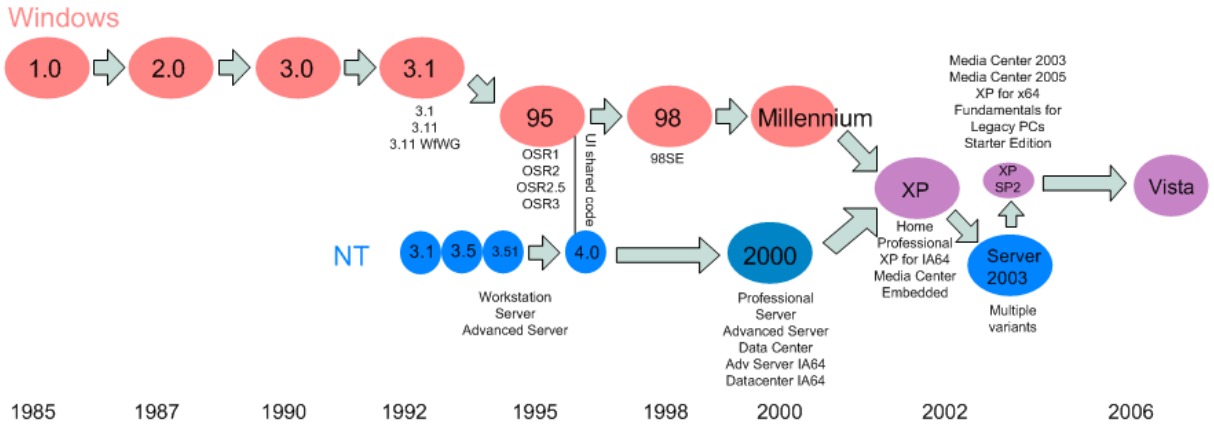
HISTORIE

1981	DOS
1985	WINDOWS 1.0 (INTERFACE MANAGER)
1987	WINDOWS 2.0
1988	WINDOWS/286; WINDOWS 386
1990	WINDOWS 3.0
	OS/2
1992	WINDOWS 3.1; WINDOWS 3.11
1992	WINDOWS NT 3.1
1995	WINDOWS 95 (5 EDITIONS)
1996	WINDOWS NT 4.0 (4 EDITIONS)
1998	WINDOWS 98 (2 EDITIONS)
2000	WINDOWS 2000 (5 EDITIONS)
2000	WINDOWS ME
2001	WINDOWS XP (15 EDITIONS)
2003	WINDOWS SERVER 2003 (5 EDITIONS)
2006	WINDOWS FUNDAMENTALS FOR LEGACY PCS
	WINPE 1.0
2007	WINDOWS VISTA (8 EDITIONS)
2008	WINDOWS 2008
	WINPE 2.0; MS DART



Jaký je rozdíl mezi 64bit a 32bit?

V adresaci – např. 32 bit je kvůli tomu schopen pojmout jen max 4GB paměti (tzn. pokud máme 4 GB RAM a 1 GB na grafické kartě, tak se bude využívat pouze 2 GB paměti, protože to bere jako RAM + VGA).

VERZE

- major a minor verze (1.0 → 6.0)
- dvě architektury (od Windows XP se spojují do jedné)
  - Windows 9x
    - běžné verze určené pro domácí použití → 95, 98, ME, ...
  - Windows NT
    - profesionální řada založená na NT jádře
- od Windows XP přichází rozdělení edicí (Home/Business)

VERZE	EDICE
Windows XP	Windows XP Professional
	Windows XP Home Edition
	Windows XP Professional x64 Edition
	Windows XP Media Center Edition 2005
	Windows XP Tablet Edition
	Windows XP Corporate
	Windows XP Embedded
	Windows Fundamentals for Legacy PCs
	Windows XP Starter Edition
	Windows XP Professional N
	Windows XP Home Edition N
Windows Vista	Windows Vista Starter
	Windows Vista Home Basic
	Windows Vista Home Premium
	Windows Vista Business
	Windows Vista Enterprise
	Windows Vista Ultimate
Windows 7	Windows 7 Home Premium
	Windows 7 Professional
	Windows 7 Ultimate
	Windows 7 Starter
	Windows 7 Home Basic
	Windows 7 Enterprise
Windows 8	Windows 8
	Windows 8 Pro
	Windows 8 Enterprise
	Windows 8 RT

**všechny edice obsahující Windows Media Playeru mohou být doplněné o písmeno N na konci celého názvu, čímž vznikne název odvozené edice bez Windows Media Playeru (vynuceno antimonopolním řízením)*

»32 bit

- limit na operační paměť 4 GB
- většina 64 bit programů nebude na 32 bit fungovat, ale naopak ano (tedy 32 bit na 64 bit)
- pro ovladače toto neplatí, musí se vždy vybírat pro konrétní verzi
- menší výkon

ORIENTACE A NASAZENÍ WINDOWS

- centralizace managementu
- objektivně orientováno (.NET)
- otevřeno pro 3rd parties
- virtualizace
  - SoftGrid
    - virtualizace aplikací
  - Hypervisor
    - součást Windows 2008
  - Shims
    - simuluje prostředí starších OS v nových verzích Windows (Vista, Windows 7), pro zajištění zpětné kompatibility s existujícími aplikacemi

- běžné nasazení Windows:
  - intranet server
  - directory services
  - workstations
  - terminal servers (Linux/WinCE client image)
  - messaging server
- není doporučeno pro DMZ a proxy

SCRIPTING

- command interpreter → **cmd.exe**
- command extensions (default) **/E:ON**
- file and directory name completion **/F:ON**
- delayed environment variable expansion **/V:ON**

»Proměnné

- výpis proměnných (set)
- systémové proměnné
- spec. proměnné (**cd**, **date**, **time**, **random**, **errorlevel**)
- parametry (%0, %1, ... %*), příkaz shift
- **set (/a) promenna = vyraz** – manipulace s proměnnými
- **%var%** – náhrada hodnotou při vstupu na řádek nebo do víceřádkové struktury; nevyhonotí se v cyklu – místo toho je lepší použít **!var!** s *cmd.exe /V:ON*
- **!var!** – náhrada hodnotou těsně před použitím (delayed variable expansion)
- **command < file** – vstup; přesměrování
- **command > file** – výstup; přesměrování
- **command 2 > file**
- **command > file 2 > &1**
- **command 1 | command 2 | command 3** – roura, filtrování
- filtry: **sort**, **find**, **more**
- speciální soubory: **nul** (černá díra), **con** (konzole), **prn** (tiskárna), **com1** (seriový port)
- **rem (::)** – poznámka v kódu
- **:label –** návěstí pro skoky v kódu
- **goto –** nepodmíněný skok
- **pause** – pauza, vhodné pro debugging

- **cd** – změna adresáře ... **cd /d d:\temp**
- **copy**, **xcopy**, **copy file1+file2+file3 file**
- **del *.***
- **rmdir /s /q %temp%**
- podřetězce: **set rok=%date:~-4%**
- matematické řetězce: **set /a rok=%rok% + 1**
- náhrada textu: **set var=%var%:old=new%**

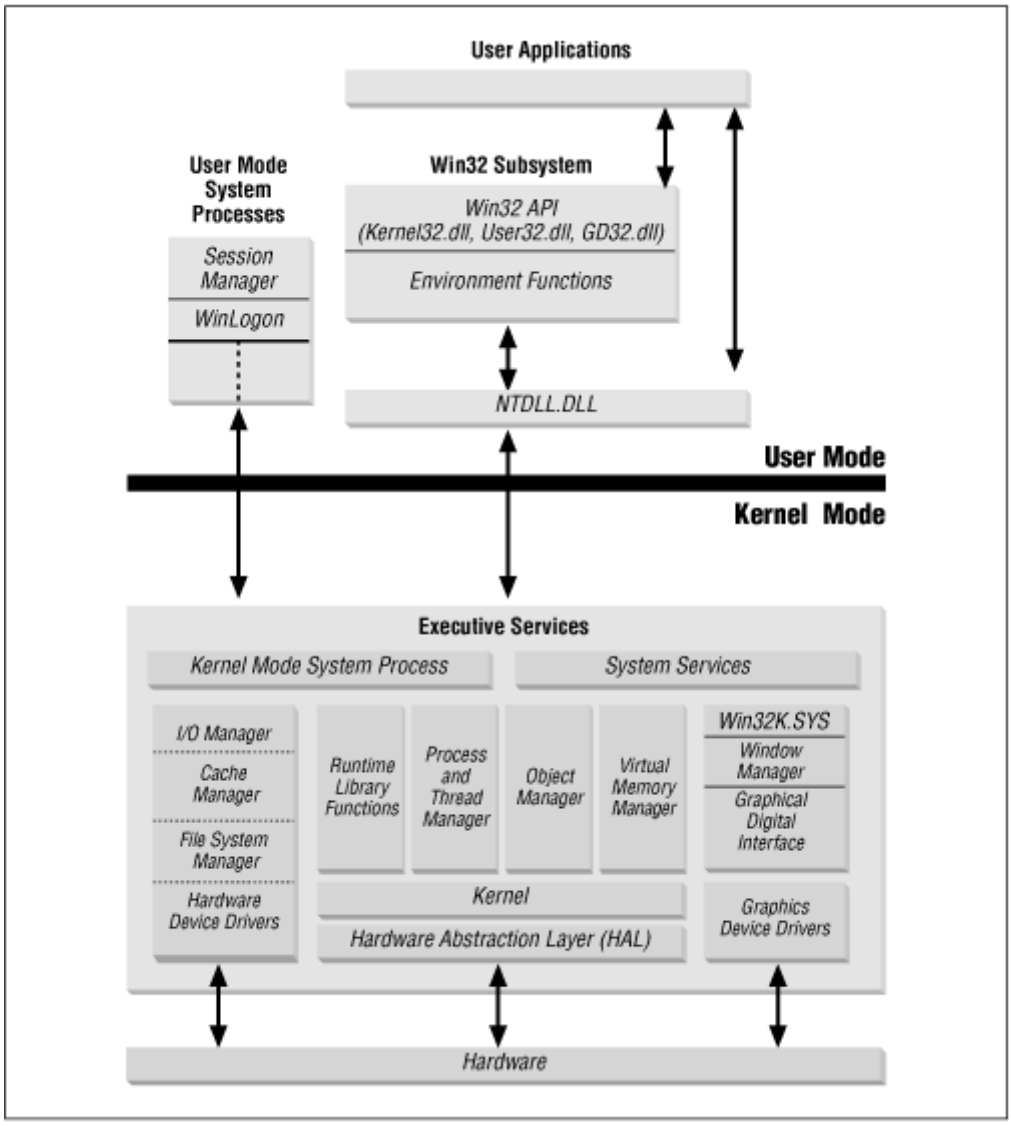
»If

- podmíněný příkaz
- IF *condition commands*
- IF *condition (commands)* ELSE *(commands)*
- **[NOT] EXIST filename/dirname** – test (ne)existence souboru nebo adresáře
- **[NOT] DEFINED var** – test existence proměnné
- **[NOT] ERRORLEVEL number** – test návratové hodnoty
- **[/I] [NOT] string1==string2** – test shody řetězců
- Místo „==“ může být **EQU**, **NEQ**, **LSS**, **LEQ**, **GTR**, **GEQ**

»for

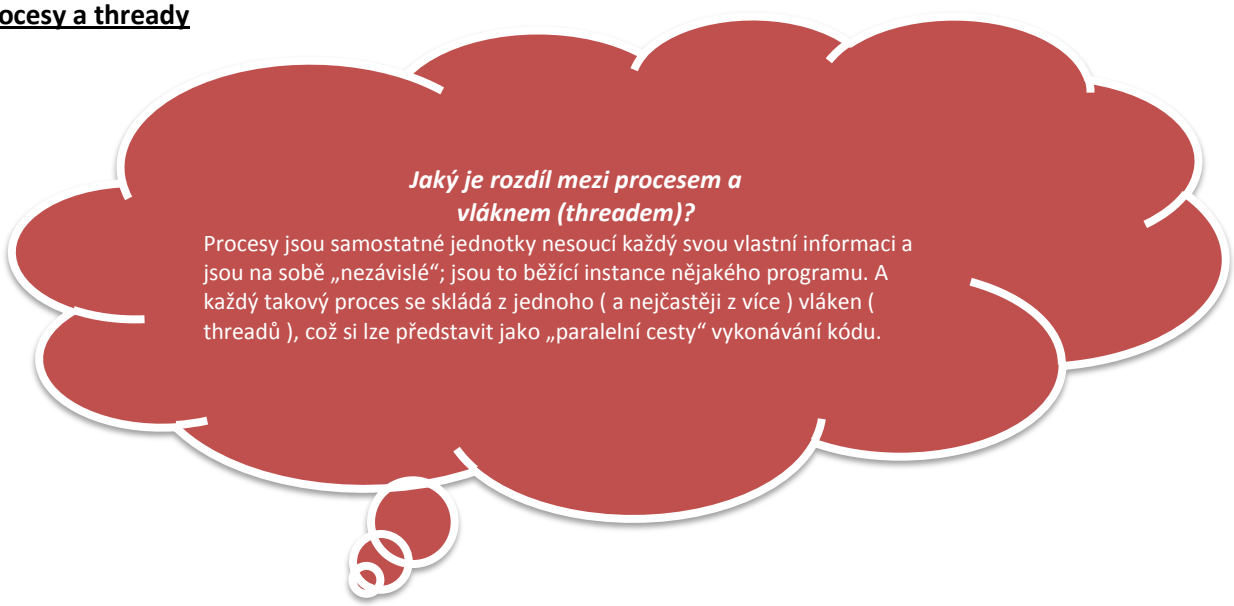
- Cyklus zpracovávající řádky souboru, stdout spuštěného programu, adresářovou strukturu
- **FOR %v IN (set) DO commands** – výučtový cyklus
- **FOR /L %v IN (start step end) DO commands** – aritmetický cyklus
- **FOR /F [“options“] %a IN (file-set** nebo **“string“** nebo **‘command’) DO commands** – options jsou **SKIP=n** (vynechání první n řádků); **EOL=c** (nastavení znaku konce řádku); **DELIMS=xxx** (nastavení oddělovačů, default mezera a tab); **TOKENS=x,y,m-n[*]** (výběr položek na řádku, značených pak %a, %b, atd.

