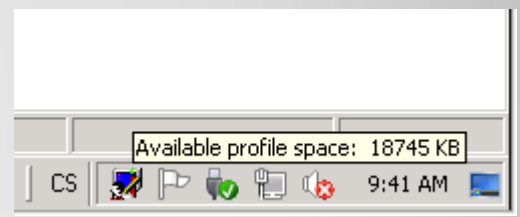
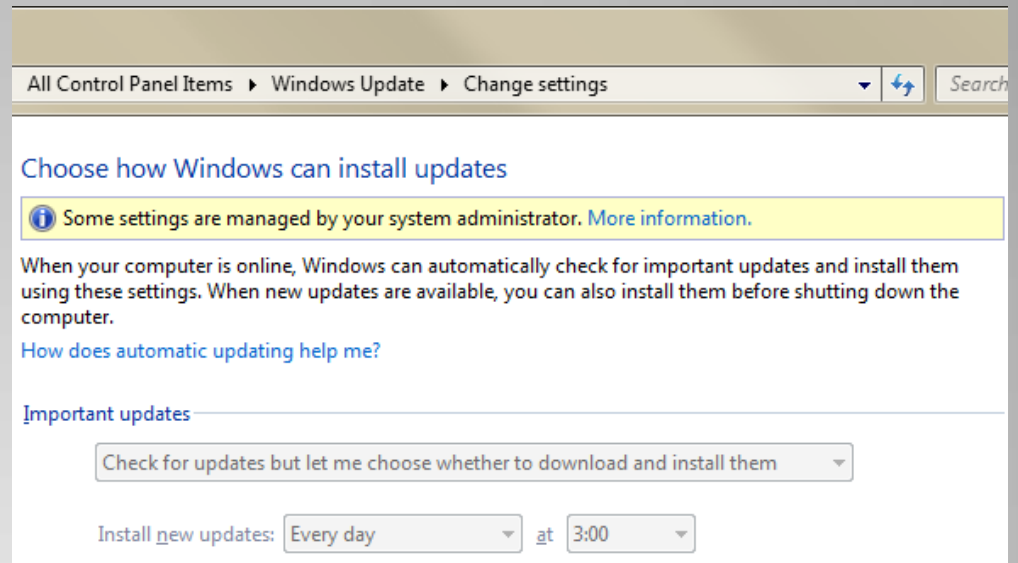
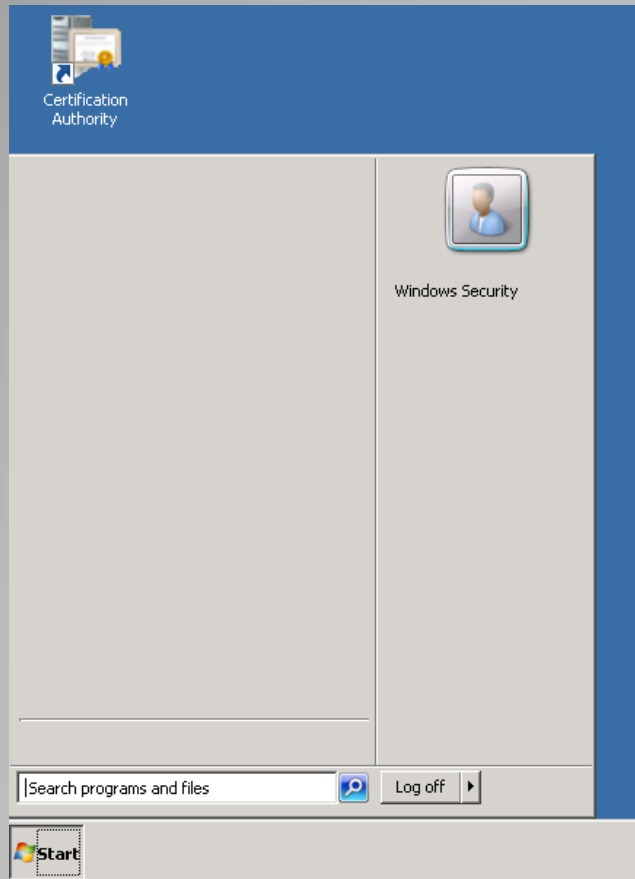


