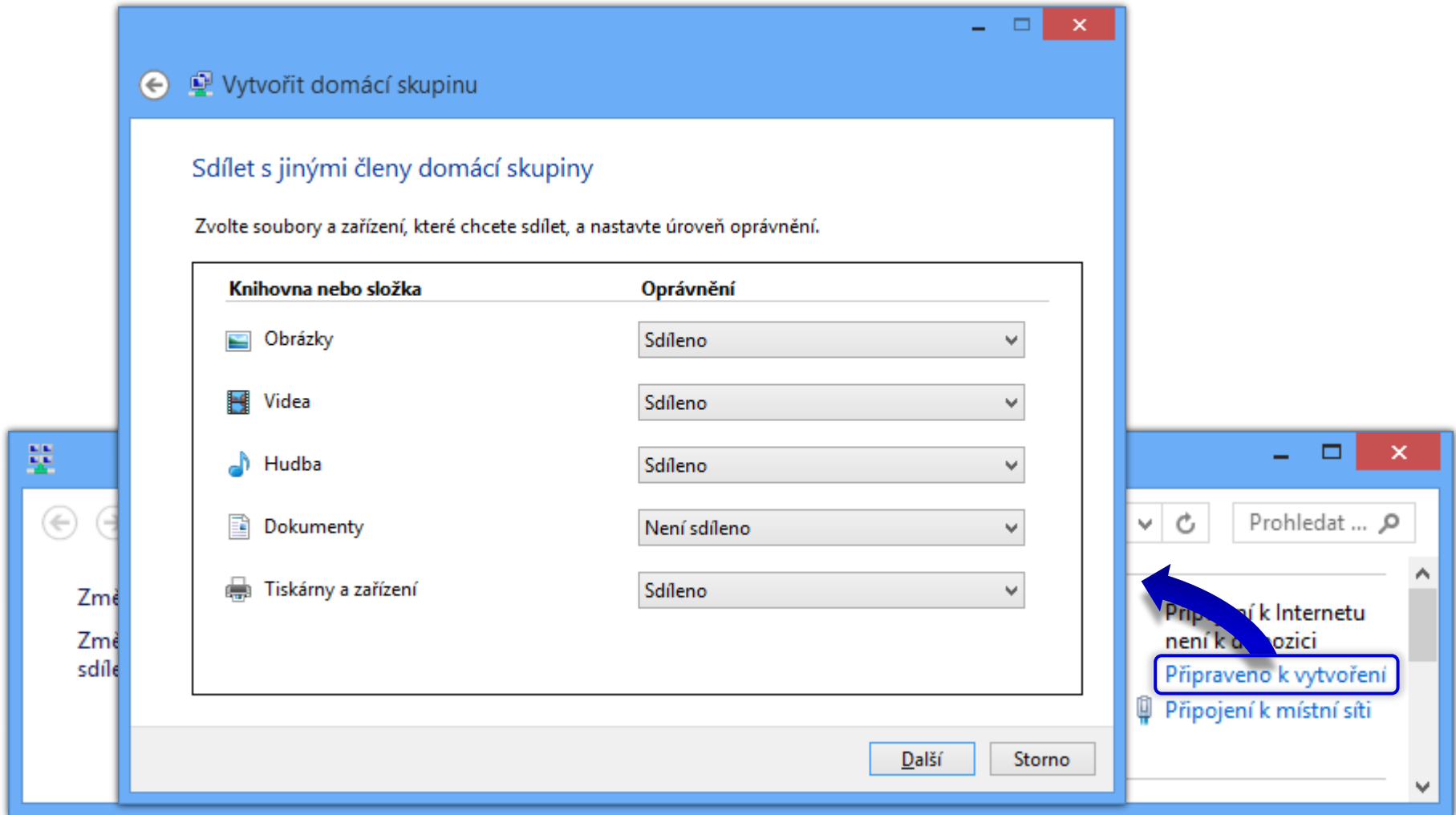
OK Storno

# Domácí skupiny (HomeGroups)

- Umožňují jednoduché sdílení souborů a tiskáren v systémech **Windows 7** a **novějších**
  - Povolení vyžaduje **oprávnění správce**
  - Co sdílet si volí jednotliví **uživatelé**
- Dostupné **pouze** v **privátní síti**



# Vytvoření domácí skupiny

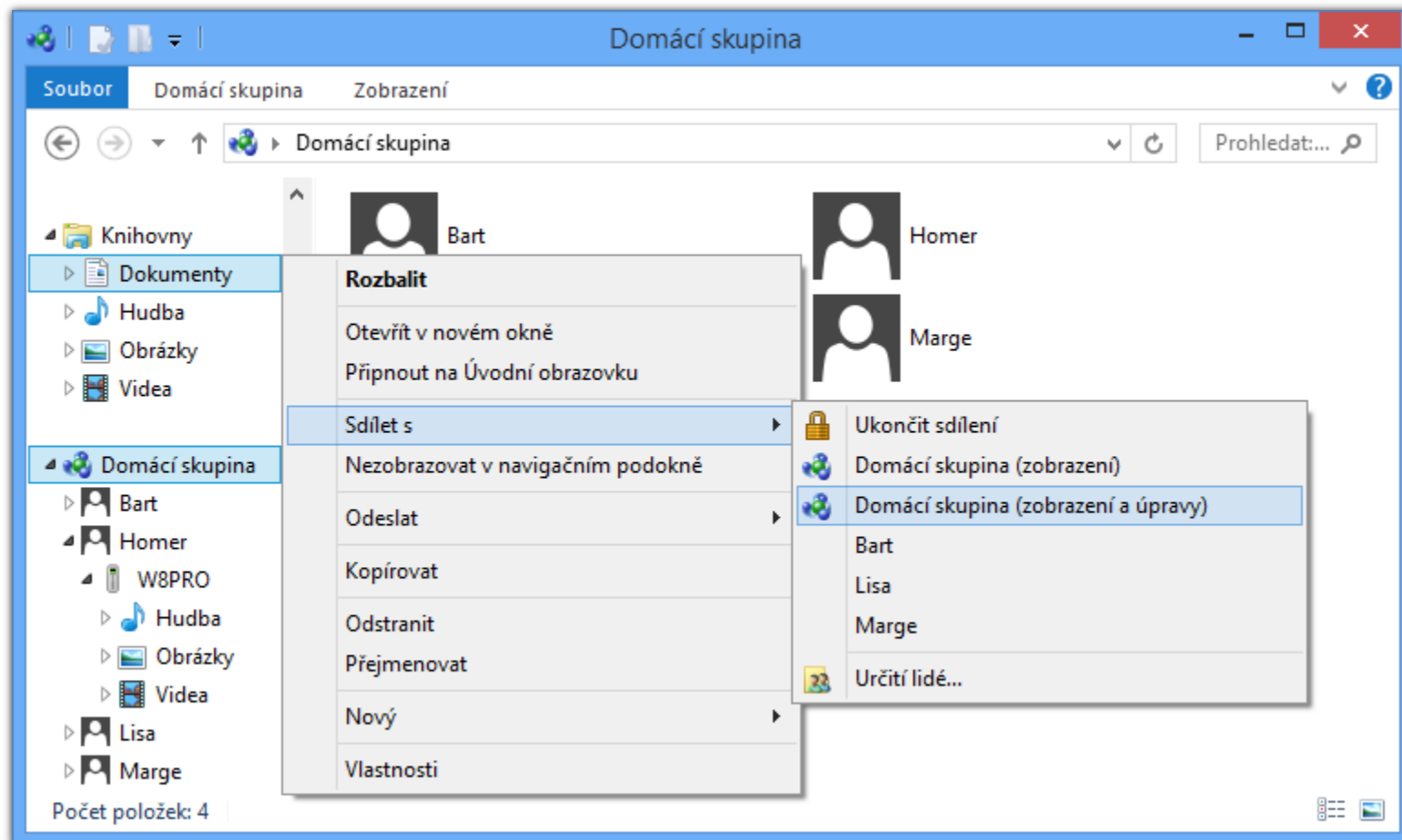


# Připojení a přístup k domácí skupině

- Připojení k domácí skupině
  - Přes **Centrum síťových připojení a sdílení**
  - Pro připojení je vyžadováno sdílené **heslo**
- Přístup k domácí skupině
  - Přes **průzkumníka Windows** (samostatný uzel)
  - Rozlišovány na základě **uživatele** a **počítače**
  - Dostupné vždy když **běží** daný **počítač** (i pokud není **přihlášen** konkrétní uživatel)
  - K přístupu lze použít **vlastní** nebo **sdílený** účet