ARCHITEKTURA MS WINDOWS



- Windows podporuje 2 Pentium ringy
  - Ring0 – kernel
  - Ring3 – user
  - Ringy si můžeme představit jako „úrovně oprávnění“ (úrovně vykonávání kódu), které se dělí na user mode a kernel mode → z důvodu bezpečnosti
    - standartně běží program v user mode, ze kterého má omezené pravomoce na provádění nebezpečných operací
    - o všechny tyto nestandartní operace se musí zažádat u operačního systému
    - tím se zajistí větší stabilita systému a nestane se, že by nějaký proces jen tak shodil systém (s případnou ztrátou dat)
    - nebezpečné/kritické operace se tak provádí pouze v kernel modu a OS má větší možnost dohlížet na procesy
- user thready se mohou přepípnat mezi user a kernel modem (na základě API)
- drivery běží v kernel mode
  - častá příčina BSOD
  - fake drivers (antivir)

»Procesy a thready



- každá aplikace obsahuje *minimálně jeden* proces
- každý proces obsahuje *minimálně jeden* thread
- každý proces má *vlastní* memory space
- thready jednoho procesu běží ve *stejném* memory space
- CPU čas je ve skutečnosti přirazovábn *threadu* ne procesu
- služby (services) členíme na několik částí:
  - API služby
  - systémové služby
  - interní služby
- nejdůležitější systémové procesy:
  - **Idle** – jeden thread na monitorování CPU idle time (nečinnost)
  - **System** – běží pod ním jen systémové thready (floppy disk driver, cache management, ...)
  - **SMSS** – session manager → jeden z prvních spuštěných procesů; definice systémových proměnných; MS DOS názvy (LPT1); natažení kernel části do subsystému Win32; spuštění winlogon
  - **CSRSS** – Client/Server Runtime Server Subsystem; Win32 subsystém; console windows, threading
  - **WinLogon** – WinLogon proces (ctrl+alt+del; shell)
- Win32 je jedním ze systémových prostředí, která obecně působí jako rozhraní mezi uživatelskou aplikací a relevantní částí Windows.
  - 32 bitové API pro řadu Windows NT
- **NTOSKRNL.exe**
  - executive
    - Process & Thread Manager
    - Virtual Memory Manager
    - I/O Manager
    - Cache Manager
    - Object Manager

- kernel
  - Thread scheduling
  - Exception handling
  - Interrupt handling
  - Synchronization of processors
  - Creating kernel objects

»Hardware Abstraction Layer

- kernel mode knihovna **HAL.DLL**
- představuje abstraktní vrstvu mezi OS a HW
- vybírá se v průběhu instalace OS (od NT 6.0 změna)
- existuje mnoho různých typů dle CPU, SMP, ...

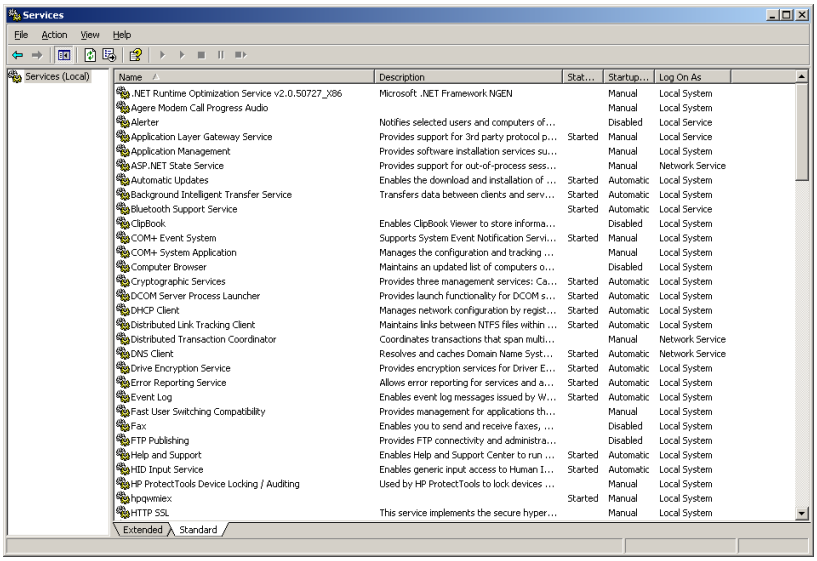
»Další subsystémy

- Cache Controller
- Configuration Manager
- I/O Manager
- Local Procedure Call (LPC)
- Memory Mamanger
- Process Structure
- PnP Manager
- Power Manager
- Security Reference Monitor (SRM)
- Window Manager
- GDI

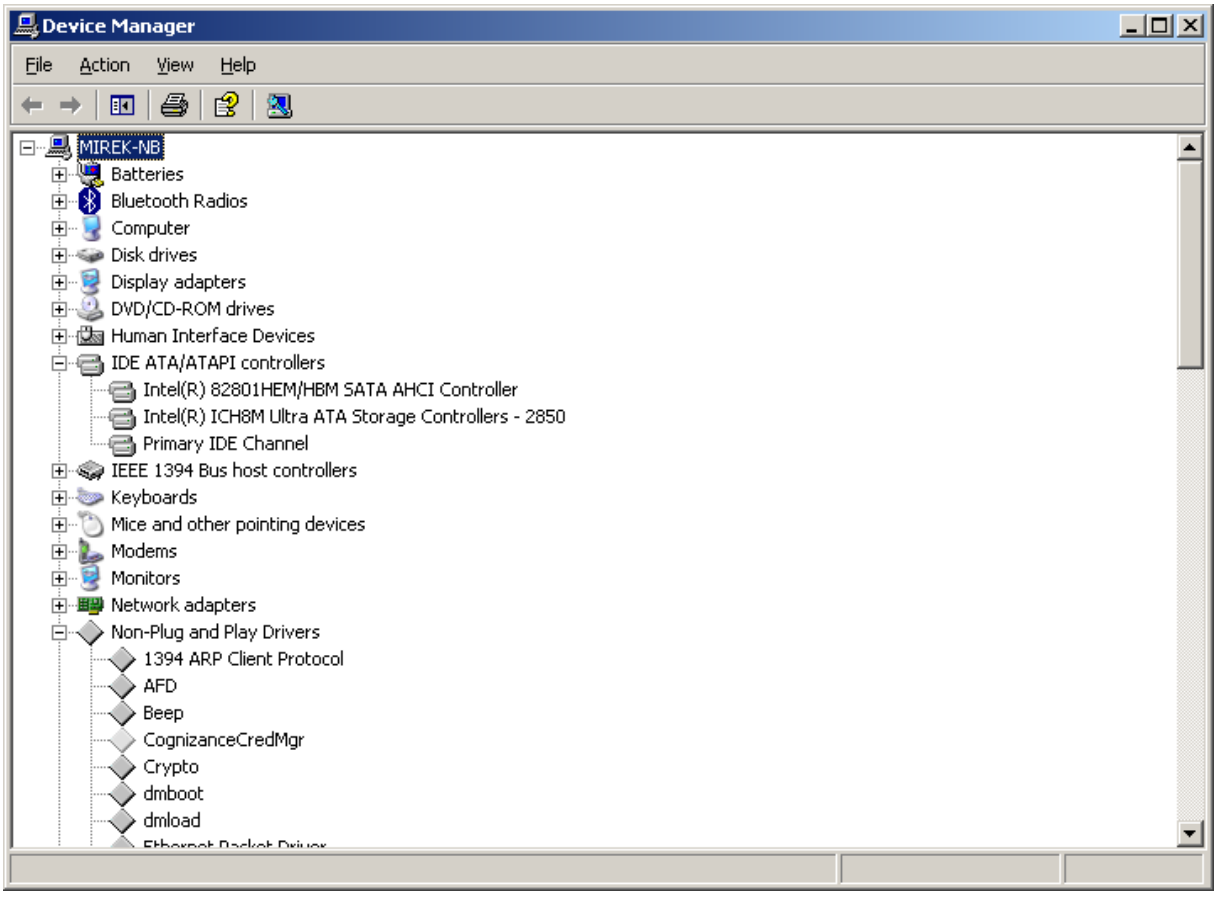
»Windows NT startup

- **ntldr**
- **boot.ini**
- **ntdetect**
- **ntoskrnl.exe**; **hal.dll**
- boot + system drivers
- **smss**
  - **Win32k.sys**
  - **csrss.exe**
- **WinLogon**
  - **Gina**
  - **Userinit**

» services.msc « - GUI aplikace pro správu služeb, konzolové ekvivalenty: **net.exe**, **sc.exe**

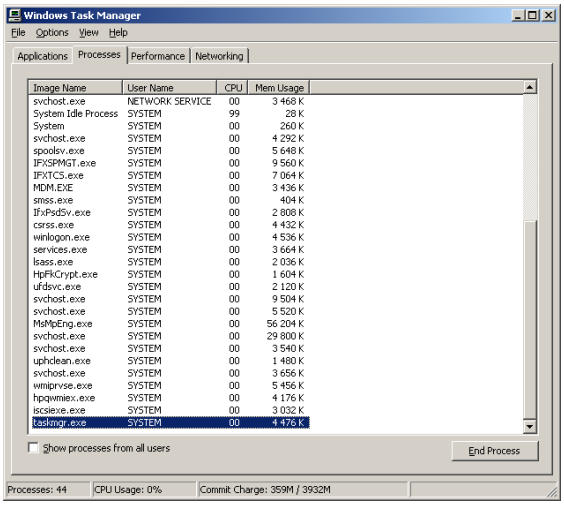


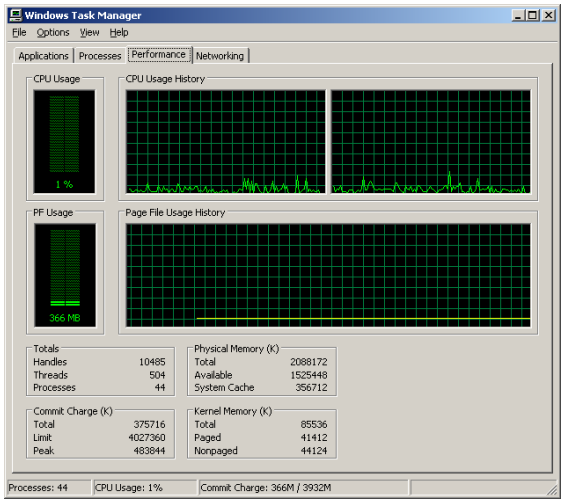
» devmgmt.msc « - GUI aplikace pro správu ovladačů, konzolové ekvivalenty: **net.exe**, **devcon.exe**



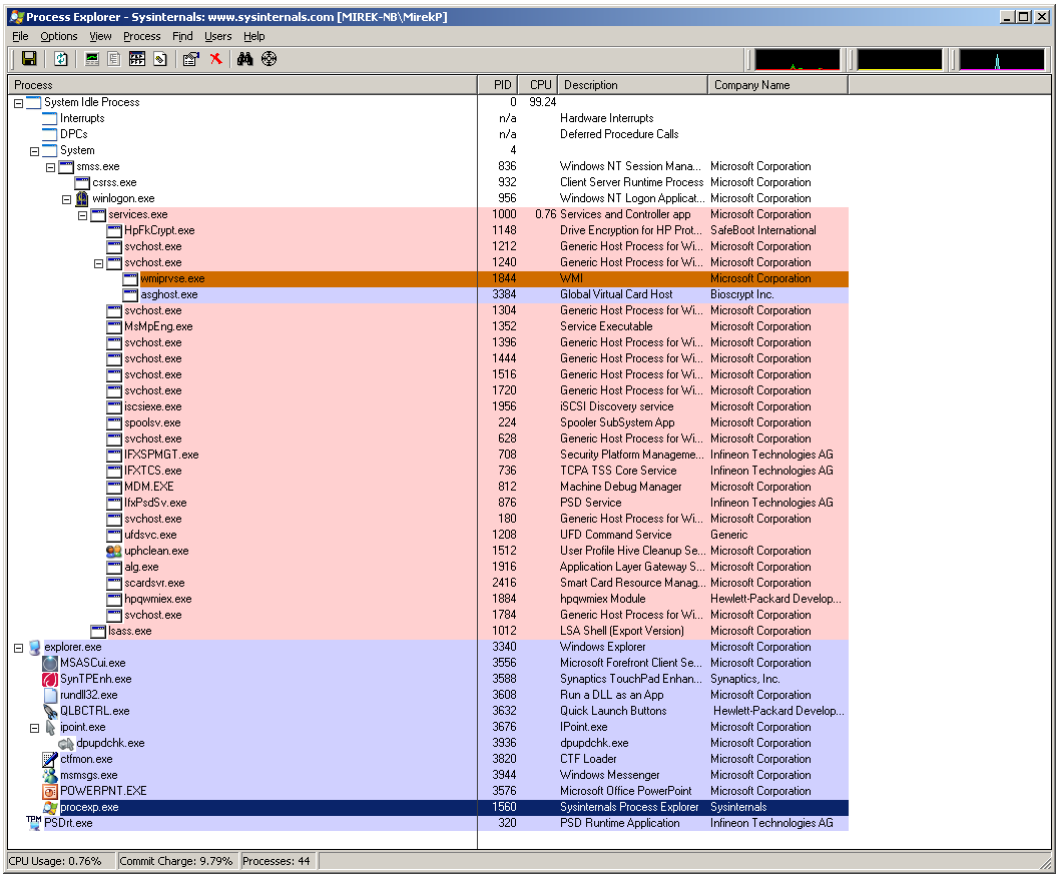
» taskmgr.exe « - základní aplikace pro zobrazení běžících procesů