# Group policy

Jan Žák


**Microsoft**  
**CERTIFIED**  
*Trainer*

Systems Administration  
Systems Engineering

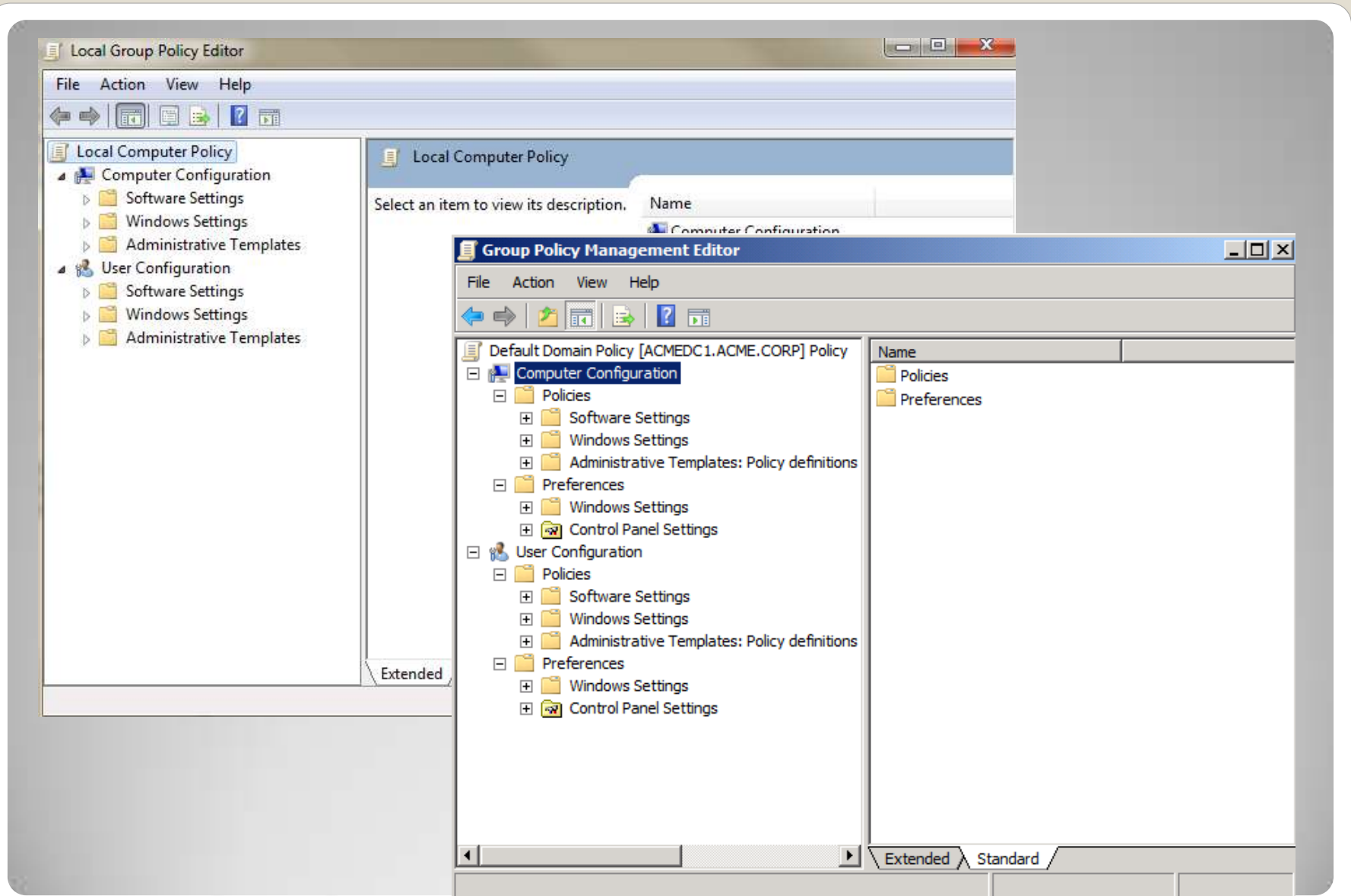


# K čemu Group Policy?

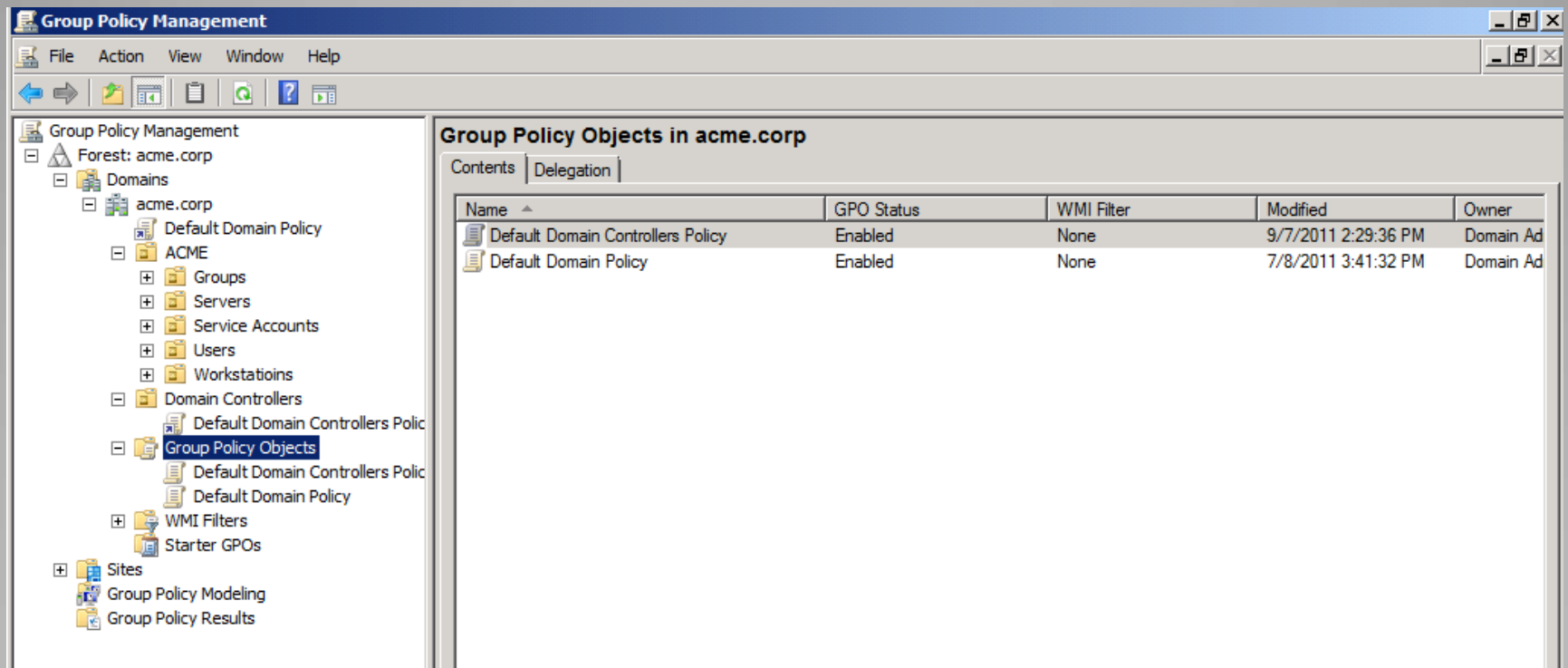
## Pořadí zpracování GP

- 
- Group Policy lokálního počítače
  - Group Policy objekty pro sídlo (site)
  - Group Policy objekty pro doménu
  - Group Policy objekty pro organizační jednotky

**Zpracování GP**



# Lokální a doménové politiky



- Administrative Tools → Group Policy Management (gpmc.msc)
- Pro editaci politik lokálního počítače: gpedit.msc

# Group Policy Management Console

Group Policy Management

File Action View Window Help

Group Policy Management

- Forest: acme.corp
  - Domains
    - acme.corp
      - Default Domain Policy
      - ACME
        - Groups
        - Servers
        - Service Accounts
        - Users
        - Workstations
      - Domain Controllers
        - Default Domain Controllers Policy
      - Group Policy Objects
        - Default Domain Controllers Policy
        - Default Domain Policy
      - WMI Filters
      - Starter GPOs
- Sites
  - Group Policy Modeling
    - Administrator on ACME DC 1
    - SQLAdm on Workstations
  - Group Policy Results
    - Administrator on ACME DC 1

**Default Domain Controllers Policy**

Scope Details Settings Delegation

Domain: acme.corp

Owner: Domain Admins (ACME\Domain Admins)

Created: 2/2/2011 1:07:05 PM

Modified: 9/7/2011 2:29:36 PM

User version: 0 (AD), 0 (sysvol)

Computer version: 5 (AD), 5 (sysvol)

Unique ID: {6AC1786C-016F-11D2-945F-00C04FB984F9}

GPO Status: Enabled

Comment:

**Policies**

\\acme.corp\sysvol\acme.corp\Policies

Organize Open New folder

Name	Date modified	Type
{6AC1786C-016F-11D2-945F-00C04FB984F9}	2/2/2011 1:07 PM	File folder
{31B2F340-016D-11D2-945F-00C04FB984F9}	2/2/2011 1:07 PM	File folder

Computer > OSDisk (C:) > Windows > System32 > GroupPolicy

Organize Include in library Share with Burn New folder

Name	Date modified	Type	Size
Machine	11.3.2011 7:55	File folder	
User	3.6.2011 15:08	File folder	
gpt.ini	12.10.2011 14:30	Configuration sett...	1 KB

# Co je Group Policy Object?

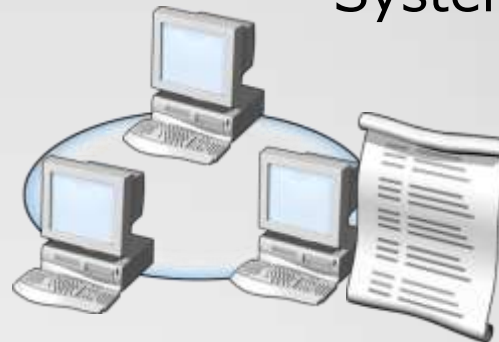
- GP pro uživatele:

- Software settings
- Windows settings
  - Folder Redirection
  - IE settings
- Administrative templates
  - Windows Components
  - Desktop settings



- GP pro počítače:

- Software settings
- Windows settings
  - Security settings
  - Startup/Shutdown scripts
- Administrative templates
  - Control Panel
  - Network
  - System



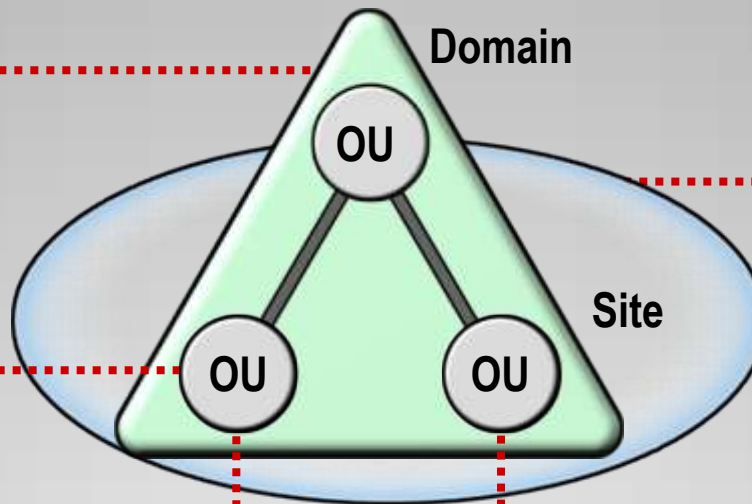
**User / Computer Configuration Settings**