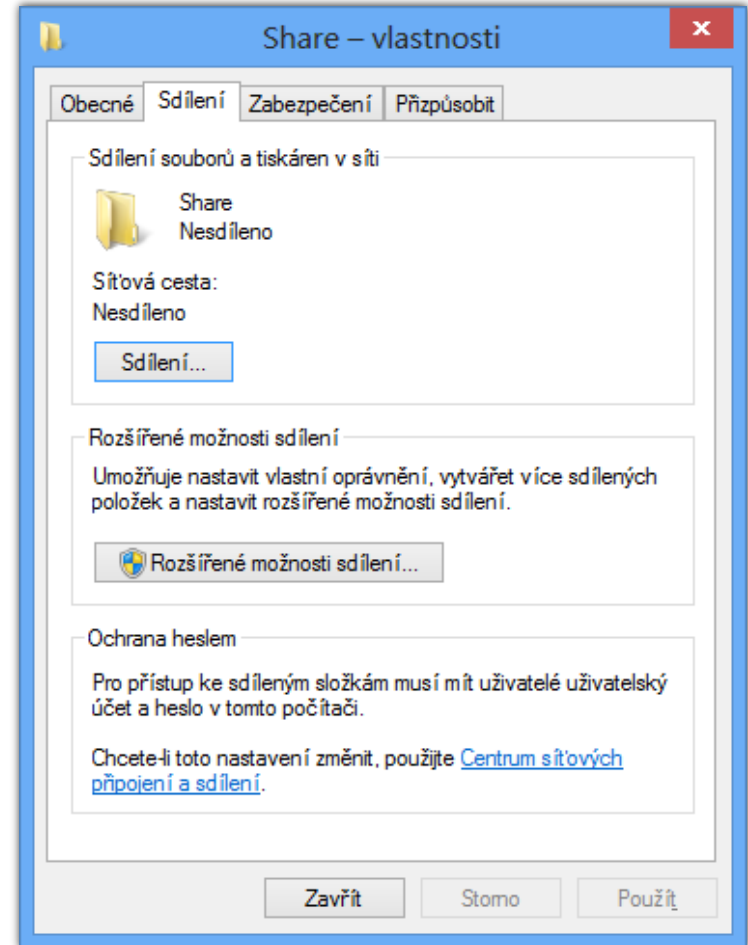


# Sdílení adresářů v domácí skupině



# Sdílené adresáře (Shared Folders)

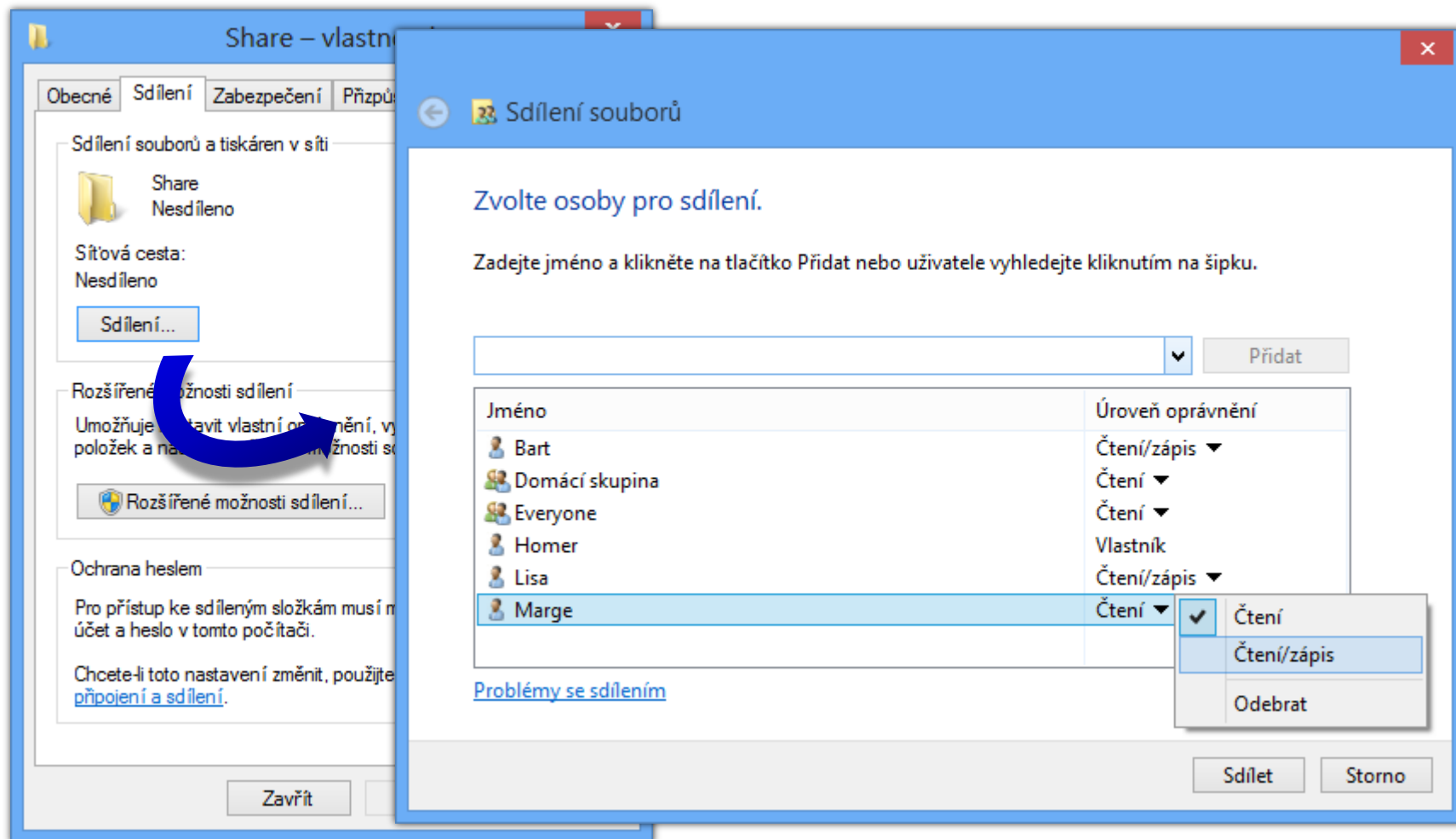
- **Povolení a nastavení** ve vlastnostech adresáře (záložka **sdílení**)
- 2 typy sdílení
  - Jednoduché (*simple*) sdílení
  - Pokročilé (*advanced*) sdílení



# Jednoduché sdílení adresářů

- Rozlišuje 3 typy oprávnění (nastavuje **vlastník**)
  - Čtení (zahrnuje i spouštění)
  - Čtení/zápis (zahrnuje i úpravy a mazání)
  - Vlastník (**nelze** nastavit, přiřazeno **automaticky** účtu uživatele, jenž daný adresář **nasdílel**)
- Oprávnění lze nastavovat **pouze**
  - Lokálním uživatelům
  - Lokálním skupinám **Everyone** a **Domácí skupina**
  - Doménovým skupinám a uživatelům

# Nastavení jednoduchého sdílení



# Pokročilé sdílení adresářů

- Rozlišuje 3 typy oprávnění
  - **Číst** (zahrnuje i spouštění)
  - **Změnit** (čtení + zápis, úpravy a mazání)
  - **Úplné řízení** (možnost nastavovat **oprávnění**)
- Oprávnění lze nastavovat
  - Lokálním i doménovým uživatelům a skupinám
- Možnost **limitování** počtu **připojeným** uživatelů
  - Maximum uživatelů je **20** (omezení **Windows 8/10**)
- Podpora **souborů offline** (*offline files*)

# Nastavení pokročilého sdílení

**Share – vlastnosti**

Obecné | **Sdílení** | Zabezpečení | Přizpůsobit

Sdílení souborů a tiskáren v síti

Share  
Nesdíleno

Síťová cesta:  
Nesdíleno

Sdílení...

Rozšířené možnosti sdílení

Umožňuje nastavit vlastní oprávnění, v položek a nastavit rozšířené možnosti s

Rozšířené možnosti sdílení...

Ochrana hesel

Pro přístup ke s...m složk...  
účet a heslo v tomto...

Chcete-li toto nastavení změnit, použijte [připojení a sdílení](#).

Zavřít

**Rozšířené možnosti sdílení**

Sdílet tuto složku

Nastavení

Název sdílené složky:  
Share

Přidat Odebrat

Omezit počet současných uživatelů na: 20

Komentáře:

Oprávnění Mezipaměť

OK Storno Použít

**Oprávnění pro Share**

Oprávnění ke sdílení

Název skupiny nebo jméno uživatele:

Everyone  
Homer (W8PRO\Homer)  
Marge (W8PRO\Marge)  
**Simpsons (W8PRO\Simpsons)**

Přidat... Odebrat

Oprávnění pro Simpsons

	Povolit	Odepřít
Úplné řízení	<input type="checkbox"/>	<input type="checkbox"/>
Změnit	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Číst	<input checked="" type="checkbox"/>	<input type="checkbox"/>

[Další informace o řízení přístupu a oprávněních](#)

OK Storno Použít

# Skryté sdílené adresáře

- Název **ukončen** znakem \$ (např. C\$)
- Nejsou viditelné při **prohledávání sítě**
  - Jsou **přístupné** pomocí **UNC cesty**
- UNC (*Uniform Naming Convention*) cesta
  - Popis **umístění** sdíleného prostředku **na síti**
  - Obecný tvar **\\<server>\<sdílení>\<prostředek>**
    - Prostředkem může být např. adresář, soubor nebo tiskárna

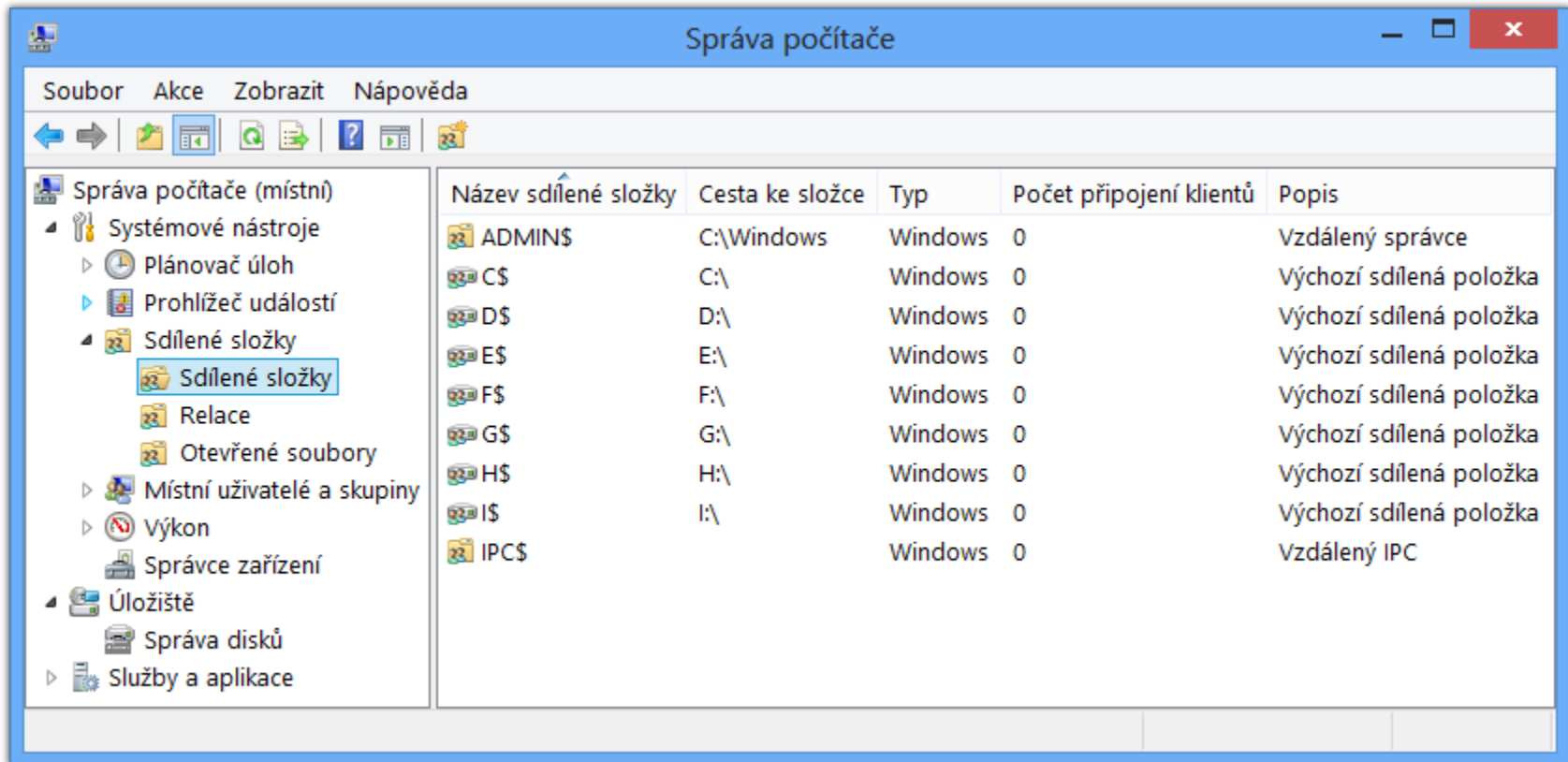
# Speciální sdílené adresáře

- Vytvářeny **automaticky** systémem **Windows**
  - Vždy **skryté**
  - Přístupné **pouze** uživatelům s **oprávněními správce**
- **ADMIN\$**
  - Sdílení kořenového adresáře systému **Windows**
- **IPC\$** (*Inter Process Communication*)
  - Sdílení souborů mezi počítači při **komunikaci procesů**
- **<jednotka>\$** pro **každý** připojený oddíl disku
  - Sdílení kořenového adresáře **oddílu disku**



# Správa pomocí MMC konzole

- Spuštění příkazem **compmgmt.msc** nebo přes **Ovládací panely** (sekce **Nástroje pro správu**)



The screenshot shows the 'Správa počítače' (Computer Management) console window. The left-hand tree view is expanded to 'Sdílené složky' (Shared Folders). The main pane displays a table of shared folders:

Název sdílené složky	Cesta ke složce	Typ	Počet připojení klientů	Popis
ADMINS	C:\Windows	Windows	0	Vzdálený správce
CS\$	C:\	Windows	0	Výchozí sdílená položka
D\$	D:\	Windows	0	Výchozí sdílená položka
E\$	E:\	Windows	0	Výchozí sdílená položka
F\$	F:\	Windows	0	Výchozí sdílená položka
G\$	G:\	Windows	0	Výchozí sdílená položka
H\$	H:\	Windows	0	Výchozí sdílená položka
I\$	I:\	Windows	0	Výchozí sdílená položka
IPCS		Windows	0	Vzdálený IPC

