Poinstalační nastavení OS

OPERAČNÍ SYSTÉM WINDOWS

Poinstalační nastavení OSW

1. Základní nastavení
    1. Zabezpečit účet Administrátor !!!
    2. Nastavení Řízení uživatelských účtů (User Account Control)
    3. Aktualizace OS (Windows update)
    4. Základní bezpečnostní nastavení (Defender, FireWall)
    5. Instalace všech potřebných aplikací
    6. Základní vyčištění systému
    7. Systém Bodu Obnovení (SBO)

Poinstalační nastavení OSW

2. Rozšířené nastavení
   1. Oddělení systému od uživatelských dat
   2. Nastavení politiky uživatelských účtů
   3. Zásady omezení software
   4. Základní záloha „čistého“ systému
3. Speciální nastavení
   1. Služby a aplikace při spuštění OSW
   2. Optimalizace pro SSD
   3. RAM disk (cache, temp)
   4. FireWall

Nastavení UAC

1.1) Zabezpečení účtu **Administrátor**:

- nejrychlejší: spustit **CMD.exe**
  - Spustit s právy Správce
- Příkaz: **net user administrator heslo**

```
C:\Windows\system32>net user administrator jupíčerte
```

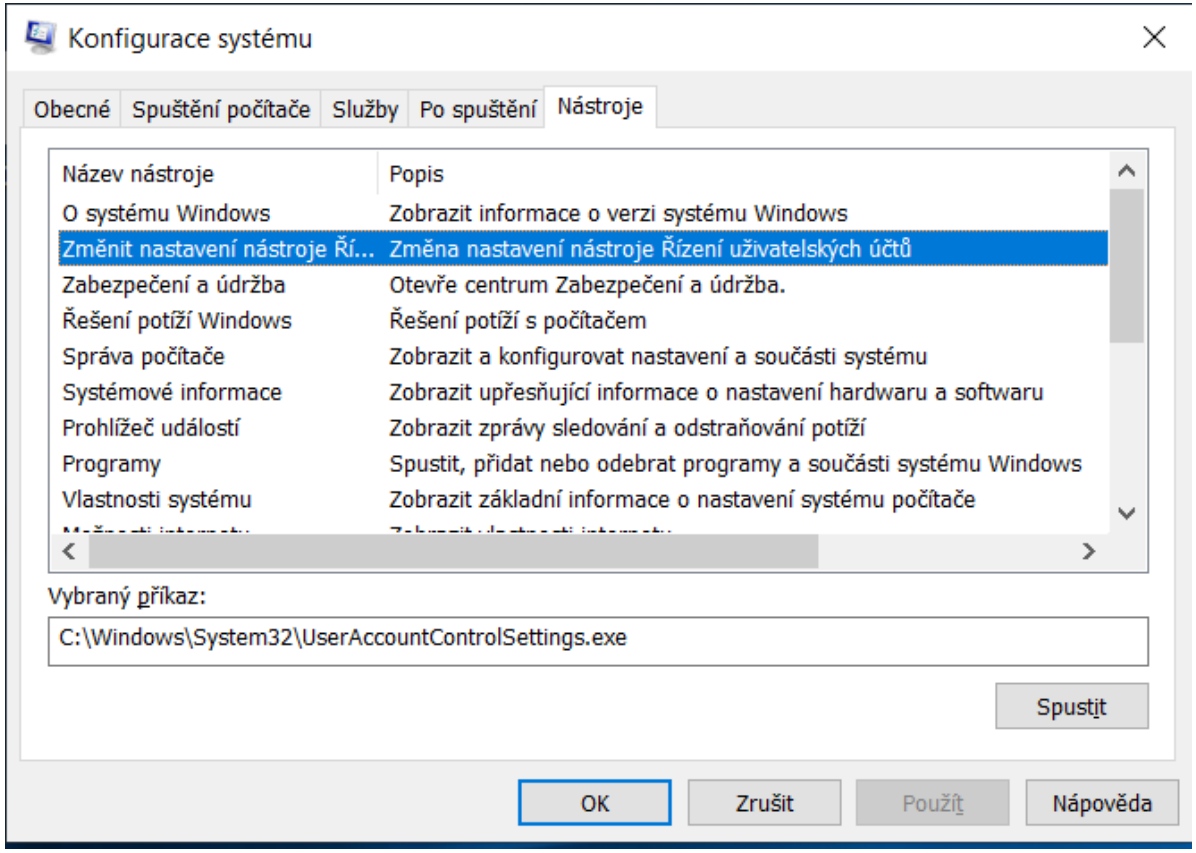
- nebo: **control userpasswords2**
  - resetovat heslo

Nastavení UAC

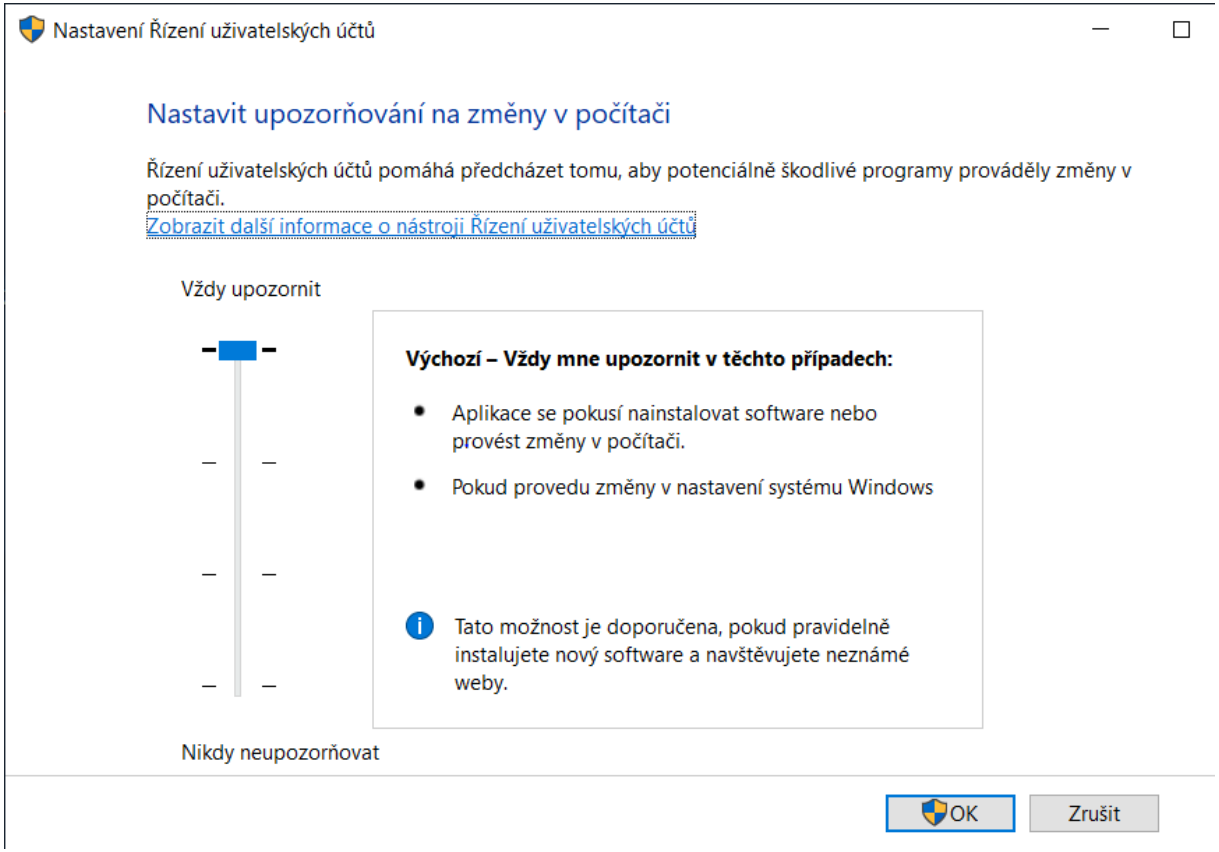
1.2) funkce **Řízení uživatelských účtů**:

- spustit **msconfig**
  - Záložka Nástroje – Změnit nastavení nástroje Řízení…
- nebo přímo **UserAccountControlSettings.exe**
  - Spustit s právy Správce
- nebo vyhledávání – **Řízení…**
- nebo vyhledávání – **Zabezpečení a údržba**

Nastavení UAC



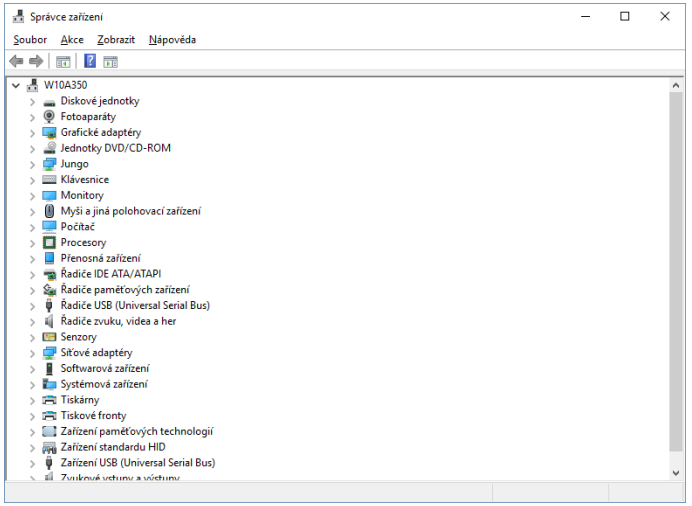
Nastavení UAC – max. úroveň



Aktualizace systému

1.3 Windows Update:

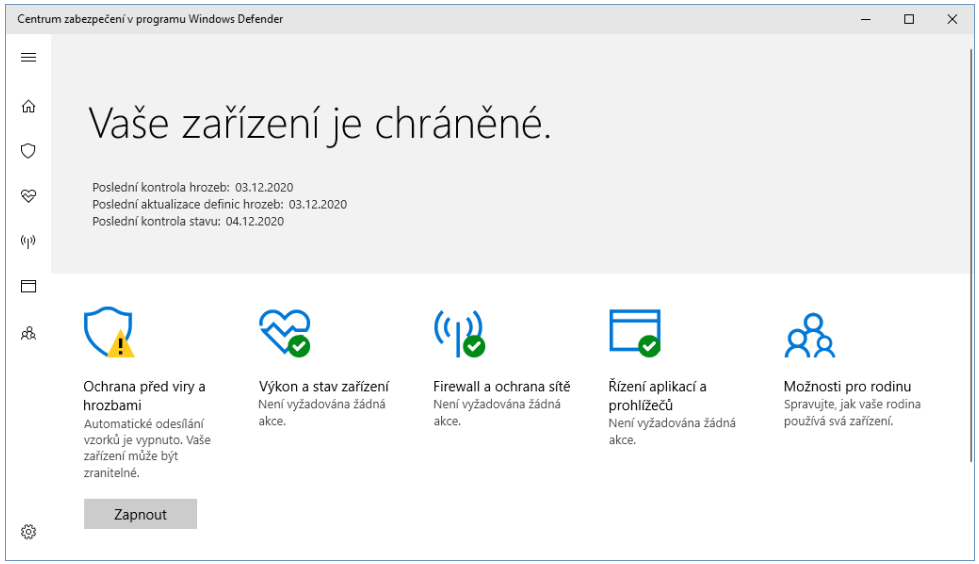
- Provést kompletní aktualizaci OS:
  - Zkontrolovat funkčnost HW driverů
  - **Systém -> Správce zařízení**
  - Doinstalovat konfliktní drivery (označeny žlutým trojúhelníkem)



Ochrana systému

1.4 Windows Defender:

- Provést kontrolu ochrany OS:
  - Zapnout Firewall, aktualizovat antivirovou databázi
  - **Centrum zabezpečení…**