- pokud chceme spustit pod vyššími právy (pod LocalSystem): */interactive taskmgr.exe*

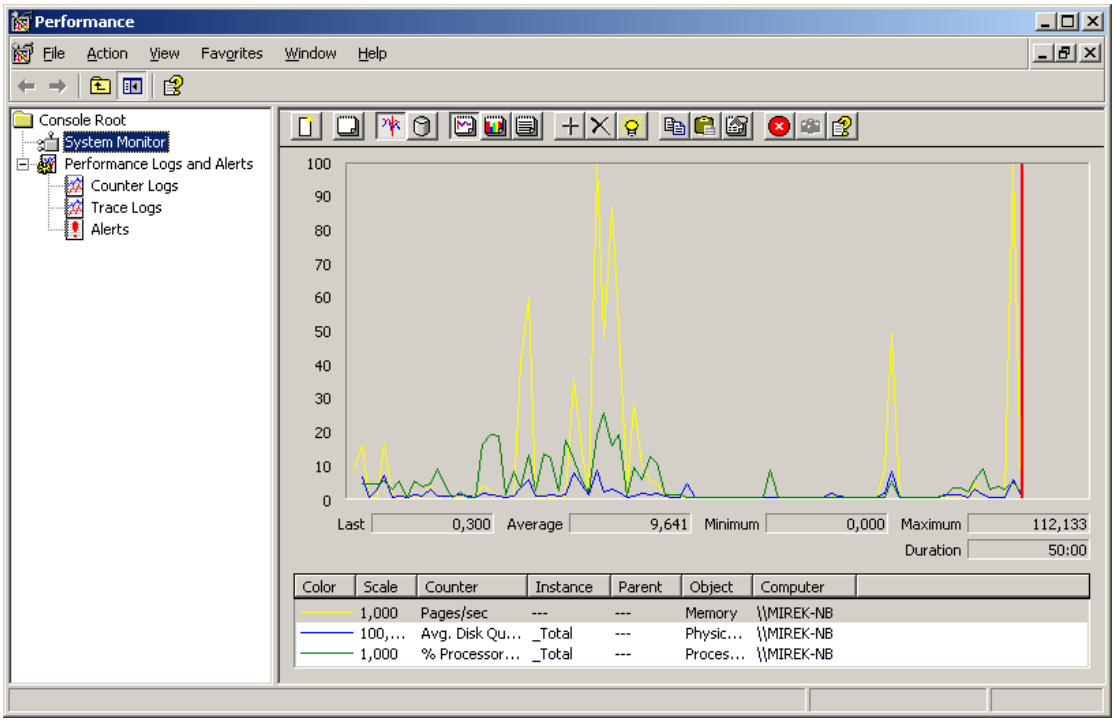




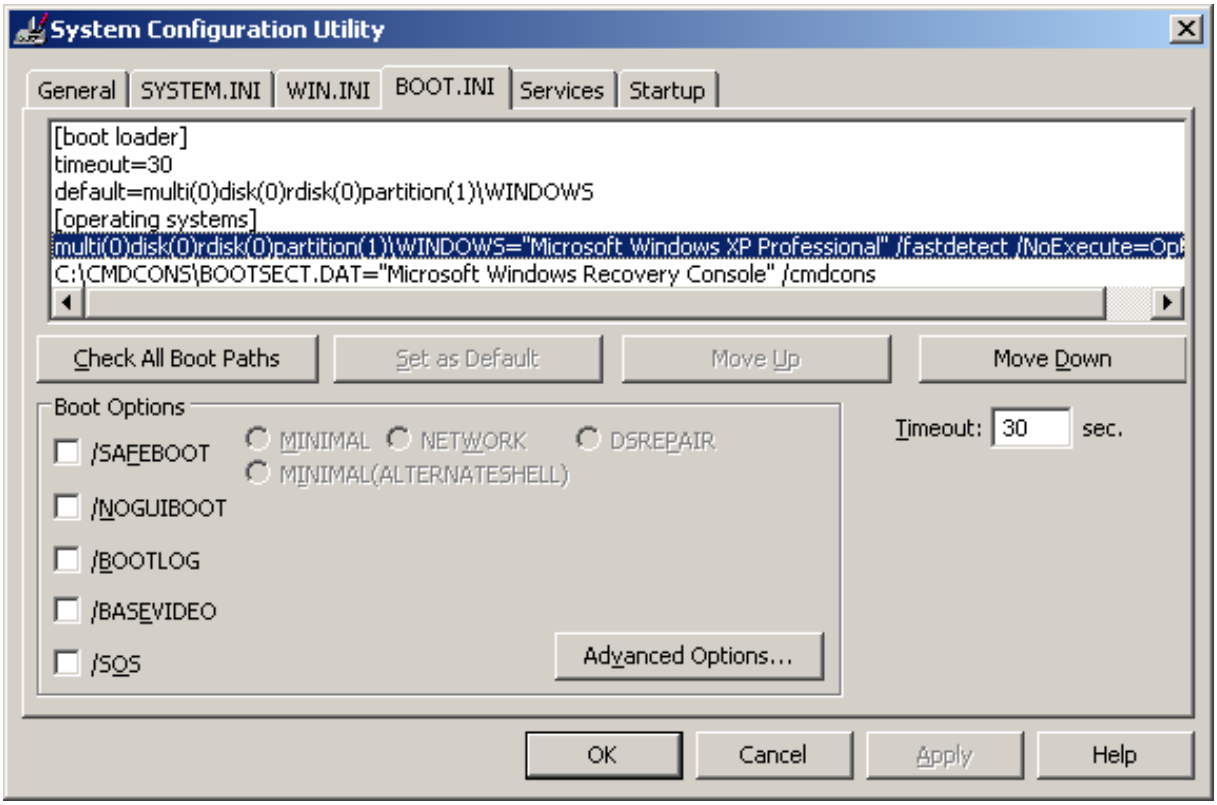
Process explorer – od sysinternals



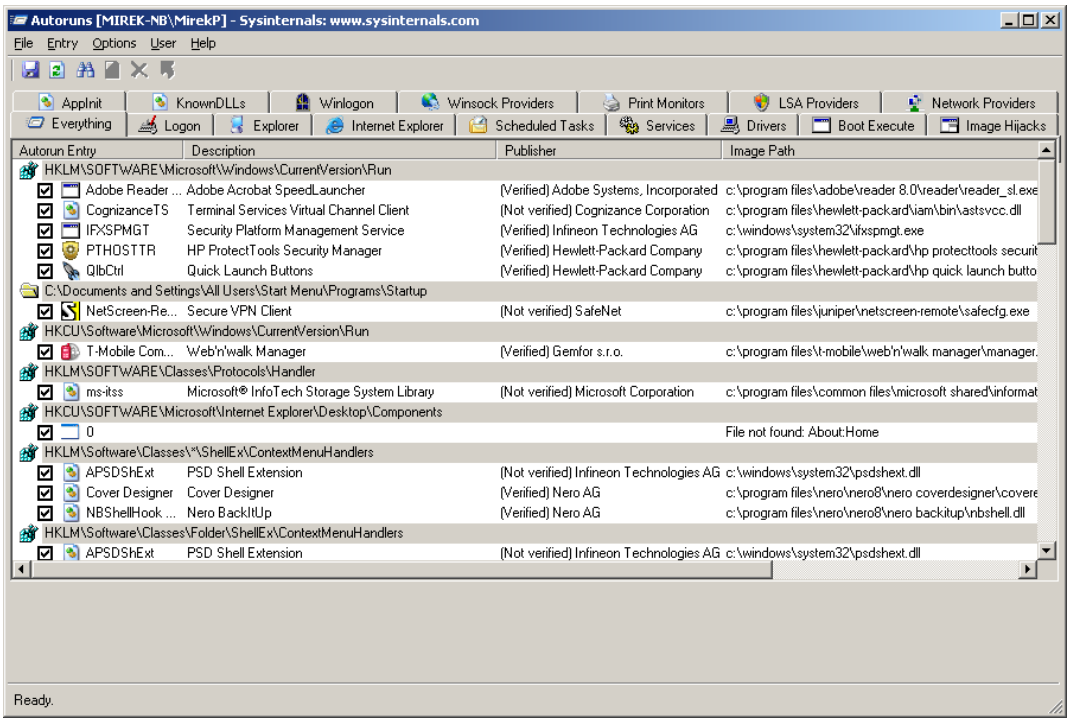
» perfmon.exe « - aplikace pro sledování výkonu (performance counters), logování a provádění akcí při překročení limitu



» msconfig.exe «



AutoRuns – od sysinternals



» cmd.exe « - spuštění programu z shellu s možností specifikovat prioritu ***start /low notepad.exe***

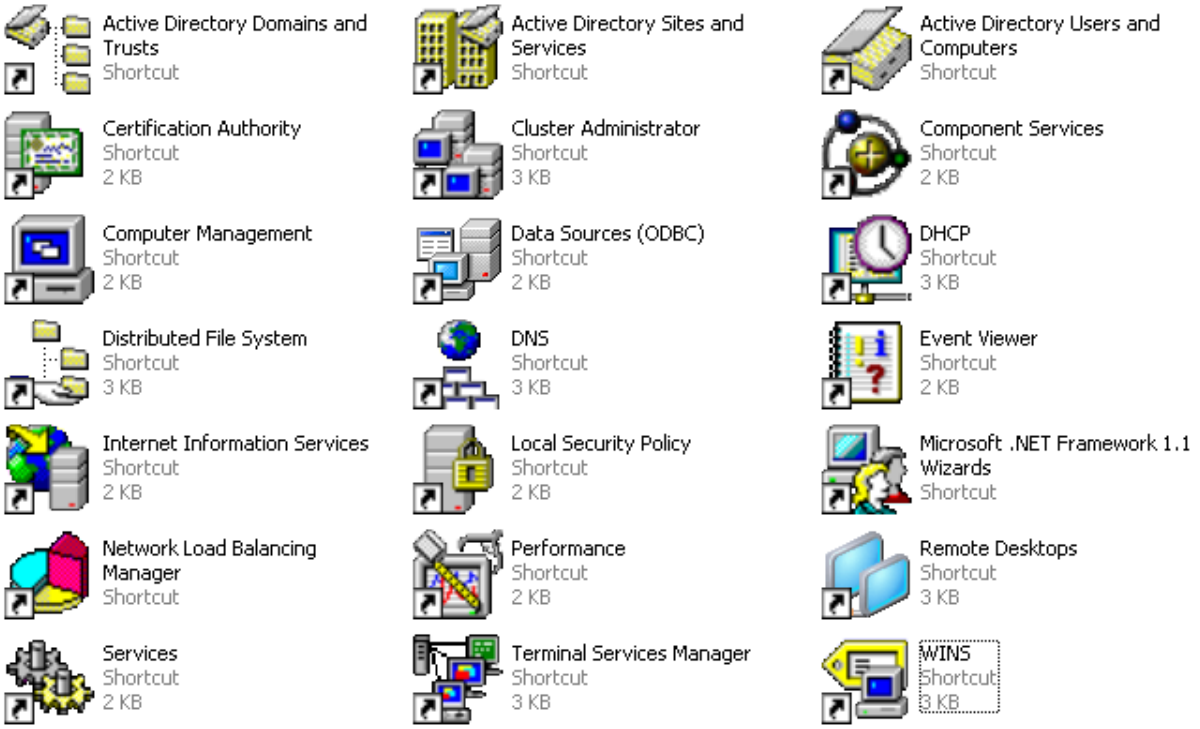
» runas.exe « - spuštění programu pod jiným
- uživatelským účtem
  - ***runas /savecred/user:MIREK-NB\Administrator sol.exe***
- oprávněním
  - ***runas /showtrustlevels***
  - ***runas /trustlevel:"Basic User" „c:\Program Files\Internet Explorer\iexplorer.exe"***

