

Bezpečnost dat

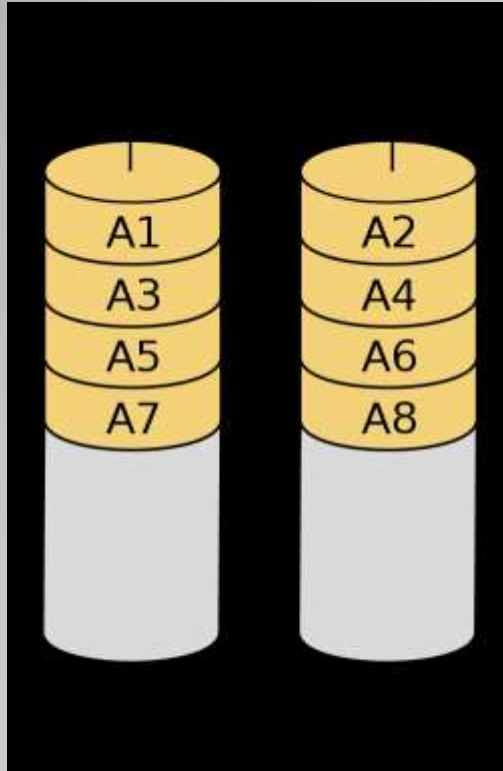
Richard Biječek

Microsoft
CERTIFIED
IT Professional

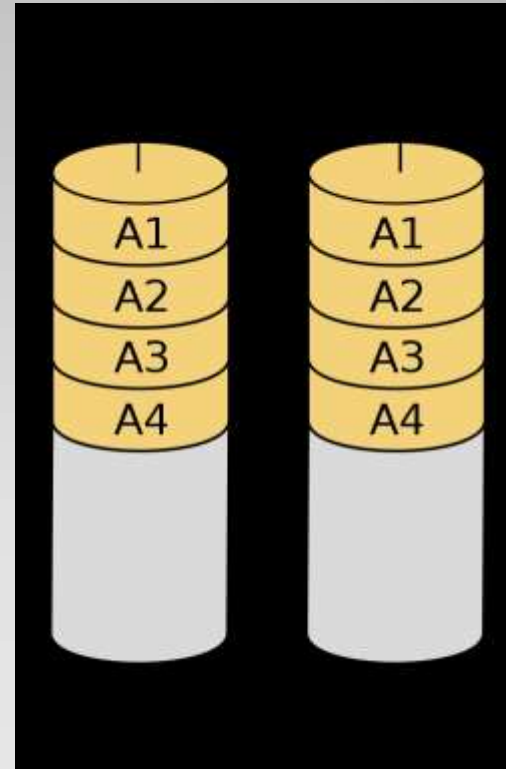
- Samostatný pevný disk
- RAID (Redundant Array of Independent Disks)
 - SW implementace (Dynamické disky)
 - HW řešení (BIOS, Řadič disků)
- Externí disková pole
 - iSCSI
 - Fiber Channel
- Virtuální disky

Možnosti ukládání dat

- RAID 0 – Striping
 - (není redundantní)