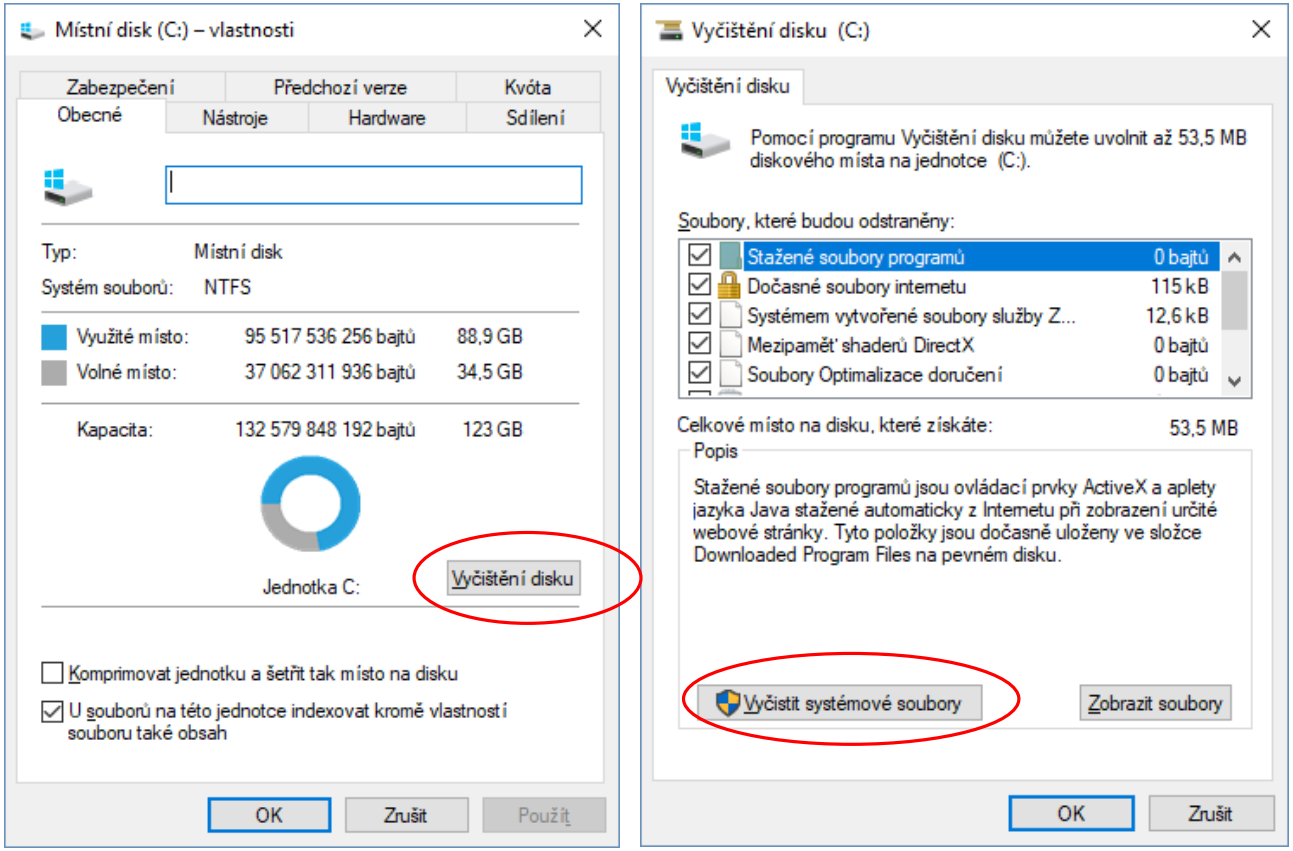
Aplikace, údržba

1.5 Instalace všech potřebných aplikací:

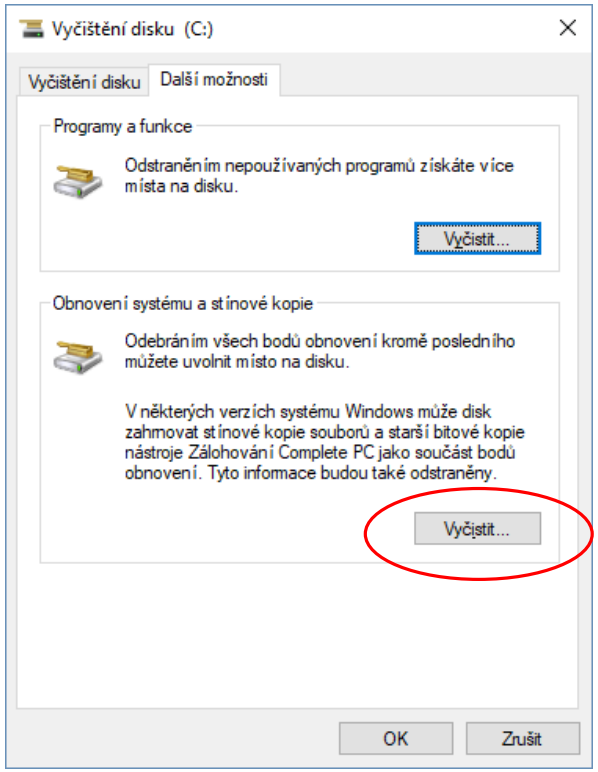
1.6 vyčištění systému:

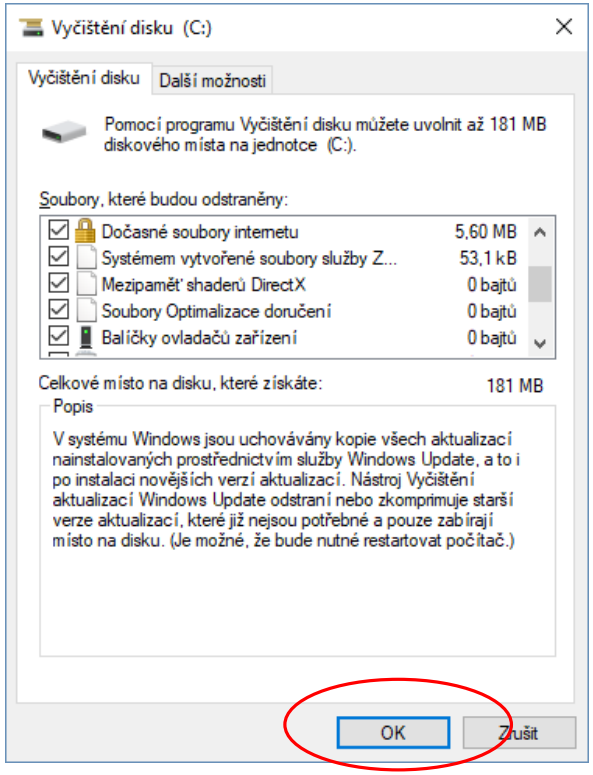
- Odstranění nepotřebných souborů:
  - Tempy, cache, instalační balíky Windows Update, logy…
  - **Disk s OS -> Vlastnosti -> Vyčištění disku**

Údržba - vyčištění



Údržba - vyčištění



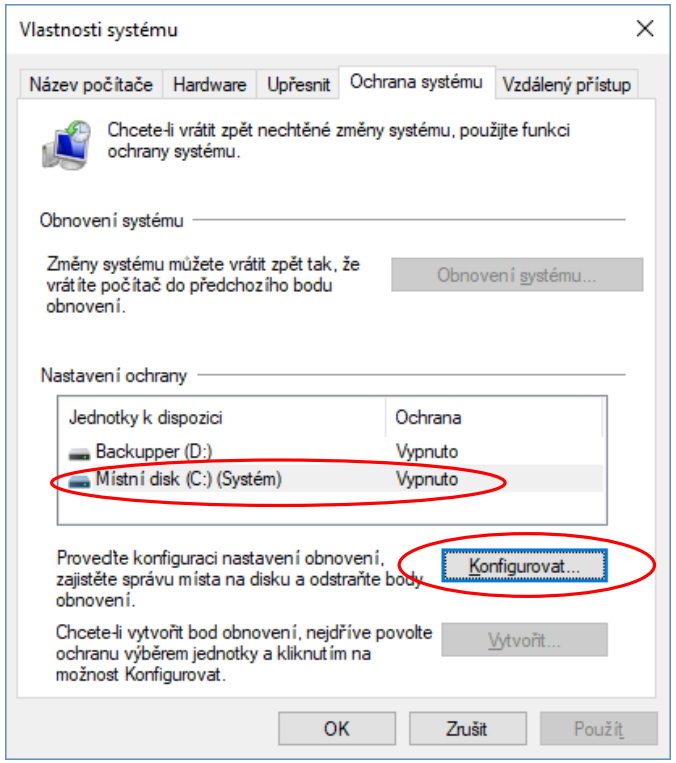


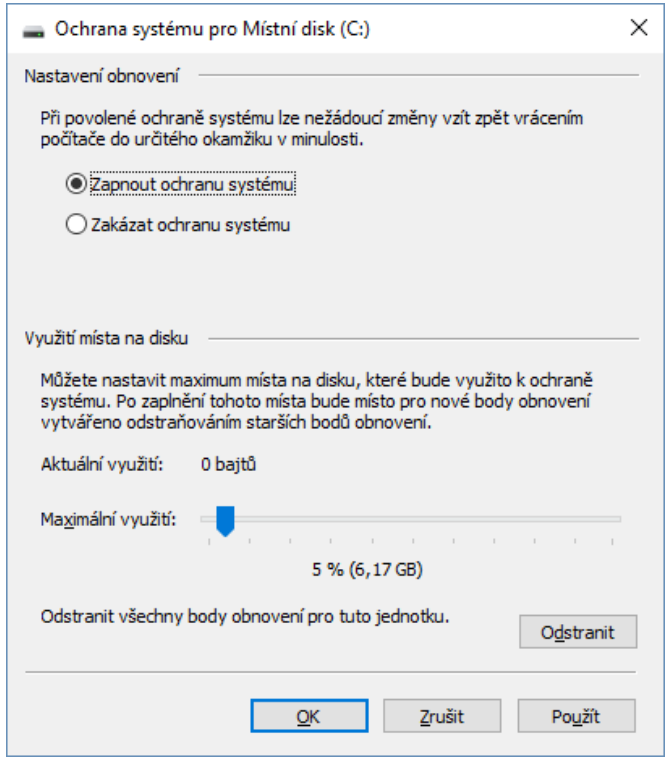
Systém Bodu Obnovení

1.7 SBO:

- Nejjednodušší obnova OS:
  - Před každou instalací čehokoliv, aktualizací… je zaevidován stav OS a uložen do „skryté složky“
  - V případě havárie systému můžeme OS obnovit do stavu před konfliktem (výběrem libovolného bodu obnovy dle data)
  - SBO musí být aktivován (zkontrolujeme popř.aktivujeme)
  - **Systém -> Upřesnit nastavení … -> Ochrana systému**

Systém Bodu Obnovení





Rozšířené nastavení OSW

2.1 Oddělení systému od uživatelských dat:

- Adresář Users na jiný oddíl/disk - výhody:
  - Lze odděleně zálohovat samotný systémový disk od uživatelských dat (systém + nainstalované programy)
  - nebo zálohovat průběžně jen uživatelská data (úspora místa – nemusíme zálohovat celý počítač)
  - Lze lépe ochránit systémový disk před „nedostatkem místa“
  - Před obnovou poškozeného systému máme důležitá data a nastavení uživatelských účtů „mimo“ systémový disk… poškozený systémový disk „rychle obnovíme“ např. z bitové kopie

