

Windows 2008 R2 - úvod



Lumír Návrat

Operační systémy Windows

Stručný přehled

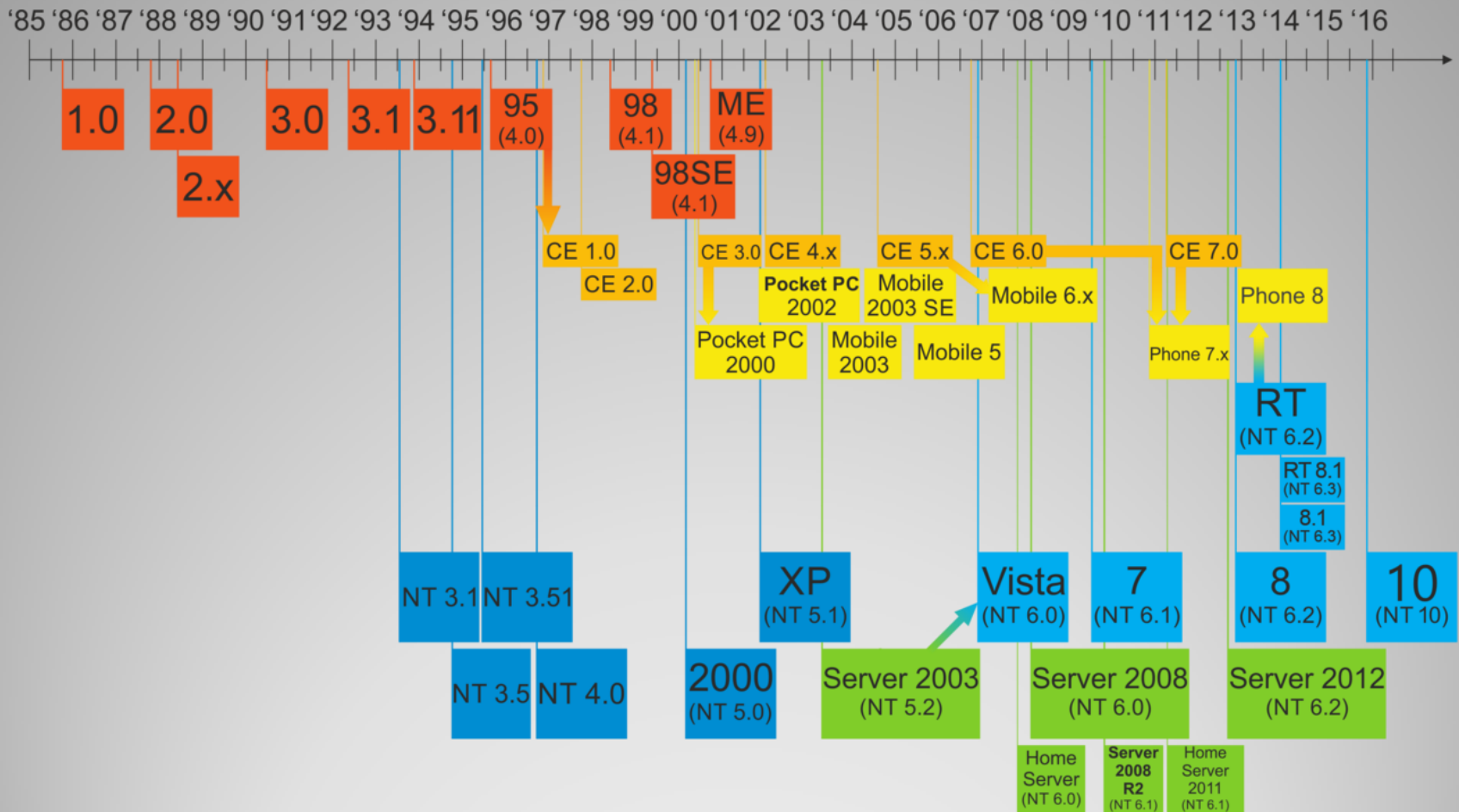
Klientské OS

- Windows 95, 98, ME
- Windows NT
- Windows 2000
- Windows XP
- Windows Vista
- Windows 7
- Windows 8
- Windows 8.1
- Windows 10
- Windows CE, Windows Mobile
- Windows Phone 7...

Serverové OS

- Windows NT
- Windows 2000 Server
- Windows 2003 (R2)
- Windows 2008
- Windows 2008 R2
- Windows 2012 (R2)
- Windows 2016 (rel. 09/16)

Stručný přehled verzí Windows



http://en.wikipedia.org/wiki/Microsoft_Windows

Poznámka: Veškeré údaje pocházející z wikipedií nelze bez dalšího ověření považovat za směrodatné a správné!

Vývoj OS Windows

32 bit

- Starší počítače
- Omezená paměť RAM (obvykle max. 4 GB)
- Nižší výkon
- Nejnovější funkce OS nemusí být dostupné
- Některé aplikace vyžadují 32bit OS

64 bit

- Je potřeba „novější“ hardware
- Vyšší výkon (aplikace však musí být také 64 bitové)
- Kompatibilní se 32 bit programy
- Výjimečně se mohou objevit problémy s ovladači zařízení
- Pozor - X64 vs. Itanium!

Kterou platformu?



Home
Premium



Home
Premium N



Professional



Professional
N



Ultimate



Ultimate N

Funkce	Home Premium	Home Premium N	Professional	Professional N	Ultimate	Ultimate N
Usnadnění každodenních činností pomocí vylepšené navigace na ploše.	✓	✓	✓	✓	✓	✓
Rychlejší a jednodušší vyhledávání programů a rychlé vyhledání nejčastěji používaných dokumentů.	✓	✓	✓	✓	✓	✓
Sledujte řadu svých oblíbených TV pořadů zdarma, kdykoli se vám zachce, s funkcí Internet TV.	✓		✓		✓	
Spouštění řady programů produktivity systému Windows XP pomocí technologie Windows XP Mode.			✓	✓	✓	✓
Snadnější a bezpečnější připojení k firemním sítím pomocí funkce Připojení k doméně.			✓	✓	✓	✓
Kromě úplné funkce Zálohování a obnovení, která je k dispozici ve všech edicích, můžete provést zálohování v domácí nebo firemní síti.			✓	✓	✓	✓
Pomoc při ochraně dat v počítači a přenosných úložných zařízeních před ztrátou nebo odcizení pomocí nástroje BitLocker.					✓	✓
Možnost práce v jazyce dle vlastní volby a přepínání mezi 35 jazyky.					✓	✓