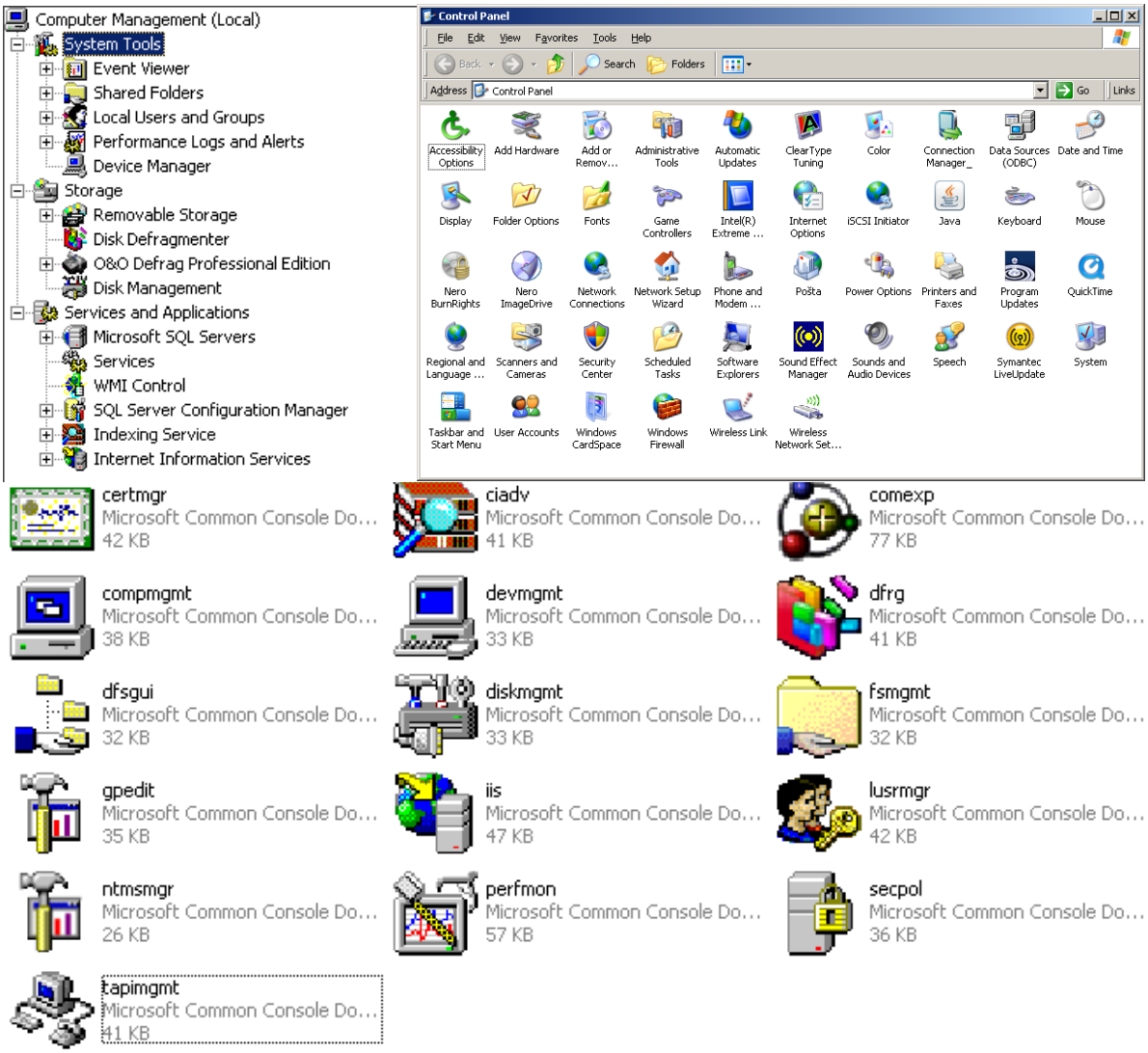
» sc.exe « - práce se službami

MECHANISMY SPRÁVY SYSTÉMU

Služby:

- grafické (GUI)
- konzolové (CMD)





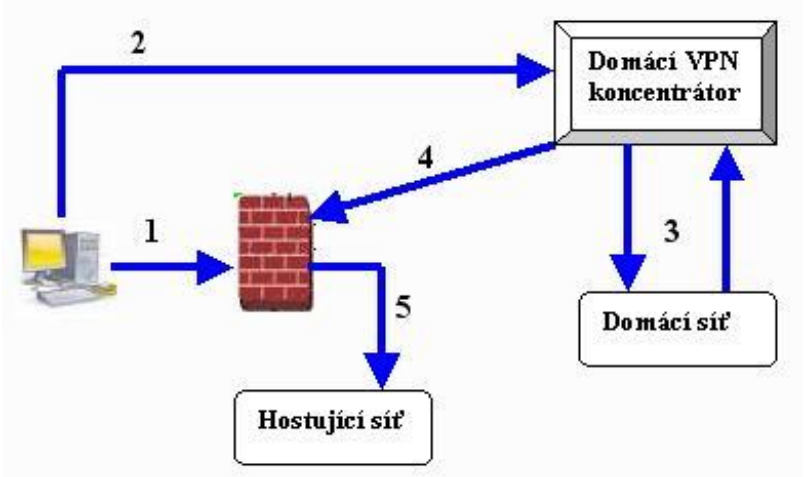
»Registry

Co je to registr?
Systém pro ukládání systémových klíčů a hesel v operačním systému MS Windows.

- registry: základní databáze obsahující nastavení systému
- nastavení uživatele (HKCU) - ***%userprofile%\ntuser.dat***
- nastavení počítače (HKLM) - ***%systemroot%\system32\config\system***
- ***regedit.exe***; ***reg.exe***

»Nastavení sítě

- LAN
  - Ethernet
  - WLAN
    - Wireless LAN
  - BT PAN
    - Bluetooth Personal Area Network
    - může v něm být až 8 zařízení ve vztahu master-slave
    - spousta dalších může být připojena v „zaparkovaném“ modu
  - 1394 (FireWire)
    - architektura sériové sběrnice pro vysokorychlostní přenos dat
    - používá se pro projení datových uložišť, průmyslových video a audio systémů
    - narozdíl od USB dosahuje vyššího trvalého, nepřerušovaného datového toku
    - méně zatěžuje systém než USB díky konstrukci řadiče, který pracuje přes DMA (přímý přístup do paměti)
      - způsob přímého přenosu dat mezi operační pamětí a vstupně/výstupními zařízeními
      - data neprocházejí skrze procesor, čímž lze dosáhnout vyššího výkonu
      - DMA se používá pro přenos větších objemů dat, např. řadič pevných disků, grafická karta, síťová karta, ...
- DialUp
  - Modem (PPP/SLIP)
  - Broadband modem (PPPoE)
  - VPN (GRE, L2TP)
- DialUp server
  - Modem
  - Kabel
  - VPN
    - Virtual Private Network
    - prostředek k propojení několika počítačů prostřednictvím nedůvěryhodné (veřejné) počítačové sítě, díky čemuž lze dosáhnout stavu, kdy propojené počítače budou mezi sebou komunikovat, jako kdyby byly v rámci jedné uzavřené privátní sítě
    - totožnost obou stran je prověřována pomocí digitálních certifikátů, veškerá komunikace je šifrovaná



- ICS (Internet connection sharing)
  - NAT
    - Network Address Translation
    - způsob úpravy síťového provozu přes router přepisem výchozí a/nebo cílové IP adresy
    - používá se nejčastěji pro přístup více počítačů z lokální sítě na Internet pod jedinou veřejnou adresou
    - může mít problémy v komunikaci mezi klienty a snížit rychlost přenosu
  - DHCP
    - Dynamic Host Configuration Protocol
    - používá se pro automatickou konfiguraci počítačů připojených do počítačové sítě
    - DHCP server přiděluje pomocí DHCP protokolu řadu parametrů (IP adresu, masku sítě, implicitní bránu a adresu DNS serveru) pro komunikaci pomocí IP protokolu
    - platnost těchto údajů je omezená, proto musí být spuštěn i DHCP klient, který jejich platnost prodlužuje
  - DNS
    - Domain Name System
    - hierarchický systém doménových jmen, který je realizován servery DNS a protokolem stejného jména, kterým si vyměňují informace

» ipconfig « - zobrazení, obnovení konfigurace TCP/IP
- ***ipconfig /release***
- ***ipconfig /renew***
- ***ipconfig /flushdns***
- ***ipconfig /registerdns***
- ***ipconfig /showclassid***

» netstat « - zobrazení aktivních síťových připojení
- ***netstat –a –b***

» nbstat « - práce s NetBT (NetBios nad TCP/IP)
- ***nbstat –R***
- ***nbstat –RR***

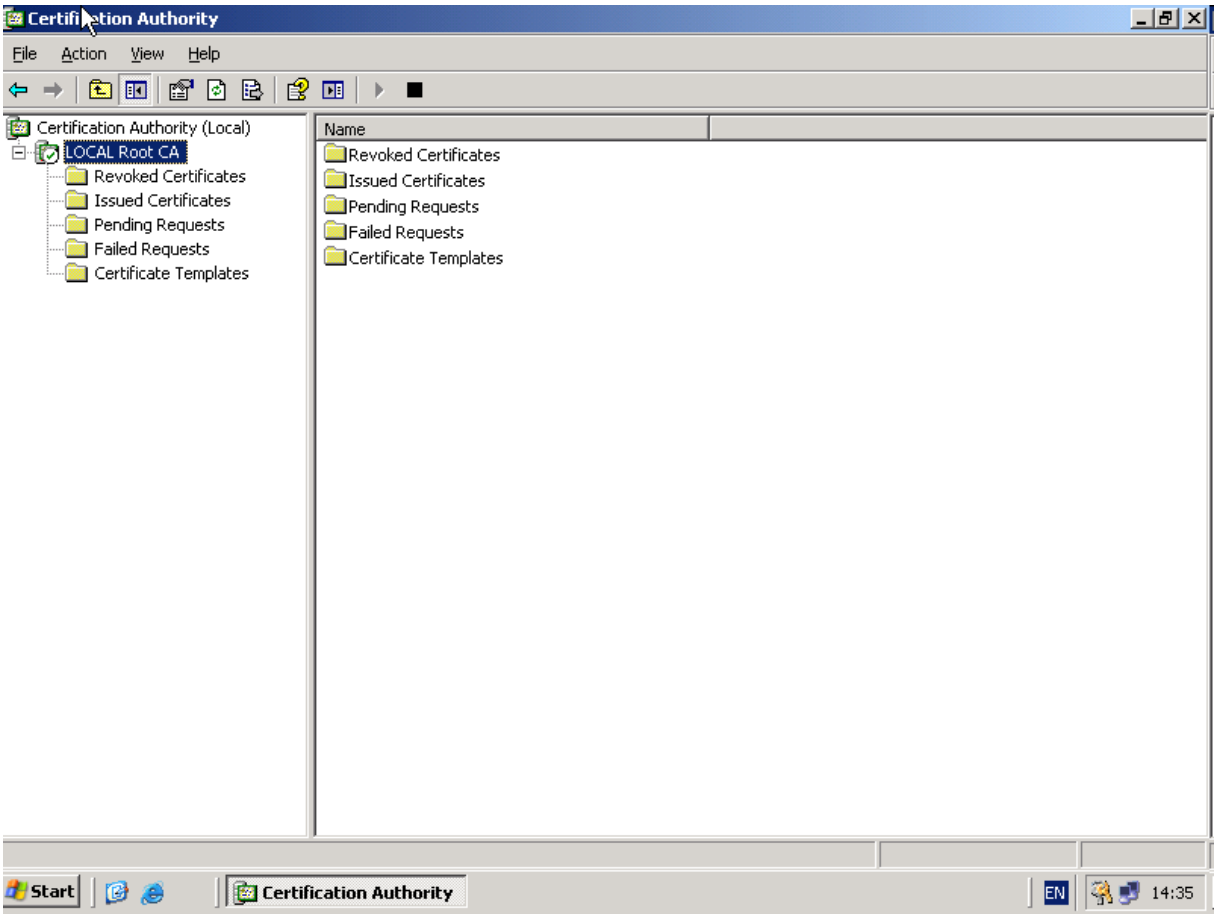
» route « - manipulace s routovací tabulkou
- ***route print***
- ***route –p add***

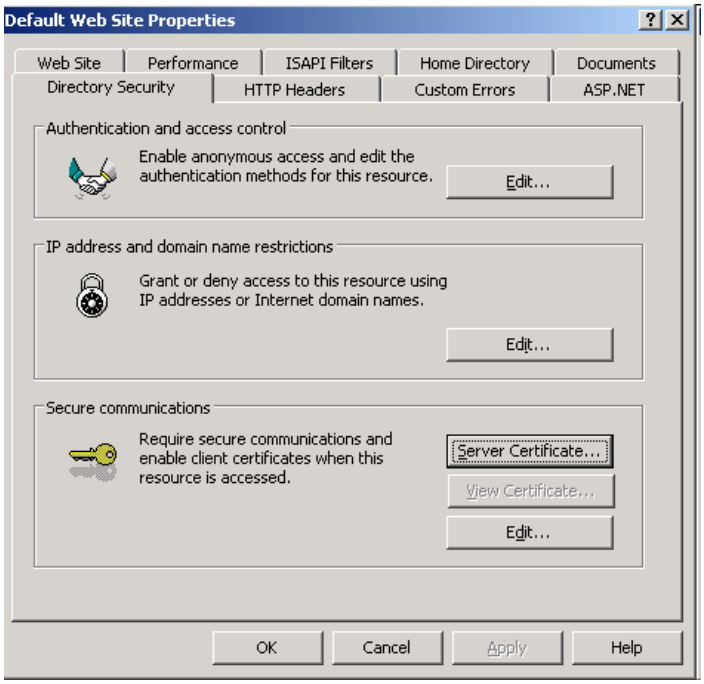
» arp « - manipulace s ARP tabulkou (protokol zabezpečuje přiřazení IP adres fyzickým adresám linkové vstvy; vlastní komunikace v síti se uskutečňuje právě pomocí fyzických adres)
- ***arp –a***