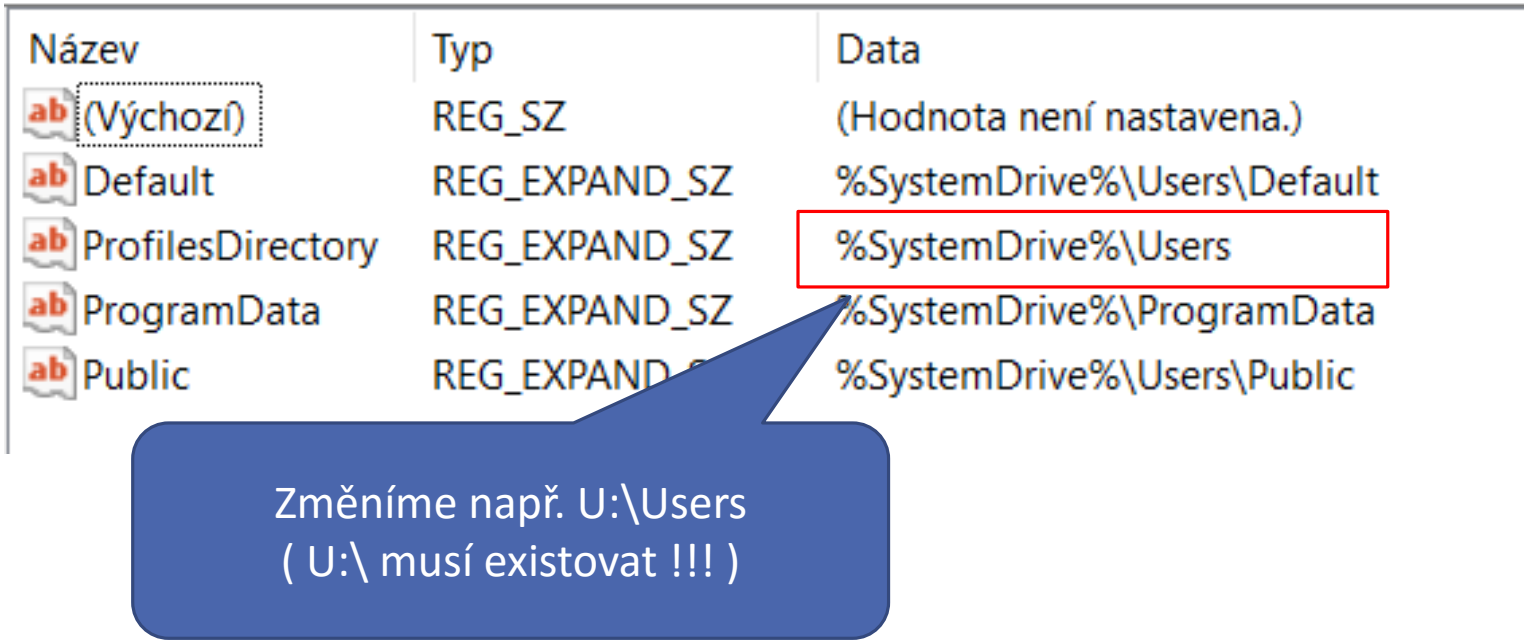
Rozšířené nastavení OSW

2.1 Oddělení systému od uživatelských dat:

- Úpravu provedeme v registrech:
  - Provádíme po instalaci OS a všech potřebných aplikací
  - Provádíme před vytvořením uživatelských účtů
  - Na novém disku systém vytvoří adresář Users
    - pro všechna data a nastavení budoucích účtů
    - !!! už existující účty budou mít data stále v „C:\Users“ !!!
- Klíč:
  - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList

Rozšířené nastavení OSW

2.1 Oddělení systému od uživatelských dat:



Rozšířené nastavení OSW

2. Nastavení politiky uživatelských účtů

1. Program konzole: gpedit.msc
2. Program konzole: secpol.msc

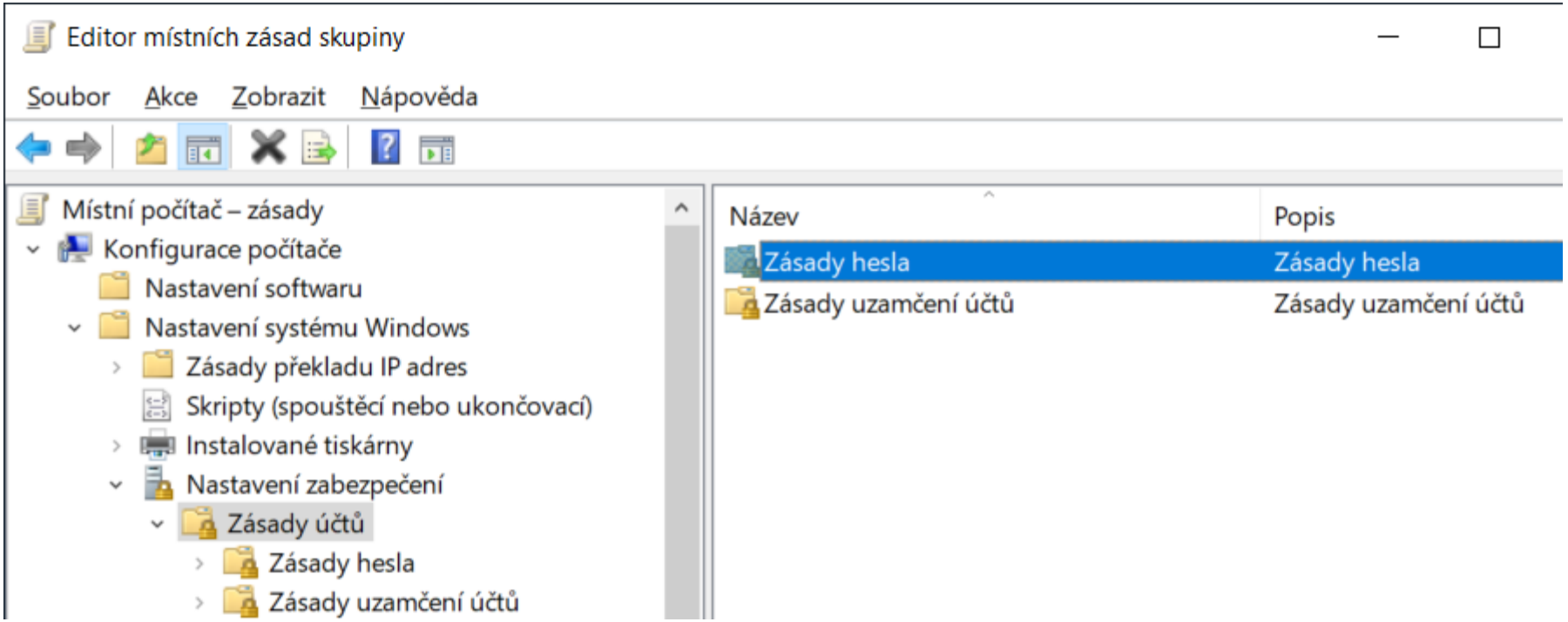
Základní pravidla pro hesla/účty:

Pro firemní PC

- složitost/stáří hesel…, počet neplatných pokusů
- uzamčení účtů (neplatné pokusy)
- audity (záznamy pokusů/změn – logy)
- … apod.

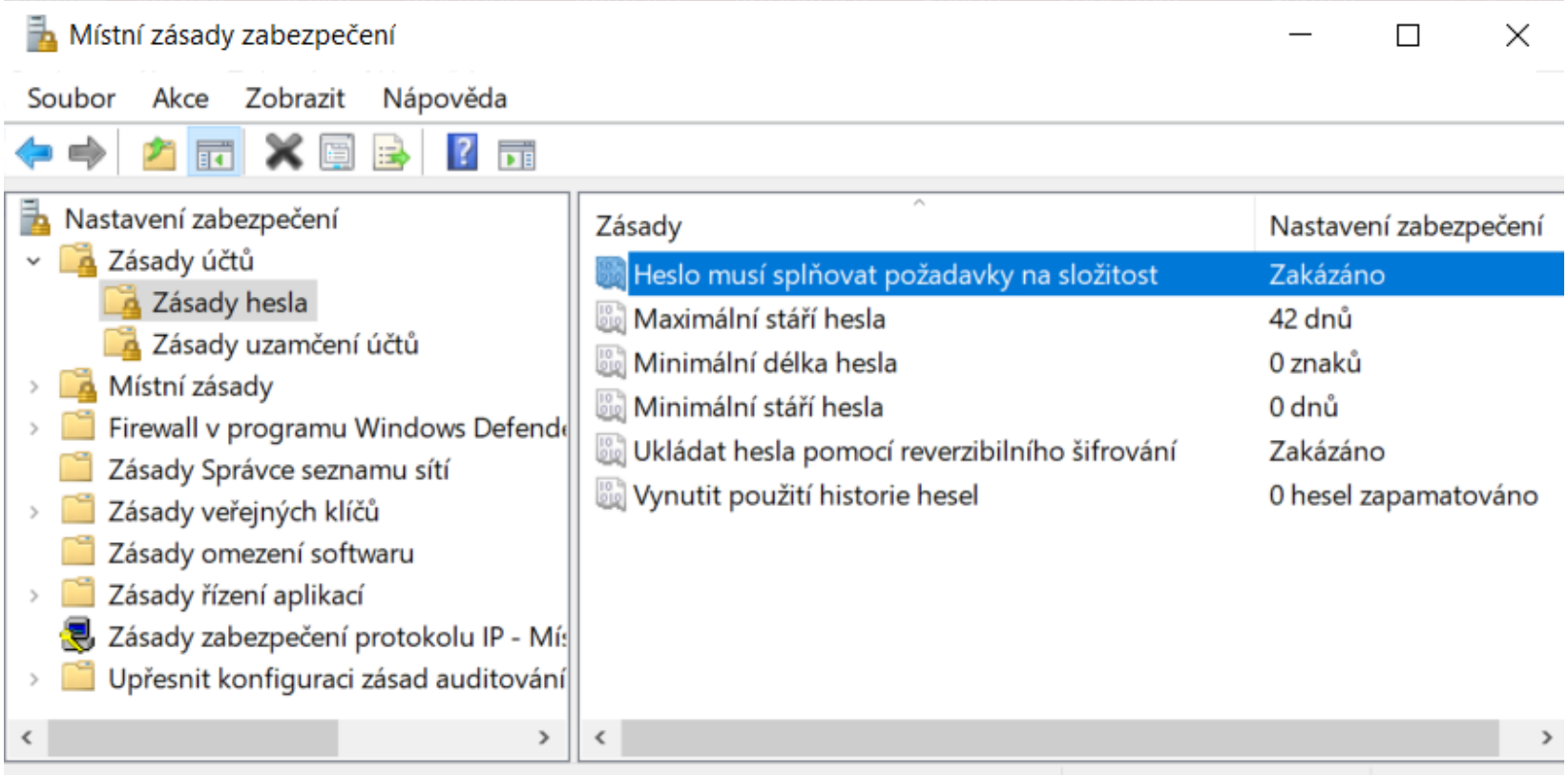
Rozšířené nastavení OSW

2. Vyhledat: **gpedit.msc** (spustit jako správce)



Rozšířené nastavení OSW

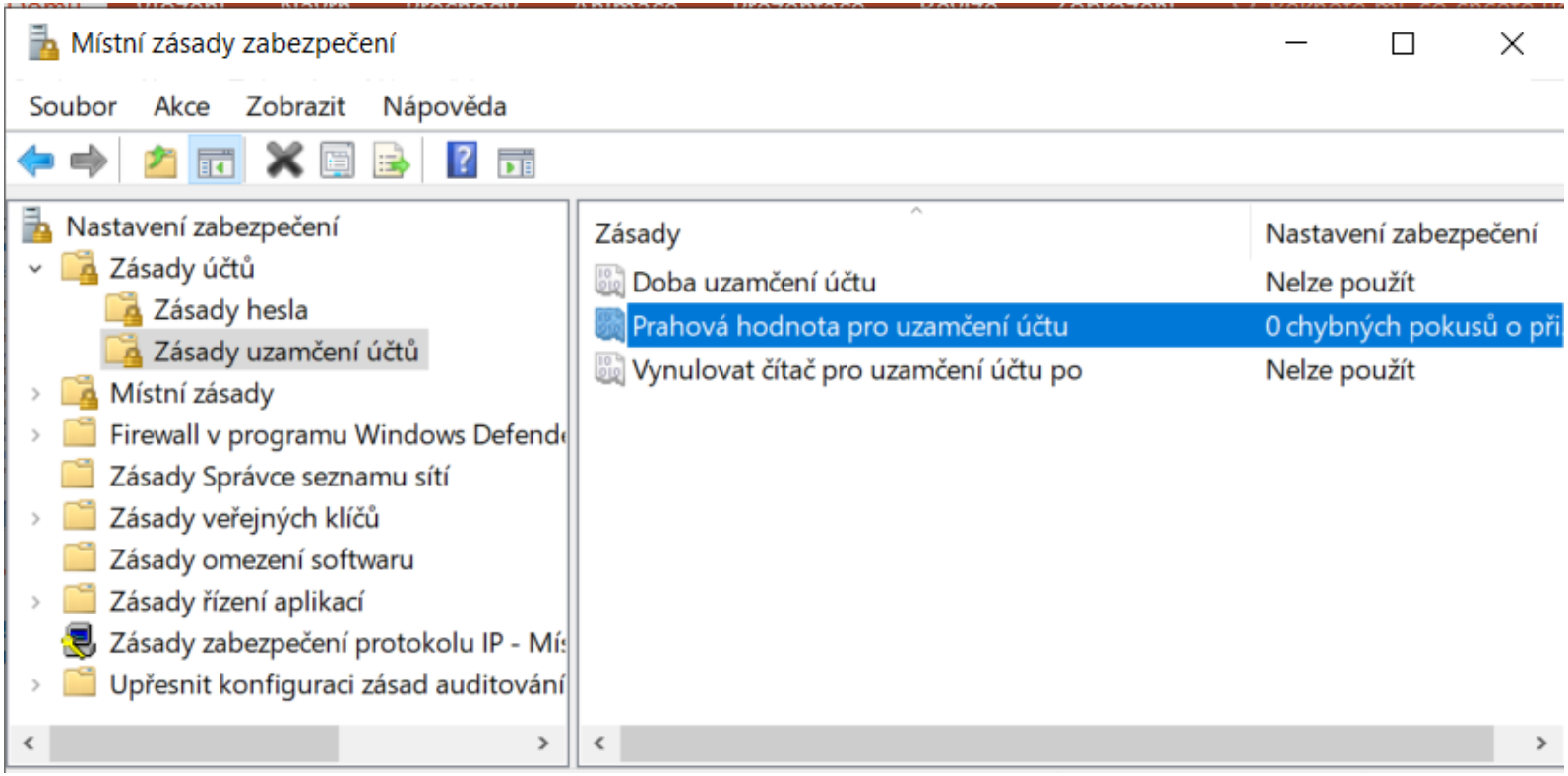
2. Vyhledat: **secpol.msc** (spustit jako správce)