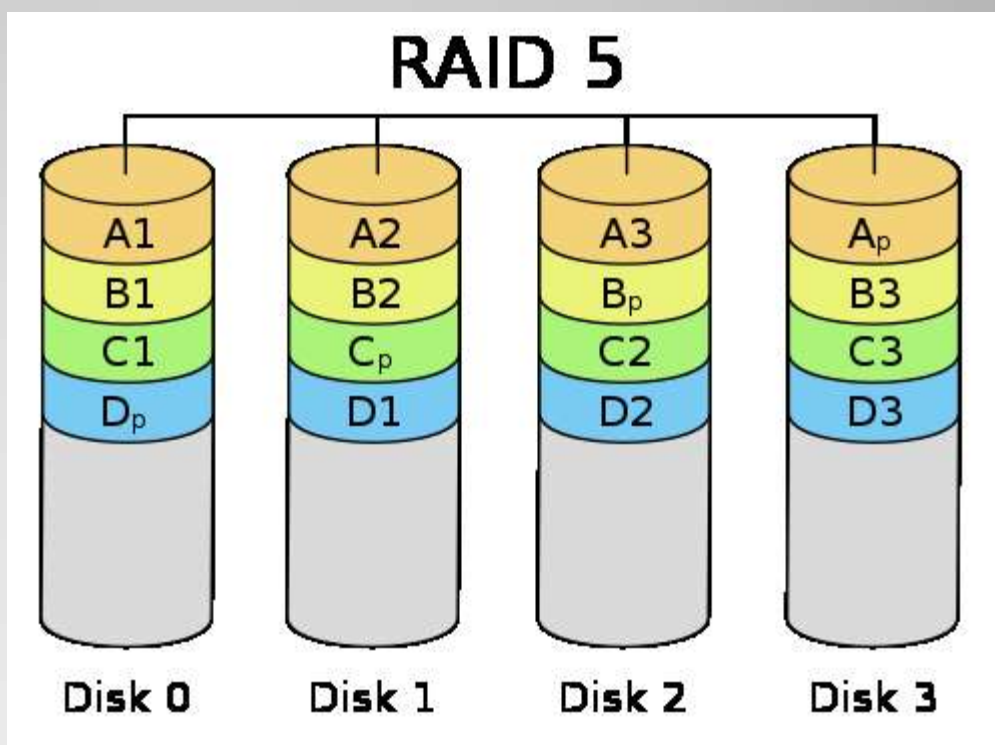


- RAID 1 - Mirroring



RAID

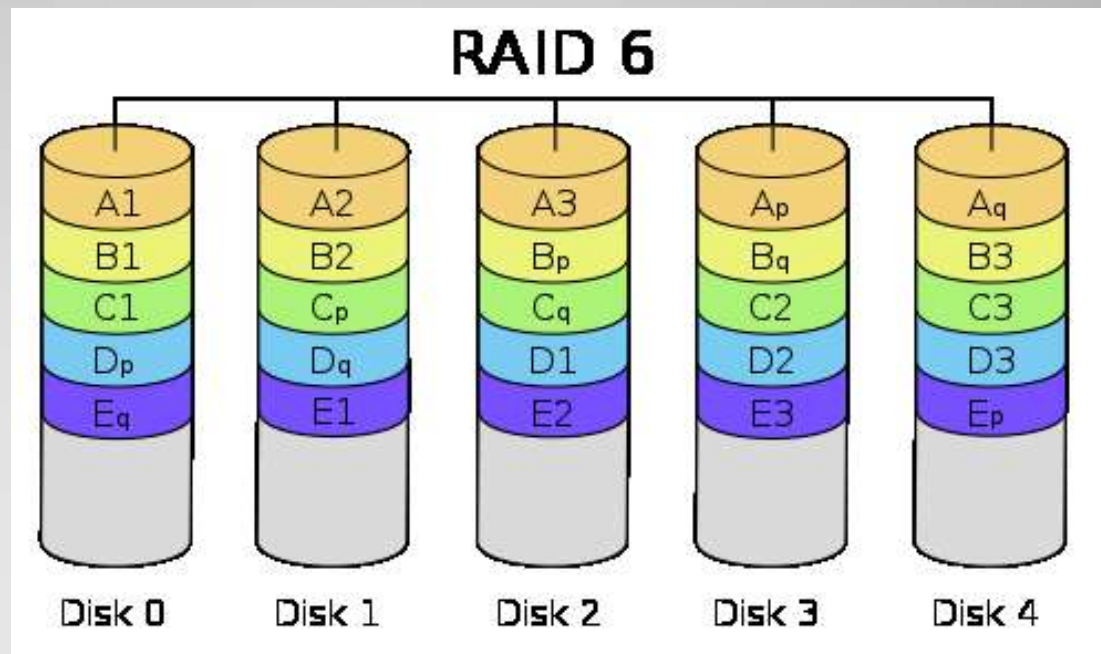
- RAID 5 – „striping s distribuovanou paritou“
 - Vyžaduje min. 3 disky, možno použiť i více
 - Není vhodný pro vysokou I/O zátěž (parita)



RAID

- RAID 6

- Jako RAID 5, ale používá dvojitou paritu
- Vhodný pro velké pole levných disků
- SAS vs. SATA



RAID

- Kombinace – RAID 0+1, 1+0, ...
 - RAID 1+0 pro max. požadavky na I/O
- Rebuild RAID pole
 - Obnova redundance
- „Spare“ disky
 - Vypnuty, aktivují se při selhání aktivního disku
- Cache na řadiči
 - Možnost nastavení Read / Write cache
 - Záloha baterií

RAID

Computer Management

File Action View Help

Volume	Layout	Type	File System	Status	Capacity	Free Space	% Free	Fault Tolerance	Overhead	Actions
(C:)	Simple	Basic	NTFS	Healthy (Boot, Page File, Crash Dump, Primary Partition)	31,90 GB	23,22 GB	73 %	No	0%	Disk Management ▲ More Actions ▶
System Reserved	Simple	Basic	NTFS	Healthy (System, Active, Primary Partition)	100 MB	72 MB	72 %	No	0%	

Disk 0 Basic 32,00 GB Online	System Reserved 100 MB NTFS Healthy (System, Active, Primary Partition)	(C:) 31,90 GB NTFS Healthy (Boot, Page File, Crash Dump, Primary Partition)
Disk 1 Unknown 40,00 GB Not Initialized	40,00 GB Unallocated	
CD-ROM 0 CD-ROM (D:)	No Media	

■ Unallocated ■ Primary partition

Disk Management

- Inicializace disku
 - „podpis“ disku pro identifikaci
- Základní (basic) / Dynamické disky
- MBR / GPT disky
 - MBR – limit 2TB

- Vytvoření oddílu
- Formátování
 - = Vytvoření souborového systému - NTFS

Správa fyz. disků

- Simple
 - „základní“ oddíl
 - Využívá celistvou část jednoho disku
- Spanned
 - „Rozprostřený“ oddíl
 - Spojuje různě velká místa z jednoho nebo více disků do jednoho oddílu
 - NEJEDNÁ se o RAID!
- Striped
 - „Prokládaný“ oddíl (SW implementace RAID 0)
 - Využívá stejně velké části z min. dvou disků

Dynamické disky

- Mirrored
 - „Zrcadlený“ oddíl (SW implementace RAID 1)
 - Využívá stejně velké části z min. dvou disků
 - Poskytuje redundanci dat
- RAID 5
 - „RAID 5“ (SW implementace)
 - Využívá stejně velké části z min. tří disků
 - Poskytuje redundanci dat

Dynamické disky

Computer Management

File Action View Help

Volume	Layout	Type	File System	Status	Capacity	Free Space	% Free	Fault Tolerance	Overhead
(C:)	Simple	Basic	NTFS	Healthy (Boot, Page File, Crash Dump, Primary Partition)	31,90 GB	23,22 GB	73 %	No	0%
Mirror (Y:)	Mirror	Dynamic	NTFS	Healthy	9,77 GB	9,69 GB	99 %	Yes	50%
RAID5 (Z:)	RAID-5	Dynamic	NTFS	Healthy	19,53 GB	19,44 GB	100 %	Yes	33%
Spanned (W:)	Spanned	Dynamic	NTFS	Healthy	51,63 GB	51,54 GB	100 %	No	0%
Striped (X:)	Striped	Dynamic	NTFS	Healthy	19,53 GB	19,44 GB	100 %	No	0%
System Reserved	Simple	Basic	NTFS	Healthy (System, Active, Primary Partition)	100 MB	72 MB	72 %	No	0%