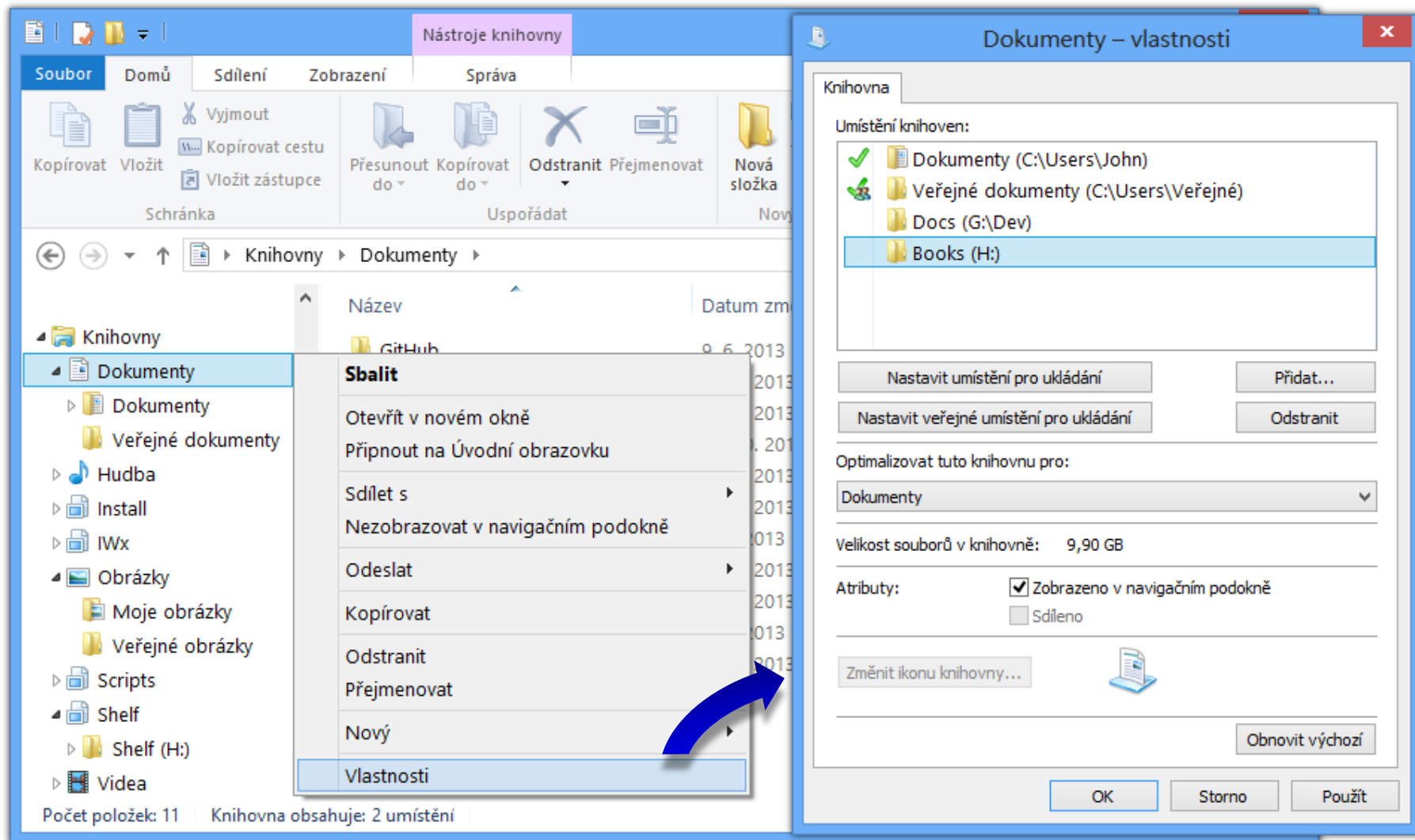
# Správa pomocí příkazové řádky

- Vypsání **seznamu** sdílených adresářů na počítači
  - **net share**
- Vypsání **informací** o sdíleném adresáři
  - **net share <název>**
- **Vytvoření** nového sdíleného adresáře
  - **net share <název>=<cesta-k-adresáři>**  
**[/users:<limit> | /unlimited]**  
**[/grant:<uživatel>,{read | change | full}]**
    - Název sdílení musí být **unikátní** v rámci počítače
    - Limit pro počet připojených uživatelů **nesmí** být **0**

# Knihovny (Libraries)

- **Virtuální adresáře** zahrnující jiné adresáře
  - Tvořeny **odkazy** na (**lokální** nebo **síťové**) adresáře
  - Fyzicky XML soubory s příponou **.library-ms**
- **Přístup** a **správa** pomocí **průzkumníka Windows**
  - Definice obsažených adresářů (a **výchozího** adresáře pro ukládání dat) ve vlastnostech dané knihovny
- Možnost **optimalizace** pro **konkrétní typy** dat
- Možnost **sdílení** (normálně nebo v rámci **domácí skupiny**)

# Přístup ke knihovnám a jejich správa



# Sdílení tiskáren

- Nastavení ve **vlastnostech tiskárny**
- 3 základní typy oprávnění
  - **Tisk** (a správa **vlastních** dokumentů v tiskové frontě)
  - **Správa této tiskárny** (změna nastavení a oprávnění tiskárny, sdílení tiskárny, pozastavení tiskárny, ...)
  - **Správa dokumentů** (správa **veškerých** dokumentů v tiskové frontě)
- Možnost dodat **ovladače** pro starší systémy
  - Automatické **stažení** a **instalace** při přidání tiskárny

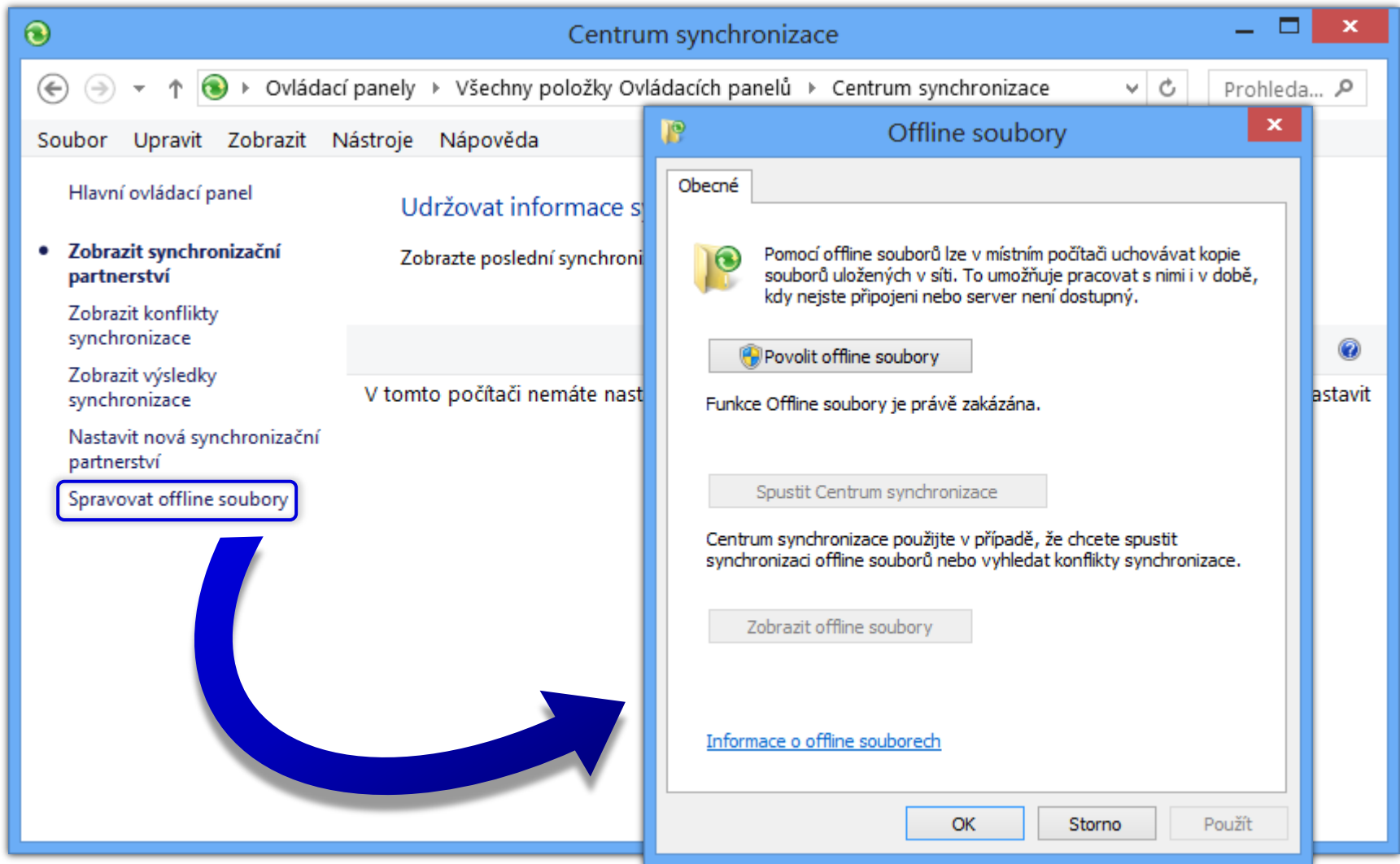
# Soubory offline (Offline Files)

- Umožňují přistupovat k souborům v síti i **bez připojení** k této síti
  - **Kešování** souborů na **lokálním** počítači
  - **Synchronizace** souborů při opětovném **připojení**
- K dispozici pouze u edicí **Pro** a **Enterprise**
- Možnost **šifrování** dat ve vyrovnávací paměti

# Povolení a nastavení souborů offline

- Povolení souborů offline v **Centru synchronizace**
- Výběr souborů, jenž budou k dispozici offline
  - **Manuálně** pomocí **průzkumníka Windows**
    - **Musí** být podporovány (resp. **povoleny**) na úrovni **adresáře** v **rozšířených možnostech sdílení**
    - **Automaticky** povolením na úrovni **adresáře**
    - Centrálně pomocí **zásad skupiny**
- Vyloučení jednotlivých **typů** souborů
  - Centrálně pomocí **zásad skupiny**

# Globální povolení souborů offline






# Povolení na úrovni sdíleného adresáře

The image shows two overlapping Windows dialog boxes. The background dialog is titled "Rozšířené možnosti sdílení" (Advanced sharing options) and has the "Sdílet tuto složku" (Share this folder) checkbox checked. The "Název sdílené složky:" (Share name) field contains "Share". The foreground dialog is titled "Nastavení pro offline režim" (Offline mode settings) and contains the following text and options:

Můžete určit, zda a jak bude obsah sdílené složky dostupný uživatelům pracujícím v offline režimu.

- Pouze soubory a programy určené uživateli jsou k dispozici offline.
- Žádné soubory ani programy ze sdílené složky nejsou k dispozici offline.
- Všechny soubory a programy otevřené uživateli ze sdílené složky jsou automaticky k dispozici offline.

Optimalizovat pro výkonost

 Před výběrem této možnosti vyhledejte podrobnosti v nápovědě.

Další informace o ukládání do mezipaměti naleznete v tématu [Konfigurace dostupnosti v offline režimu pro sdílenou složku](#).

A blue arrow points from the "OK" button in the background dialog to the "OK" button in the foreground dialog.