<http://windows.microsoft.com/cs-CZ/windows7/products/compare>

Kterou edici? (W7)

Porovnání edic podle rolí serveru

Legenda: ○ = Nedostupné ● = Dostupné částečně/omezeně ✓ = Plně dostupné

Server Role	Enterprise	Datacenter	Standard	Itanium	Web	Foundation	HPC
Active Directory Certificate Services	✓	✓	● ¹	○	○	● ¹	● ¹
Active Directory Domain Services	✓	✓	✓	○	○	✓	✓
Active Directory Federation Services	✓	✓	○	○	○	○	○
Active Directory Lightweight Directory Services	✓	✓	✓	○	○	✓	○
Active Directory Rights Management Services	✓	✓	✓	○	○	✓	○
Application Server	✓	✓	✓	✓	○	✓	○
DHCP Server	✓	✓	✓	○	○	✓	✓
DNS Server	✓	✓	✓	○	✓	✓	✓
Fax Server	✓	✓	✓	○	○	✓	○
File Services	✓	✓	● ²	○	○	● ²	● ²
Hyper-V	✓	✓	✓	○	○	○	✓
Network Policy and Access Services	✓	✓	● ³	○	○	● ⁵	● ³
Print and Document Services	✓	✓	✓	○	○	✓	○
Remote Desktop Services	✓	✓	● ⁴	○	○	● ⁶	● ⁴
Web Services (IIS)	✓	✓	✓	✓	✓	✓	✓
Windows Deployment Services	✓	✓	✓	○	○	✓	✓
Windows Server Update Services (WSUS)	✓	✓	✓	○	✓	✓	✓

1 Omezeno na vytváření certifikačních autorit – bez dalších funkcí ADACS (NDES, Online Responder Service). Více informací naleznete v dokumentaci role ADACS na webu TechNet.

2 Omezeno na 1 samostatný kořenový adresář (standalone DFS root).

3 Omezeno na 250 RRAS připojení, 50 IAS připojení a na 2 IAS Server Groups.

4 Omezeno na 250 připojení Remote Desktop Services.

5 Omezeno na 50 RRAS připojení, 10 IAS připojení.

6 Omezeno na 50 připojení Remote Desktop Services.

Kterou edici? (W2008 R2)

Porovnání edic podle technické specifikace

Legenda: ○ = nedostupné ● = dostupné

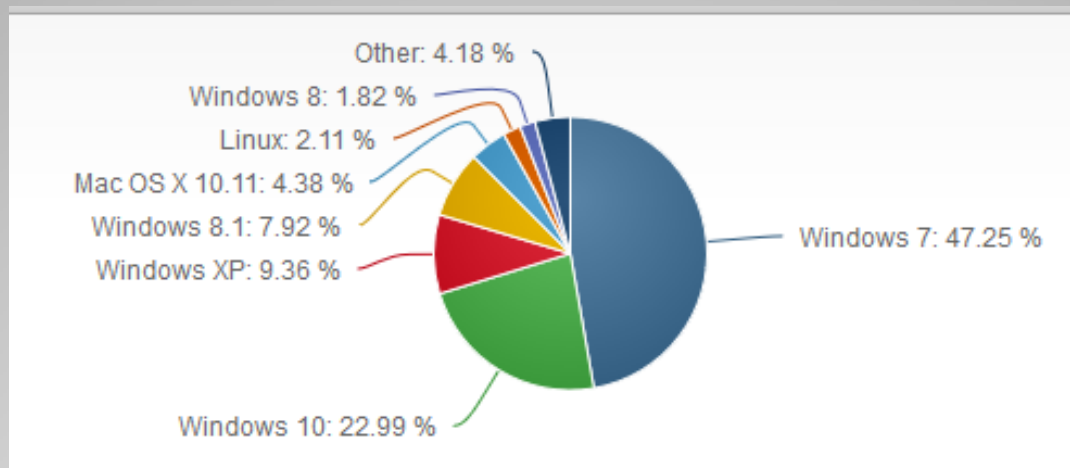
Specifikace	Web	Standard	Enterprise	Datacenter	Itanium	Foundation	HPC
Cross-File Replication (DFS-R)	○	○	●	●	●	○	○
Failover Cluster Nodes (Nodes)	○	○	16	16	8	○	○
Fault Tolerant Memory Sync	○	○	●	●	●	○	○
Hot Add Memory	○	○	●	●	●	○	○
Hot Add Processors	○	○	○	●	●	○	○
Hot Replace Memory	○	○	○	●	●	○	○
Hot Replace Processors	○	○	○	●	●	○	○
IA64 RAM	○	○	○	○	2 TB	○	○
IA64 Sockets	○	○	○	○	64	○	○
Network Access Connections (IAS)	○	50	Neomezeno	Neomezeno	2	10	○
Network Access Connections (RRAS)	○	250	Neomezeno	Neomezeno	○	50	250
Remote Desktop Admin Connections	2	2	2	2	2	2	2
Remote Desktop Services Gateway	○	250	Neomezeno	Neomezeno	○	50	○
Virtual Image Use Rights	Guest	Host+1VM	Host+4VM	Neomezeno	Neomezeno	○	Host+1VM
X64 RAM	32 GB	32 GB	2 TB	2 TB	○	8 GB	128 GB
X64 Sockets	4	4	8	64	○	1	4

Kterou edici? (W2008 R2)

Windows Server 2008 R2...	Orientační cena (ne OEM verze)	
Foundation	cca 5 000,-	Základ pro malé firmy
Standard	cca 16 000,-	Běžný standard
Enterprise	cca 65 000,-	Clustering
Datacenter	cca 150 000,-	
Web Server	cca 10 000,-	
For Itanium-Based Systems		Mnoho omezení, hlavně web služby
HPC		Super servery
Windows Small Business Server 2008 Standard /Premium	cca 19 000,- cca 31 000,-	Omezený počet uživatelů, mnoho sw navíc