Actions
Disk Managem...
More Actions ▶

Disk 0
Basic
32,00 GB
Online

System Reserved 100 MB NTFS Healthy (System, Active, Primary Partition)	(C:) 31,90 GB NTFS Healthy (Boot, Page File, Crash Dump, Primary Partition)
--	--

Disk 1
Dynamic
40,00 GB
Online

RAID5 (Z:) 9,77 GB NTFS Healthy	Mirror (Y:) 9,77 GB NTFS Healthy	Striped (X:) 9,77 GB NTFS Healthy	Spanned (W:) 10,70 GB NTFS Healthy
--	---	--	---

Disk 2
Dynamic
40,00 GB
Online

RAID5 (Z:) 9,77 GB NTFS Healthy	Mirror (Y:) 9,77 GB NTFS Healthy	Striped (X:) 9,77 GB NTFS Healthy	Spanned (W:) 10,70 GB NTFS Healthy
--	---	--	---

Disk 3
Dynamic
40,00 GB
Online

RAID5 (Z:) 9,77 GB NTFS Healthy	Spanned (W:) 30,23 GB NTFS Healthy
--	---

CD-ROM 0
CD-ROM (D:)
No Media

■ Unallocated ■ Primary partition ■ Spanned volume ■ Striped volume ■ Mirrored volume ■ RAID-5 volume

Ukázka dynamických disků

```
C:\>Administrator: C:\Windows\system32\cmd.exe - diskpart

C:\>diskpart

Microsoft DiskPart version 6.1.7600
Copyright (C) 1999-2008 Microsoft Corporation.
On computer: WIN2008R2TEMPLA

DISKPART> list disk

   Disk ###  Status         Size         Free         Dyn  Gpt
   -----  -
   Disk 0    Online         32 GB         0 B
   Disk 1    Online         40 GB        2048 KB    *
   Disk 2    Online         40 GB        2048 KB    *
   Disk 3    Online         40 GB        2048 KB    *

DISKPART> list volume

   Volume ###  Ltr  Label          Fs          Type          Size      Status      Info
   -----  -
   Volume 0    Z    RAID5          NTFS        RAID-5        19 GB     Healthy
   Volume 1    W    Spanned        NTFS        Spanned        51 GB     Healthy
   Volume 2    X    Striped        NTFS        Stripe         19 GB     Healthy
   Volume 3    Y    Mirror         NTFS        Mirror         9 GB      Healthy
   Volume 4    D    CD-ROM         NTFS        CD-ROM         0 B       No Media
   Volume 5    C    System Rese   NTFS        Partition     100 MB    Healthy    System
   Volume 6    C    System Rese   NTFS        Partition     31 GB     Healthy    Boot

DISKPART> select volume 0

Volume 0 is the selected volume.

DISKPART> delete

Microsoft DiskPart version 6.1.7600

DISK
- Delete a missing disk from the disk list.
PARTITION
- Delete the selected partition.
VOLUME
- Delete the selected volume.

DISKPART> delete volume

DiskPart successfully deleted the volume.

DISKPART> _
```

Diskpart

- Souborový systém NTFS
 - Teoretická max. velikost oddílu $2^{64}-1$ clusteru
 - Teoretická max. velikost souboru 16 EB
 - Žurnálování operací (netýká se dat)
 - Podpora přístupových oprávnění, audity
 - Limit 255 znaků (UTF) pro název souboru
 - Podpora transparentní komprese dat
 - Podpora „sparse files“, „alternate data streams“
 - Volume shadow copy (copy-on-write)
 - ...

NTFS

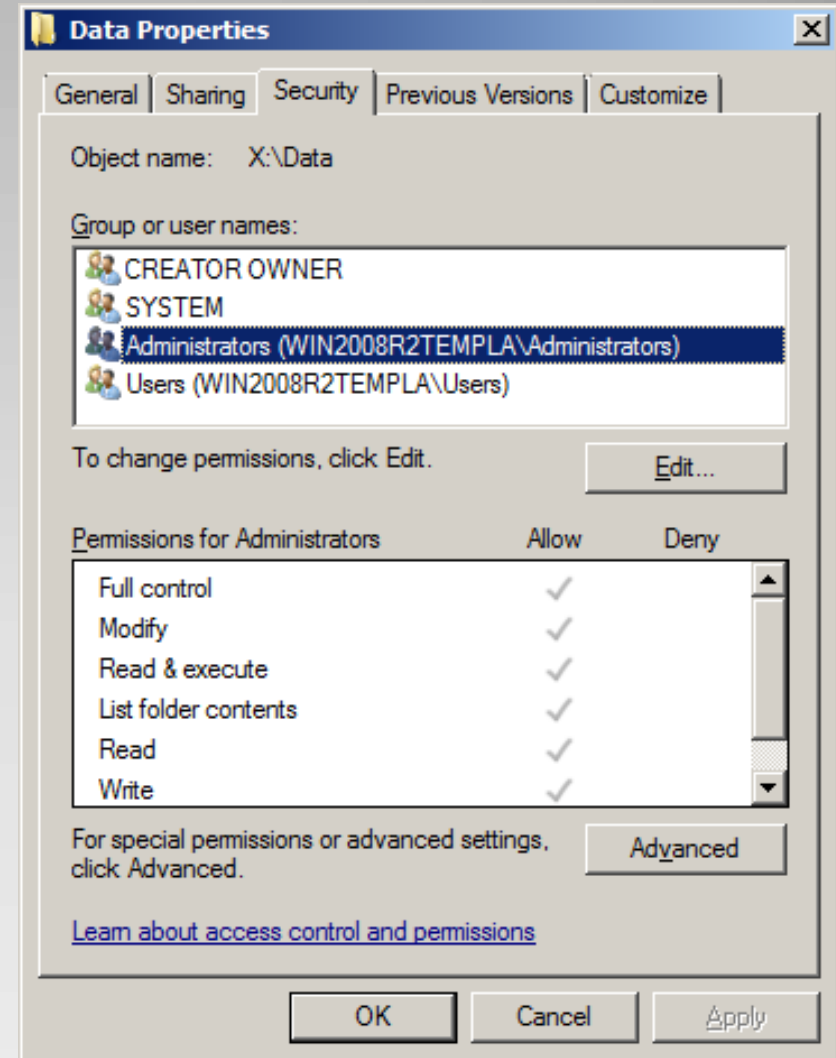
- Prakticky každý objekt v systémech Windows NT má přístupová oprávnění
- Soubory (složky) na NTFS oddílech
- Klíče registru
- Tiskárny
- Objekty Active Directory
- Služby
- Procesy
- ...
- Pozor, ne vždy je k dispozici GUI