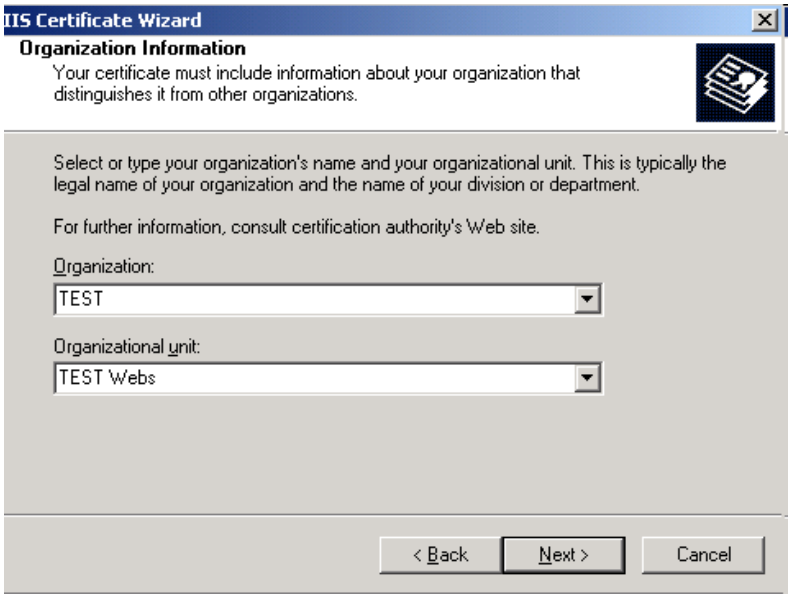
» netsh « - silný nástroj pro konfiguraci sítě
- ***netsh winsock reset***
- ***netsh interface ip reset resetlog.txt***

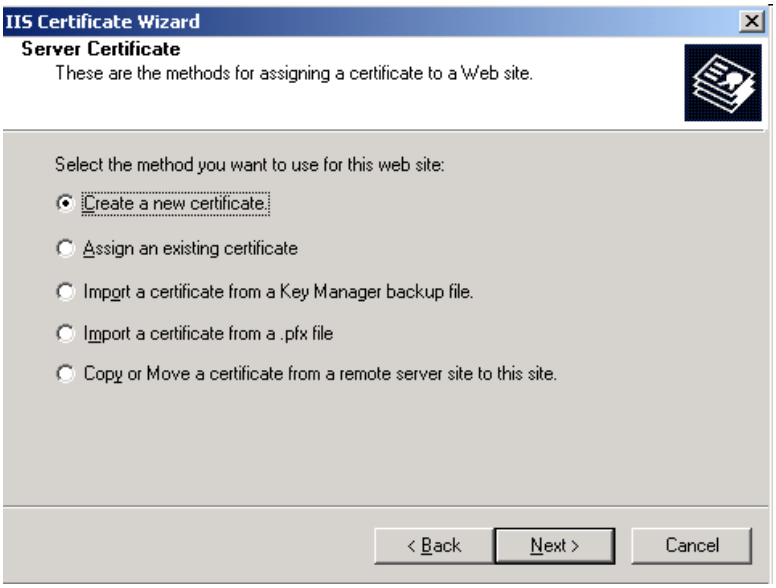
»Certification Authority
- typicky se používá pro generování serverových SSL certifikátů pro IIS (https), osobních certifikátů pro šifrování/podpis e-mailů, ...

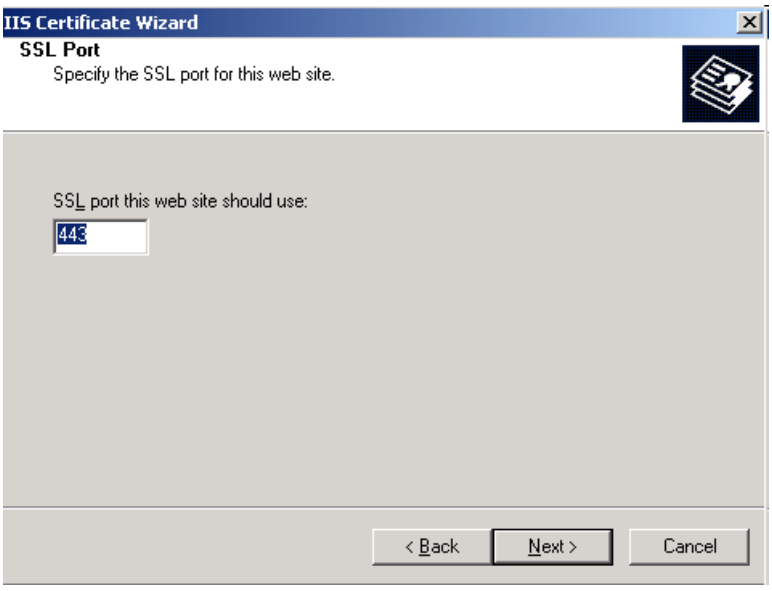
» certutil.exe « - commandline nástroj
» cipher.exe /r « - generování certifikátu pro EFS recovery agent

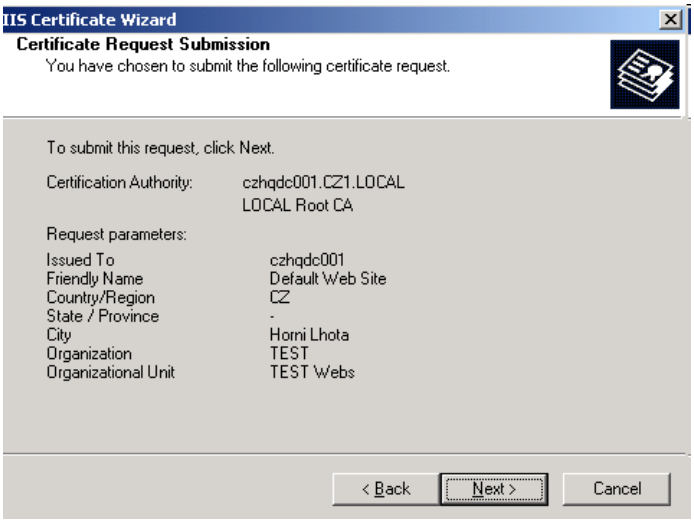




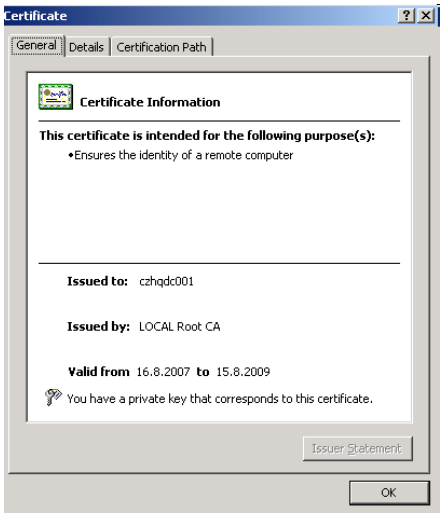

IIS Certificate Wizard
Organization Information
Your certificate must include information about your organization that distinguishes it from other organizations.
Select or type your organization's name and your organizational unit. This is typically the legal name of your organization and the name of your division or department.
For further information, consult certification authority's Web site.
Organization:
TEST
Organizational unit:
TEST Webs
< Back
Next >
Cancel


IIS Certificate Wizard
Server Certificate
These are the methods for assigning a certificate to a Web site.
Select the method you want to use for this web site:
Create a new certificate.
Assign an existing certificate
Import a certificate from a Key Manager backup file.
Import a certificate from a .pfx file
Copy or Move a certificate from a remote server site to this site.
< Back
Next >
Cancel


IIS Certificate Wizard
SSL Port
Specify the SSL port for this web site.
SSL port this web site should use:
443
< Back
Next >
Cancel

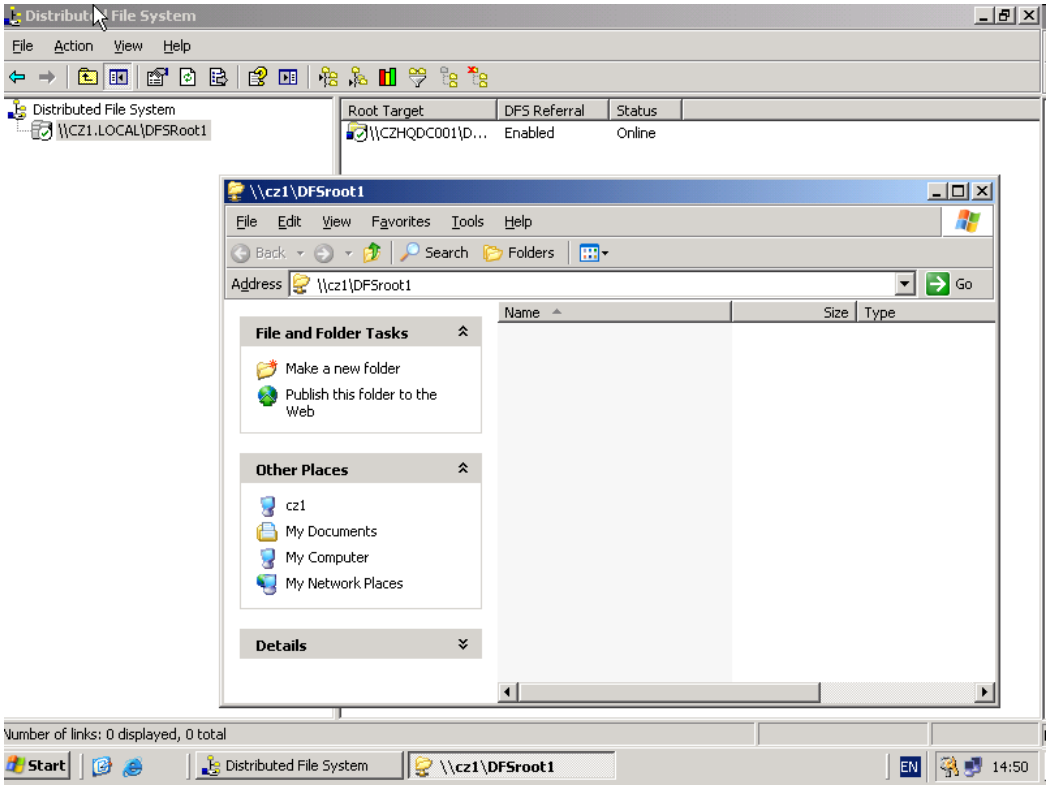

IIS Certificate Wizard
Certificate Request Submission
You have chosen to submit the following certificate request.
To submit this request, click Next.
Certification Authority: czhqdc001.CZ1.LOCAL
LOCAL Root CA
Request parameters:
Issued To czhqdc001
Friendly Name Default Web Site
Country/Region CZ
State / Province -
City Horni Lhota
Organization TEST
Organizational Unit TEST Webs
< Back
Next >
Cancel


IIS Certificate Wizard
Completing the Web Server Certificate Wizard
You have successfully completed the Web Server Certificate wizard.
A certificate is now installed on this server.
If you need to renew, replace, or delete the certificate in the future, you can use the wizard again.
To close this wizard, click Finish.
< Back
Finish
Cancel


Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
•Ensures the identity of a remote computer
Issued to: czhqdc001
Issued by: LOCAL Root CA
Valid from 16.8.2007 to 15.8.2009
You have a private key that corresponds to this certificate.
Issuer Statement
OK

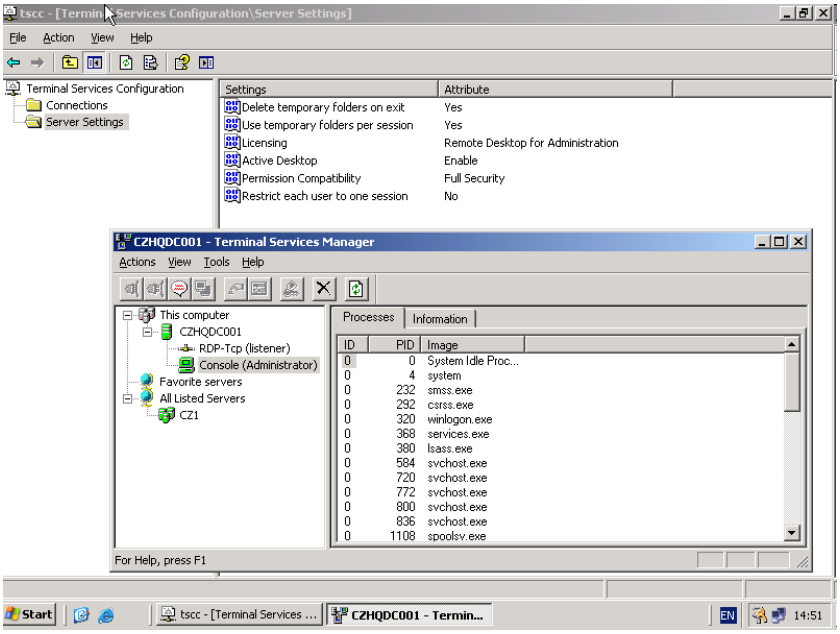
»Distributed File System

- standalone
  - virtualizace filesystému
- domain based
  - replikace pomocí FRS - fault tolerance