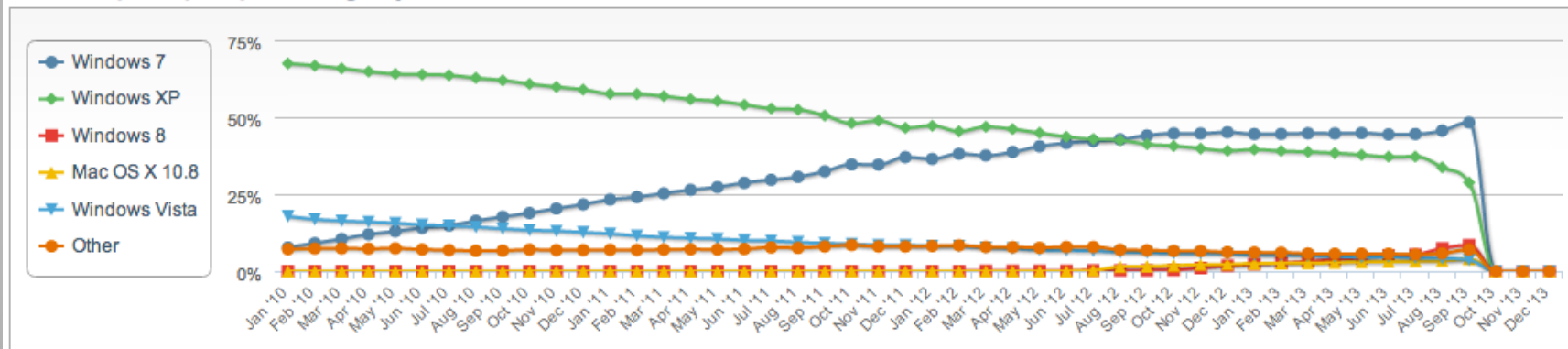
Kterou edici? (W2008 R2)

- Klientské desktopové OS (Web klienti)



Desktop Top Operating System Share Trend

Year 2010 to Year 2013



http://en.wikipedia.org/wiki/Usage_share_of_operating_systems

<http://www.netmarketshare.com/operating-system-market-share.aspx>

Poznámka: Veškeré údaje pocházející z wikipedií nelze bez dalšího ověření považovat za směrodatné a správné!

Podíly OS na trhu
(odhad Q3 2016 a Q3 2013)

• Serverové OS

Servery	%
Windows	50,2
NIX	38,9
Ostatní	10,9

Web Servery	%
Apache	61,45
IIS (Microsoft)	14,62
NGINX	11,09
GWS (Google)	3,4
Ostatní	9,44

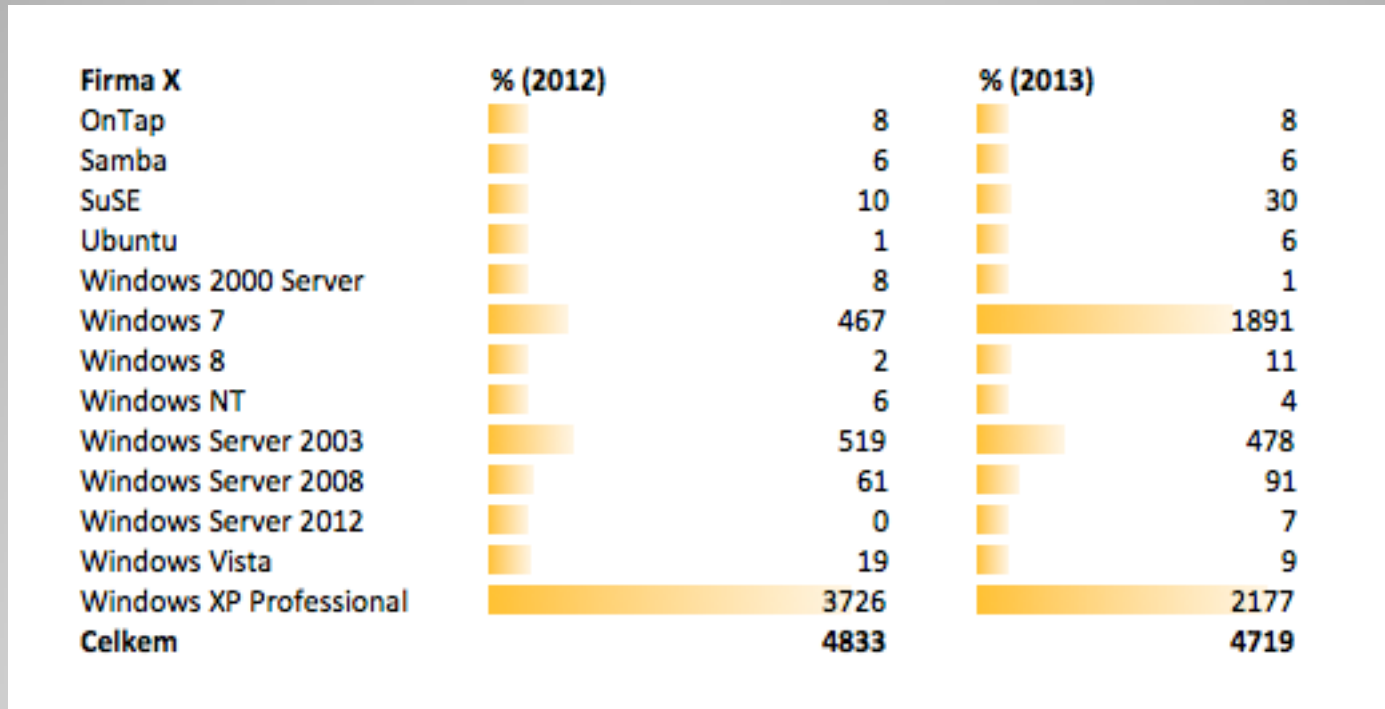
Top 500 Servery	%
Linux	92,4
Unix	4,8
Mixed	2,2
Windows	0,4
BSD	0,2

http://en.wikipedia.org/wiki/Usage_share_of_operating_systems
http://en.wikipedia.org/wiki/Web_server

Podíly OS na trhu

(velmi hrubý odhad Q2 2012)

- Firma „X“ (export z produkční Active Directory náhodně vybraného zákazníka)