Domain GPO



Organizational Unit GPO



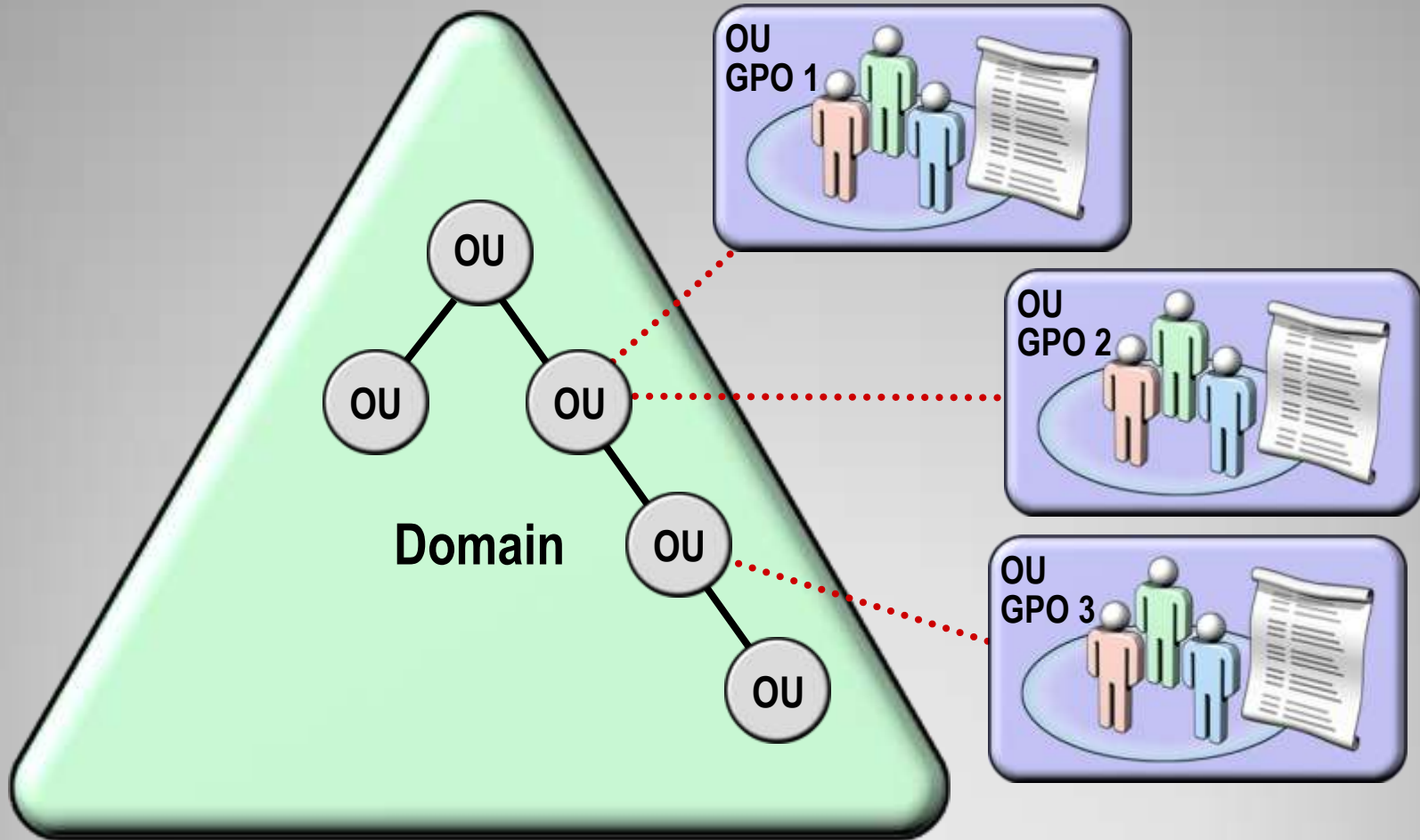
Site GPO



Organizational Unit GPO

# GPO Link





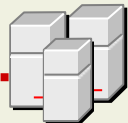
# Dědění politik

- Enforced
  - Má přednost před ostatními politikami - „vždy vyhraje“
- Link Enabled / Disabled
  - Link lze dočasně deaktivovat, např. při řešení problémů
- Deleted
  - Links lze smazat, GPO zůstane zachován
- Multiple Links
  - Při aplikaci více GPO na jeden kontejner, opět je důležité stanovit pořadí aplikování politik.

## Atributy GPO linků



GPO



Domain



Production



Sales



GPO  
se neaplikuje

## Blokování dědění GPO

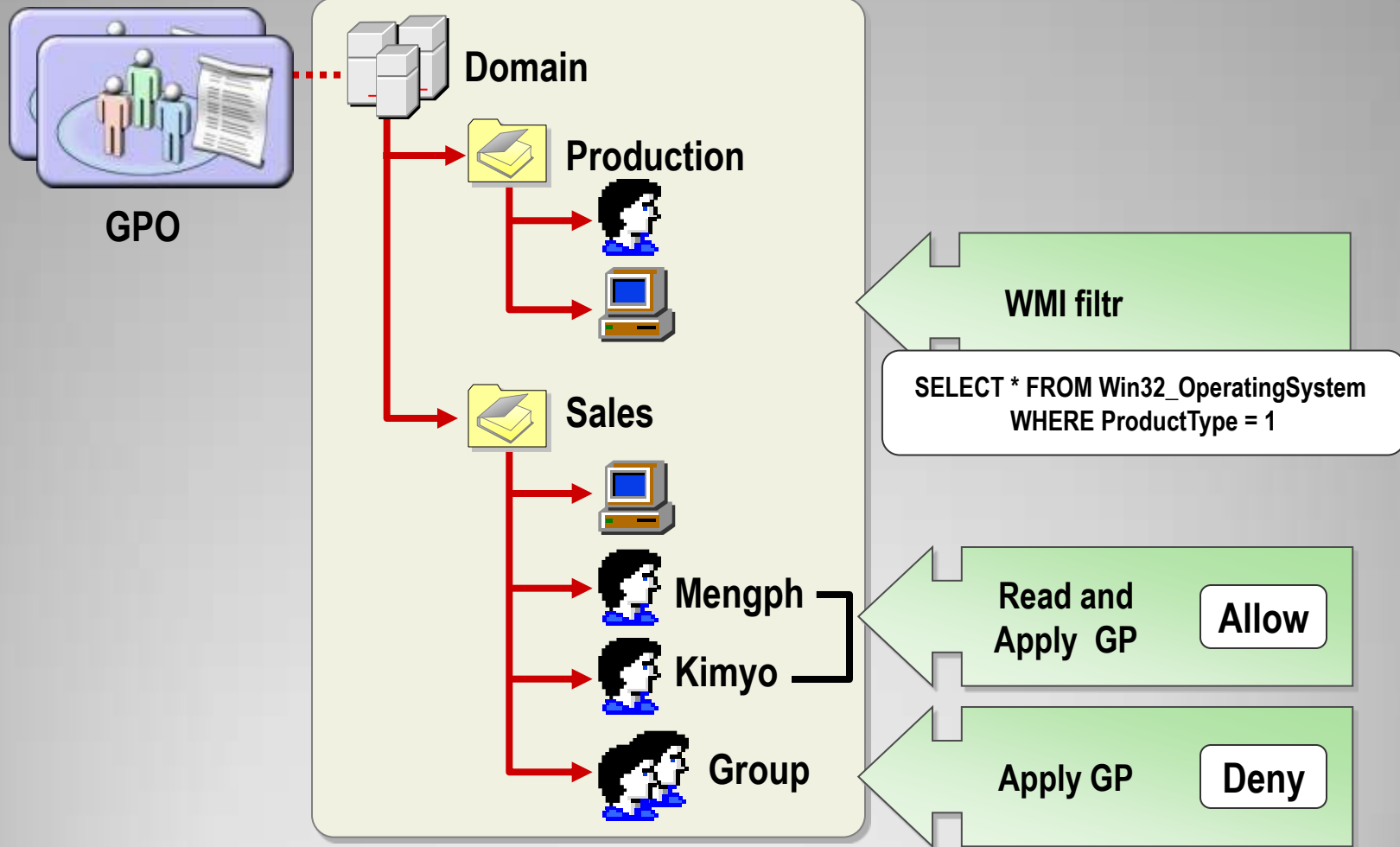
Pokud nastane konflikt při nasazení GPO, vyhrává GPO podřízeného kontejneru.

Konfliktní jsou jednotlivá nastavení, nikoliv celé GPO.

Také „enforced“ GPO vyhrává.

...

## Konflikty GPO



# Filtrování při nasazení GP

- Správa uživatelů a počítačů
- Nasazení softwaru
- Vynucení zabezpečení
- Vynucení konfigurace pracovního prostředí
- Vynutit a spravovat členství ve skupinách
- Použití „loopback processingu“

**Typické využití GP**

**Prohibit access to the Control Panel**

Prohibit access to the Control Panel

Previous Setting    Next Setting

Not Configured    Comment:

Enabled

Disabled

Supported on:

Options:

Help:

Disables all Control Panel programs

This setting Prohibit access to the Control Panel, from the Control Panel, from the Control Panel, or run any Control Panel programs.

This setting Prohibit access to the Control Panel, from the Control Panel, from the Control Panel, or run any Control Panel programs. This setting also Prohibit access to the Control Panel, from the Control Panel, from the Control Panel, or run any Control Panel programs. Explorer.

If users try to access the Control Panel on a context menu, this setting prevents the Control Panel from opening.

**Proxy Settings**

Proxy Settings

You can specify what proxy servers, if any, you want your users to connect to. Use semicolons (;) to separate entries. Gopher cannot be customized in Internet Explorer 7 and later.

Enable proxy settings

Proxy Servers	Address of proxy	Port
1. HTTP:	<input type="text"/>	<input type="text" value="80"/>
2. Secure:	<input type="text"/>	<input type="text" value="80"/>
3. FTP:	<input type="text"/>	<input type="text" value="80"/>
4. Gopher:	<input type="text"/>	<input type="text" value="80"/>
5. Socks:	<input type="text"/>	<input type="text"/>

Use the same proxy server for all addresses

**Exceptions**

Do not use proxy server for addresses beginning with:

Do not use proxy server for local (intranet) addresses.