# Režimy souborů offline (1)

- Online režim
  - Čtení z **vyrovnávací paměti** (*cache*), zápis do **sdílení**
  - Synchronizace prováděna **automaticky**
- Automatický offline režim
  - Čtení a zápis do **vyrovnávací paměti** (*cache*)
  - Ověřování připojení do sítě co 2 minuty

# Režimy souborů offline (2)

- Manuální offline režim
  - Čtení a zápis do **vyrovnávací paměti** (*cache*)
  - Ověřování **neprobíhá**
  - **Zapnutí** / **vypnutí** v **průzkumníkovi Windows**
- Režim pomalé linky (*slow-link*)
  - Čtení a zápis do **vyrovnávací paměti** (*cache*)
  - **Povolen** automaticky při **pomalém** připojení do sítě (**práh** lze nastavit v **zásadách skupiny**)
  - Pouze **manuální** synchronizace

# Synchronizace

- Probíhá **automaticky** nebo **manuálně**
- Řešení **konfliktů** při synchronizaci
  - Ponechání **lokální** verze (**přepsání** verze ve sdílení)
  - Ponechání verze **ve sdílení** (**přepsání** lokální verze)
  - Ponechání **obou** verzí (**přejmenování** lokální verze)

# Řešení konfliktů při synchronizaci

**Konflikty**

Centrum synchronizace > Konflikty

Soubor Upravit Zobrazit Nástroje Nápověda

Hlavní ovládací panel

Zobrazit synchronizační partnerství

- **Zobrazit konflikty synchronizace**

Zobrazit výsledky synchronizace

Nastavit nová synchronizační partnerství

Spravovat offline soubory

Tyto položky spolu kolidují a synchronizovány.

Vyberte jeden nebo více konfliktů s kliknutím na tlačítko Vyřešit a zobrazíte podrobnosti. Vyberte si, jak mají být vyřešeny.

Název	Datum změny
Offline soubory (1)	
offline.txt	2. 11. 2013 17:11

**Zobrazit možnosti řešení...**

- Ignorovat
- Vlastnosti

**Vyřešení konfliktu**

Klikněte na verzi, kterou chcete zachovat.  
Od poslední aktualizace byly obě verze aktualizovány.

- **Zachovat tuto verzi**  
**offline.txt**  
V tomto počítači  
Velikost: 9 bajtů  
Datum změny: 2. 11. 2013 17:13 (novější)
- **Zachovat tuto verzi**  
**offline.txt**  
\\192.168.12.10\Share  
Velikost: 9 bajtů  
Datum změny: 2. 11. 2013 17:11
- **Zachovat obě verze**  
(Nejvyšší verze bude přejmenována offline (John v1).txt.)

[Jak odstranit konflikty synchronizace?](#)

Storno

# Zabezpečení prostředků

- **Oprávnění**
  - Sdílení
  - Tiskáren
  - Souborového systému **NTFS**
- **Šifrování**
  - **EFS** (*Encrypted File System*)
  - **BitLocker**

# NTFS oprávnění

- Zabezpečení na úrovni **přístupů** k datům
- Lze nastavovat **lokálním** i **doménovým** skupinám a uživatelům (a předdefinovaným skupinám)
  - Předdefinované skupiny **Everyone** a **Creator Owner**
    - Zahrnují všechny uživatele, resp. uživatele, jenž vlastní daný adresář nebo soubor (v době definice oprávnění)
- **Nelze** použít u souborových systémů **FAT** a **FAT32**
- Ověřovány i při přístupu ze **sítě**
- Uloženy v **ACL seznamech** (*Access Control Lists*)

# Základní (skupiny) NTFS oprávnění

Oprávnění	Prostředek	Popis
Úplné řízení	<b>Adresář</b>	Zobrazení a přístup k obsahu, vytváření souborů a adresářů, změny oprávnění, <b>odstraňování</b> souborů a adresářů
	<b>Soubor</b>	Čtení, zápis, úpravy a odstraňování, změny oprávnění
Měnit	<b>Adresář</b>	Zobrazení a přístup k obsahu, vytváření souborů a adresářů
	<b>Soubor</b>	Čtení, zápis, úpravy a odstraňování
Číst a spouštět	<b>Adresář</b>	Přístup k obsahu ( <b>ne</b> jeho zobrazení) a jeho spouštění
	<b>Soubor</b>	Přístup k souboru a jeho spouštění
Zobrazovat obsah složky	<b>Adresář</b>	Zobrazení obsahu
Číst	<b>Adresář</b>	Přístup k obsahu ( <b>ne</b> jeho zobrazení)
	<b>Soubor</b>	Přístup k souboru
Zapisovat	<b>Adresář</b>	Vytváření souborů a adresářů ( <b>ne</b> jejich odstraňování)
	<b>Soubor</b>	Zápis a úpravy ( <b>ne</b> odstraňování)



# Nastavení a změny NTFS oprávnění

- Ve **vlastnostech** souboru nebo adresáře (záložka **Zabezpečení**), případně přes **příkazovou řádku**
- Oprávnění může **nastavovat** nebo **měnit**
  - Uživatel nebo skupina, jenž má přiděleno oprávnění **Měnit oprávnění** (zahrnuto ve skupině **Úplné řízení**)
  - **Vlastník** souboru nebo adresáře
    - Ve výchozím nastavení uživatel, jenž vytvořil daný soubor nebo adresář
    - Může být kdykoliv nahrazen jiným uživatelem, jenž má oprávnění **Přebírat vlastnictví** (**správci počítače** mohou přebírat vlastnictví i **bez** tohoto **oprávnění**)

# Dědičnost NTFS oprávnění

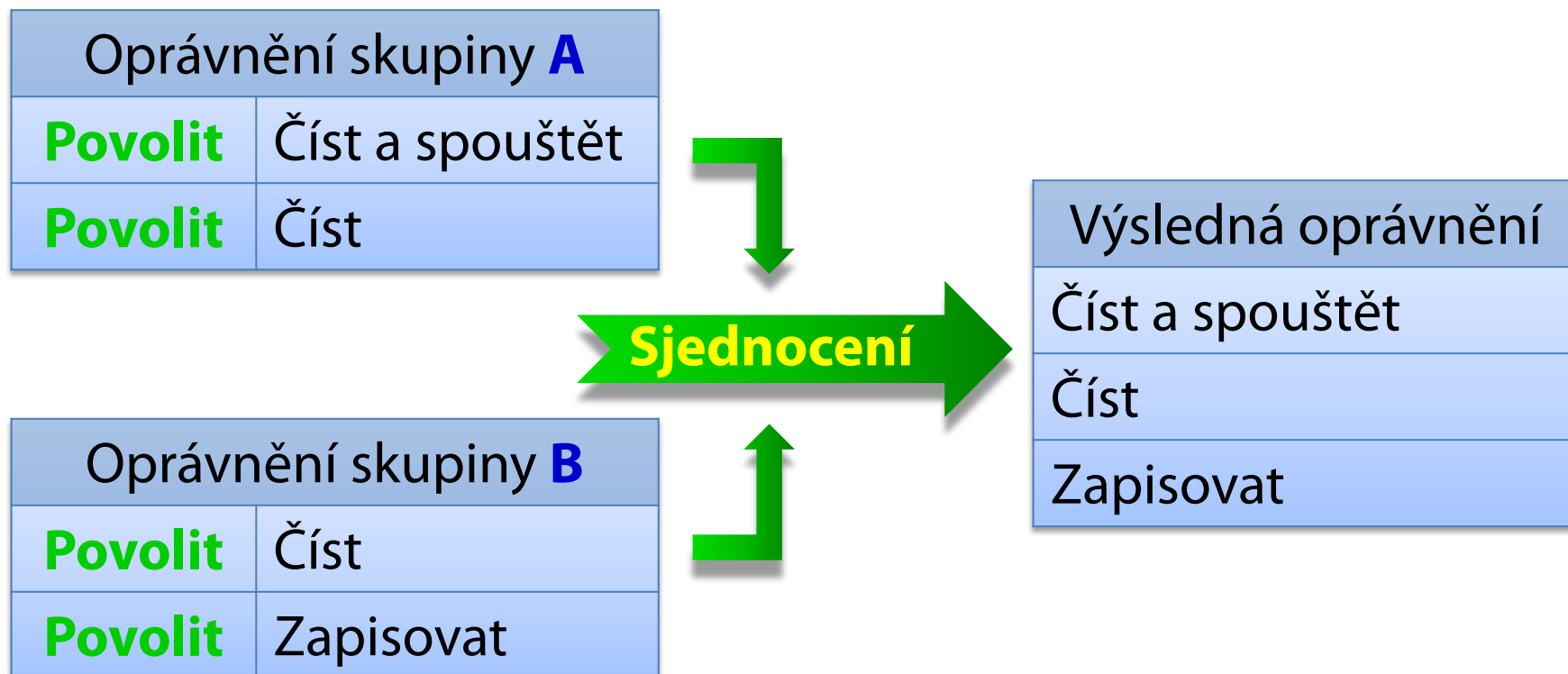
- Nově **vytvářené** soubory a adresáře dědí **NTFS** oprávnění **adresáře**, ve kterém byly vytvořeny
  - Zděděná oprávnění mají **nižší prioritu** než explicitní
- Lze **zakázat** ve vlastnostech souboru/adresáře
  - **Zkopírování** / **odstranění** zděděných NTFS oprávnění
- Lze **vynutit** dědičnost na **podřízených** souborech a adresářích (*child objects*)
  - **Přepsání** NTFS oprávnění u podřízených objektů
    - Uživatel **musí** být schopen **měnit oprávnění**

# Výpočet výsledných NTFS oprávnění

- Každé oprávnění lze **povolit** nebo **odepřít**
  - **Odepření** má vždy **vyšší** prioritu (**přepisuje** **povolení**)
- Obecný algoritmus
  - 1) Vytvoř **prázdnou** množinu oprávnění **S**
  - 2) **Přidej** do **S** zděděná oprávnění, která jsou **povolená** pro daného uživatele nebo skupinu, jenž je členem
  - 3) **Odeber** z **S** zděděná oprávnění, která jsou **odepřena** pro daného uživatele nebo skupinu, jenž je členem
  - 4) Opakuj body 2) a 3) pro explicitní oprávnění
  - 5) Vrať oprávnění **obsažená** v množině **S**