Přístupová oprávnění

- ACL = Access Control List
 - Seznam přístupových oprávnění
- ACE = Access Control Entry
 - Položka přístupových oprávnění
 - Definuje typ přístupu pro konkrétní SID
 - SID reprezentuje typicky skupinu / uživatele
- Prázdné ACL = NIKDO nemá přístup

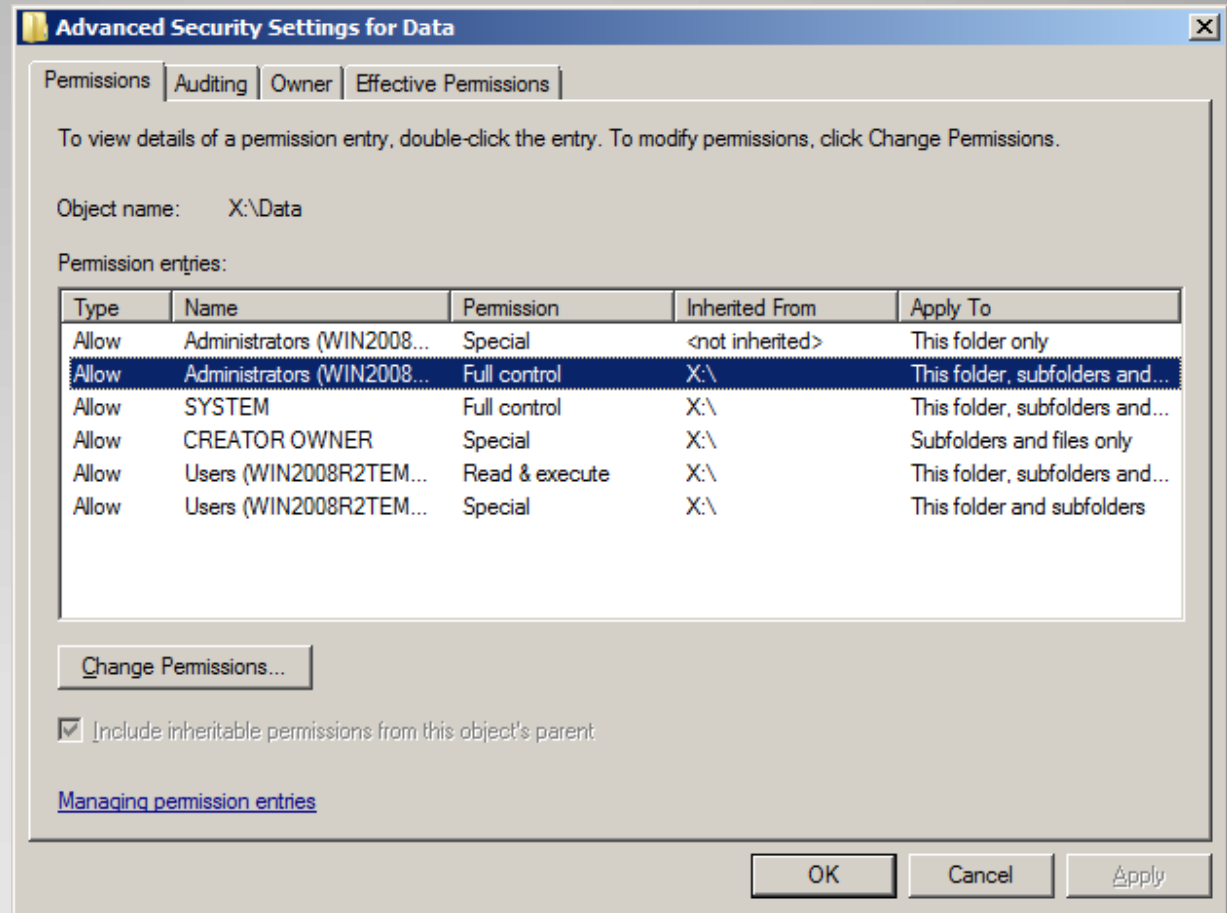
Přístupová oprávnění

- NTFS oprávnění
 - Full Control
 - Modify
 - Read & Execute
 - Read
 - Write
- „Allow“ povoluje
- „Deny“ odepírá
 - POZOR - Odepření má přednost !!!