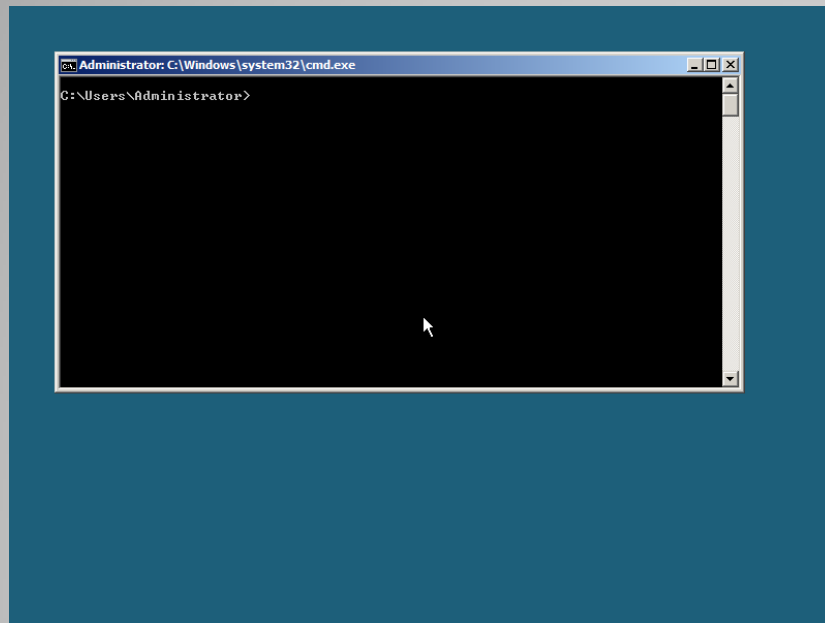


Get-ADComputer -Filter * -Properties * |Select-Object Name,OperatingSystem |ConvertTo-Csv |Out-File .\compy.csv

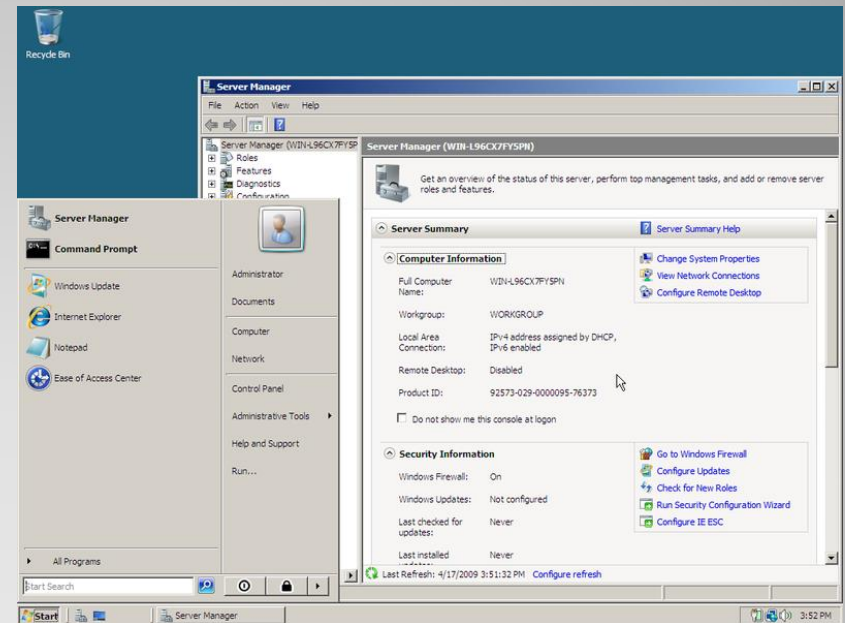
Příklad podílu OS ve firmě
(Q3 2012 a Q3 2013)

Windows Server 2008 R2

Core



Full



Windows Server 2008 R2



Install Windows



Select the operating system you want to install

Operating system	Architecture	Date modified
Windows Server 2008 R2 Standard (Full Installation)	x64	7/14/2009
Windows Server 2008 R2 Standard (Server Core Installation)	x64	7/14/2009
Windows Server 2008 R2 Enterprise (Full Installation)	x64	7/14/2009
Windows Server 2008 R2 Enterprise (Server Core Installation)	x64	7/14/2009
Windows Server 2008 R2 Datacenter (Full Installation)	x64	7/14/2009
Windows Server 2008 R2 Datacenter (Server Core Installation)	x64	7/14/2009
Windows Web Server 2008 R2 (Full Installation)	x64	7/14/2009
Windows Web Server 2008 R2 (Server Core Installation)	x64	7/14/2009

Description:

This option installs a minimal installation of Windows Server without the standard Windows user interface, and with a subset of server roles that can be managed from a command prompt, reducing management requirements and attack surface.

Windows Server 2008 R2

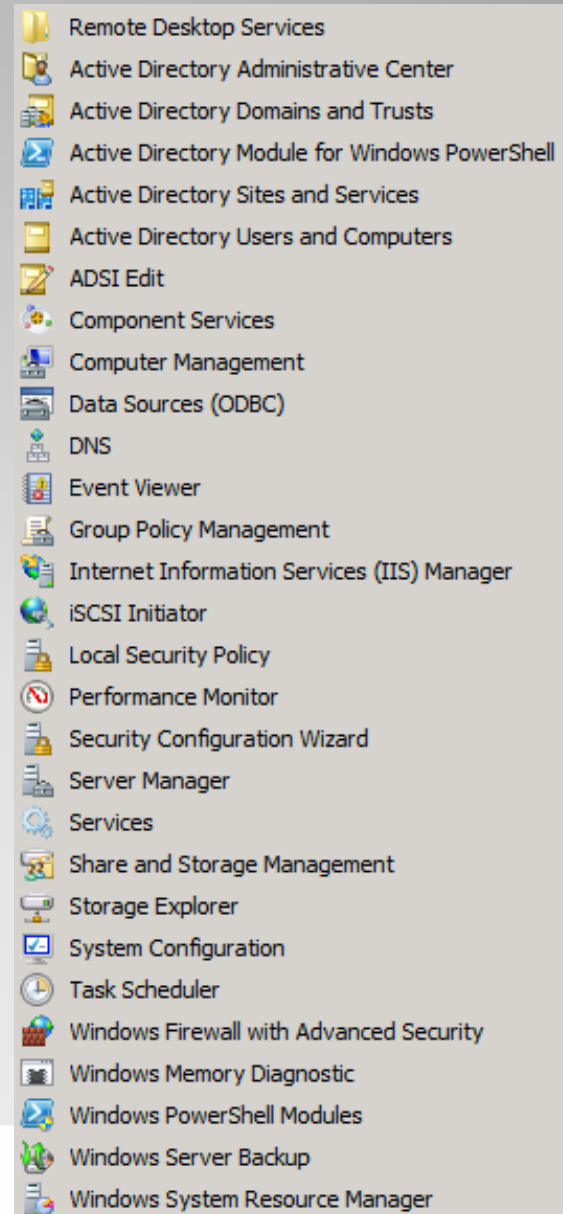
Výběr OS

Správa Windows serverů

Nástroje pro správu

- Nástupce AdminPaku z Windows 2000/2003
- Sada nástrojů umožňuje spravovat role a funkce („**roles**“ a „**features**“), které jsou nainstalovány na lokálním či vzdáleném počítači.