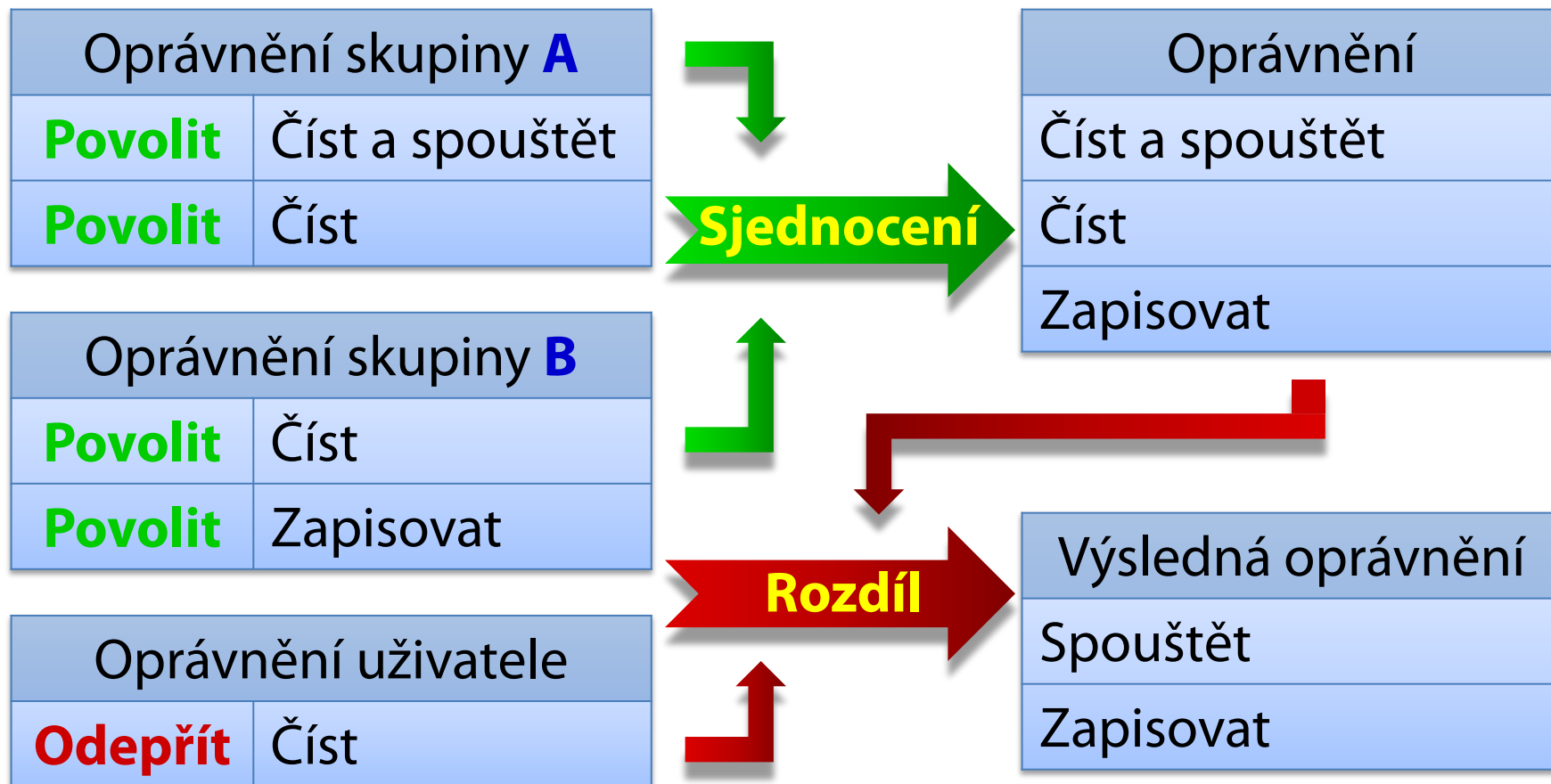
# Příklad s povolením (allow) oprávnění

- Uživatel je členem skupin **A** a **B**



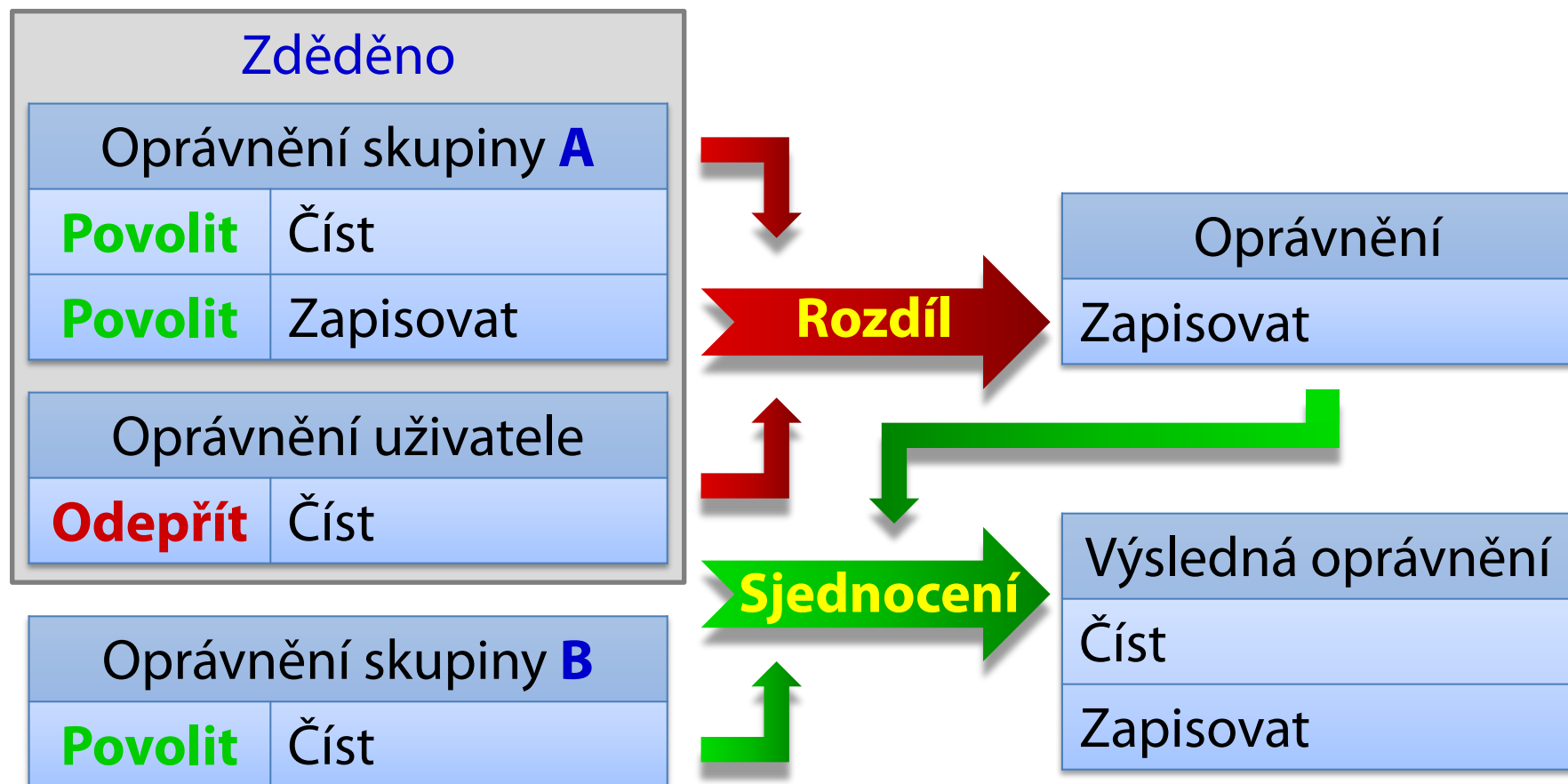
# Příklad s odepřením (deny) oprávnění

- Uživatel je členem skupin **A** a **B**

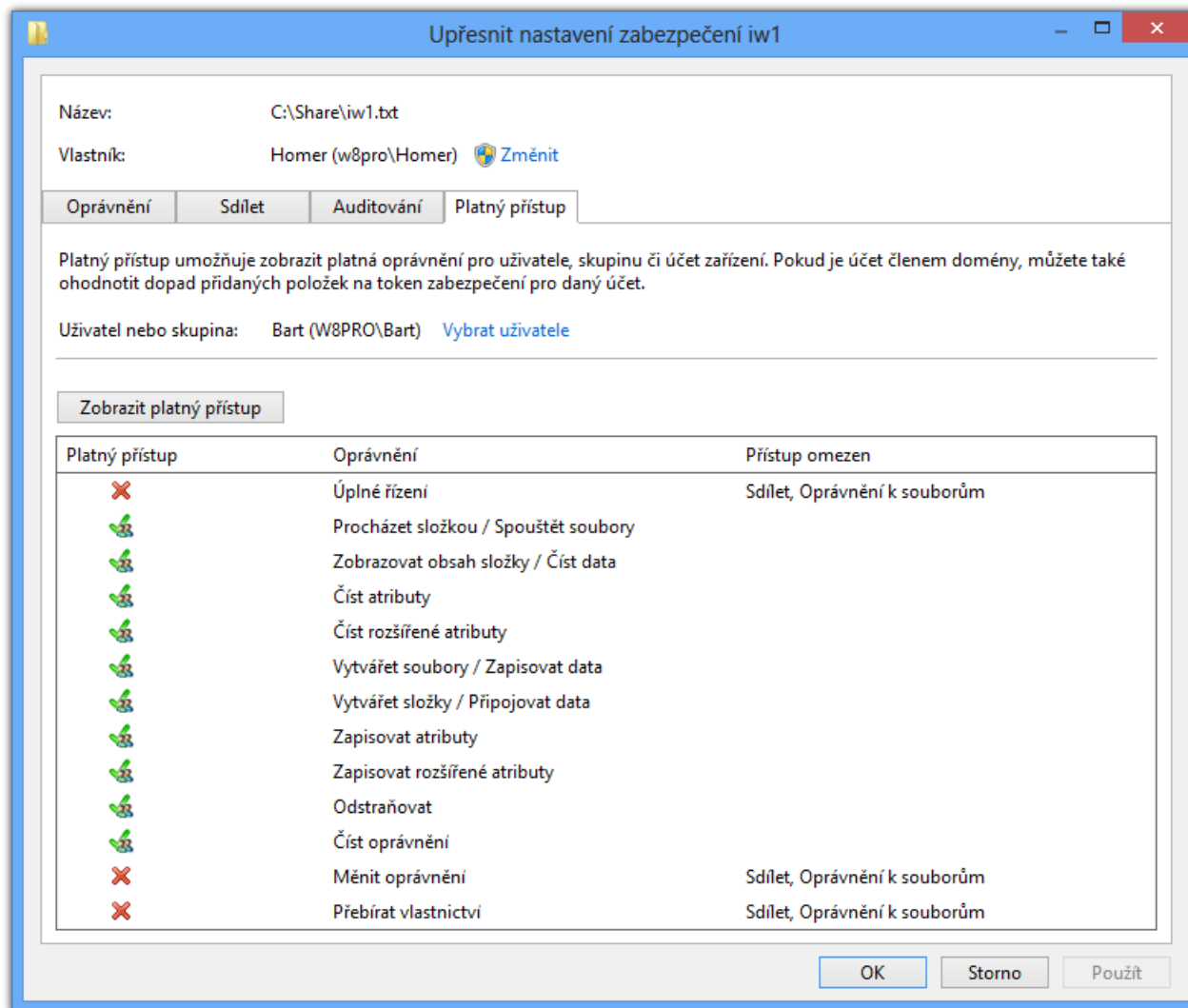


# Příklad se zděděnými oprávněními

- Uživatel je členem skupin **A** a **B**



# Zjištění výsledných NTFS oprávnění



# Kopírování a přesun

- Standardní chování

	V rámci stejného oddílu	Mezi různými oddíly	Na oddíl FAT/FAT32
<b>Přesun</b>	Zachovává oprávnění	Dědí oprávnění od cílového adresáře	Nezachovává oprávnění
<b>Kopírování</b>	Dědí oprávnění od cílového adresáře	Dědí oprávnění od cílového adresáře	Nezachovává oprávnění

- Při použití nástroje **robocopy**

	V rámci stejného oddílu	Mezi různými oddíly	Na oddíl FAT/FAT32
<b>Přesun</b>	Zachovává oprávnění	Zachovává oprávnění	Nezachovává oprávnění
<b>Kopírování</b>	Zachovává oprávnění	Zachovává oprávnění	Nezachovává oprávnění