OK    Cancel    Apply    Help

# Konfigurace nastavení

- Pro počítače
  - Startup scripty
  - Shutdown scripty
- Pro uživatele
  - Logon scripty
  - Logoff scripty

Skripty mohou být umístěny ve složce SYSVOL a replikovány na všechny DC

**Skripty v GP**



Skripty v politikách mohou:

- Provádět úkoly, které nelze nakonfigurovat v GP (nebo by bylo nutné zkompilovat vlastní GP)
- Vyčistit prostředí a vrátit počítač do původního stavu
- Zajistit bezpečné prostředí např. smazáním temp složek atd.

Od Windows 2008 lze často místo skriptů využít „preferences“

**Proč skripty?**



# Software a GP

Omezení spouštění aplikací  
Instalace aplikací

- SRP identifikuje a řídí spouštění softwaru na klientských počítačích
- Omezuje instalaci softwaru a pomáhá chránit před nákazou
- Základní komponenty jsou skupiny softwaru
  - Unrestricted
  - Disallowed
  - Výjimky z výchozích pravidel

## Software Restriction Policy

### Hash Rule

- Pro identifikaci softwaru se používají MD5 nebo SHA1 hashe
- Používá se pro povolení nebo omezení konkrétních verzí programu/souboru

### Certificate Rule

- Kontroluje přítomnost digitálních podpisů aplikace
- Lze využít např. pro omezení spuštění Win32 aplikací nebo ActiveX komponent

### Path Rule

- Umožní definovat cestu k souboru
- Vhodné pro více souborů v programové složce
- Klíčové při zpřísněném režimu

### Internet Zone Rule

- Řídí přístupy pro jednotlivé zóny
- Pro maximální možnosti zabezpečení přístupů k webovým aplikacím

# Pravidla pro SRP

**Group Policy Management Editor**

File Action View Help

Default Domain Policy [ACMEDC1.ACME.CORP] Policy

- Computer Configuration
  - Policies
    - Software Settings
    - Windows Settings
      - Name Resolution Policy
      - Scripts (Startup/Shutdown)
      - Security Settings
        - Account Policies
        - Local Policies
        - Event Log
        - Restricted Groups
        - System Services
        - Registry
        - File System
        - Wired Network (IEEE 802.3) Policies
        - Windows Firewall with Advanced Security
        - Network List Manager Policies
        - Wireless Network (IEEE 802.11) Policies
        - Public Key Policies
        - Software Restriction Policies
        - Network Access Protection
        - Application Control Policies
          - AppLocker**
            - Executable Rules
            - Windows Installer Rules
            - Script Rules

**Create Executable Rules**

**Conditions**

Before You Begin

Permissions

**Conditions**

Publisher

Exceptions

Name

Select the type of primary condition that you would like to create.

- Publisher**  
Select this option if the application you want to create the rule for is signed by the software publisher.
- Path**  
Create a rule for a specific file or folder path. If you select a folder, all files in the folder will be affected by the rule.
- File hash**  
Select this option if you want to create a rule for an application that is not signed.

Action	User	Name	Condition
✓ Allow	Everyone	(Default Rule) All files located in the Program Files folder	Path
✓ Allow	Everyone	(Default Rule) All files located in the Windows folder	Path
✓ Allow	BUILTIN\Admini...	(Default Rule) All files	Path
✓ Allow	Everyone	Program Files: MICROSOFT® WINDOWS® OPERATING SYSTEM signe...	Publisher
✓ Allow	Everyone	Program Files: MICROSOFT SQL SERVER signed by O=MICROSOFT C...	Publisher
✓ Allow	Everyone	Program Files: WINDOWS® INTERNET EXPLORER signed by O=MICR...	Publisher

# Application Control Policies (AppLocker, jen pro W7 Ult+Ent)

**Create Executable Rules**

### Publisher

Before You Begin  
Permissions  
Conditions  
**Publisher**  
Exceptions  
Name

Browse for a signed file to use as a reference for the rule. Use the slider to select which properties define the rule; as you move down, the rule becomes more specific. When the slider is in the any publisher position, the rule is applied to all signed files.

Reference file:  
C:\Thunderbird\ThunderbirdPortable.exe

Any publisher  
 Publisher: O=RARE IDEAS, LLC, L=NEW YORK, S=NY, C=l  
 Product name: MOZILLA THUNDERBIRD, PORTABLE EDITION  
 File name: THUNDERBIRDPORABLE.EXE  
 File version: 1.6.11.0

Use custom values  
Rule scope:  
Applies to the publisher, product name, file name, and file version

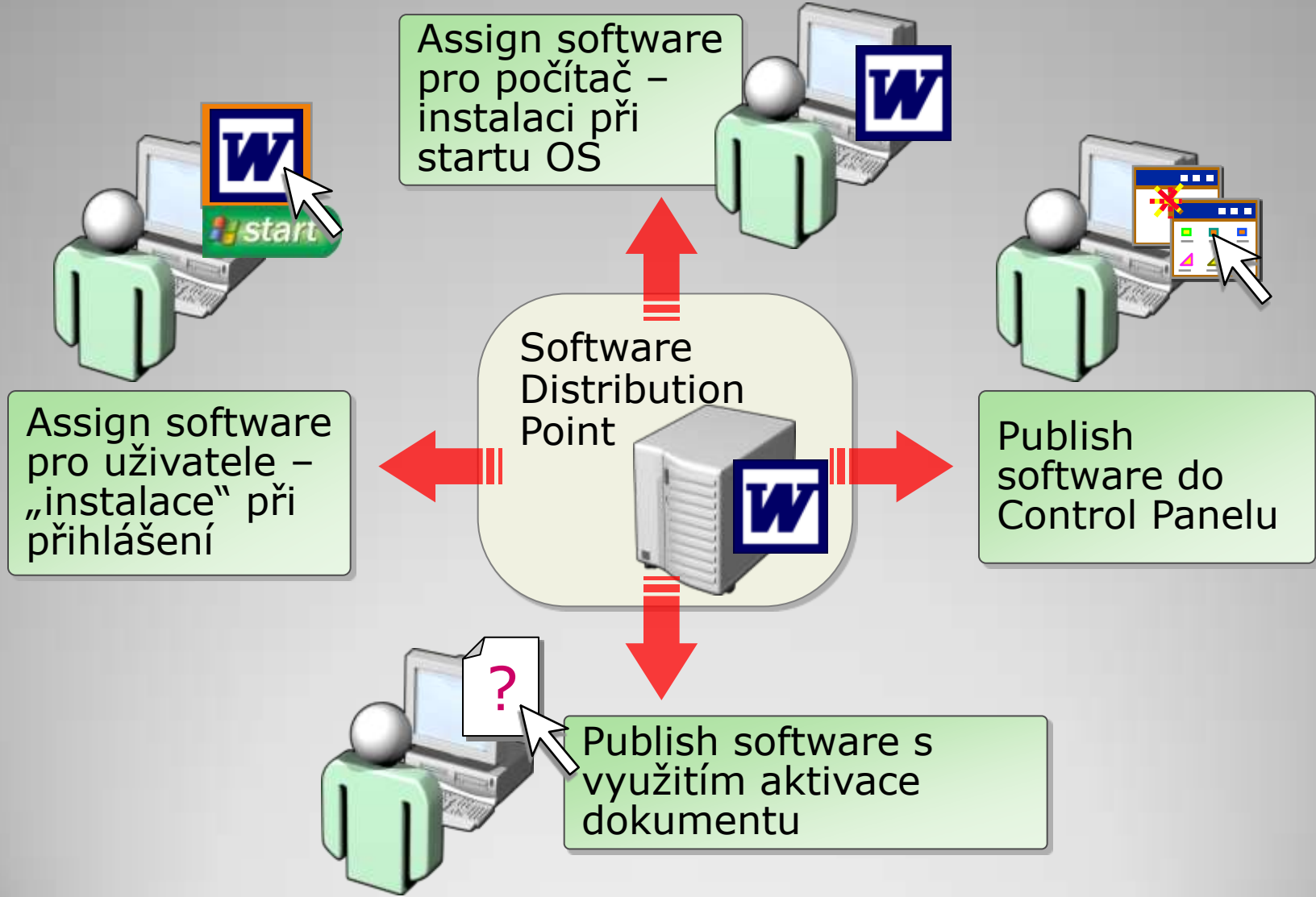
[More about publisher rules](#)

< P

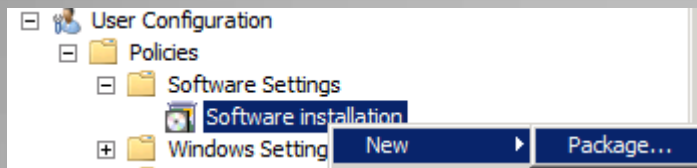
Any publisher  
 Publisher: O=RARE IDEAS, LLC, L=NEW YORK, S=NY, C=l  
 Product name: MOZILLA THUNDERBIRD, PORTABLE EDITION  
 File name: \*  
 File version: \*

Use custom values  
Rule scope:  
Applies to all files signed by the specified publisher with this product name.