RSAT (Remote Server Administration Tools)



- **Microsoft Management Console**
 - Poskytuje rozhraní pro „snap-in“, které slouží pro správu hardware, software a síťových služeb
- **MMC** se pro vzdálenou správu používá k:
 - Provádění rutinních i příležitostných úkolů
 - Provádění stejných úkolů na více vzdálených počítačích
 - Urychluje přístup ke konfiguraci (není nutné používat vzdálenou plochu atd.)

MMC.EXE

```
Administrator: C:\Windows\system32\cmd.exe

C:\Users\Administrator>netsh interface ip show interfaces

Idx      Met      MTU      State      Name
-----
3        5        1500     connected  Local Area Connection
1        50       4294967295  connected  Loopback Pseudo-Interface 1

C:\Users\Administrator>netsh interface ipv4 set address name="Local Area Connection" source=static address=10.10.10.10 mask=255.255.255.0 gateway=10.10.10.1

C:\Users\Administrator>netsh interface ipv4 add dnsserver name="Local Area Connection" address=10.10.10.2 index=1
```

```
Administrator: C:\Windows\system32\cmd.exe

C:\Users\Administrator>hostname
WIN-R14UE6TN33Q

C:\Users\Administrator>netdom renamecomputer %computename% /NewName:SRV01
This operation will rename the computer WIN-R14UE6TN33Q
to SRV01.

Certain services, such as the Certificate Authority, rely on a fixed machine
name. If any services of this type are running on WIN-R14UE6TN33Q,
then a computer name change would have an adverse impact.

Do you want to proceed (Y or N)?
y
The computer needs to be restarted in order to complete the operation.
The command completed successfully.

C:\Users\Administrator>shutdown -r -t 5_
```

Příkazová řádka

PowerGUI Script Editor

File Edit View Go Debug Tools Help

<Input script parameters here>

certcheck.ps1

```

1 #Number of days to look for expiring certificates
2 $cthreshold = 30
3 #Set deadline date
4 $cdeadline = (Get-Date).AddDays($cthreshold)
5 $cstore=new-object System.Security.Cryptography.X509Certificates.X509Store("My", "LocalMachine")
6 $cstore.open("ReadOnly")
7 $cstore.certificates | % {
8
9 If ($_.NotAfter -lt $cdeadline) {
10
11 #$_ | Select Issuer, Subject, NotAfter, @{Label="ExpiresIn"; Expression={($_.NotAfter - (Get-Date)).Days}}
12
13 [void] [System.Reflection.Assembly]::LoadWithPartialName("System.Windows.Forms")
14
15 $objNotifyIcon = New-Object System.Windows.Forms.NotifyIcon
16
17 # $objNotifyIcon.Icon = "C:\Windows\Installer\{27B3563C-561C-4924-8C0E-EA102264873F}\CERTMgr.Ico"
18 $objNotifyIcon.Icon = "c:\Windows\System32\appverif.ico"
19 $objNotifyIcon.BalloonTipIcon = "Error"
20 $objNotifyIcon.BalloonTipText = "Certificate for this computer is about to expire. Please check certificate or co

```

Variables

- \$\$ C:\Users\zak
- Length 48
- \$^ .
- Length 1
- \$ \$null
- \$args \$null
- \$cdeadline 9.10.2011 10
- \$objNotifyIcon System.Wind
- BalloonTipText Certificate for t
- BalloonTipIcon Error
- value__ 3
- BalloonTipTitle Certificate expi
- Length 24
- ContextMenu \$null
- ContextMenuStrip \$null
- Icon (Icon)
- Text
- Visible True
- Tag \$null
- Site \$null

Windows PowerShell

```

PS C:\Users> get-host | format-table

```

Name	Version	InstanceId	UI	CurrentCulture	CurrentUICulture	PrivateData	IsRunspacePushed	Runspace
ConsoleHost	2.0	32fb72d6-b...	System.Ma...	cs-CZ	en-US	Microsoft...	False	System.Ma...

```

PS C:\Users> get-host | format-list

```

```

Name           : ConsoleHost
Version        : 2.0
InstanceId     : 32fb72d6-b49e-4fe7-8747-b714fd691d2a
UI             : System.Management.Automation.Internal.Host.InternalHostUserInterface
CurrentCulture : cs-CZ
CurrentUICulture : en-US
PrivateData    : Microsoft.PowerShell.ConsoleHost+ConsoleColorProxy
IsRunspacePushed : False
Runspace      : System.Management.Automation.Runspace.LocalRunspace

```

PowerShell

- Hromadná konfigurace s využitím „**Group Policy**“ (zásad skupin) v rámci domény
- Konfigurační **skripty**:
 - **WMIC** (Windows Management Instrumentation Command-line)
 - **Windows Script Host** (jazykově nezávislé prostředí pro spouštění skriptů – např. Jscript .JS, .JSE; VBScript .VBS, .VBE; ...)
- **Windows Remote Management**
- **System Center Configuration Manager**
- ...

Další možnosti pro správu

The screenshot displays the Windows Server Manager interface. On the left, a tree view shows the 'Roles' section expanded, listing various server roles like Active Directory Domain Services, DNS Server, File Services, and Web Server (IIS). The main pane shows the 'Roles' page with a summary of 4 installed roles: Active Directory Domain Services, DNS Server, File Services, and Web Server (IIS). Below this, the 'Active Directory Domain Services' role is selected, showing its status and a message about the Best Practices Analyzer. A 'Command Prompt' window is overlaid on top, showing the command 'servermanagercmd' being executed, with a warning message that the command is deprecated and should be replaced by PowerShell cmdlets.

Server Manager

File Action View Help

Server Manager (ACMEDC1)

- Roles
 - Active Directory Domain Services
 - DNS Server
 - File Services
 - Web Server (IIS)
- Features
 - Group Policy Management
- Diagnostics
 - Event Viewer
 - Windows System Resource
 - Performance
 - Device Manager
- Configuration
 - Task Scheduler
 - Windows Firewall with Advanced Security
 - Services
 - WMI Control
- Storage

Roles

View the health of the roles installed on your server and add or remove roles and features.