Rozšířené nastavení OSW

- Heslo musí splňovat požadavky na složitost:
  - Př: **aHo1jV@claVe** (malá/velká písmena, čísla, znaky…)
- Minimální stáří hesla
  - Po vypršení – zadat při přihlášení původní a nové heslo
- Minimální délka hesla
  - Minimum: 8 a více znaků !!!
- Minimální stáří hesla
  - Doba platnosti „defaultního“ hesla zadaného správcem
  - 0: ihned, po vypršení – změnit při přihlášení na nové heslo
- Ukládat hesla pomocí reverz….
  - Pro aplikace vyžadující hesla (nezašifrovíno!!!!)
- Vynutit použití historie hesel
  - Zamezit opakování např. 2 hesel (počet odlišných hesel)

Rozšířené nastavení OSW

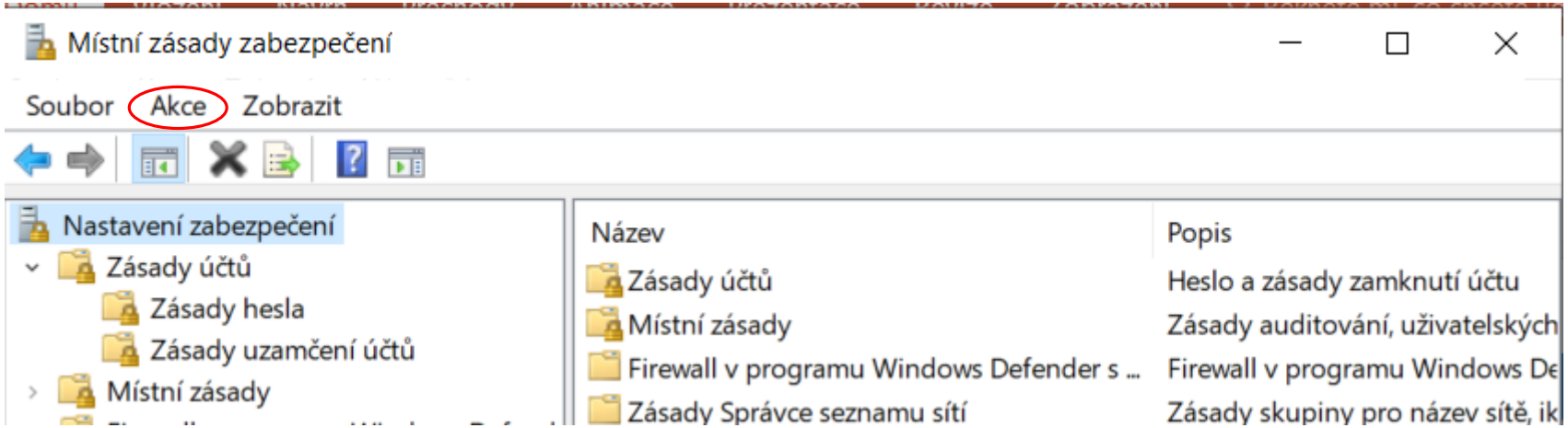


Rozšířené nastavení OSW

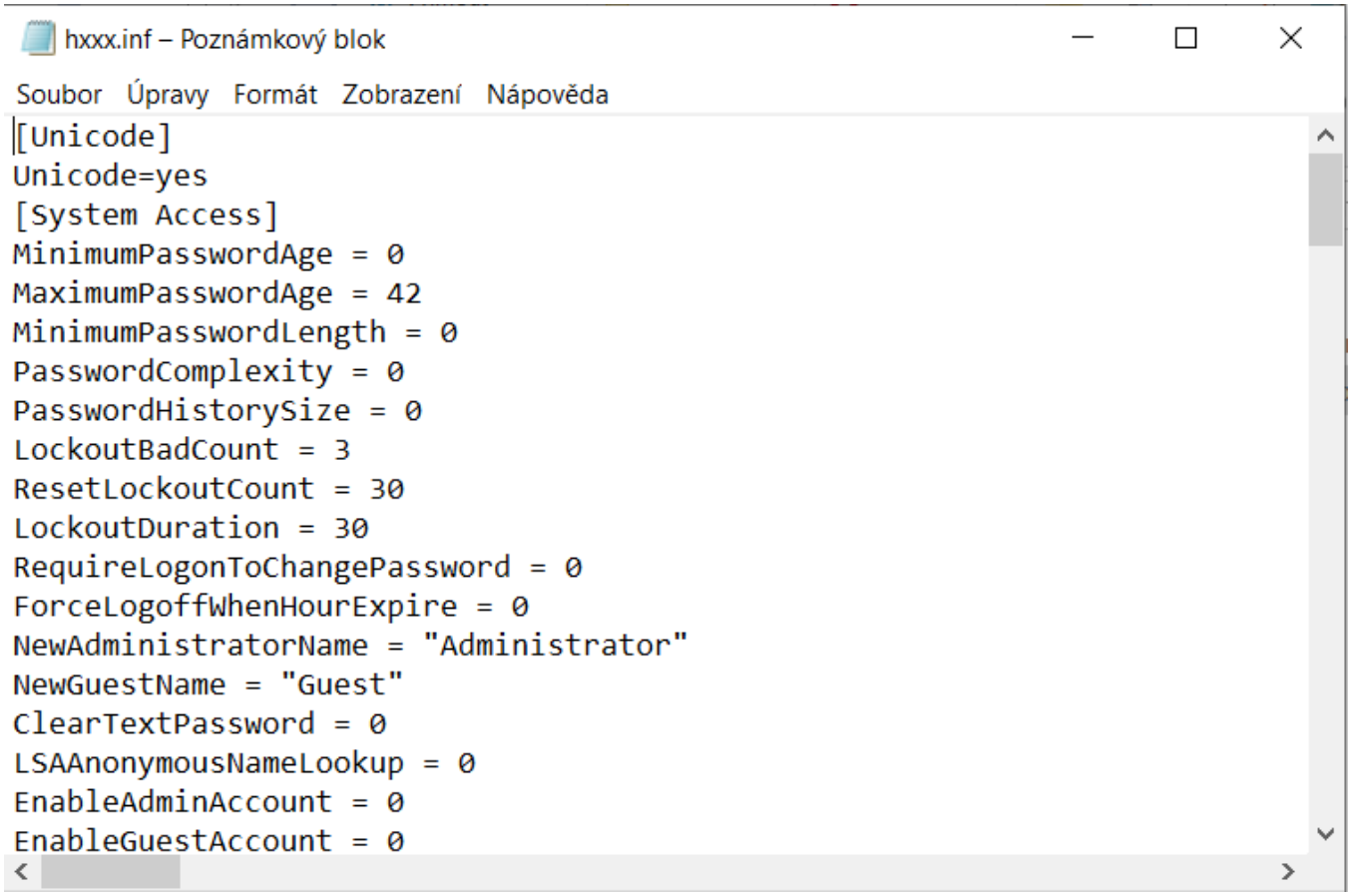
- Nejprve nastavit „Prahovou hodnotu…“
  - Vyčerpáním pokusů je lokální/doménový účet zablokován
  - Platí i pro CTRL+ALT+DEL, odhlášení
  - Platí i pro spořič obrazovky (je-li nastaveno heslo)
  - Lze pokusy logovat (viz položka **Místní zásady**…)

Rozšířené nastavení OSW

- Export/Import zásad (menu: Akce)
  - Nastavíme veškeré zásady na prvním PC
  - Exportujeme do souboru *.inf
  - Na druhém počítači importujeme ze souboru *.inf



Rozšířené nastavení OSW



Rozšířené nastavení OSW

3. **Nastavení Zásad omezení software**

   Software Restriction Policies (SRP):

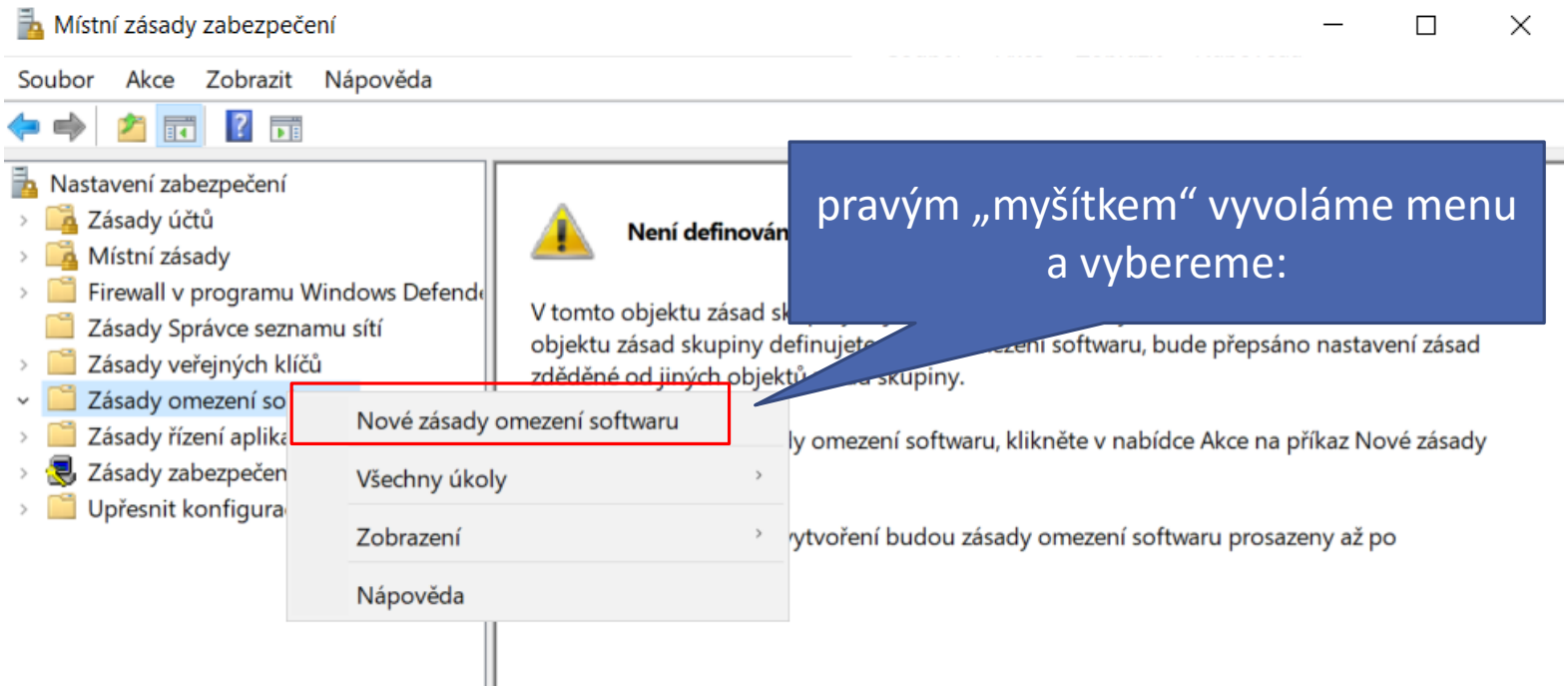
- účinná ochrana před neznámým malware
- funkční pouze v účtech Standardní uživatel
- zakáže spustit neověřený SW
  - ověřený SW – nainstalovaný administrátorem
  - Veškeré spustitelné soubory
  - *.exe, *.dll, skripty, makra, …