# Application Control Policies (AppLocker)



# Ukázky možností instalace SW



**7-Zip 9.10 (x64 edition) Properties** [?] [X]

General | Deployment | Upgrades | Categories | Modifications | Security

Name:

Product information

Version: 9.10  
Publisher:  
Language: English (United States)  
Platform: x64

Support information

Contact:  
Phone:  
URL:

OK Cancel

**7-Zip 9.10 (x64 edition) Properties** [?] [X]

General | Deployment | Upgrades | Categories | Modifications | Security

Deployment type

Published  
 Assigned

Deployment options

Auto-install this application by file extension activation  
 Uninstall this application when it falls out of the scope of management  
 Do not display this package in the Add/Remove Programs control panel  
 Install this application at logon

Installation user interface options

Basic  
 Maximum

Advanced...

OK Cancel

# Nasazení nového balíčku


















Pracovní prostředí

Folder Redirection umožňuje:

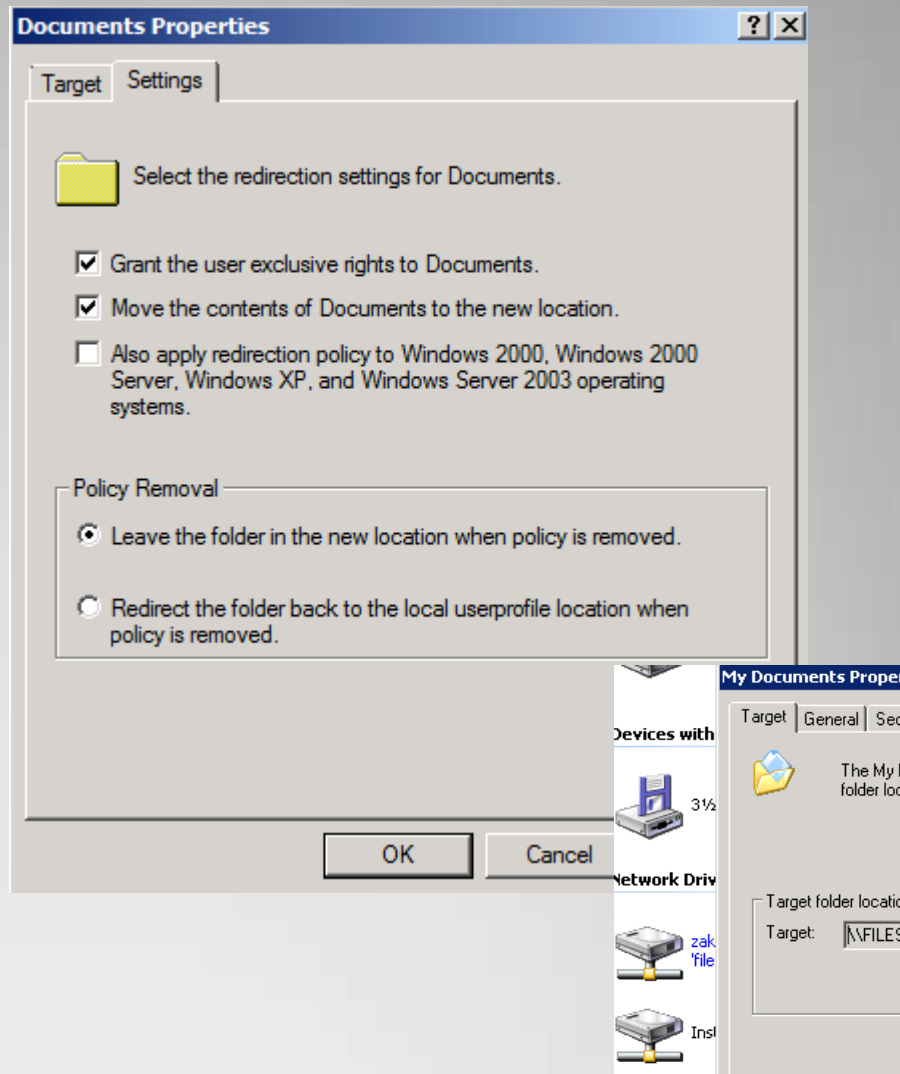
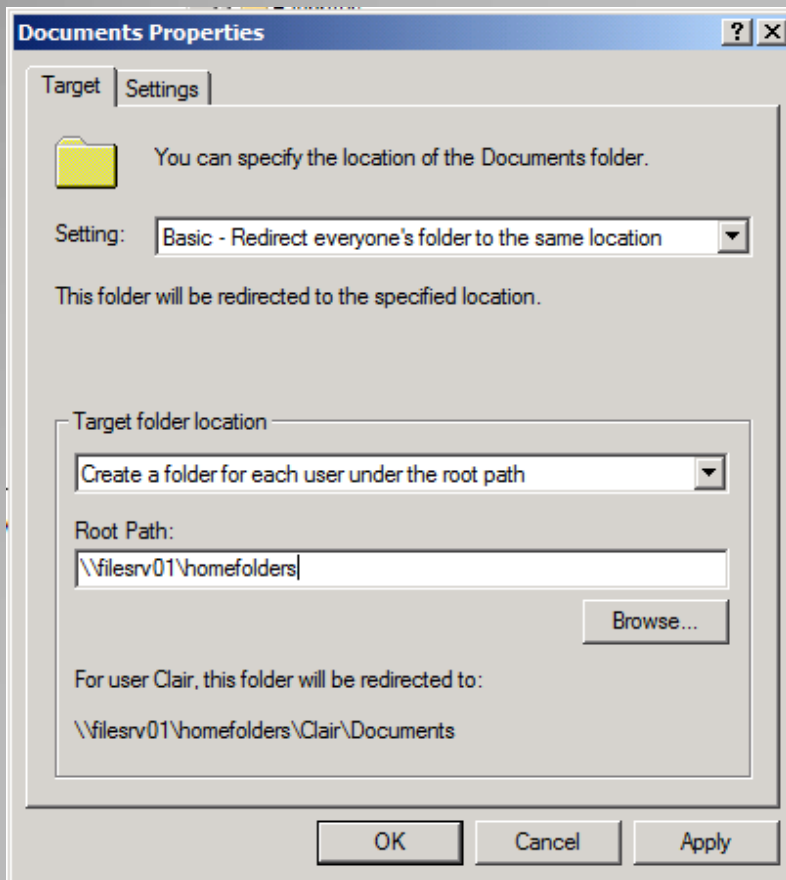
- Přesměrování složek v rámci lokálního počítače nebo na síťový disk
- Transparentnost vůči uživatelům – uživatel nevidí rozdíl
- Usnadní použití cestovních profilů (roaming profiles)
- Uživatel neřeší U:\ , X:\

**Přesměrování složek  
(Folder Redirection)**

- **Basic**  
stejné nastavení pro všechny
- **Advanced**  
rozdílné nastavení pro různé skupiny uživatelů
- **Follow the Documents folder**  
vytvoří podsložku ve složce Documents
- **Not configured**

Name
 AppData(Roaming)
 Desktop
 Start Menu
 Documents
 Pictures
 Music
 Videos
 Favorites
 Contacts
 Downloads
 Links
 Searches
 Saved Games

## Konfigurace Folder Redirection



# Přesměrování složky Documents

- NTFS práva pro root složku
- Shared folder práva pro root složku
- NTFS práva pro každou uživatelskou složku
- IPSec
- Dostatečný výkon serveru a sítě
- Zálohování
- Nastavení diskových kvót
- ...