Roles Summary [Roles Summary Help](#)

Roles: 4 of 17 installed

- Active Directory Domain Services
- DNS Server
- File Services
- Web Server (IIS)

[Add Roles](#)

[Remove Roles](#)

Active Directory Domain Services [AD DS Help](#)

Stores directory data and manages communication between users and domains, including user logon processes, authentication, and directory searches.

Role Status [Go to Active Directory Domain Services](#)

Messages: 1

System Services: 8 Running, 2 Stopped

Events: 1 warning, 13 informational in the last 24 hours

Best Practices Analyzer: To start a Best Practices Analyzer scan, go to the Best Practices Analyzer tile on this role's homepage and click Scan this Role

Role Services: 1 installed [Add Role Services](#)

Administrator: Command Prompt

```
C:\Users\Administrator>servermanagercmd
```

Servermanagercmd.exe is deprecated, and is not guaranteed to be supported in future releases of Windows. We recommend that you use the Windows PowerShell cmdlets that are available for Server Manager.

Server Manager

Administrator: C:\Windows\system32\cmd.exe

C:\Users\Administrator>oclist | more

Use the listed update names with Ocsetup.exe to install/uninstall a server role or optional feature.

Adding or removing the Active Directory role with OCSetup.exe is not supported. It can leave your server in an unstable state. Always use DCPromo to install or uninstall Active Directory.

=====
Microsoft-Windows-ServerCore-Package

Not Installed:BitLocker

Not Installed:BitLocker-RemoteAdminTool

Not Installed:CertificateServices

Not Installed:ClientForNFS-Base

Not Installed:CoreFileServer

Not Installed:DFSN-Server

Not Installed:DFSR-Infrastructure-ServerEdition

Not Installed:DHCPServerCore

Not Installed:DNS-Server-Core-Role

Not Installed:FRS-Infrastructure

Not Installed:IIS-WebServerRole

--- Not Installed:IIS-FTPService

--- Not Installed:IIS-FTPExtensibility

NOT INSTALLED-WCF WITH ACTIVATION

--- Not Installed:WCF-NonHTTP-Activation

Not Installed:WindowsServerBackup

--- Not Installed:WindowsServerBackupCommandlet

Not Installed:WINS-SC

C:\Users\Administrator>start /W ocsetup WindowsServerBackup

C:\Users\Administrator>

OCLIST.EXE , OCSETUP.EXE

```
C:\Administrator: C:\Windows\system32\cmd.exe - sconfig
Microsoft (R) Windows Script Host Version 5.8
Copyright (C) Microsoft Corporation. All rights reserved.

Inspecting system...

=====
                          Server Configuration
=====

1) Domain/Workgroup:                Workgroup:  WORKGROUP
2) Computer Name:                   SRU01
3) Add Local Administrator
4) Configure Remote Management

5) Windows Update Settings:
6) Download and Install Updates
7) Remote Desktop:

8) Network Settings
9) Date and Time

10) Log Off User
11) Restart Server
12) Shut Down Server
13) Exit to Command Line

Enter number to select an option:
```

```
Manual
C:\Administrator: C:\Windows\system32\cmd.exe - sconfig
Enter number to select an option: 4

-----
                          Configure Remote Management
-----

1) Allow MMC Remote Management
2) Enable Windows PowerShell
3) Allow Server Manager Remote Management
4) Show Windows Firewall settings

5) Return to main menu

Enter selection: _
```

SCONFIG (core)

Administrator: C:\Windows\system32\cmd.exe

```
D:\>Start_Coreconfig.wsf
```

```
D:\>
```

C:\Windows\System32\cscript.exe

```
Microsoft (R) Windows Script Host Version 5.8  
Copyright (C) Microsoft Corporation. All rights reserved.
```

```
Manufacturer : Microsoft Corporation  
ComputerModel: Virtual Machine  
ScriptContext: [x64 - Extended 64bit]  
OSSku: 18  
OSName: Microsoft Windows Server 2008 R2 Standard  
OSType: 18  
OSDisplay: Core Edition  
CSDVersion: No Service Pack
```

```
*****
```

```
Checking for NetFx-ServerCore Feature. Please wait...
```

```
Not Installed:NetFx2-Ser
```

Install NetFx-ServerCore and Powershell Feature



No NetFx-ServerCore and Powershell Feature has been detected!

This Server:[SRV01]

needs the NetFx-ServerCore and Powershell feature
in order for Core Configurator 2.0 to function

Are you sure you wish to continue?

Yes

No

**Core Configurator 2.0
(není součástí systému)**

Core Configurator 2.0

Tools Logs Help

CoreConfigurator 2.0 Main Menu

Setup tool for configuring Licencing,Networking and all other components of Windows Server Core 2008 R2

Computer Name	SRV01
Workgroup/ Domain	WORKGROUP
SKU Version	Enterprise Server



Computer settings

Configure computer name, domain configuration and computer roles and features.

Computer settings...



Control panel settings

Windows update, display settings and configuration of windows firewall.

Control panel...



Network settings

Configuration of all networking adapter settings and proxy settings

Network settings...



Hyper-V settings

Virtual machine manager for server-core starting and stopping of virtual machines

Hyper-V settings...



Licence settings

Current server licence status,online and offline activation and product key configuration.

Licence settings...

Exit

Core Configurator 2.0
Tools Logs Help

CoreConfigurator 2.0 Computer Menu
Configuration of all computer settings,Domain controller and Roles in Windows Server Core 2008 R2

Computer Name	SRV01
Workgroup/ Domain	WORKGROUP
Version	Enterprise Server Core R2

Computer settings
Computer name and domain join functionality.
Computer and domain...

Domain settings
Complete domain join functionality and removal using a wizard.
DCPromo...

Role and Features
Install new roles and features on this computer.
Add or Remove Roles...

Remote Management settings
Remote management settings and remote desktop.
Remote Desktop...
WinRM...

Services
Currently installed services,name and description.
Services...

Core Configurator 2.0
Tools Logs Help

CoreConfigurator 2.0 Network Menu
Configuration of all network settings and connection settings to the internet in Windows Server Core 2008 R2

Computer Name	SRV01
Workgroup/ Domain	WORKGROUP
Version	Enterprise Server Core R2

Network settings
Current network configuration,renaming and enabling,disabling of network cards.
Network interface cards...

Internet settings
Current server licence status,online and offline activation and product key configuration.
Proxy configuration...

Users and Share settings
Current administrator access to this computer and share creation and deletion.
Group membership...
Share management...

Storage settings
iSCSI devices are storage devices on another computer on your network that you can connect to.
iSCSI configuration...
iFIPID configuration...