Rozšířené nastavení OSW

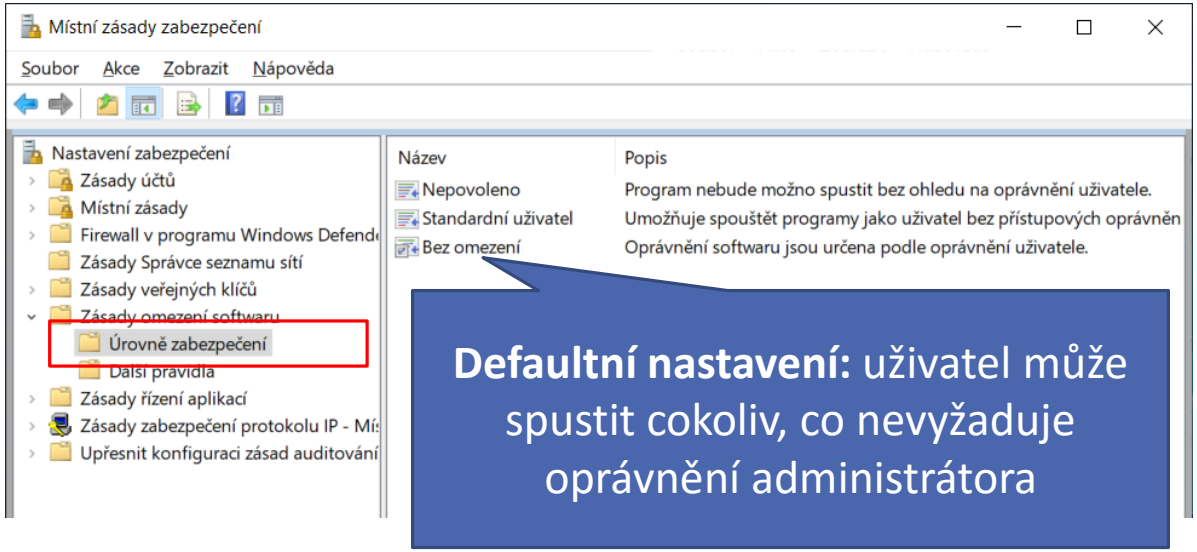
Software Restriction Policies (SRP):

- Standardní uživatel nespustí:
  - jakýkoliv „portable“/ instalační program z SSD/HDD
  - programy z USB/CD/DVD
  - falešné přílohy emailu …
  - skript…
  - neověřený SW - jen s právy administrátora
    (pokud to dovolíme)

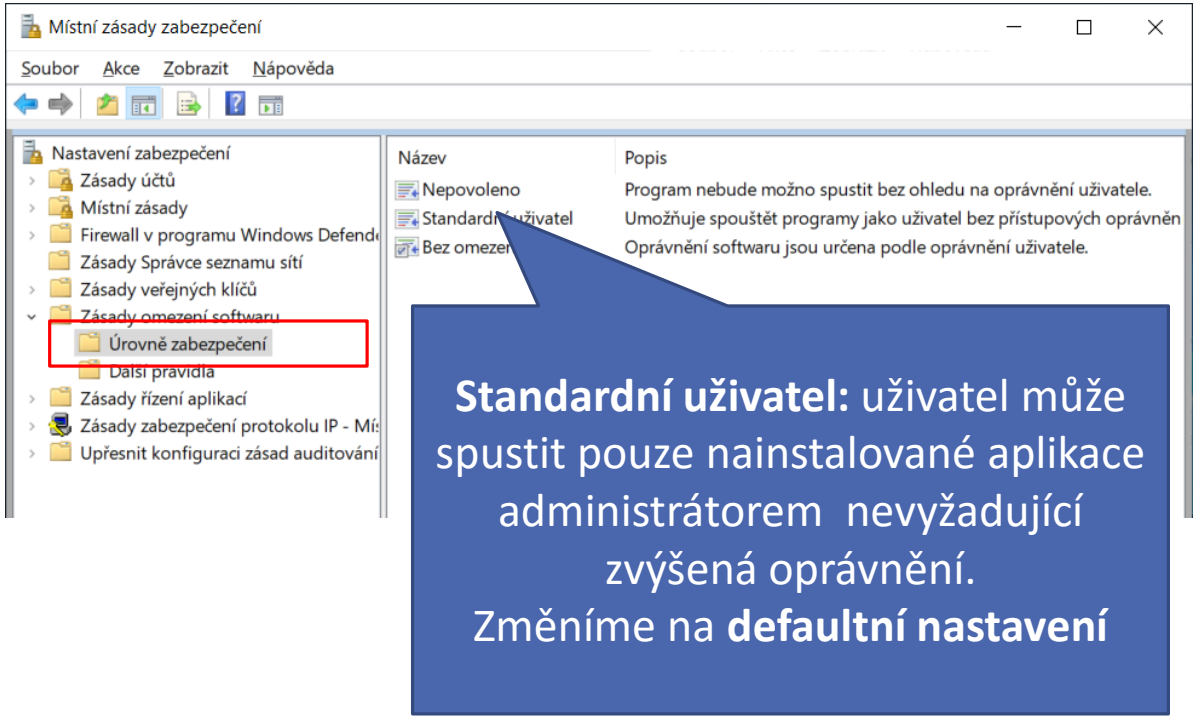
Rozšířené nastavení OSW



Rozšířené nastavení OSW

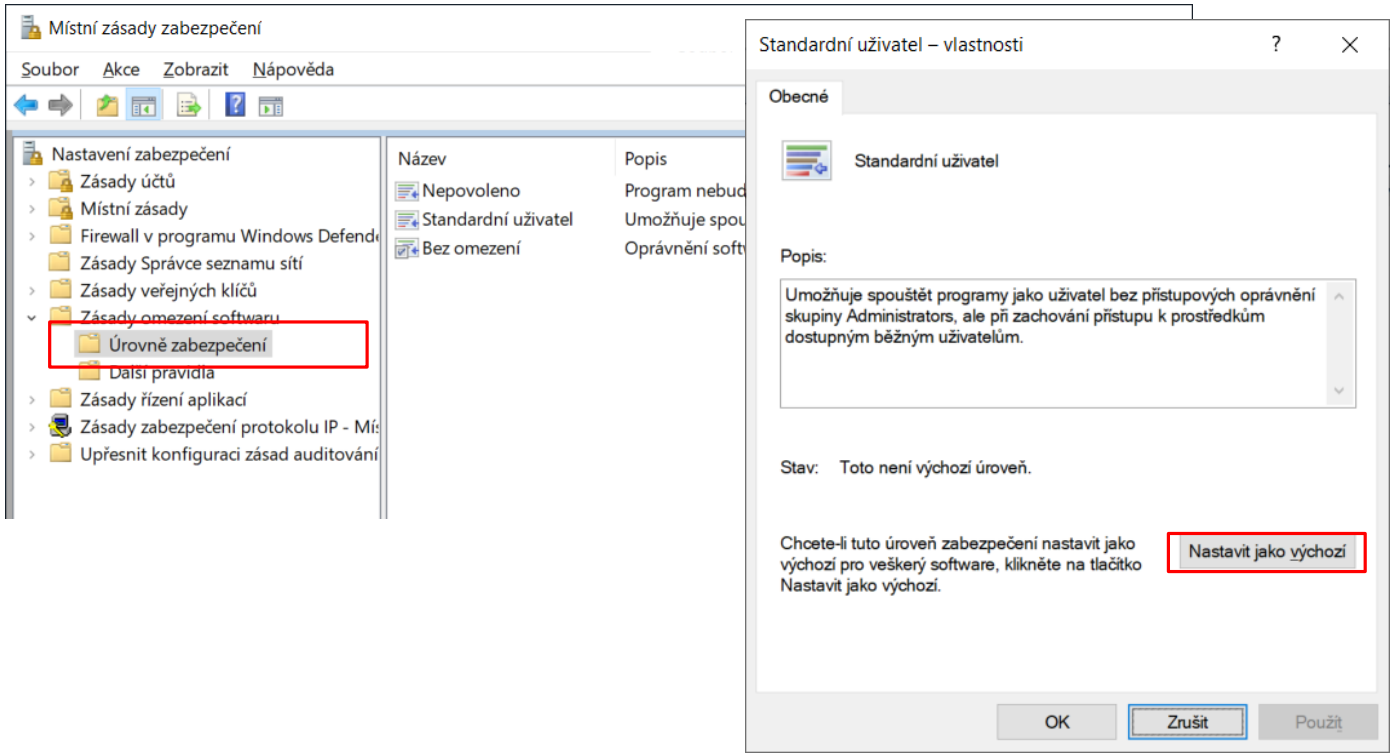


Rozšířené nastavení OSW



Standardní uživatel: uživatel může spustit pouze nainstalované aplikace administrátorem nevyžadující zvýšená oprávnění.
Změníme na **defaultní nastavení**

Rozšířené nastavení OSW

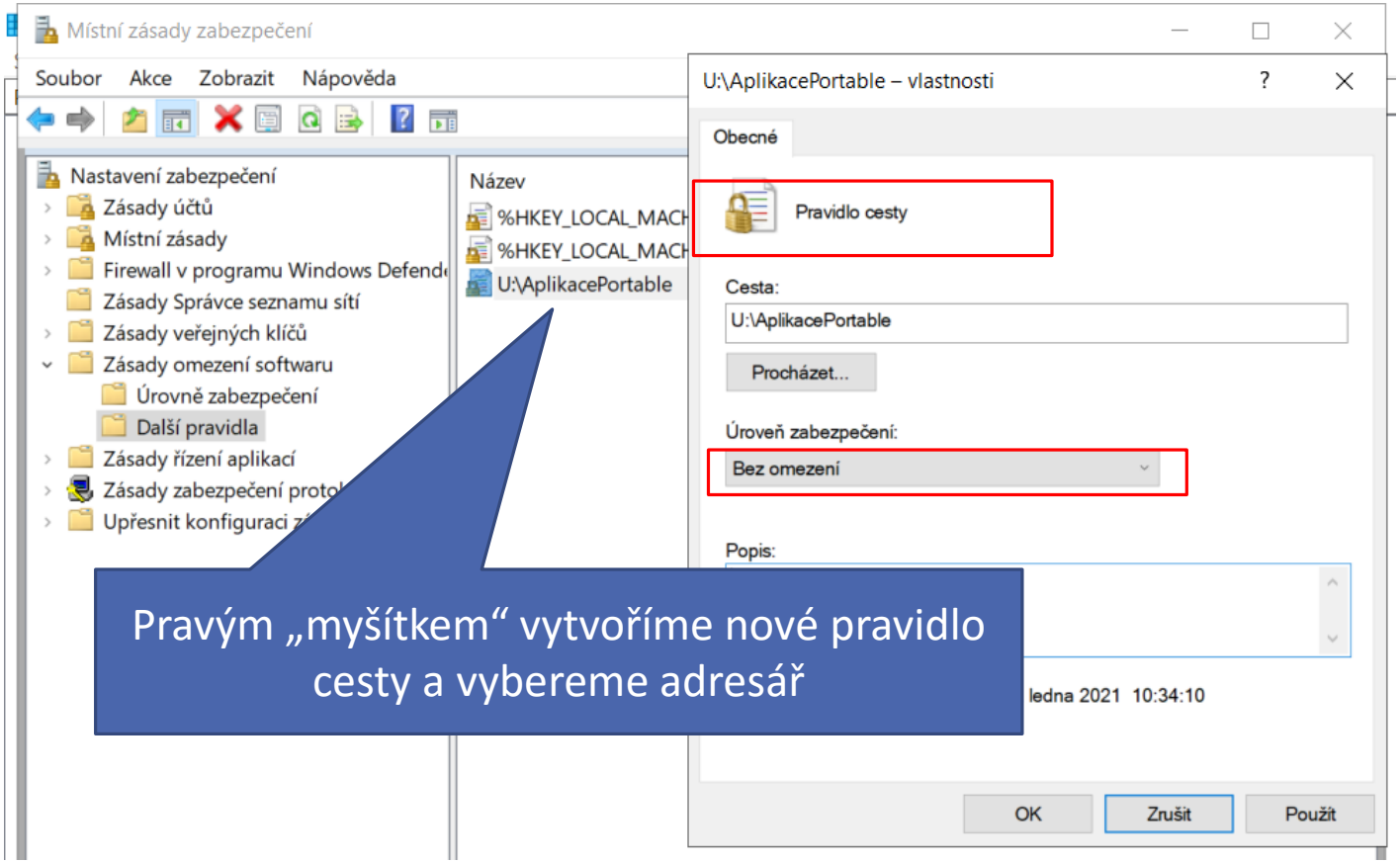


Rozšířené nastavení OSW

Vlastní whitelist podle cesty:

- Definujeme adresář kde neplatí omezení
  - Běžný uživatel může spouštět např. portable aplikace
  - !!! Může do něj stahovat programy z INETu
  - Bezpečnostní díra !!!
  - !!! Používat s rozmyslem/opatrně !!!
  - Většinou použijeme – nejde-li z nějakého důvodu spustit potřebný SW
  - Systémový SW můžeme omezit službou AppLocker

Rozšířené nastavení OSW



Vytvoření uživatelských účtů

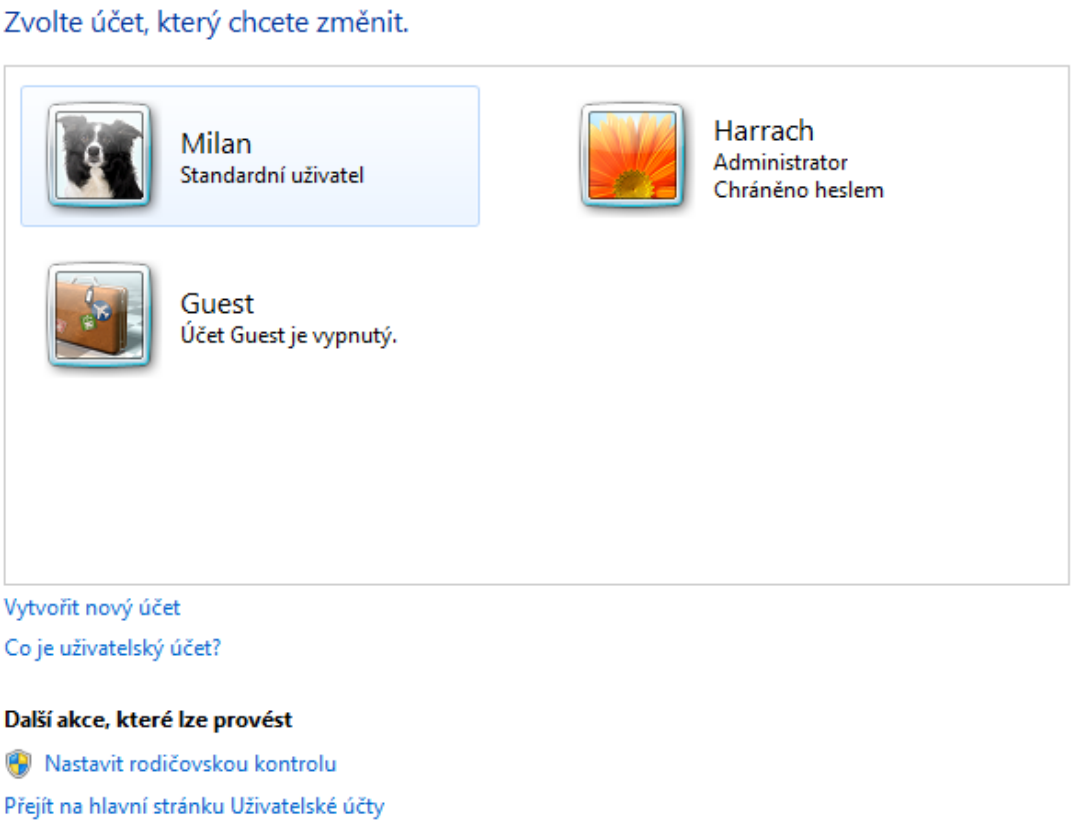
1) **Uživatelské účty** (standardní uživatel):

- Nastavení -> Účty
- Ovládací panely -> Uživatelské účty
- CMD: net user
- lusrmgr.msc
- mmc.exe (konzole)

Rozšířené nastavení OSW

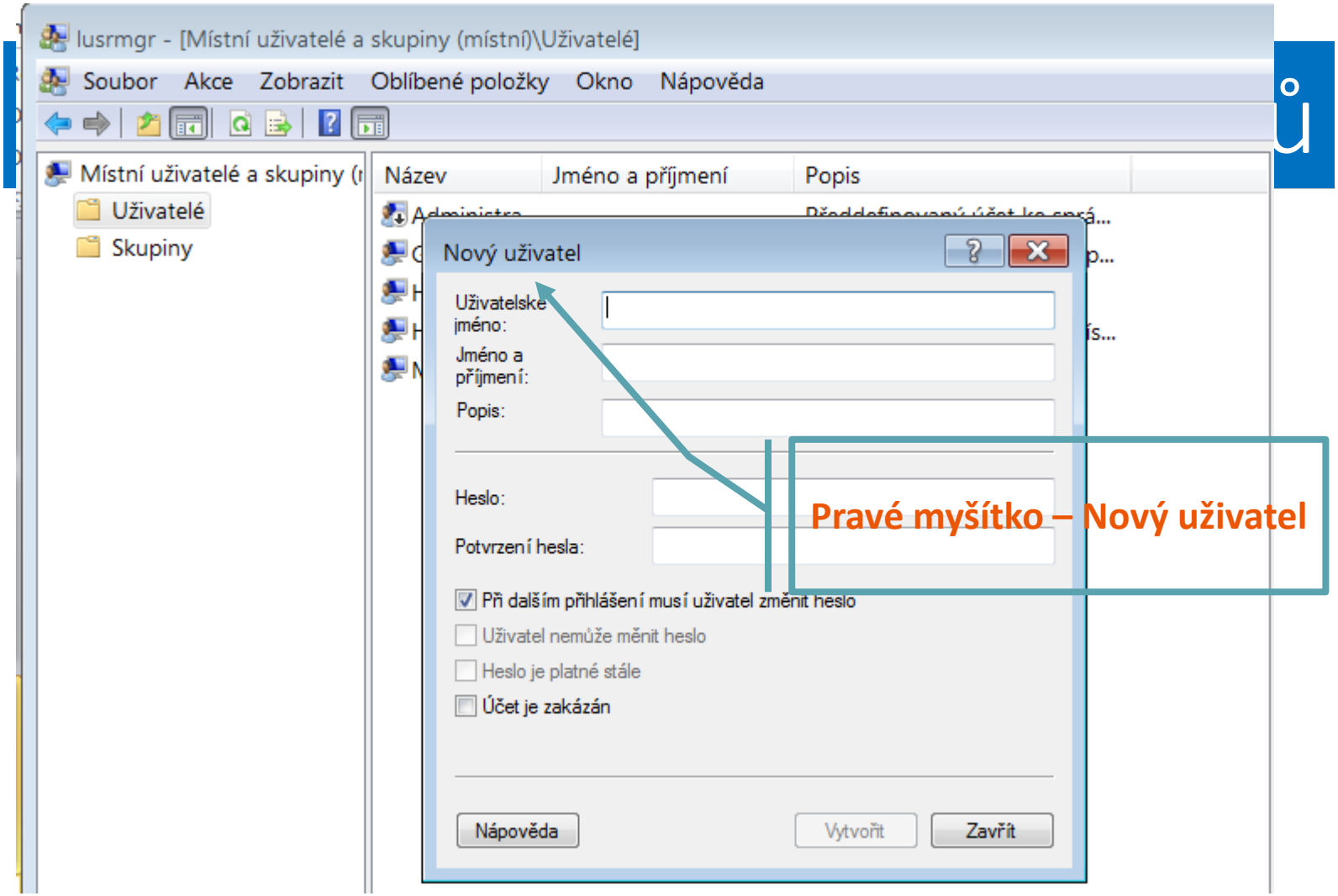
2. Rozšířené nastavení
   1. Oddělení systému od uživatelských dat
   2. Nastavení politiky uživatelských účtů
   3. Základní záloha „čistého“ systému
3. Speciální nastavení
   1. Služby a aplikace při spuštění OSW,skripty
   2. Optimalizace pro SSD
   3. RAM disk (cache, temp)
   4. FireWall

Vytvoření uživatelských účtů



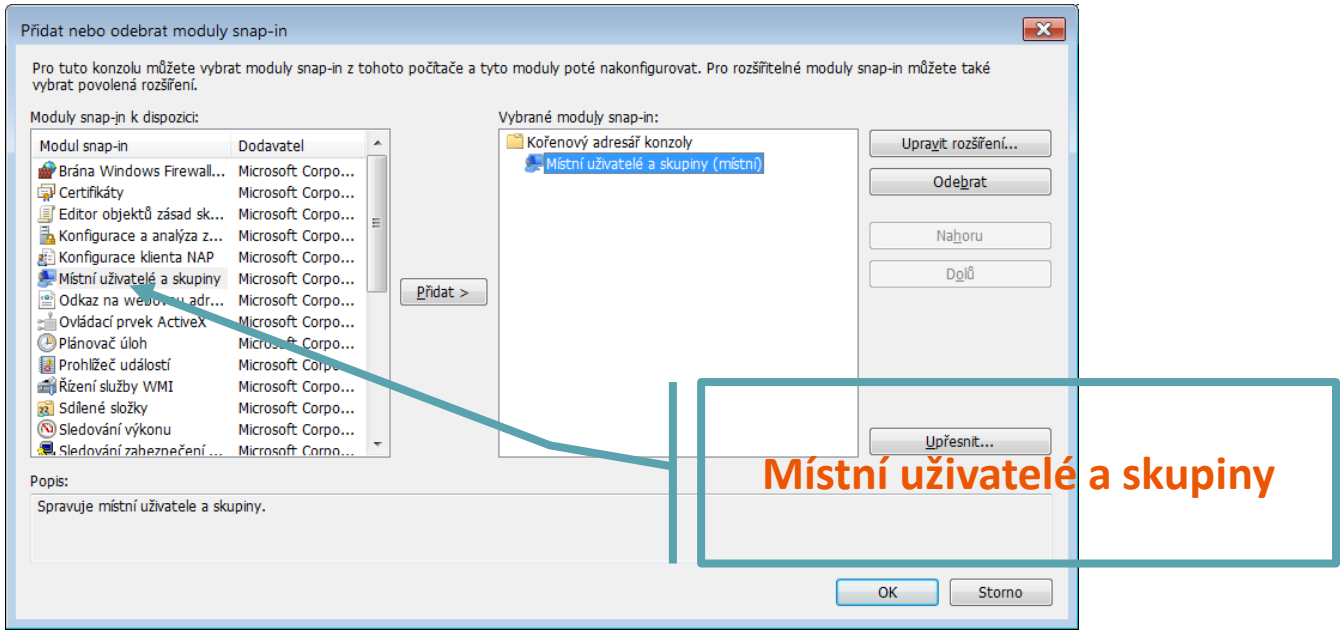
3) Vytvoření uživatelských účtů/skupin

2) Microsoft konzole – Spustit: **lusrmgr.msc**


lusrmgr - [Místní uživatelé a skupiny (místní)\Uživatelé]
Soubor Akce Zobrazit Oblíbené položky Okno Nápověda
Místní uživatelé a skupiny (
Uživatelé
Skupiny
Název
Jméno a příjmení
Popis
Nový uživatel
Uživatelské jméno:
Jméno a příjmení:
Popis:
Heslo:
Potvrzení hesla:
Při dalším přihlášení musí uživatel změnit heslo
Uživatel nemůže měnit heslo
Heslo je platné stále
Účet je zakázán
Nápověda
Vytvořit
Zavřít
Pravé myšítko – Nový uživatel