»Terminal Services Manager

- Správa terminal services a RDP



»Event Viewer

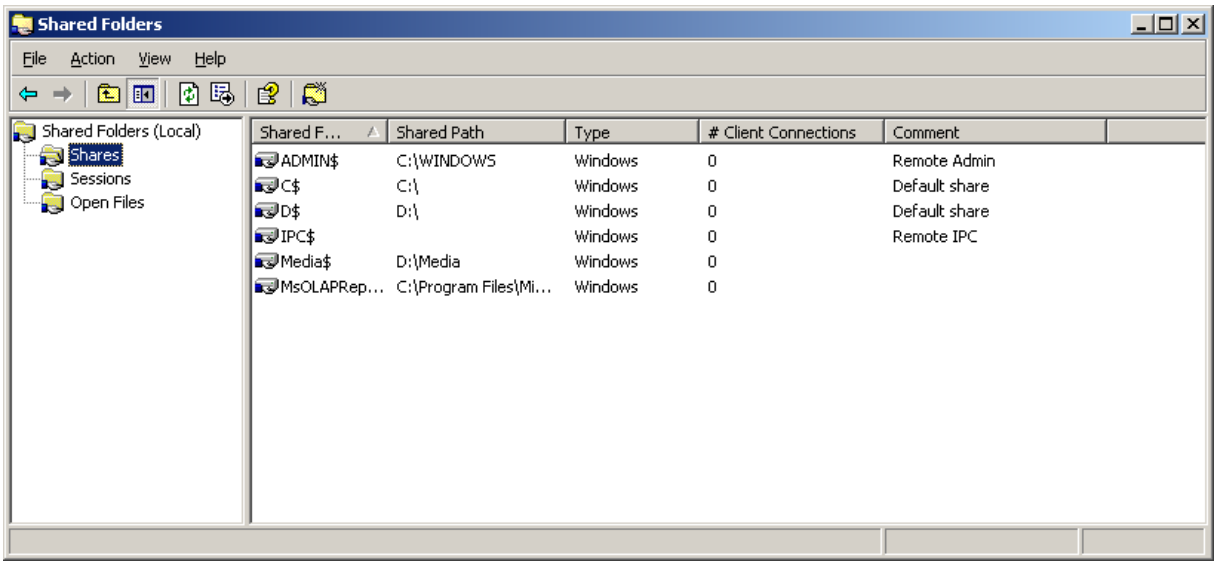
- základní nástroj pro kontrolu systémových logů

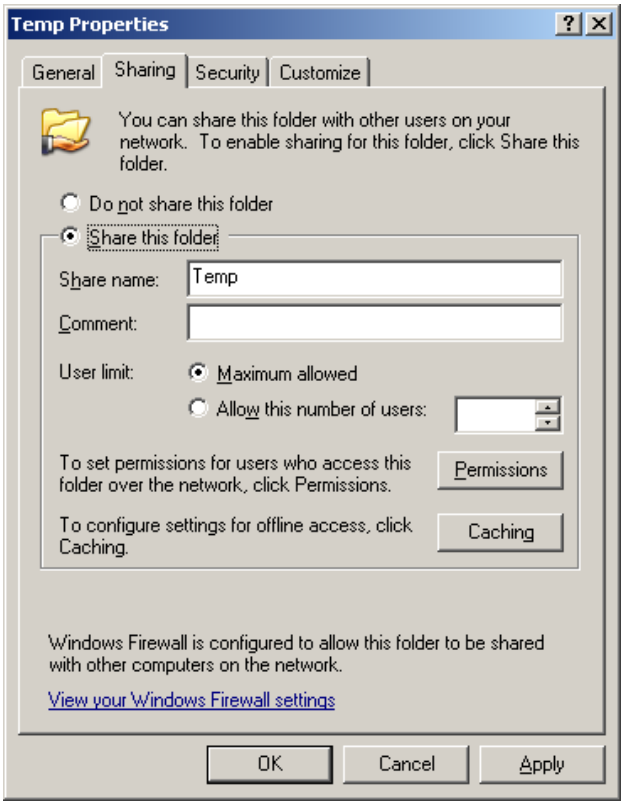
» eventtriggers.exe «

»Shared Folders

- sdílení složek protokolem CIFS
- rozšíření explorer.exe

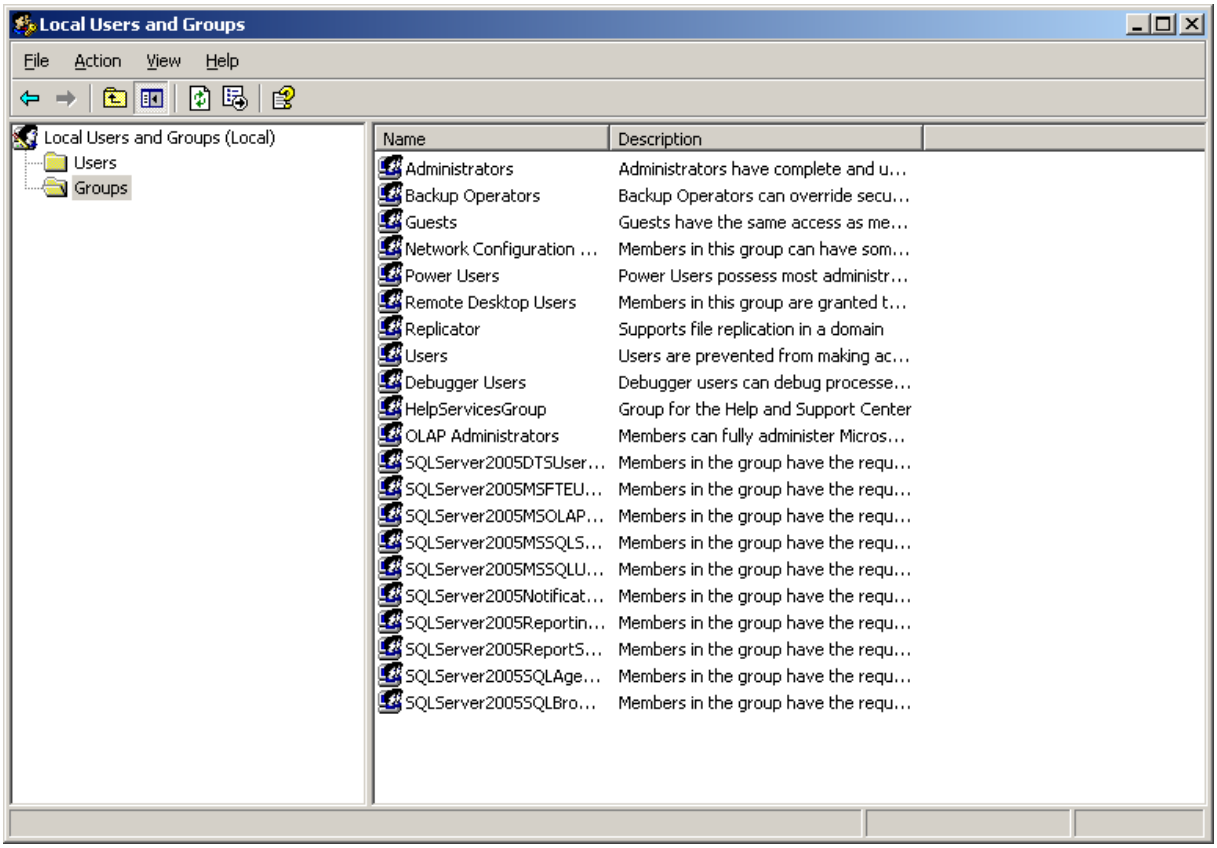
» net.exe « - share
» subinacl.exe « - práva





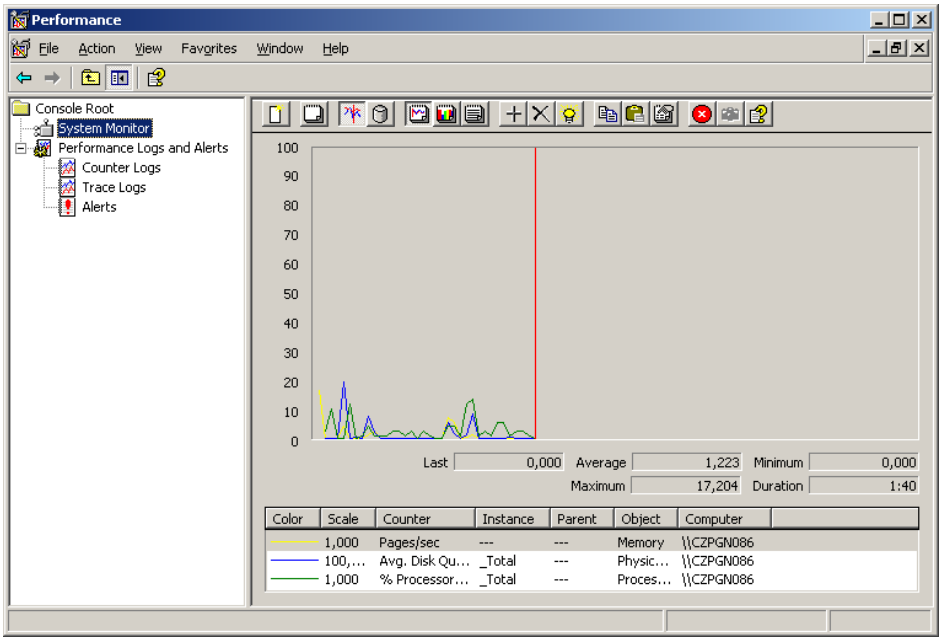
»Local Users and Groups

- dostupné nástroje ve všech OS řady Win2000 a výše
- na doménových řadičích správa pomocí nástrojů Active Directory



»Performance monitor

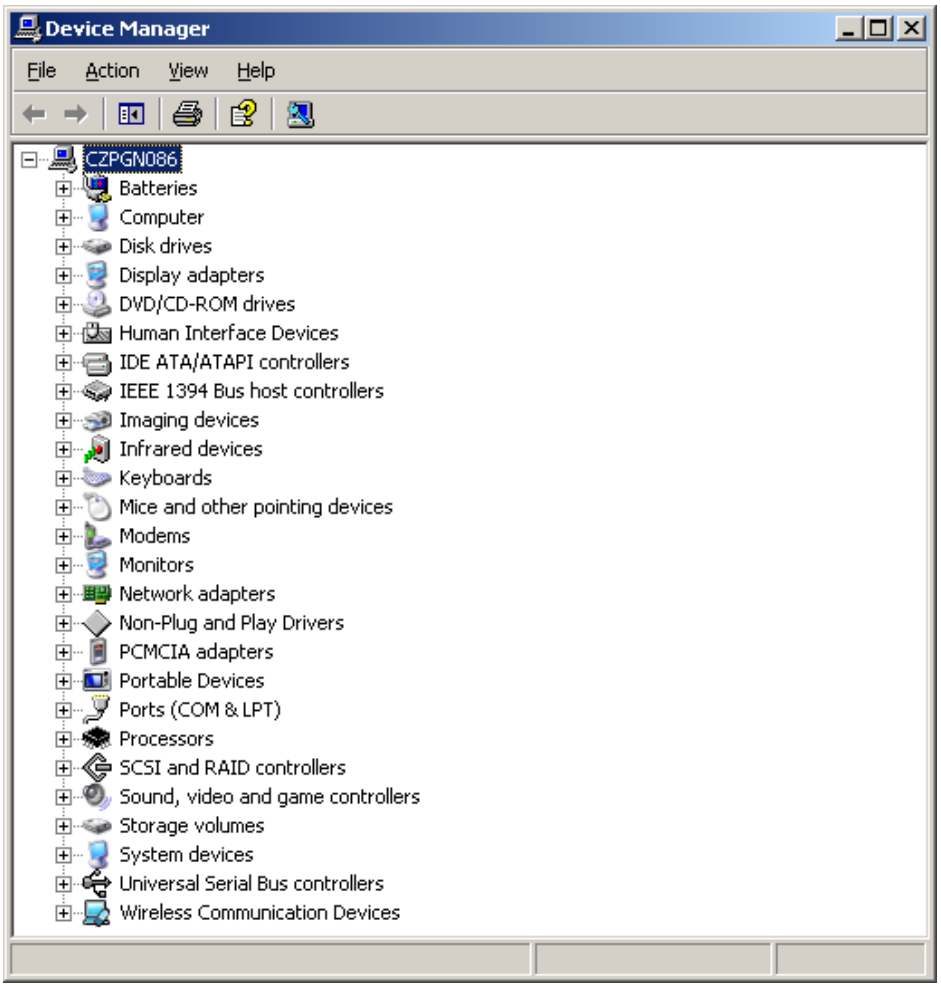
- základní nástroj pro sledování systému
- možnost hlášení mezních situací (dlouhodobé zatížení CPU, atd. ...)