Core Configurator 2.0
Tools Logs Help

CoreConfigurator 2.0 Control Panel Menu
Configuration of all control panel settings in Windows Server Core 2008 R2

Computer Name	SRV01
Workgroup/ Domain	WORKGROUP
SKU Version	Enterprise Server Core R2

Windows Update settings
Configuration of Windows Updates using direct connection or WSUS Server.
Windows Updates...

Personalisation settings
Configuration of display settings and screensaver timeout.
Display Resolution...

Firewall settings
Current firewall status and rule configuration
Firewall...

Hardware settings
Add and Remove Windows certified drivers.
Add Drivers...

Regional settings
Keyboard configuration and date and time settings.
Keyboard...
Date and Time...

Program settings
Add or remove programs from this computer.
Add Remove Programs...

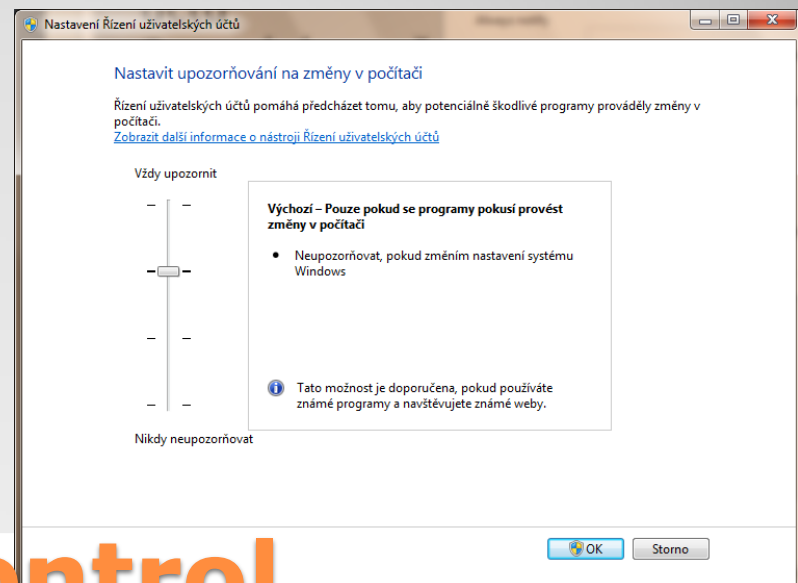
< Back

Core Configurator 2.0

Správa Windows serverů

Základy UAC

- Řízení uživatelských účtů
- 3 nové úrovně UAC
- Uživatel si může nastavit úroveň upozorňování vs. pohodlí
- Aplikuje se na administrátory
- Ztlumení plochy (Secure Desktop)



User Account Control

- **High:** (obdoba Windows Vista)
 - Dotazuje se na: všechny žádosti o zvýšení práv
 - Dotazuje se: na zabezpečeném desktopu
- **Medium:** (výchozí nastavení)
 - Dotazuje se na: zvýšení oprávnění, která nejsou součástí Windows
 - Windows znamená:
 - Podepsané certifikátem Windows
 - Bezpečné umístění
 - Neumožňuje kontrolu nad příkazovou řádkou (např. cmd.exe)
 - Dotazuje se: na zabezpečeném desktopu
- **Low:**
 - Dotazuje se na: zvýšení oprávnění, která nejsou součástí Windows
 - Dotazuje se: na standardním desktopu
 - Uživatel může pracovat/spolupracovat s desktopem
 - Možné problémy s kompatibilitou produktů třetích stran, které nabízejí zjednodušený přístup
- **Off:** (UAC vypnuté)
 - Žádný Protected Mode v IE
 - Žádná virtualizace souborového systému a registry

Úrovně User Account Control

- Vyžadují lepší izolaci nežli tomu je u stávajících účtů služeb
 - Nechci se starat o správu hesel
- Virtual accounts jsou jako servisní účty:
 - Process spuštěn s virtuálním SID
 - Je možné nastavit ACL objekty na tento SID
 - Systém spravuje hesla
 - Při přístupu na síť využívá účet počítače
- Služby mohou mít definovaný virtual account
 - Jméno účtu musí odpovídat konvenci "NT SERVICE\<>service>"
 - Service control manager kontroluje, jestli jméno služby odpovídá jménu účtu
 - Service control manager vytváří uživatelský profil pro účet
- Využívá také IIS app pool a SQL Server
- Managed Service Accounts

Virtuální účty, izolace služeb

cmd Správce: C:\Windows\system32\cmd.exe

```
Název_služby: rpcss
Typ_identifikátoru_SID_služby: UNRESTRICTED

C:\Windows\system32>sc qsidtype mpssvc
[SC] QueryServiceConfig2 úspěch

Název_služby: mpssvc
Typ_identifikátoru_SID_služby: RESTRICTED
```

cmd Správce: C:\Windows\system32\cmd.exe

```
C:\Windows\system32>sc showsid rpcss

NAZEV: rpcss
SID SLUŽBY: S-1-5-80-979556362-403687129-3954533659-2335141334-1547273080

C:\Windows\system32>sc showsid mpssvc

NAZEV: mpssvc
SID SLUŽBY: S-1-5-80-3088073201-1464728630-1879813800-1107566885-823218052
```