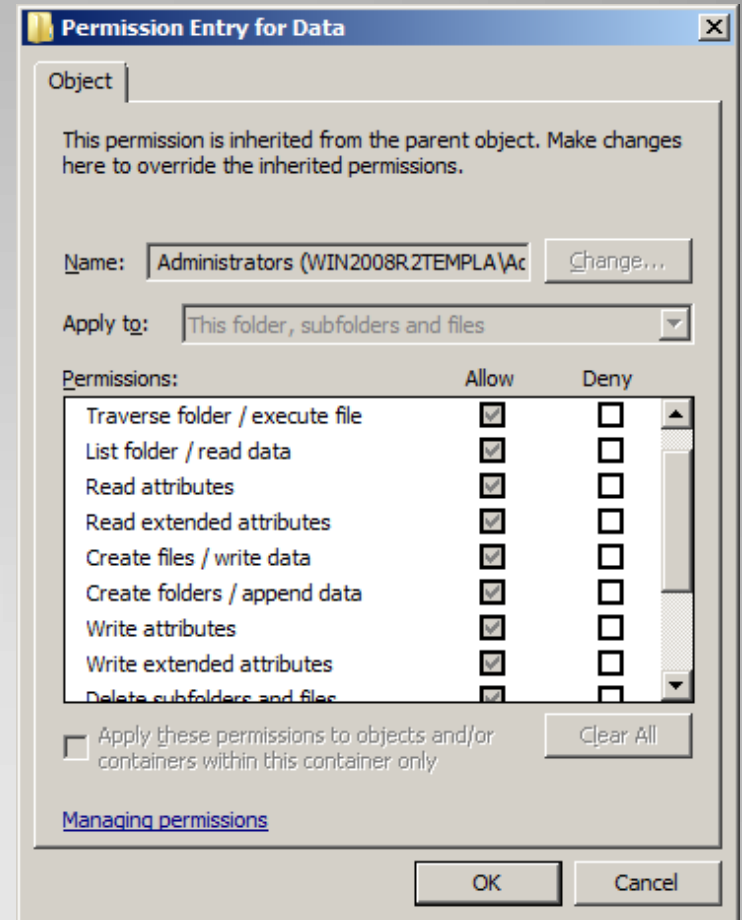
ACL složky

- Oprávnění jsou děděna z nadřazených objektů



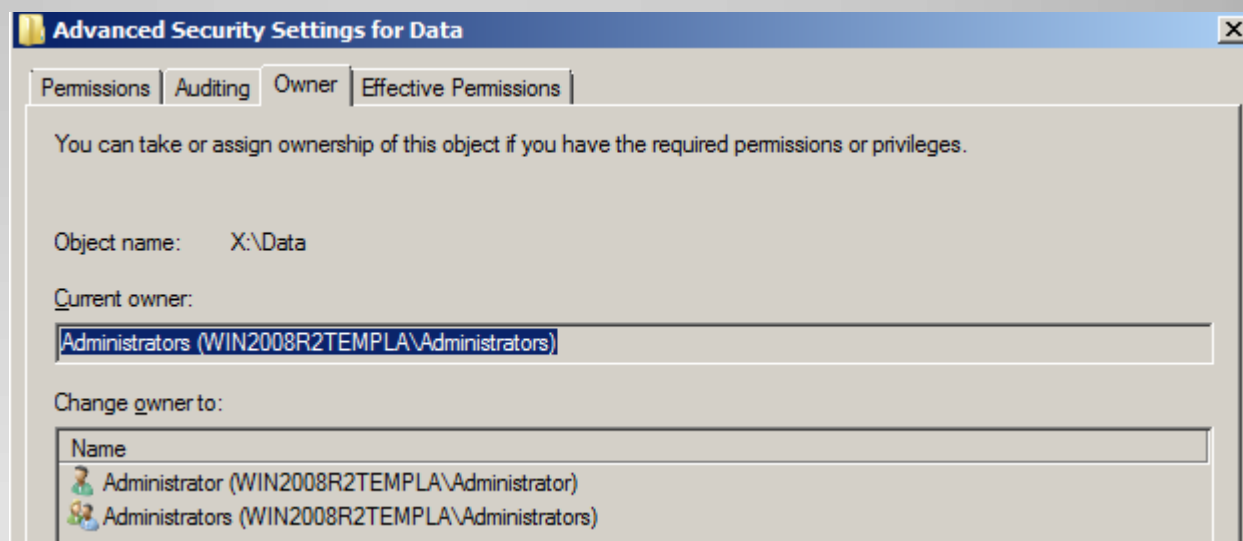
Dědičnost oprávnění

- „Special permissions“
- Reprezentují přesné ACL
- Běžně není potřeba nastavovat