Nebo spustit:mmc

Soubor: **Přidat odebrat snap-in…**



3) Vytvoření uživatelských účtů

3) cmd: net user

- Rychlý způsob ***zobrazení / nastavení / vytváření / rušení účtů***
- **vyžaduje administrátorská práva**
- NET ACCOUNTS – aktuální info o aktuálním účtu
- NET USER – zobrazí všechny účty
- NET USER *jméno* * /ADD – vytvoří účet
  - * - požaduje zadat heslo
  - místo * lze vložit heslo přímo

3) Vytvoření uživatelských účtů

3) cmd: **net user**

- NET USER *jméno* * – změní heslo
  - * - požaduje zadat nové heslo
  - místo * lze vložit heslo přímo
- NET USER *jméno* /DELETE – zruší účet
  - je-li účet „poškozen“ – jediný způsob

4) Nastavení práv přístupu

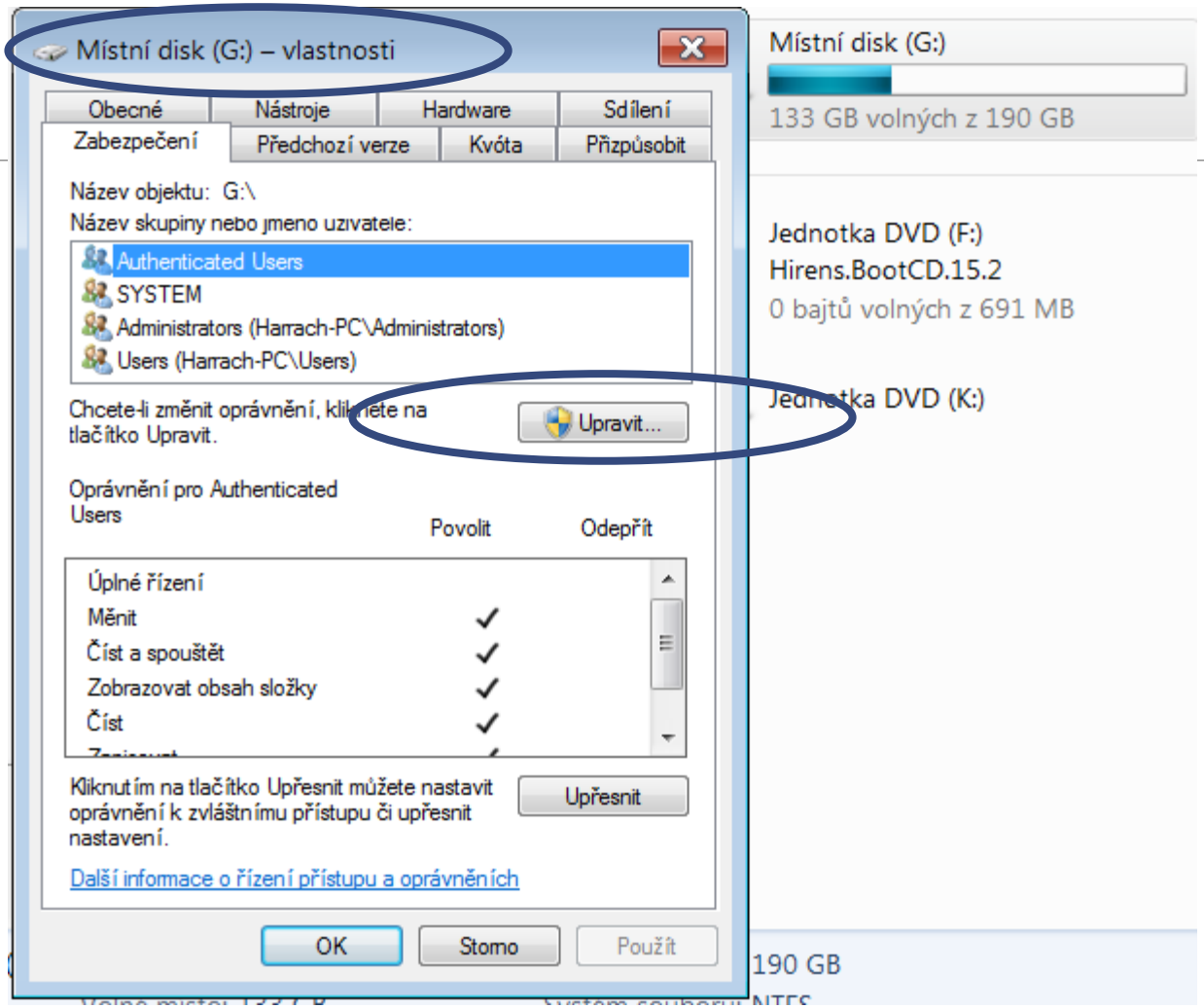
Práva k přístupu k disku / složce / souboru:

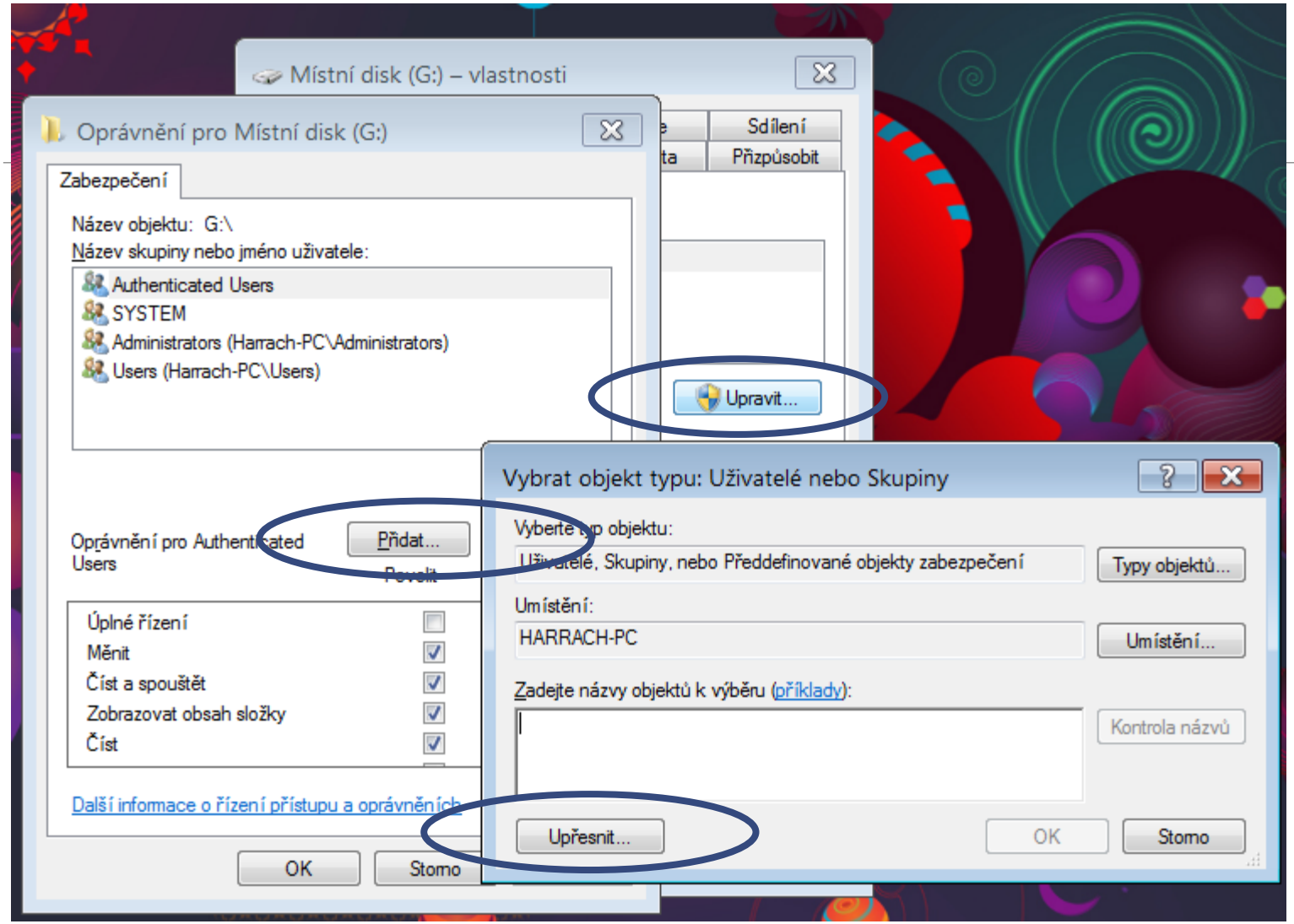
- Podmínka:
  - Disk – souborový systém NTFS!
  - Administrátorský účet