»Device manager

- správa zařízení
- zobrazení odpojených zařízení ***set devmgr_show_nonpresent_devices=1***

» devcon.exe « - náhrada za device manager, navíc poskytuje informaci pro vývojáře, která v základním device manageru není dostupná



»Removable Storage

- správa výměnných médií, určeno zejména pro páskové jednotky a ntbackup

» rsm.exe «

»Disk defragmenter

- vliv fragmentace na výkon disku
- optimalizace doby startování OS – MS Bootvis

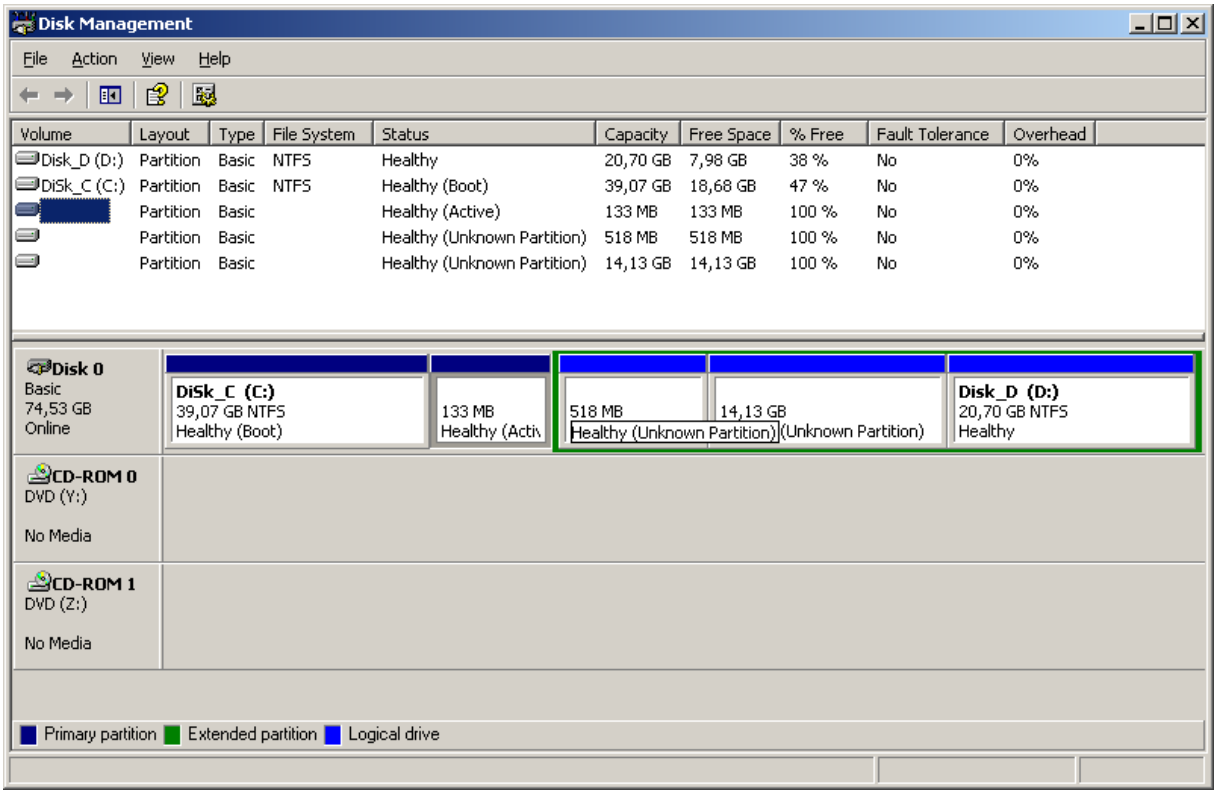
» defrag.exe «

- ***defrag /b***

»Disk management

- správa diskových oddílů, disků, FT svazků (RAID, JBOD)

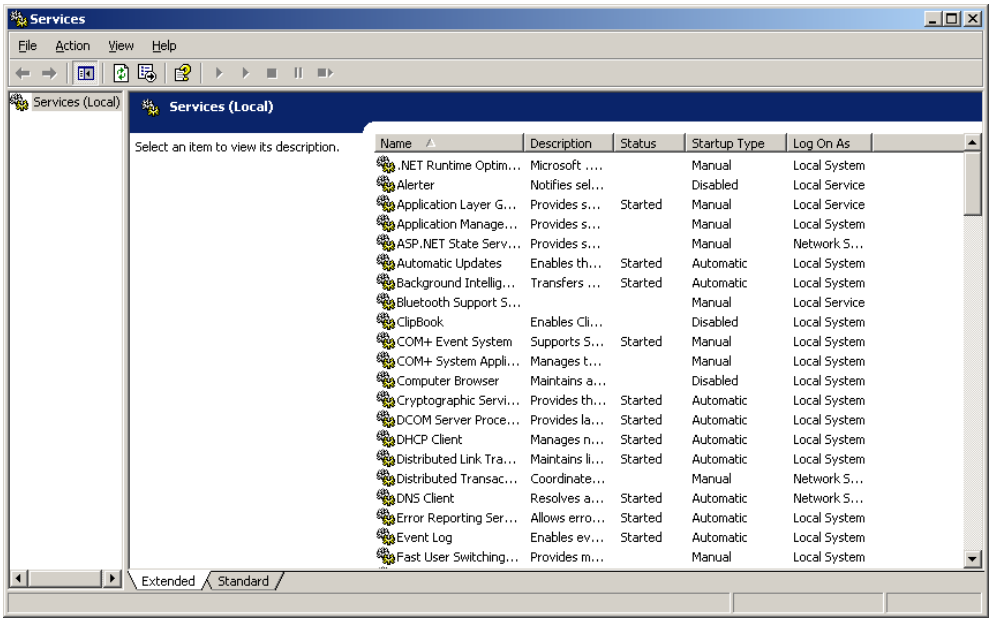
» diskpart.exe «



»Services

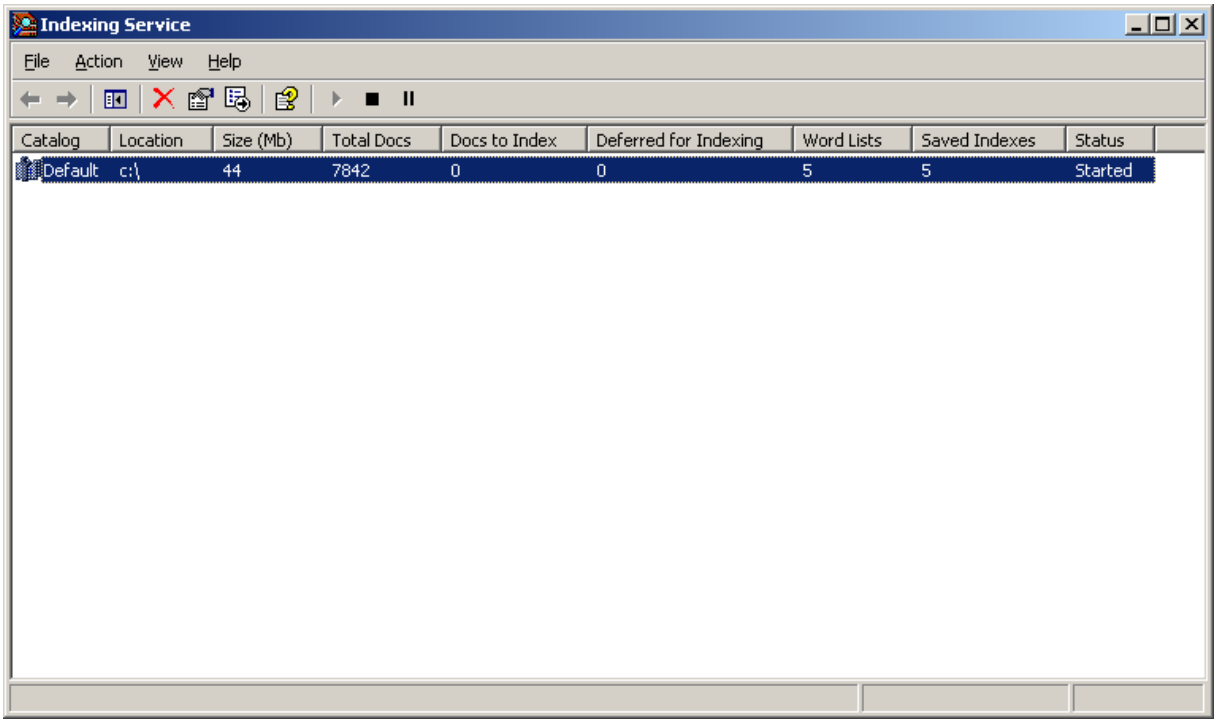
- správa služeb (způsob spuštění, účet, recovery, závislosti)

» sc.exe «



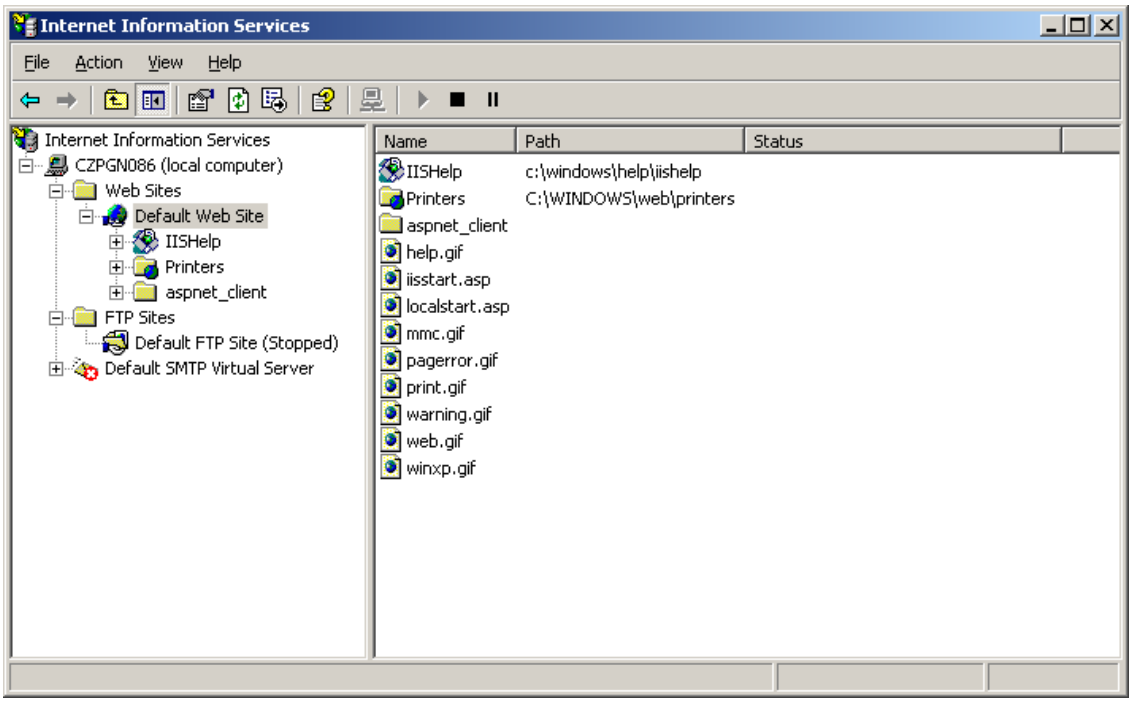
»Indexing service

- prohledávání a indexace souborů (ifilter)
- integrace do explorer včetně síťových složek
- skriptování, využití na www



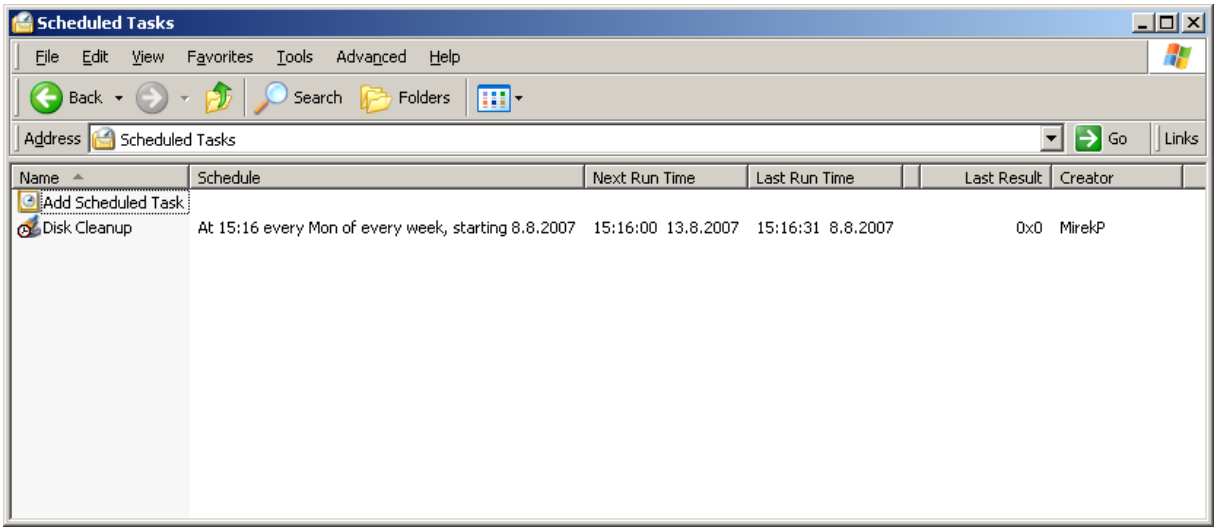
»IIS (Internet information services)

- http a ftp server
- dynamicky generované stránky (asp, asp.net)
- WebDAV (Win 2003)



»Scheduled tasks

- nástroj pro spuštění úloh v zadaném čase
- výběr účtu pod kterým úloha běží



BEZPEČNOST

- Windows má pověst nebezpečného systému
- Největší slabiny:
  - ignorování Least User Privileges konceptu (s vyjímkou Windows Vista)
    - cílem je přiřadit uživateli minimální oprávnění
    - nástroje:
      - EPAL
      - FileMon\RegMon\ProcMon
      - Standart User Analyzer
      - ACT (Application Compatibility Toolkit)
      - GPO
  - kompatibilita s předchozími verzemi vs. bezpečnost
    - největším problémem jsou nekorektní aplikace
  - boot-time security
  - jedna z historicky největších slabin Windows:
    - EFS (Encrypted FileSystem)
    - BitLocker (software & hardware)
    - SAM database (syskey.exe)
      - Brute force
      - Dictionary based
      - Hybrid based
      - Rainbow tables (ophcrack)

»Síťový přístup

- ochrana proti odposlechu / MiM attack
  - SMB a LDAP signing
  - IPSEC (transparentní šifrování)
  - SSL, S/MIME
- zapezpečení komunikace