**Zabezpečení přesměrovaných složek**



Další nástroje pro diagnostiku GP

- Manuální obnovení aktualizovaných politik
- Vynucení aplikování nastavení
- Další možnosti jako restart nebo odhlášení v případě potřeby

```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>gpupdate
Updating Policy...

User Policy update has completed successfully.
Computer Policy update has completed successfully.

C:\Users\Administrator>gpupdate /force /logoff
Updating Policy...

User Policy update has completed successfully.
Computer Policy update has completed successfully.
```

**Gpupdate.exe**

```
Administrator: Command Prompt
C:\Users\Administrator>gpresult /r

Microsoft (R) Windows (R) Operating System Group Policy Result tool v2.0
Copyright (C) Microsoft Corp. 1981-2001

Created On 10/12/2011 at 3:37:26 PM

RSOP data for ACME\Administrator on ACME/DC1 : Logging Mode
-----
OS Configuration:           Primary Domain Controller
OS Version:                 6.1.7600
Site Name:                  Default-First-Site-Name
Roaming Profile:            N/A
Local Profile:              C:\Users\Administrator
Connected over a slow link?: No

COMPUTER SETTINGS
-----
CN=ACME/DC1,OU=Domain Controllers,DC=acme,DC=corp
Last time Group Policy was applied: 10/12/2011 at 3:35:39 PM
Group Policy was applied from: ACME/DC1.acme.corp
Group Policy slow link threshold: 500 kbps
Domain Name: ACME
Domain Type: Windows 2000

Applied Group Policy Objects
-----
Default Domain Controllers Policy
Default Domain Policy

The following GPOs were not applied because they were filtered out
-----
Local Group Policy
Filtering: Not Applied (Empty)

The computer is a part of the following security groups
-----
BUILTIN\Administrators
Everyone
BUILTIN\Users
BUILTIN\Pre-Windows 2000 Compatible Access
Windows Authorization Access Group
NT AUTHORITY\NETWORK
NT AUTHORITY\Authenticated Users
This Organization
ACME/DC1$
Domain Controllers
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS
Denied RODC Password Replication Group
System Mandatory Level

USER SETTINGS
```

- Zobrazení výsledné sady zásad pro uživatele a počítač
- Vygenerování souboru v výslednými zásadami (htm)

Gpresult.exe



The screenshot displays the Group Policy Management console. The left pane shows the tree structure for the Forest: acme.corp, with the path Group Policy Results > Administrator on ACMEDC1 selected. The right pane shows the 'Group Policy Results' for the user 'Administrator on ACME\ACMEDC1', with data collected on 10/12/2011 at 2:31:43 PM. The results are categorized into Computer Configuration, Policies, Windows Settings, Security Settings, and Account Policies. The Account Policies section is expanded to show three sub-sections: Account Policies/Password Policy, Account Policies/Account Lockout Policy, and Account Policies/Kerberos Policy, each with a table of policy settings and their winning GPO.

**Administrator on ACMEDC1**  
 Summary Settings Policy Events

**Group Policy Results**

ACME\Administrator on ACME\ACMEDC1  
 Data collected on: 10/12/2011 2:31:43 PM

**Computer Configuration** [hide all](#) [hide](#)

**Policies** [hide](#)

**Windows Settings** [hide](#)

**Security Settings** [hide](#)

**Account Policies/Password Policy** [hide](#)

Policy	Setting	Winning GPO
Enforce password history	24 passwords remembered	Default Domain Policy
Maximum password age	0 days	Default Domain Policy
Minimum password age	1 days	Default Domain Policy
Minimum password length	7 characters	Default Domain Policy
Password must meet complexity requirements	Enabled	Default Domain Policy
Store passwords using reversible encryption	Disabled	Default Domain Policy

**Account Policies/Account Lockout Policy** [hide](#)

Policy	Setting	Winning GPO
Account lockout threshold	0 invalid logon attempts	Default Domain Policy

**Account Policies/Kerberos Policy** [hide](#)

Policy	Setting	Winning GPO
Enforce user logon restrictions	Enabled	Default Domain Policy
Maximum lifetime for service ticket	600 minutes	Default Domain Policy
Maximum lifetime for user ticket	10 hours	Default Domain Policy
Maximum lifetime for user ticket renewal	7 days	Default Domain Policy
Maximum tolerance for computer clock synchronization	5 minutes	Default Domain Policy

**Reporty – výsledné zásady**

## Group Policy Management

File Action View Window Help



- Group Policy Management
  - Forest: acme.corp
    - Domains
      - acme.corp
        - Default Domain Policy
        - ACME
          - Groups
          - Servers
          - Service Accounts
          - Users
          - Workstations
        - Domain Controllers
          - Default Domain Controllers Policy
        - Group Policy Objects
          - Default Domain Controllers Policy
          - Default Domain Policy
        - WMI Filters
        - Starter GPOs
      - Sites
      - Group Policy Modeling
        - Administrator on ACMEDC1
        - SQLAdm on Workstations
      - Group Policy Results
        - Administrator on ACMEDC1

## Group Policy Modeling

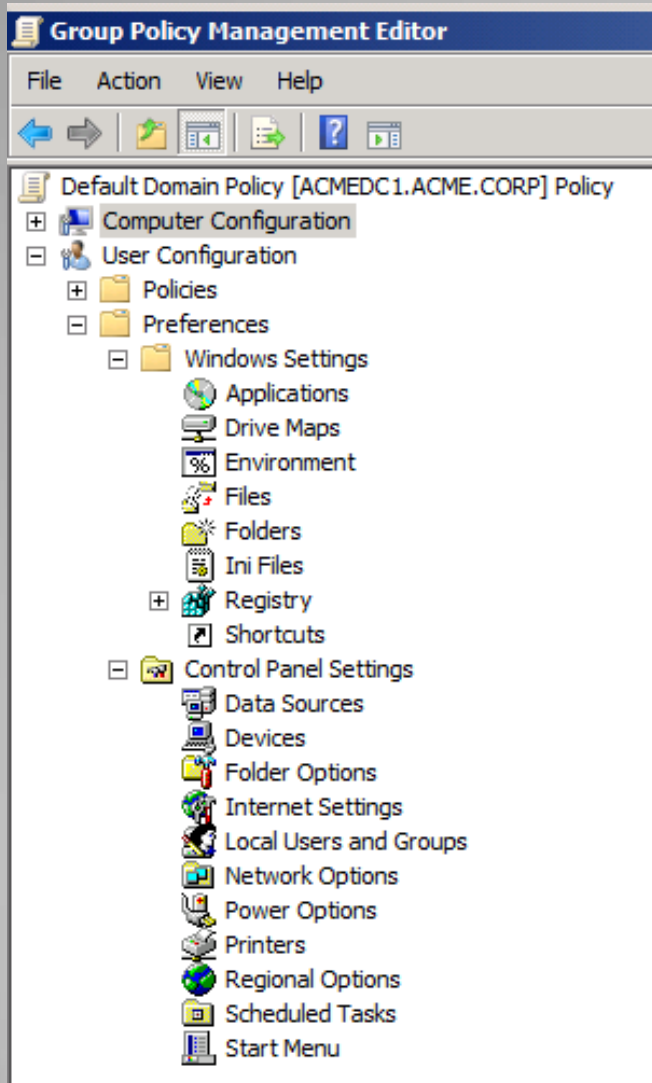
Contents

Name ^	User	Computer
Administrator on ACMEDC1	ACME\Administrator	ACME\ACMEDC1\$
SQLAdm on Workstations	ACME\SQLAdm	

# Group Policy Modeling



Preferences




- **Policies** neumožňují uživateli změnit nastavení.
- **Preferences** přidávají další možnosti. Mohou se aplikovat jednorázově nebo opakovaně. Uživatel má možnost provádět změny nastavení.

# Preferences

**New Drive Properties** [X]

General | Common

 Action: Create

Location: \\filesrv01\install ...

Reconnect:  Label as: Instalacni media

Drive Letter

Use first available, starting at:  Use: U

Connect as (optional)

User name:

Password:  Confirm password:

Hide/Show this drive

No change  
 Hide this drive  
 Show this drive


Hide/Show all drives

No change  
 Hide all drives  
 Show all drives

OK Cancel Apply Help

**New Environment Properties** [X]

General | Common

 Action: Update

User Variable  
 System Variable

Name: PATH or  PATH  Partial

Value: C:\Tools

Details

The PATH variable contains a list of semicolon delimited folder paths that Windows uses when locating files. Update will replace the FULL path variable as specified. This will remove all previously existing path values.

OK Cancel Apply Help

# Preferences - příklady

**New Shortcut Properties**

General Common

Action: Create

Name: Poznamkovy blok

Target type: File System Object

Location: Desktop

Target path: notepad.exe

Arguments:

Start in:

Shortcut key: None

Run: Normal Window

Comment:

Icon file path:

Icon index: 0

OK Cancel

**New Shortcut Properties**

General Common

Options common to all items

- Stop processing items in this extension if an error occurs
- Run in logged-on user's security context (user policy option)
- Remove this item when it is no longer applied
- Apply once and do not reapply
- Item-level targeting Targeting...