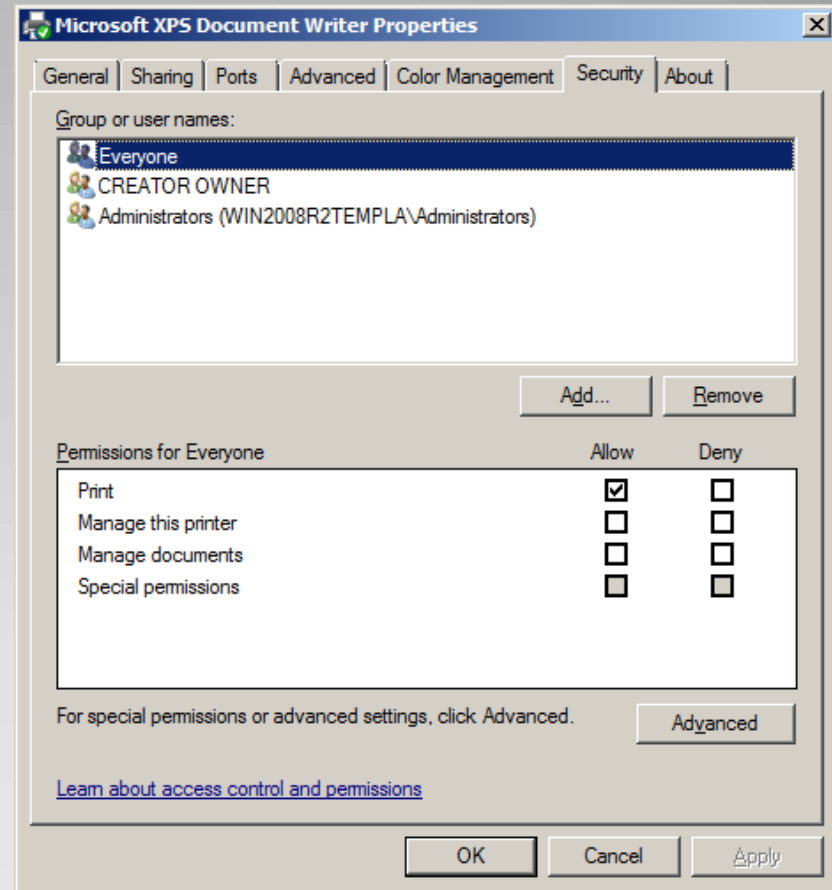
Speciální oprávnění

- Každý objekt má „vlastníka“ (owner)
- Vlastník může VŽDY editovat ACL
- Administrátor může převzít vlastnictví



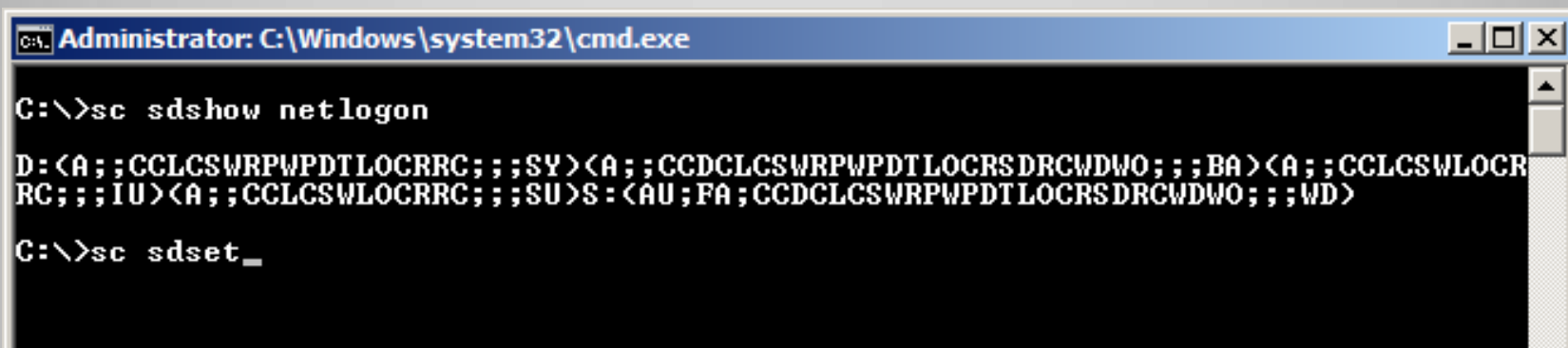
Vlastník

- Print
 - Umožňuje tisk
- Manage printer
 - Správa tiskárny
- Manage documents
 - Správa tiskové fronty
- Nemá „special“ permissions



Oprávnění tiskáren

- Oprávnění služeb nemá GUI
 - Není „záložka Security“
- Jen příkazy SC SDSHOW, SC SDSET
- Pracují s tzv. SDDL
 - Security Descriptor Definition Language



```
Administrator: C:\Windows\system32\cmd.exe
C:\>sc sdshow netlogon
D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWLOCRRC;;;SU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)
C:\>sc sdset_
```

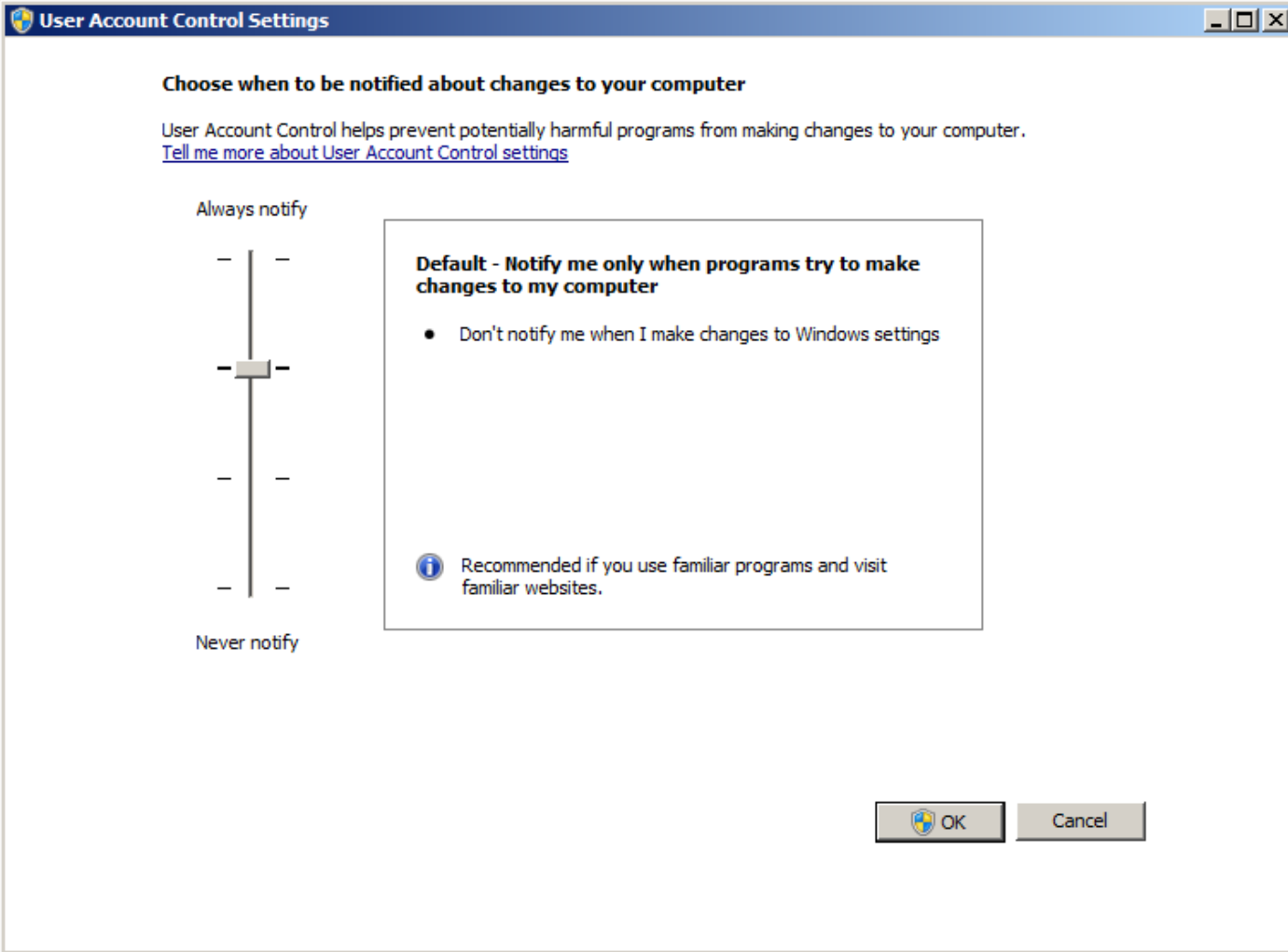
Oprávnění služeb (SDDL)