cmd Správce: C:\Windows\system32\cmd.exe

```
C:\Windows\system32>sc qprivs rpcss
[SC] QueryServiceConfig2 úspěch

Název_služby: rpcss
Oprávnění : SeChangeNotifyPrivilege
           : SeCreateGlobalPrivilege
           : SeImpersonatePrivilege

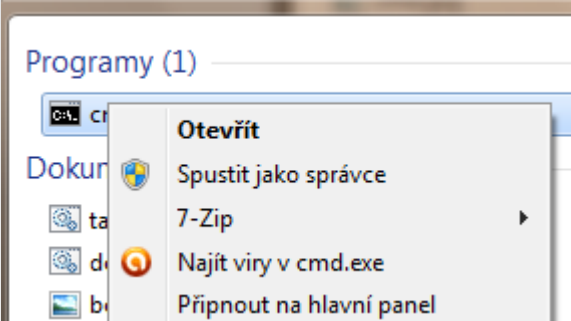
C:\Windows\system32>sc qprivs mpssvc
[SC] QueryServiceConfig2 úspěch

Název_služby: mpssvc
Oprávnění : SeAssignPrimaryTokenPrivilege
           : SeAuditPrivilege
           : SeChangeNotifyPrivilege
           : SeCreateGlobalPrivilege
           : SeImpersonatePrivilege
           : SeIncreaseQuotaPrivilege
```

```

C:\Windows\System32\cmd.exe
INFORMACE O OPRAVNĚNÍCH
-----
Název oprávnění      Popis      St
-----
av
=====
SeIncreaseQuotaPrivilege  Upravit kvóty paměti pro proces  Za
kázáno
SeSecurityPrivilege      Spravovat auditování a protokol zabezpečení  Za
kázáno
SeTakeOwnershipPrivilege  Převzít vlastnictví souborů a dalších objektů  Za
kázáno
SeLoadDriveObjectsPrivilege  Kázat načítání objektů souborového systému  Za
kázáno
SeSystemProcessPrivilege    Kázat spuštění systémových procesů  Za
kázáno
SeSystemtimePrivilege       Kázat změnu času  Za
kázáno
SeProfileSingleProcessPrivilege  Kázat profilování procesů  Za
kázáno
SeIncreaseBasePriorityPrivilege  Kázat zvýšení priorit procesů  Za
kázáno
SeCreatePagefilePrivilege      Kázat vytvoření souboru stránkové sady  Za
kázáno
C:\Windows\system32\cmd.exe
INFORMACE O OPRAVNĚNÍCH
-----
Název oprávnění      Popis      Stav
-----
SeShutdownPrivilege  Vypnout systém  Zakázáno
SeChangeNotifyPrivilege  Nepoužívat kontrolu procházení  Povoleno
SeUndockPrivilege       Vymout počítač z dokovací stanice  Zakázáno
SeIncreaseWorkingSetPrivilege  Zvýšit pracovní sadu procesu  Zakázáno
SeTimeZonePrivilege      Změnit časové pásmo  Zakázáno

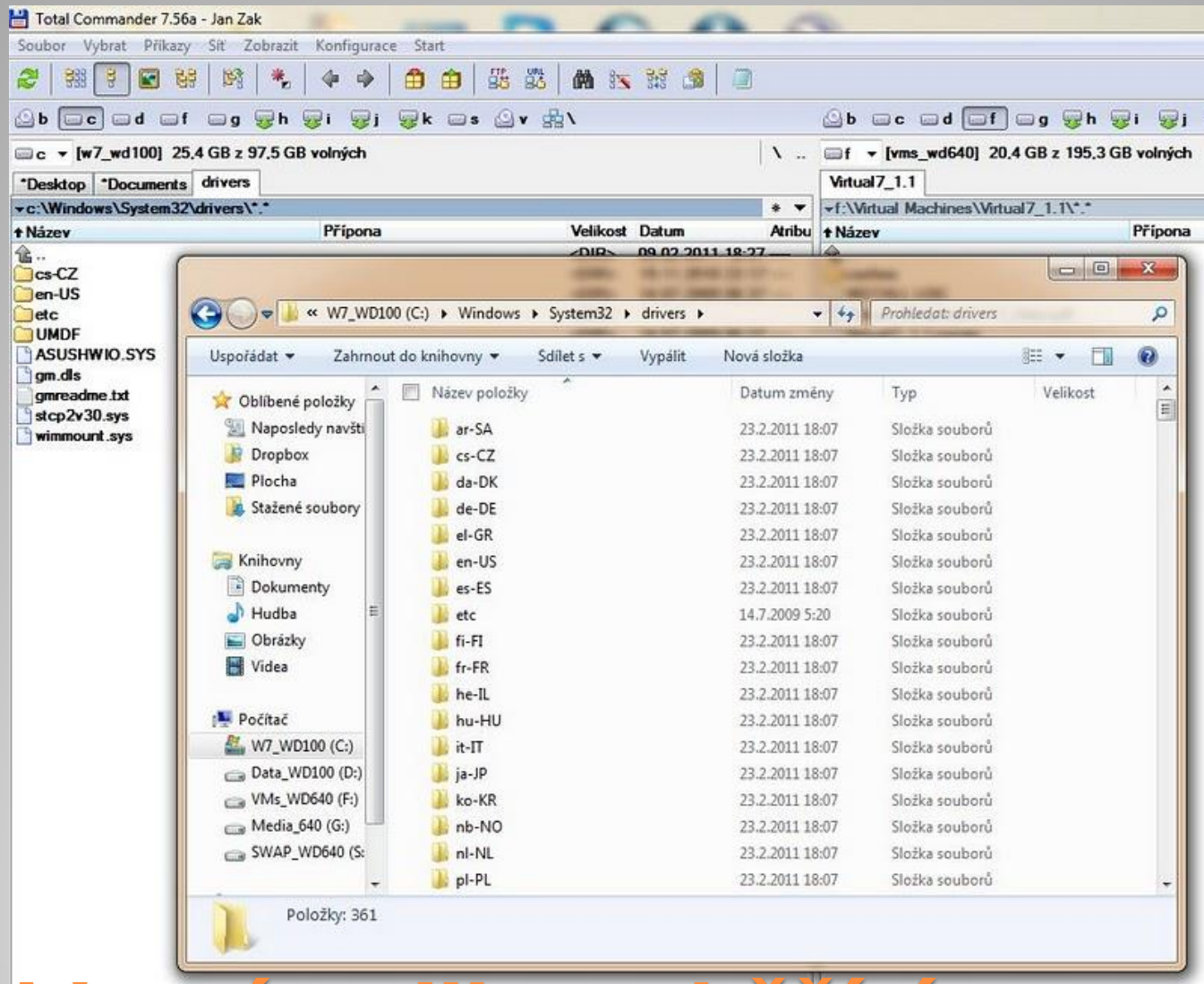
```



Spustit jako...

- Windows hlídá události a při zjištění pokusu o zápis do zabezpečených lokací, ať již adresář „Program files“, „Windows“ či registry, přesměruje takový požadavek do tzv. virtual store.
 - C:\Users\%username%\AppData\Local\VirtualStore
 - HKCU\Software\Classes\VirtualStore\MACHINE
- Virtualizace zápisů je prezentována jako přechodná možnost pro přechod na novější verze aplikací.
- Problémem tady zůstává zápis do složky dostupné jen aktuálně přihlášenému uživateli, například konfigurační změna aplikace se nepromítne všem uživatelům.

Virtual stores



**32bitová aplikace běžící v
64bitovém systému**

- <http://goo.gl/cyHmy>



- <http://www.cs.vsb.cz/navrat/>

**Odkazy pro stažení dalších
prezentací a materiálů**