# Správa pomocí příkazové řádky

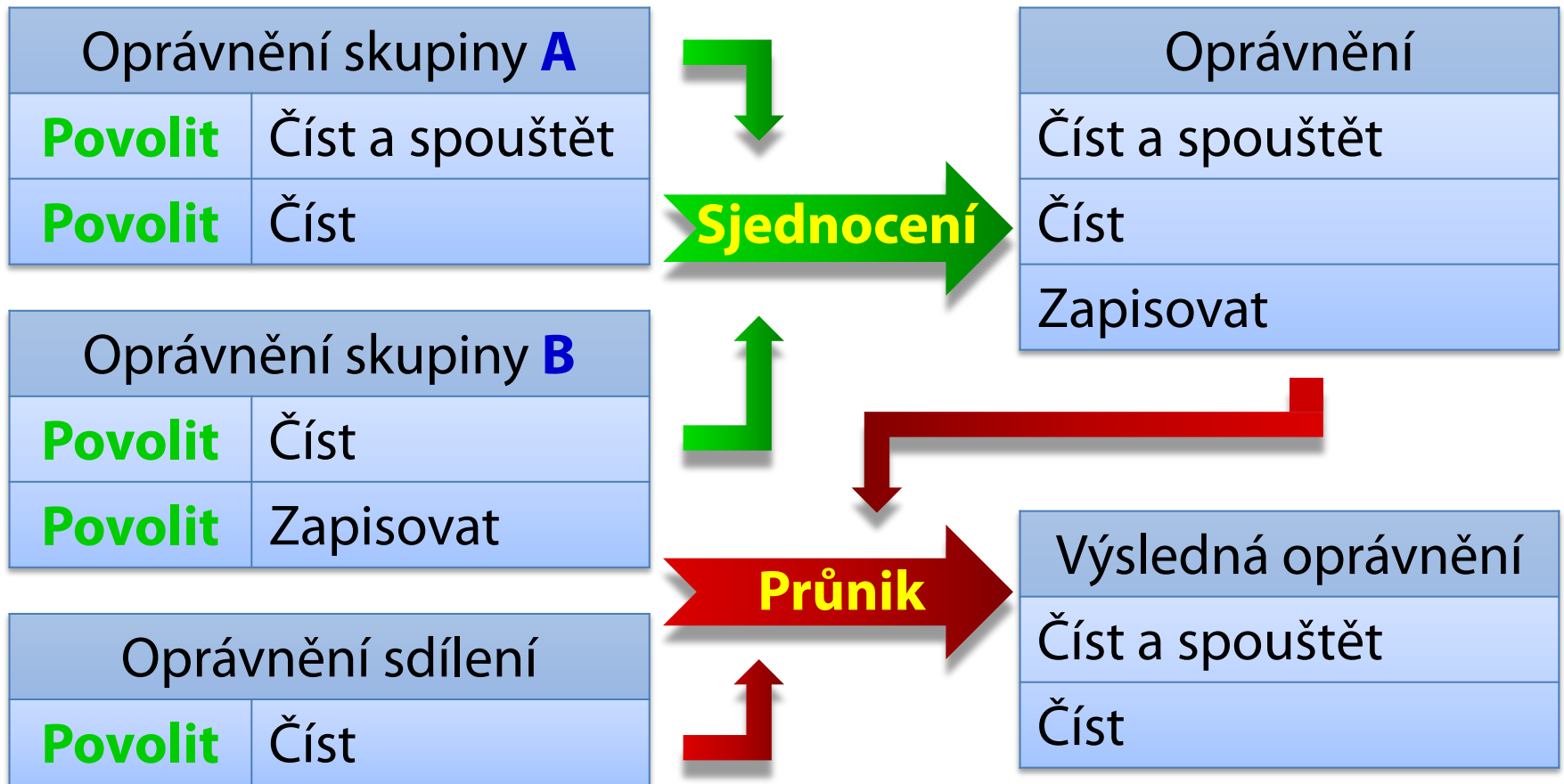
- **Výpis** NTFS oprávnění
  - `icacls <subor/adresář>`
- **Změna** NTFS oprávnění
  - **Povolení**
    - `icacls <subor/adresář> /grant <uživatel>:<oprávnění>`
  - **Odepření**
    - `icacls <subor/adresář> /deny <uživatel>:<oprávnění>`
  - Oprávnění mohou být jak **skupiny**, tak **konkrétní** NTFS oprávnění (odděleny čárkami a uvedeny v závorce)

# Vypočet oprávnění při přístupu ze sítě

- Ověřují se **oprávnění sdílení** i **NTFS oprávnění**
- Obecný algoritmus
  - 1) Vypočti množinu výsledných **oprávnění sdílení**
  - 2) Vypočti množinu výsledných **NTFS oprávnění**
  - 3) Vrať oprávnění obsažená v **obou** množinách

# Příklad s oprávněními sdílení (share)

- Uživatel je členem skupin **A** a **B**



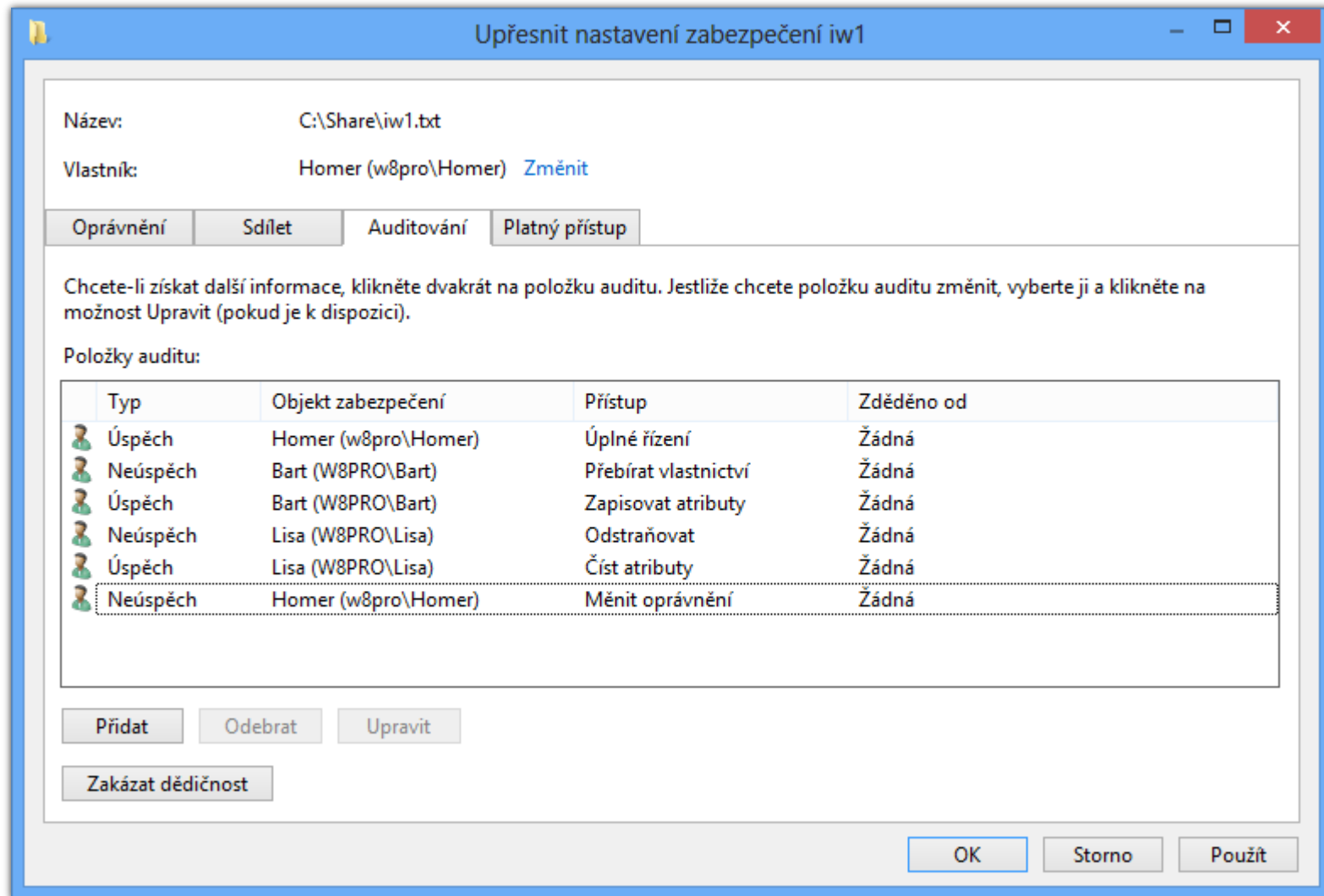
# Auditování přístupu k prostředkům

- Monitorování **přístupu** k souborům a adresářům
  - **Uložení** informací o přístupech v protokolu událostí (protokol **Zabezpečení**)
- **Povolení** v zásadách skupiny
  - Zásada **Auditovat přístup k objektům**
    - Od **Windows Vista** lze povolovat auditování jednotlivých typů objektů (musí se **explicitně** povolit)
  - Lze monitorovat **úspěšné** a/nebo **neúspěšné** pokusy
  - Pouze **umožňuje** monitorovat přístup k **souborům** a **adresářům** (**nespouští** monitorování)

# Nastavení auditování

- **Nastavení** ve vlastnostech jednotlivých souborů a adresářů (**spuštění** monitorování)
  - Výběr **oprávnění**, jejichž **aplikace** (čtení, zápis, apod.) má být monitorována a zaznamenána
  - Výběr **uživatelů** a **skupin**, kteří mají být monitorováni (pro monitorování **všech** uživatelů a skupin lze použít skupinu **Everyone**)

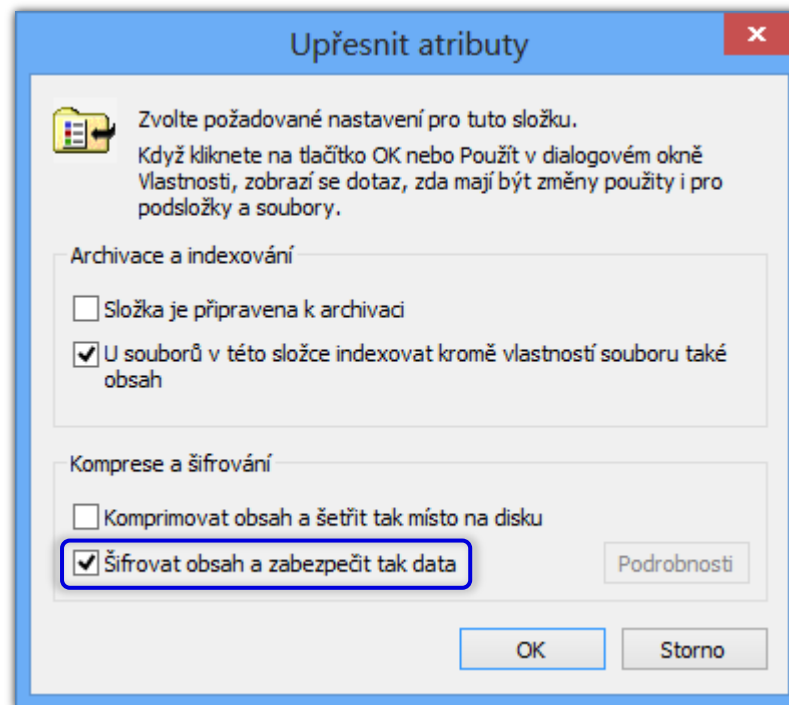
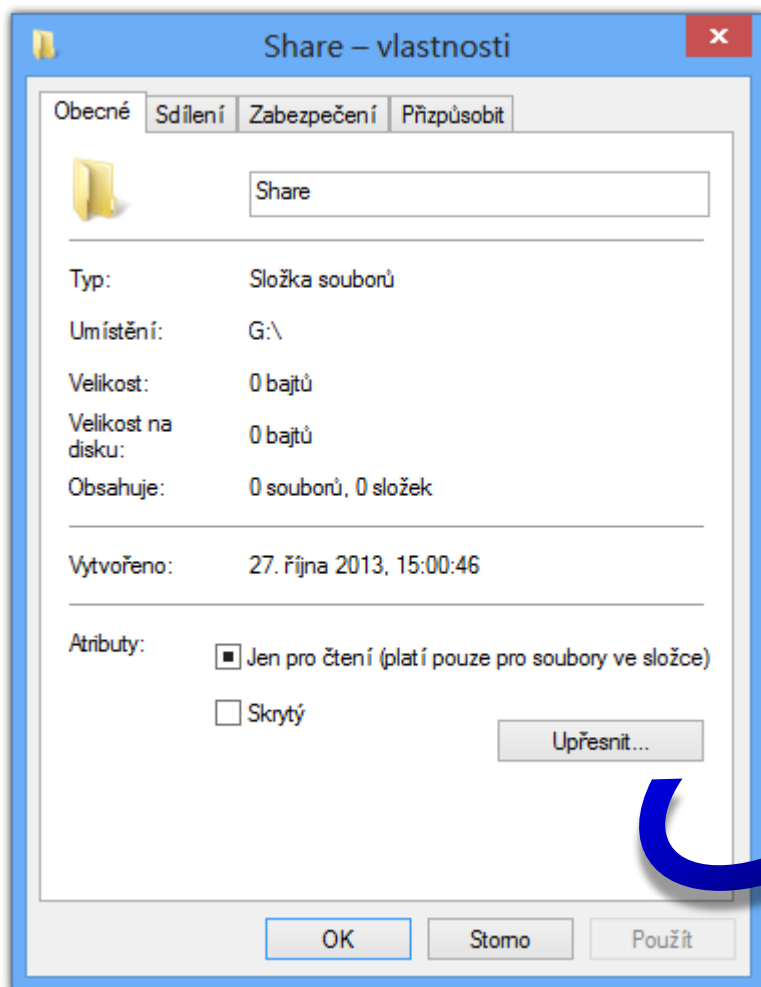
# Výběr monitorovaných oprávnění