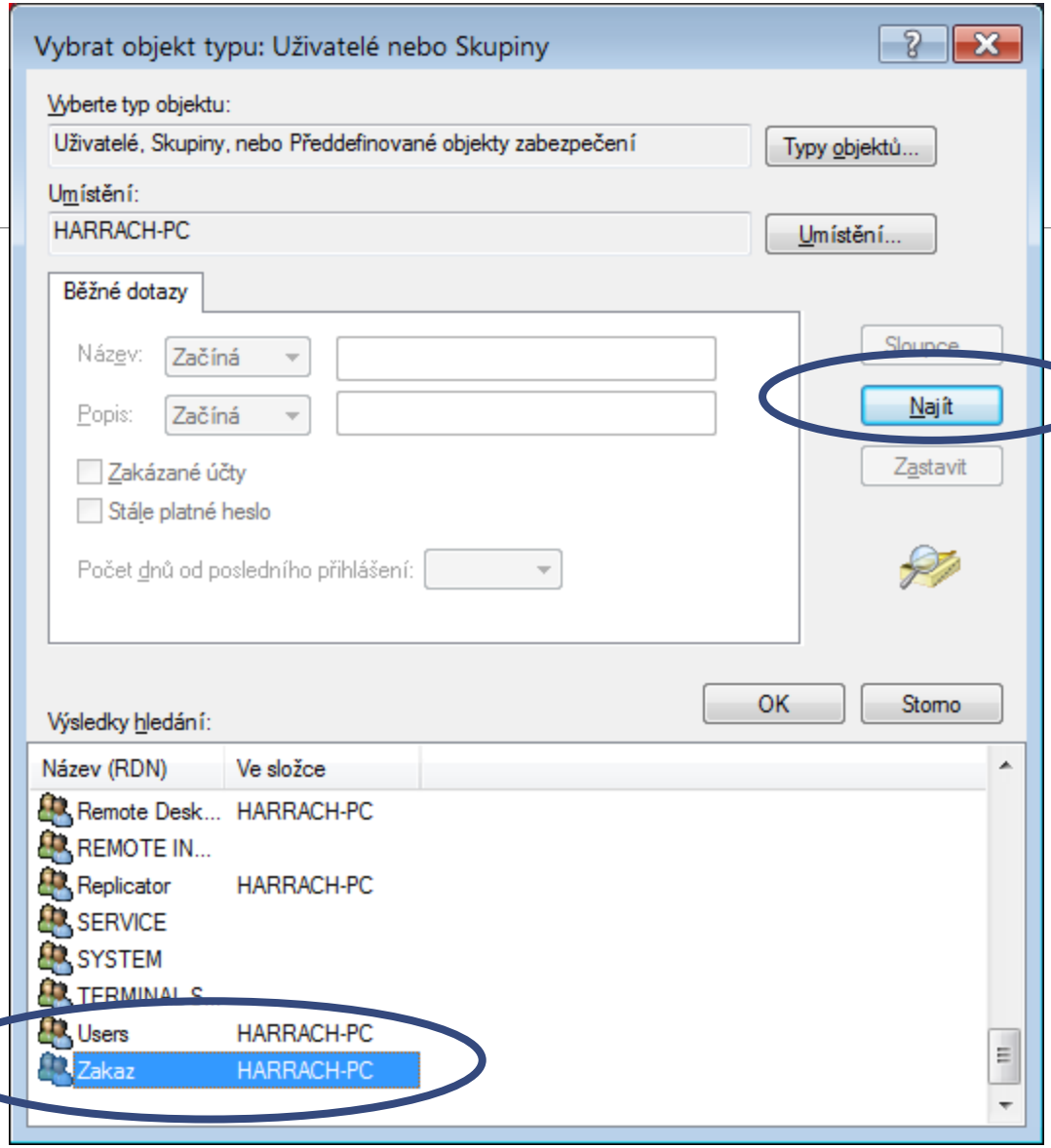
4) Nastavení práv přístupu

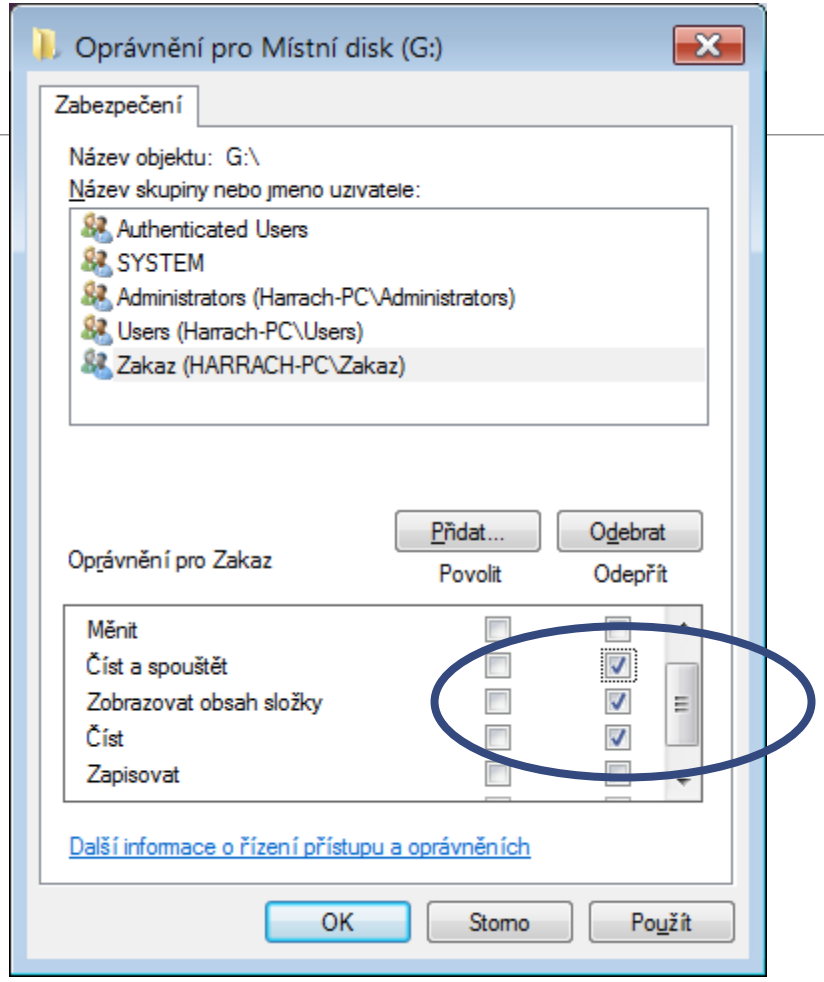
Postup:

1) Vytvořit **Novou skupinu** – např. **Zákaz**
   - *mmc – snap-in – Místní uživatelé a **skupiny***
2) Přidat do skupiny **Zákaz** účty
   - Zařadíme všechny uživatele kterým zamezíme přístup k *disku/složce/souboru*
3) Nastavit *disku/složce/souboru* práva
   - Pro skupinu **Zákaz**


Místní disk (G:) – vlastnosti
Obecné
Nástroje
Hardware
Sdílení
Zabezpečení
Předchozí verze
Kvóta
Přizpůsobit
Název objektu: G:\
Název skupiny nebo jmeno uzivatele:
Authenticated Users
SYSTEM
Administrators (Harrach-PC\Administrators)
Users (Harrach-PC\Users)
Chcete-li změnit oprávnění, klikněte na tlačítko Upravit.
Upravit...
Oprávnění pro Authenticated Users
Povolit
Odepřít
Úplné řízení
Měnit
Číst a spouštět
Zobrazovat obsah složky
Číst
Kliknutím na tlačítko Upřesnit můžete nastavit oprávnění k zvláštnímu přístupu či upřesnit nastavení.
Upřesnit
Další informace o řízení přístupu a oprávněních
OK
Storno
Použít
Místní disk (G:)
133 GB volných z 190 GB
Jednotka DVD (F:)
Hirens.BootCD.15.2
0 bajtů volných z 691 MB
Jednotka DVD (K:)
190 GB


Místní disk (G:) – vlastnosti
Sdílení
Přizpůsobit
Oprávnění pro Místní disk (G:)
Zabezpečení
Název objektu: G:\
Název skupiny nebo jméno uživatele:
Authenticated Users
SYSTEM
Administrators (Harrach-PC\Administrators)
Users (Harrach-PC\Users)
Upravit...
Oprávnění pro Authenticated Users
Přidat...
Povolit
Úplné řízení
Měnit
Číst a spouštět
Zobrazovat obsah složky
Číst
Další informace o řízení přístupu a oprávněních
OK
Storno
Vybrat objekt typu: Uživatelé nebo Skupiny
Vyberte typ objektu:
Uživatelé, Skupiny, nebo Předdefinované objekty zabezpečení
Typy objektů...
Umístění:
HARRACH-PC
Umístění...
Zadejte názvy objektů k výběru (příklady):
Kontrola názvů
Upřesnit...
OK
Storno


Vybrat objekt typu: Uživatelé nebo Skupiny
Vyberte typ objektu:
Uživatelé, Skupiny, nebo Předdefinované objekty zabezpečení
Typy objektů...
Umístění:
HARRACH-PC
Umístění...
Běžné dotazy
Název: Začíná
Popis: Začíná
Zakázané účty
Stále platné heslo
Počet dnů od posledního přihlášení:
Sloupce...
Najít
Zastavit
OK
Storno
Výsledky hledání:
Název (RDN)
Ve složce
Remote Desk... HARRACH-PC
REMOTE IN...
Replicator HARRACH-PC
SERVICE
SYSTEM
Users HARRACH-PC
Zakaz HARRACH-PC


Oprávnění pro Místní disk (G:)
Zabezpečení
Název objektu: G:\
Název skupiny nebo jmeno uzivatele:
Authenticated Users
SYSTEM
Administrators (Harrach-PC\Administrators)
Users (Harrach-PC\Users)
Zakaz (HARRACH-PC\Zakaz)
Přidat...
Odebrat
Oprávnění pro Zakaz
Povolit
Odepřít
Měnit
Číst a spouštět
Zobrazovat obsah složky
Číst
Zapisovat
Další informace o řízení přístupu a oprávněních
OK
Storno
Použít

5) Nastavení diskových kvót

Kvóty omezující množství dat

- Které mohou jednotliví uživatelé uložit na *disk/diskový oddíl*
- Používáme - využívá-li PC více uživatelů

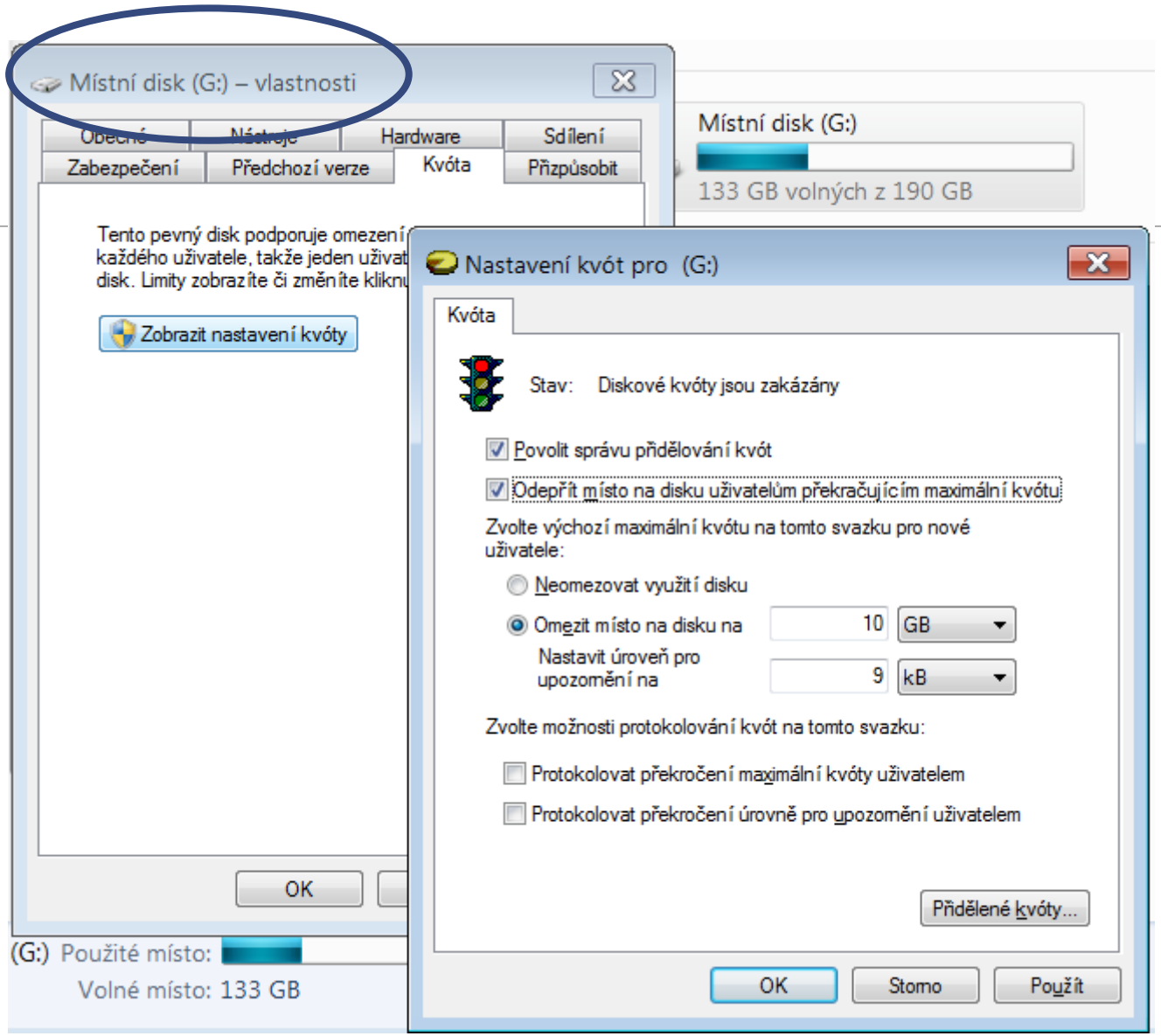
Kvótami předejdete zaplnění veškerého volného místa

5) Nastavení diskových kvót

Pouze pro uživatele kteří byli vytvořeni **až po přidělení diskových kvót**

Nastavení kvóty pro již existující uživatele

- Tlačítko **Přidělené kvóty**
- Výběr uživatele, **Vlastnosti**.


Místní disk (G:) – vlastnosti
Obecné
Nástroje
Hardware
Sdílení
Zabezpečení
Předchozí verze
Kvóta
Přizpůsobit
Tento pevný disk podporuje omezení
každého uživatele, takže jeden uživat
disk. Limity zobrazíte či změníte kliknu
Zobrazit nastavení kvóty
OK
Místní disk (G:)
133 GB volných z 190 GB
Nastavení kvót pro (G:)
Kvóta
Stav: Diskové kvóty jsou zakázány
Povolit správu přidělování kvót
Odepřít místo na disku uživatelům překračujícím maximální kvótu
Zvolte výchozí maximální kvótu na tomto svazku pro nové uživatele:
Neomezovat využití disku
Omezit místo na disku na
10
GB
Nastavit úroveň pro upozornění na
9
kB
Zvolte možnosti protokolování kvót na tomto svazku:
Protokolovat překročení maximální kvóty uživatelem
Protokolovat překročení úrovně pro upozornění uživatelem
Přidělené kvóty...
OK
Storno
Použít
(G:) Použité místo:
Volné místo: 133 GB