- Everyone
 - Reprezentuje každého uživatele
- Users
 - Všichni uživatelé – zahrnuje také doménového administrátora (je členem Domain Users)
- Creator Owner
 - Definuje přístup k nově vzniklému objektu pro jeho tvůrce (=vlastníka)
- System
 - Reprezentuje systémové účty např. pro provoz služeb. Uživatel nemůže být členem

Často používané skupiny

- UAC umožňuje řídit používání administrátorských práv
- Každý administrátor (člen skupiny Administrators) má systémem přiděleny dva „tokeny“
- Procesy (běžné GUI) takového uživatele běží pouze se základním oprávněním
- Operace vyžadující práva Administrátora si vyžádají potvrzení (elevaci oprávnění)
- Elevace je se týká vždy konkrétního procesu

User Account Control (UAC)



Konfigurace UAC

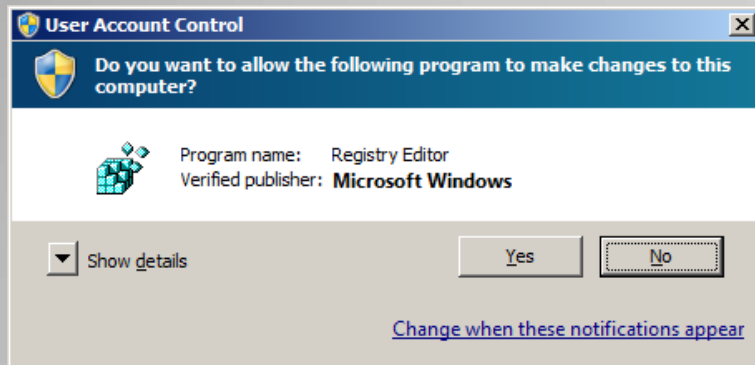
- Ve Windows 7 a 2008 R2 jsou 4 úrovně:
 - „Always notify“ (také ve Vista a 2008 R1)
 - Vyžaduje potvrzení pro všechny použití Administrátorských práv
 - „Default“ – Vyžádání oprávnění pro programy
 - Nevyžaduje notifikaci pro konfiguraci systému
 - „Default without secure desktop“ - Vyžádání oprávnění pro programy bez zabezpečené plochy (secure desktop)
 - „Never notify“ (také ve Vista a 2008 R1)
 - Vypnutí funkce UAC

Konfigurace UAC

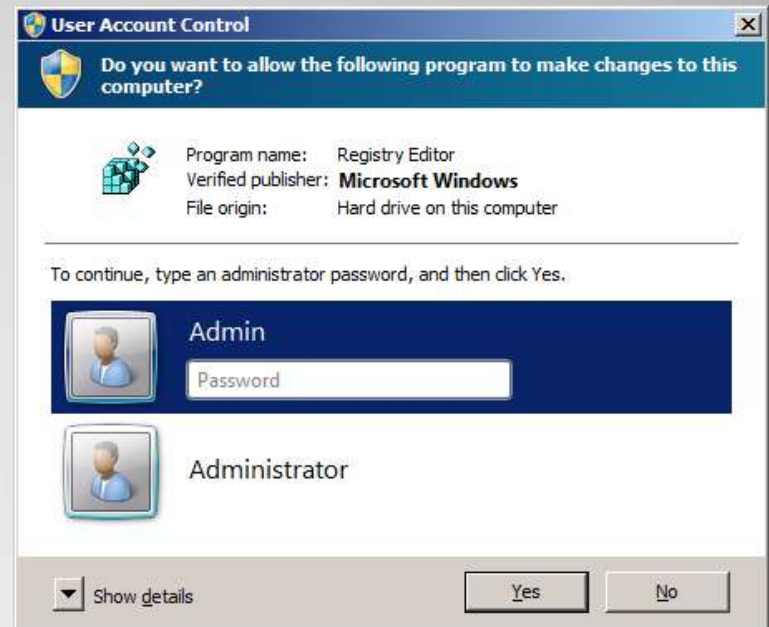
- Pro uživatele „Administrator“ = vestavěného administrátora systému je definována výjimka.