**Targeting Editor**

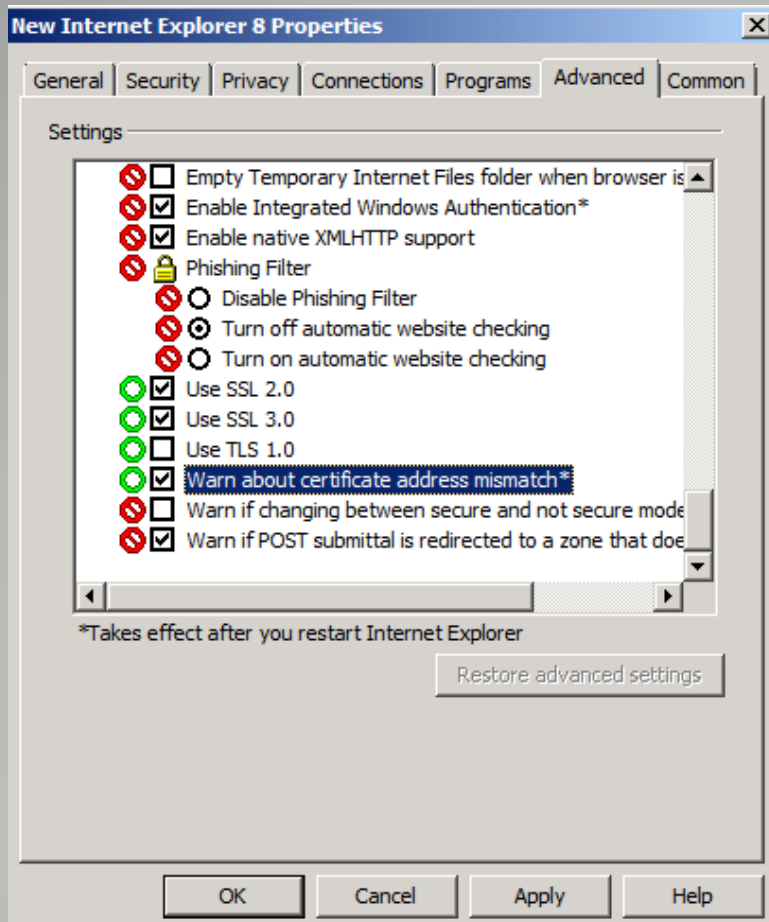
New Item Add Collection Item Options Delete Help

- the CPU speed is greater than or equal to 1000 MHz
- AND the total RAM is greater than or equal to 2048 MB
- AND this collection is true
- the operating system is Windows Vista
- OR the operating system is Windows 7
- OR this collection is true
- AND the date is December 24

greater than or equal to 1000 MHz

A CPU Speed targeting item allows a preference item to be applied to computers or users only if the processing

# Preferences – možnosti



- **F5** – Konfigurace všech nastavení
- **F6** – Konfigurace vybraného nastavení
- **F7** – Ignorování vybraného nastavení
- **F8** – Ignorování všech nastavení

**Preferences – F5 F6 F7 F8**

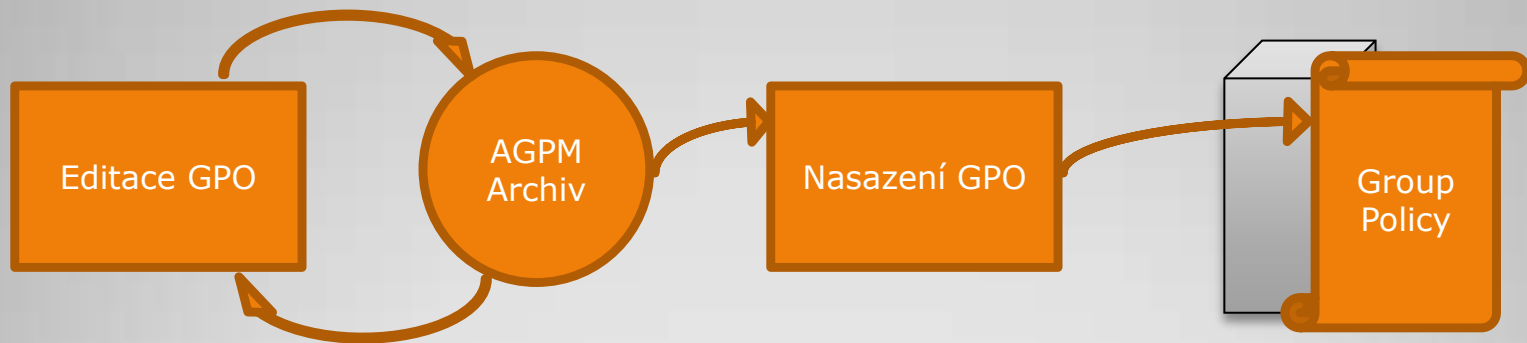


# Advanced Group Policy Management

AGPM



- Archiv AGPM poskytuje offline úložiště pro GPO
- Změny v GPO jsou ukládány do archivu a neovlivňují produkční prostředí dokud nejsou schváleny a nasazeny do produkce.



**Offline editace**

**Group Policy Management**

File Action View Window Help

Group Policy Management

- Forest: app.te
  - Domains
    - app.te
      - Default Domain P...
      - gpo1
      - gpo2
      - gpo3
      - Change Control
      - Domain Controller
      - Group Policy Obj...
      - WMI Filters
      - Starter GPOs
    - Sites
      - Group Policy Modeling
      - Group Policy Results

**Change Control for app.te**

Contents | Domain Delegation | AGPM Server | Production Delegation

Search Group Policy objects

Controlled | Uncontrolled | Pending | Templates | Recycle Bin

Group Policy objects:

Name	State	Changed By	Change Date	Comment
gpo2	Checked in	Administrator (APP\Administrator)	2/4/2011 4:26:28 PM	
New Group Policy Object	Checked out	Administrator (APP\Administrator)	2/7/2011 12:56:18 PM	

These groups and users have these roles for the selected GPO in the archive:

Name	Roles	Inherited
Administrator (APP\Administrator)	Full Control	Yes
SVC_AGPM (svc_agpm@app.te)	Full Control	Yes

Add... Remove Properties Advanced...

**History for gpo2**

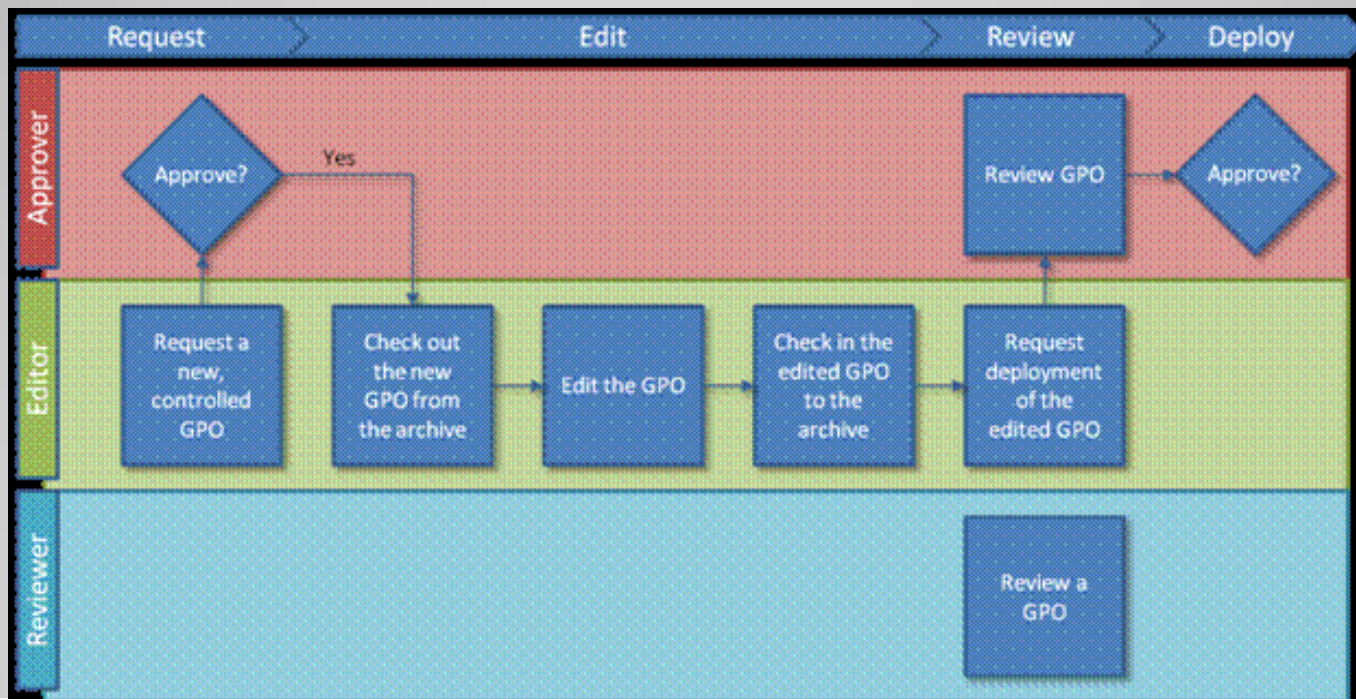
The history of this Group Policy object:

All States | Unique Versions

Change Date	State	Changed By	Comment	Deletable	Comput
2/4/2011 4:26:28 PM	Controlled	Administrator (APP\A...		Yes	1
2/4/2011 4:26:28 PM	Production: Current	SVC_AGPM (svc_agp...		Not applicable	1
2/4/2011 2:28:52 PM	Production: Created	*		Not applicable	*

# Integrace do GPMC

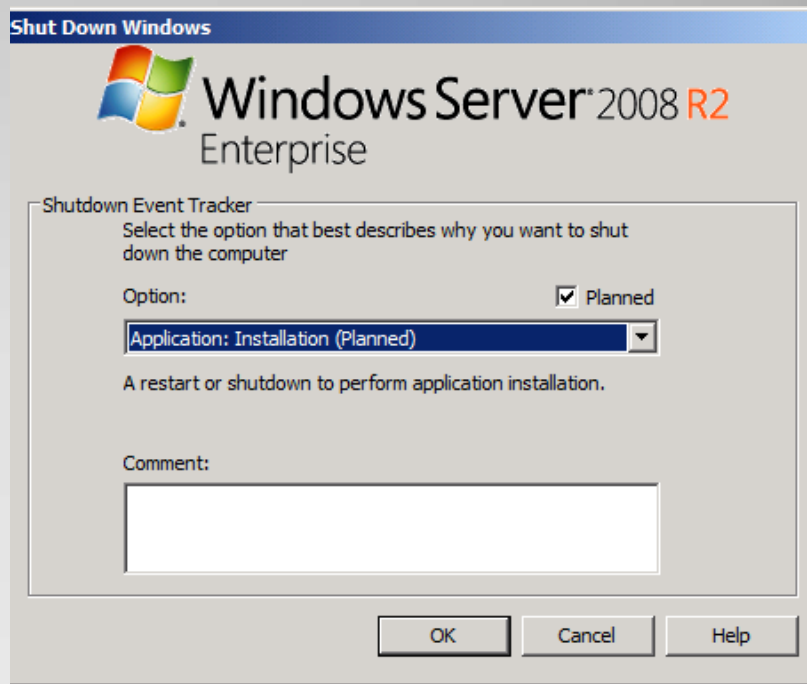
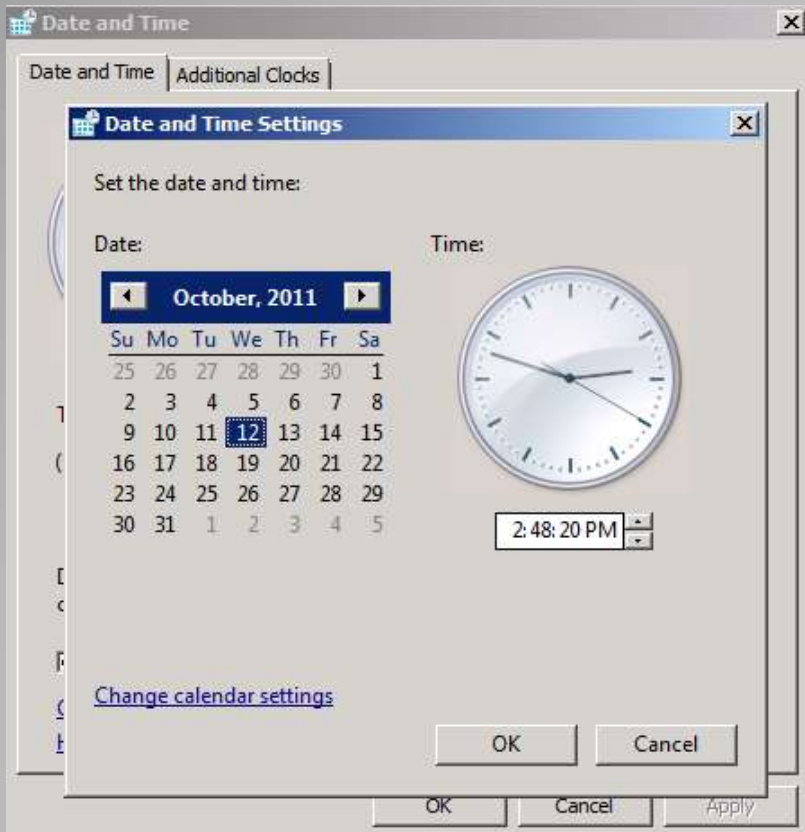
- **Reviewer** může číst a porovnávat GPO. Nemůže GPO editovat ani nasazovat do produkce (deploy).
- **Editor** může číst a porovnávat GPO. Může vyjmout GPO z archivu (check out), editovat GPO a vkládat je zpět (check in). Může požádat a o nasazení.
- **Approver** může schválit či zamítnout vytvoření nebo nasazení GPO.



## AGPM – delegování rolí

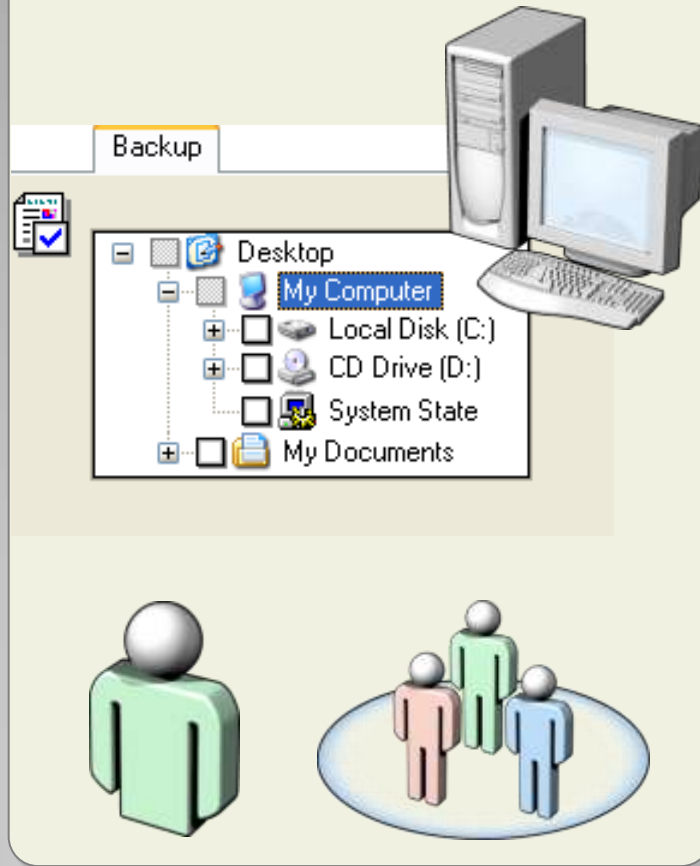


# Rights vs. Permissions

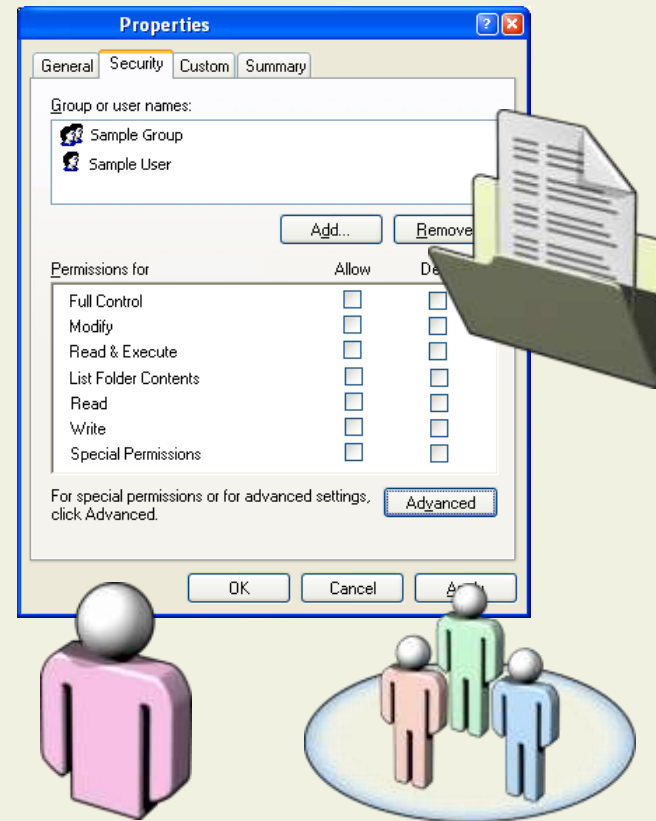


# Příklady „User Rights“

## User Rights: Akce v systému



## Permissions: Operace s objekty



# Rights vs. Permissions