# EFS (Encrypted File System)

- Pouze u edicí **Pro** a **Enterprise**
- Šifrování jednotlivých **souborů**
  - Zabezpečení na úrovni **dat**
  - Šifrování na úrovni **uživatele**
  - **Nelze** šifrovat systémové soubory
- Služba **souborového systému NTFS**
  - **Nelze** použít u souborových systémů FAT ani FAT32
- **Transparentní** uživateli
  - Práce s **šifrovanými** soubory stejná jako s normálními

# Šifrování obsahu souborů (a složek)





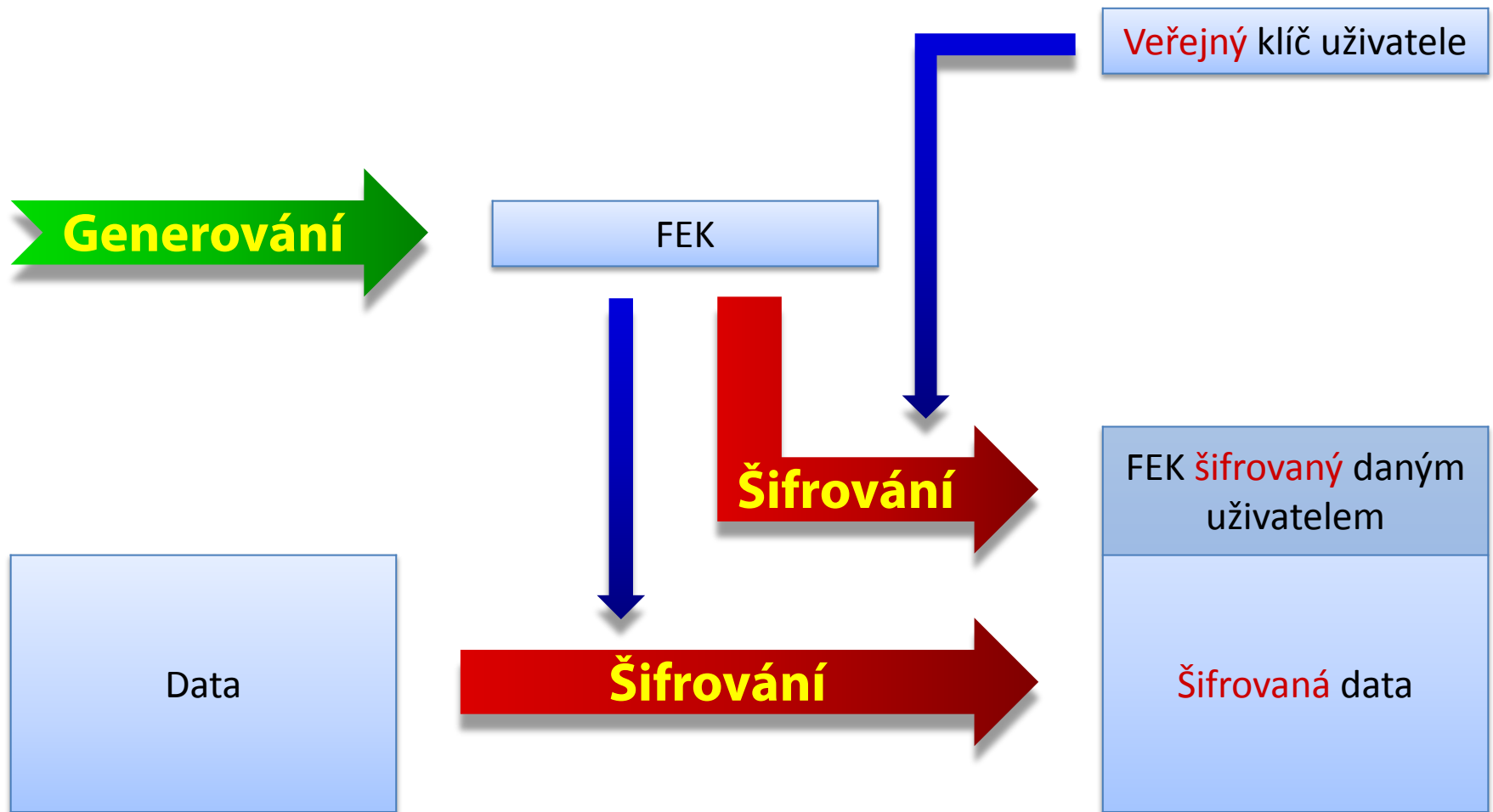
# Šifrování

- Založeno na hybridní kryptografii
  - Data šifrována (a dešifrována) **sdíleným** klíčem (FEK, *File Encryption Key*) pomocí **symetrické** kryptografie
  - FEK klíč šifrován **veřejným** (a dešifrován **privátním**) klíčem **uživatele** pomocí **asymetrické** kryptografie
- Výhody hybridní kryptografie
  - **Rychlé** šifrování dat (**symetrická** kryptografie)
  - **Bezpečné** sdílení FEK klíče (**asymetrická** kryptografie)
  - **Jednoduchá** (a také **efektivní**) realizace přístupu **více** uživatelů k šifrovaným souborům

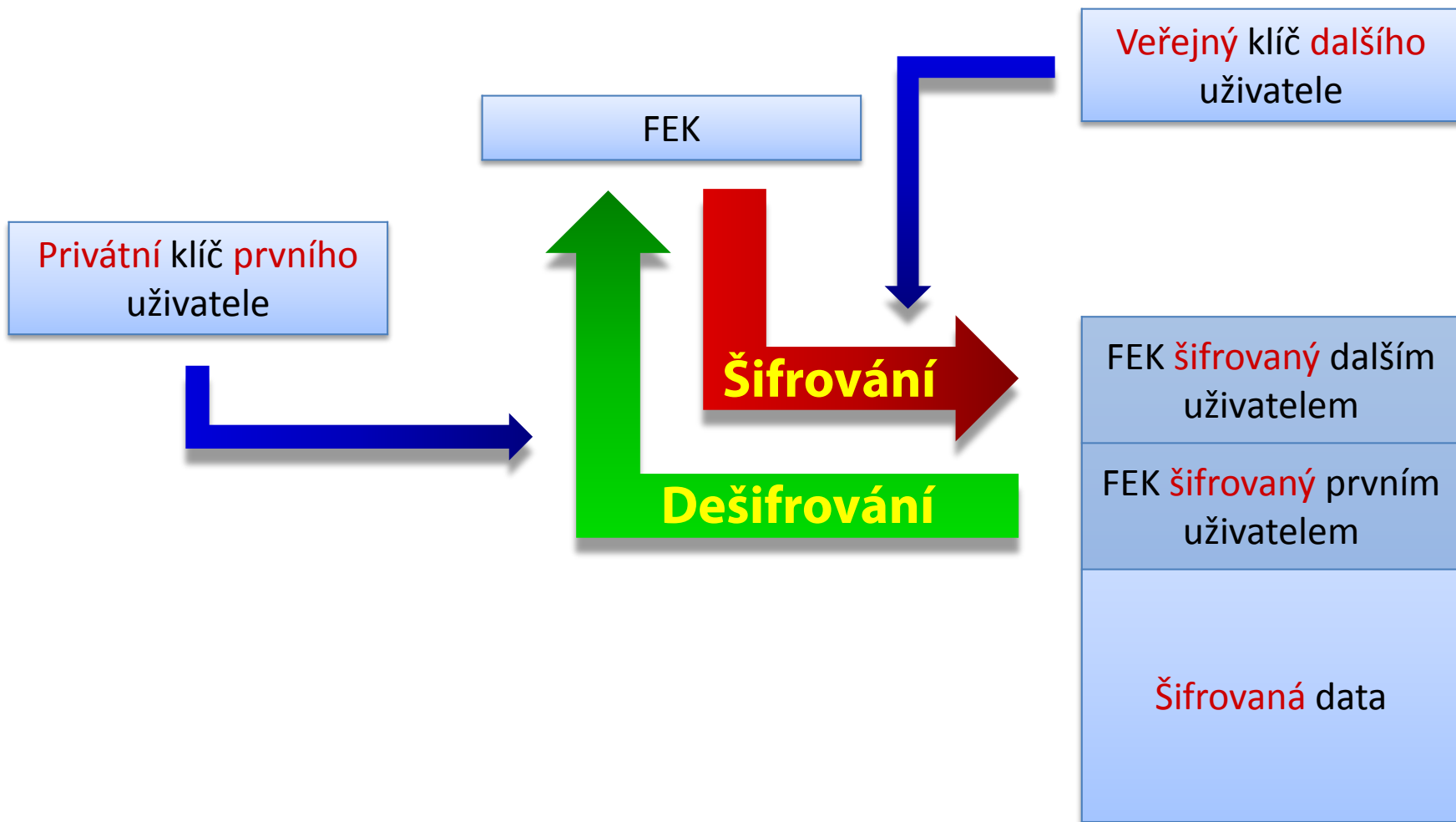
# Klíče

- FEK klíč (*File Encryption Key*)
  - Unikátní pro každý šifrovaný soubor
  - Generován při šifrování souboru prvním uživatelem
- Veřejný klíč (*public key*)
  - Uložen ve formě certifikátu v úložišti certifikátů
  - K dispozici všem uživatelům
- Privátní klíč (*private key*)
  - Uložen ve formě certifikátu v úložišti certifikátů
  - K dispozici pouze danému uživateli