Admin Approval mode

- Potvrzení
 - Pouze pro administrátory













- Zadání pověření
 - Zobrazí se uživatelům bez admin. práv
 - Možno vynutit také pro administrátory



UAC potvrzení

- Pokročilé nastavení UAC
- Security Policy

 User Account Control: Admin Approval Mode for the Built-in Administrator account	Disabled
 User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop	Disabled
 User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode	Prompt for consent for non-Windows binaries
 User Account Control: Behavior of the elevation prompt for standard users	Prompt for credentials
 User Account Control: Detect application installations and prompt for elevation	Enabled
 User Account Control: Only elevate executables that are signed and validated	Disabled
 User Account Control: Only elevate UIAccess applications that are installed in secure locations	Enabled
 User Account Control: Run all administrators in Admin Approval Mode	Enabled
 User Account Control: Switch to the secure desktop when prompting for elevation	Disabled
 User Account Control: Virtualize file and registry write failures to per-user locations	Enabled

UAC

- Windows Server Backup
- System state backup
 - Záloha stavu OS
 - Pro obnovu nastavení OS, ovladačů, ...
- Bare metal recovery
 - Záloha instalace OS
 - Po selhání disku, nebo když SSB nestačí
 - Obnovuje se z WinRE (instalační médium)

Obnova systému

Select Items

Specify items to include in the backup by selecting or clearing the associated check boxes. The items that you have included in the current backup are already selected.

- Bare metal recovery
- System state
- System Reserved
- Local disk (C:)
- Mirror (Y:)
- Striped (X:)
- Spanned (W:)

Backup Once Wizard



Backup Progress

Backup Options

Select Backup Configur...

Select Items for Backup

Specify Destination Type

Select Backup Destination

Confirmation

Backup Progress

Status: 46 % of backup completed for System Writer...

Status details

Backup location: W:

Data transferred: 3,36 GB

Items

Item	Status	Data transferred
System state	46 % of backup com...	3,36 GB of 7,32 GB

You may close this wizard and the backup operation will continue to run in the background.

< Previous

Next >

Close

Cancel

Vytvoření zálohy

System Recovery Options

Use recovery tools that can help fix problems starting Windows. Select an operating system to repair.

If your operating system isn't listed, click Load Drivers and then install drivers for your hard disks.

Operating System	Partition Size	Location
Windows Server 2008 R.2	32665 MB	(E:) Local Disk

Restore your computer using a system image that you created earlier.

Load Drivers

System Recovery Options

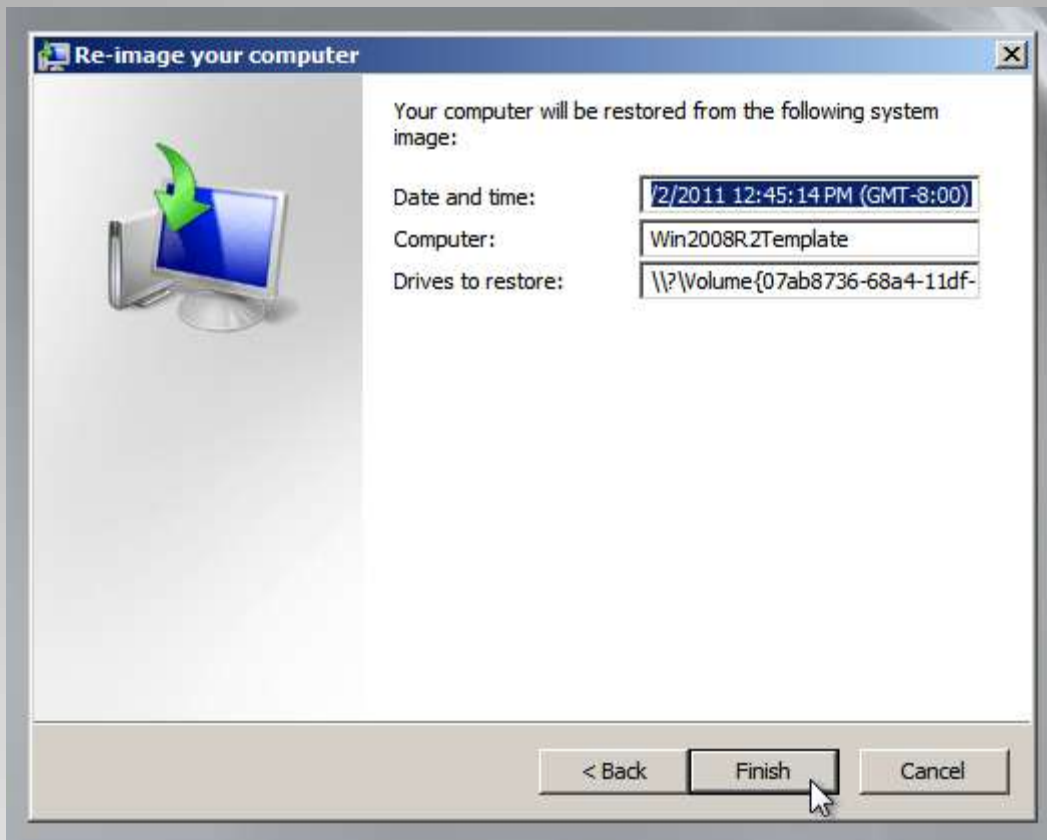
Choose a recovery tool

Operating system: Windows Server 2008 R.2 on (E:) Local Disk

-  **System Image Recovery**
Recover your computer using a system image you created earlier
-  **Windows Memory Diagnostic**
Check your computer for memory hardware errors
-  **Command Prompt**
Open a command prompt window

Shut Down Restart

WinRE



Obnova zálohy