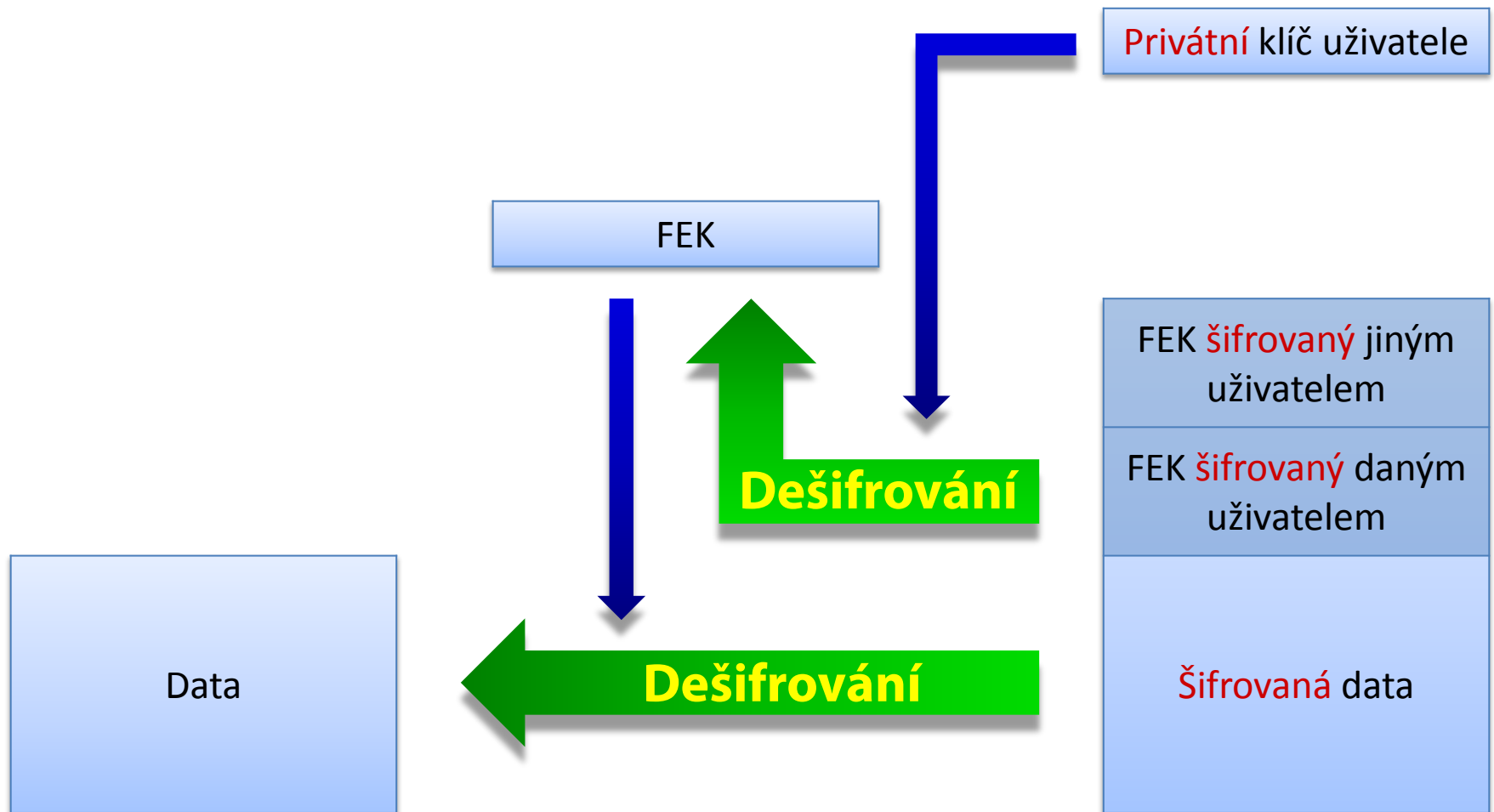
# Šifrování souboru prvním uživatelem



# Šifrování souboru dalším uživatelem



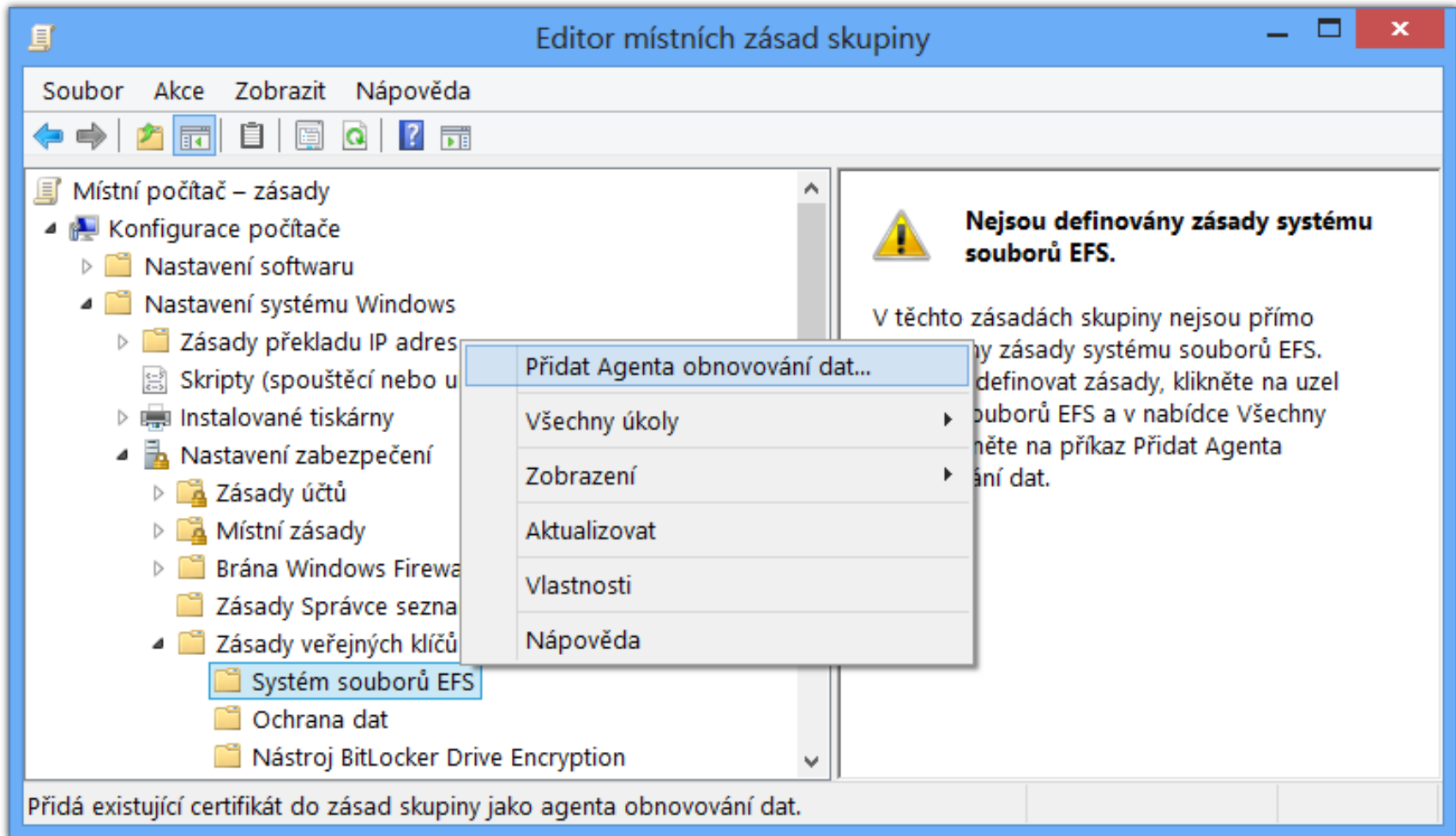
# Dešifrování souboru uživatelem



# Agent obnovení (RA, Recovery Agent)

- Umí **dešifrovat jakákoliv** data zašifrovaná pomocí **EFS** v době **po jeho vytvoření**
  - Při šifrování je FEK klíč (navíc) **automaticky** zašifrován pomocí **veřejného** klíče **agenta obnovení**
    - Zašifrování dříve vytvořených FEK klíčů pomocí **cipher /u**
- **Vytvoření** agenta obnovení
  - 1) Vygenerování **veřejného** a **privátního** klíče **agenta obnovení** (certifikátu) pomocí **cipher /r:<název>**
  - 2) Vytvoření **agenta obnovení** (RA) v **zásadách skupiny importováním** certifikátu obsahujícího **veřejný** klíč

# Vytvoření agenta obnovení



# BitLocker

- Pouze u edicí **Pro** a **Enterprise**
- Šifrování celých **oddílů disků**
  - Zabezpečení na úrovni **dat**
  - Šifrování na úrovni **počítače**
  - **Lze** šifrovat i systémový oddíl (systémové soubory)
- Chrání **integritu** operačního systému
  - Nemožnost **externí** modifikace systémových souborů
- Pro **šifrování** a **dešifrování** se používá **sdílený** klíč (FVEK, *Full Volume Encryption Key*)



# Základní pojmy

- TPM (*Trusted Platform Module*)
  - Speciální **čip** (většinou na základní desce) pro uložení celého (nebo části) **FVEK klíče**
- PIN (*Personal Identification Number*)
  - **Heslo** ověřované při **startu** počítače
  - Uloženo v **TPM čipu** nebo na **klíči pro start**
- Klíč pro start (*Startup key*)
  - **Zařízení USB** obsahující soubor s celým (nebo částí) **FVEK klíče** (tzv. *keying material*)

# BitLocker režimy

- Pouze TPM
- TPM + PIN
- TPM + Klíč pro start
- TPM + PIN + Klíč pro start
- BitLocker bez TPM

# Pouze TPM

- Klíč pro dešifrování dat je uložen na **TPM čipu**
  - **Nejméně** bezpečný režim (**celý** FVEK v TPM čipu)
- Plně **transparentní** uživateli
  - Dešifrování obsahu probíhá **automaticky**
- **Chrání** proti
  - Zpřístupnění dat při odcizení pevného disku
  - Změně nebo úpravám bootovacího prostředí
- **Nechrání** proti
  - Zpřístupnění dat při odcizení počítače

# TPM + PIN a/nebo klíč pro start

- Při použití TPM pouze s PINem
  - Uložení **celého** FVEK klíče i PINu v TPM čipu
- Při použití TPM s **klíčem pro start** a/nebo PINem
  - Uložení **½** FVEK klíče v TPM čipu a **½** na klíči pro start
  - Při použití PINu je PIN uložen na klíči pro start
- **Chrání** proti
  - Zpřístupnění dat při odcizení pevného disku
  - Zpřístupnění dat při odcizení počítače
  - Změně nebo úpravám bootovacího prostředí

# BitLocker bez TPM

- **Celý** FVEK klíč je uložen na **klíči pro start**
  - Klíč **není** nijak chráněn (**žádné** šifrování apod.)
- **Chrání** proti
  - Zpřístupnění dat při odcizení pevného disku
  - Zpřístupnění dat při odcizení počítače
- **Nechrání** proti
  - Změně nebo úpravám bootovacího prostředí

# Dešifrování oddílu (při použití TPM)

- 1) Aktualizace PCR registrů TPM čipu
- 2) Dešifrování (celého nebo ½) FVEK klíče pomocí klíče daného obsahem PCR registrů TPM čipu
  - Při jakékoliv změně bootovacího prostředí (procesu bootování) nebude možné FVEK klíč dešifrovat
- 3) Doplnění 2. ½ FVEK klíče z klíče pro start
- 4) Ověření PINu
- 5) Dešifrování obsahu oddílu disku pomocí FVEK klíče

# Agent obnovení (Recovery Agent)

- Umí **dešifrovat** oddíly disku zašifrované pomocí technologie **BitLocker**
- Založen na **certifikátech**
  - Importování certifikátu s **veřejným** klíčem, jenž bude použit pro **zašifrování** FVEK klíče, v **zásadách skupiny**
  - Zašifrovaný VFEK klíč je uložen na **šifrovaném** oddíle
- **Obnovení** dat
  - **manage-bde.exe -unlock <oddíl> -Certificate -ct <otisk> [-PIN]**

# BitLocker To Go

- BitLocker umožňující šifrování oddílů **USB disků**
- Lze **nastavit** v edicích **Pro** a **Enterprise**
  - **Číst** a **zapisovat** lze ve všech edicích **Windows 7/8/10**
  - U předchozích verzí systému **Windows** lze pouze **číst** (vyžaduje **BitLocker To Go Reader**)
- Data chráněná **heslem** nebo **čipovou kartou**
  - Nepotřebuje **TPM** čip
- Možnost zakázat **zápis** na USB disky **nechráněné** technologií **BitLocker**