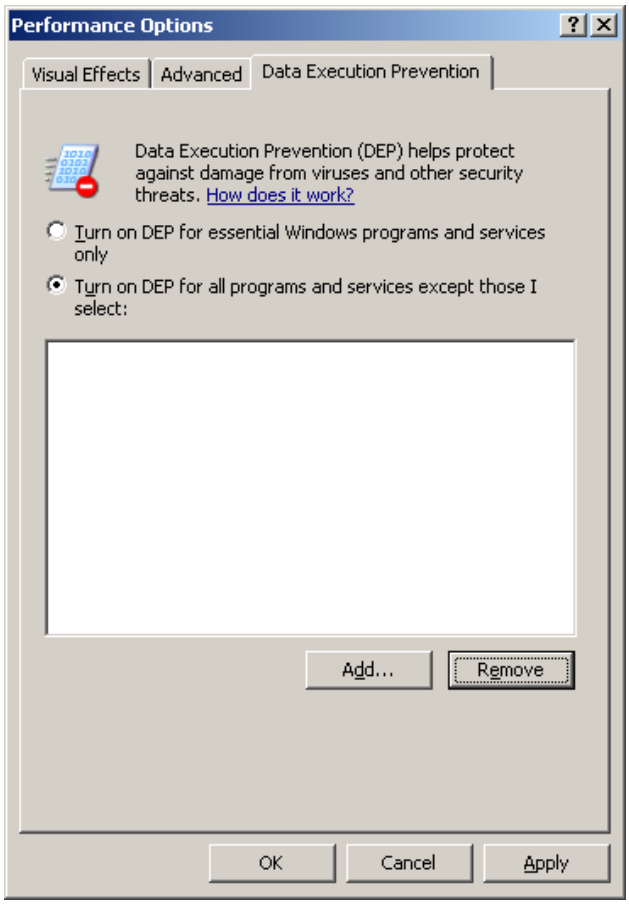
- Windows firewall
- odchozí http spojení – podceňované riziko

»Software Restriction Policies

- umožňuje nastavení podle pravidel
  - hash
    - dle hashe programu, nevýhodou je, že pokud se náhodou změní aspoň trochu hash, pravidlo přestává platit
  - certificates
    - nehodí se, pokud máme dva programy od stejného výrobce, tedy se stejným certifikátem a chceme jeden povolit a druhý zakázat
    - ale když například výrobce vydá novou verzi programu (změní se hash), tak díky restrikci certifikátu zákaz stále bude platit
  - path
    - zákaz spuštění programů z konkrétní složky
  - internet zone
    - „žádný program, který pochází z internetu se nesmí spustit“

»Buffer overflow

- bezpečnostní prvek
- „Zabránění spuštění dat“
- dva typy:
  - DEP HW flags
    - omezení na HW bázi
  - software „cookies“
    - limituje CPU



»Services Permissions

- services SIDs
- services
  - LOCAL SYSTEM
  - NETWORK SYSTEM

»Windows Updates

- řeší se centrálně pomocí WSUS (3.0)
- Microsoft Tuesday
  - druhé úterý v měsíci se vydávají aktualizace (pokud nejde o nic kritického), aby uživatelé nemuseli aktualizovat OS tak často

»Group Policy

- jedna ze základních částí bezpečného systému
- umožňují nejen všeobecné nastavení, ale také detailní nastavení práv na filesystém, případně registry

» gpedit.msc « - editor, ve kterém lze nastavovat pravidla

- neaplikují se v safe modu
- lze nastavit např. aby se pravidla aplikovala pouze pro administrátory
- zákaz programu se při spuštění tohoto programu loguje do Event Vieweru
- ***jushed.exe*** – cokoliv, bez ohledu na to, kde je to umístěno, a jmenuje se to *jusched.exe*, bude zakázané
- cokoliv na základě certifikátu může být velmi užitečné, ale často je potřeba mít na paměti jak se s certifikáty pracuje – např. je potřeba mít připojení k internetu pro určité podmínky

MBSA – Microsoft Baseline Security Analyzer
IIS Lockdown Tool – secure IIS server
EventCombNT – parsování event logs
SysInternals security tools
ISA server

»Nejčastější problémy

- servisní účty
- neopatchované systémy
- defaultní nastavení systému
- jednoduchá hesla

SOUBOROVÉ SYSTÉMY WINDOWS

- ***FAT***
  - File Allocation Table
  - souborový systém FAT je klasický systém pocházející z OS DOS a Windows 9x
  - podpora FAT ve Windows NT:
    - možnost upgrade z jiných verzí Windows
    - kompatibilita se staršími OS v multi-boot prostředích
    - nativní formát pro flash disky
  - podpora FAT je implementována ovladačem *fastfat.sys*
  - každá verze FAT obsahuje číslo udávající počet bitů, které jsou použity pro identifikaci clusteru na disku

- nejrozšířenější souborový systém (použití ve spotřební elektronice)
- podporován většinou současných OS

Schéma FAT

- *FAT12*
  - 12 bit
  - identifikace clusteru omezuje velikost oddílu na max 2^{12} (4096) clusterů
  - velikost clusteru ve Windows se pohybuje od 512 B do 8 KB, což dává teoretickou max. velikost FAT12 oddílu na 32 MB
  - pro floppy disky
- *FAT16*
  - použití v MS DOS
- *FAT32*
  - nejnovější souborový formát založený na FAT formátu
  - je součástí OS Windows 95 OSR2, Windows 98 a Windows Millennium Edition
  - používá 32 bitovou identifikaci clusterů, ale nejvyšší 4 bity jsou rezervovány (efektivně tedy adresuje pomocí 28 bitů)
  - podpora dlouhých názvů souborů
  - velká nevýhoda je omezená velikost jednoho souboru (4 GB)
  - kořenový adresář ale oproti FAT12/16 nemá omezení velikosti ani místa
  - Windows NT může pracovat s velkými FAT32 oddíly, ale velikost nově vytvořeného oddílu je limitována na max. 32 GB
- *exFat*
  - Extended File Allocation Table
  - flash disky, Windows CE 6.0
  - možnost transakčního zpracování (závisí na implementaci výrobce zařízení)
  - řeší problém s vysokokapacitnými médii, se kterými si staré FAT neumí moc dobře poradit
  - stále má v sobě tabulku narozdíl od NTFS (který používá strukturu stromu), takže se v exFatu vyhledává pomaleji (méně efektivně) – z tohoto důvodu je vhodný pro disky a média pro archivaci většího množství souborů, které se příliš často nepřepisují
  - konkuruje NTFS, má výrazně snazší implementaci než NTFS
  - Windows Vista SP1 přidává podporu exFat, ve vyšších Windowsech je to již nativně
  - pro Windows XP a Windows Server 2003 byl vydán hotfix doplňující podporu exFat

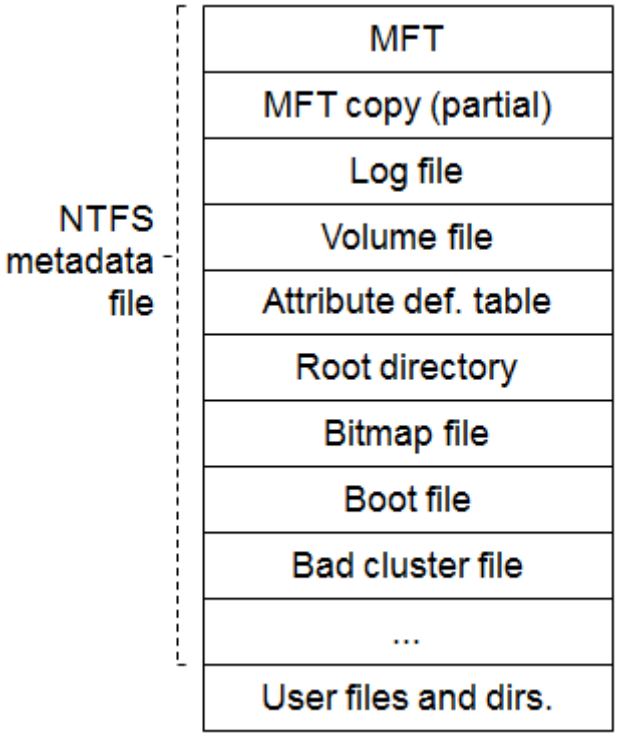
- ***CIFS***
  - Common Internet File System
  - standartní síťový file system
  - sdílení souborů – základ CIFS – vychází z protokolu SMB (Server Message Back)
  - protokol SMB byl původně navržen pro funkci v sítích založených na protokolu NetBIOS (Network Basic Input Output System)
    - NetBIOS byl až do roku 2000 nezbytný pro CIFS

- ***DVD-RAM***
  - random acces media
  - velká disketa
  - je přepisovateíná
  - ve Windows lze naformátova na FAT32
  - garantovaná kvalita (životnost cca 50 – 100) let
  - pomalé
- ***CDFS***
  - CD-ROM File System
  - jednoduchý souborový formát definovaný v roce 1988 jako read-only standart pro CD-ROM média
  - implementace ISO 9660-compliant pomocí ovladače *cdfs.sys* s podporou dlouhých názvů souborů
  - omezení:
    - názvy souborů a adresářů jsou omezeny na 32 znaků
    - omezení počtu úrovní na 8 podadresářů
  - považován za zastaralý, standartem pro read-only media se stává UDF
- ***UDF***
  - Universal Disk Format
  - OSTA (Optical Storage Technology Association) definovala v roce 1995 jako nástupce CDFS pro magneto-optická média (zejména DVD-ROM)
  - Windows 2000 podporuje UDF File System dle ISO 13346, verze 1.02 a 1.5
  - hlavní rysy:
    - název souboru až 255 znaků
    - délka cesty až 1023 znaků
  - omezení:
    - ovladač UDF *udfs.sys* poskytuje pouze čtení
- ***NTFS***
  - New Technology File System
  - nativní souborový formát OS Windows
  - 64 bitová adesace clusterů
    - teoreticky může adresovat svazky velikosti až 16 exabytů (16 mld. GB)
    - Windows 2000 používá pouze 32 bitovou adresaci, takže může adresovat až 128 TB (pomocí 64 KB clusterů)
  - větší režie
  - velice propracovaný
  - drží si transakční logy
  - disky se vzpamatují relativně dobře když je vyndáme za chodu
  - větší soubory i disky
  - vyšší výkon při velkých discích, obsáhlých adresářích a malých souborech
  - spolehlivost bezpečnost

»NTFS Security a Recoverability

- Windows podporují softwarový RAID
- při kopírování z NTFS na FAT32 se ztratí alternativní data streamy
- podpora síťových symlinků
- *sparse files* - soubor, který se tváří, že má strašně velkou velikost (i větší než disk); naalokuje prázdný např. 8 GB soubor, ale začíná zabírat místo až když se začne plnit (např. stahování torrentů)
- nastavení práv může provádět administátor nebo vlastník objektu

- podpora previous versions
- *System Protection*
  - log změn na disku, k jednotlivým verzím se lze vrátit
- *VSC (Volume Shadow Copy)*
  - ve chvíli kdy se provede, vyšle se signál všem aplikacím, aby uložili svůj aktuální stav (uveď do konzistentního stav a řekni hotovo)
- *HSM (Hierarchical Storage Management)*
  - kontroluje kdy byly soubory naposledy použity a podle toho je třídí
- *SIS (Single Instance Storage)*
  - maže kopie a ostatní nahradí linkami
- *kvóta*
  - limit úložného prostoru pro uživatele
- rozšíření NFS
- zpětně kompatibilní s POSIX
- všechny soubory a adresáře mají na NTFS atributy
- například při každém čtení souboru dochází k zápisu metadat
- audit log
- při smazání se vytvoří log o tom, že uživatel ten a ten smazal log
- možnost mountu NTFS svazku do adresáře



- NTFS metadata
  - NTFS log file ($LogFile)
    - záznam všech příkazů které mění strukturu svazku
  - Root directory
    - odsud probíhá prohledávání při prvním pokusu o otevření NTFS souboru
    - po nalezení souboru je uložena MFT reference
      - MFT je hlavní součástí NTFS (podobně jako file allocation table je hlavní součástí FAT)

        - udržuje informace o rozložení všech souborů, adresářů i metadat na disku
        - MFT je také soubor – tzn. je také zaznamenán „sám v sobě“
    - další přístupy mohou použít přímo MFT záznam
- Bitmap file ($Bitmap)
    - ukládá stav alokace jednotlivých clusterů (1 bit ~ 1 cluster)
- Boot file ($Boot)
    - uložen bootstrap code
    - musí být umístěn na pevně dané adrese
- Bad-cluster file ($BadClus)
    - záznam chybných clusterů
- Volume file ($Volume)
    - obsahuje: volume name; NTFS version
    - Dirty Bit – indikuje poškození dat na svazku
- Attribute Definition Table ($AttrDef)
    - definuje jaké typy atributů jsou podporovány na svazku
    - indikuje jestli mohou být indexovány, obnoveny, ...

- standartní atributy souborů na NTFS:
    - standartně podřazené soubory dědí práva z nadřazených adresářů
    - pokud někomu něco nepovolíme, tak to platí stejně jako Deny, takže vyloženě zakazova t většinou nemá sysl
    - má to význam například pokud soubor zdědí právo Allow po adresáři, ale my chceme ten konkrétní soubor zakázat
    - explicitní právo má vyšší prioritu než zděděné
    - full control
        - modify + možnost přidělovat práva ostatním
    - pokud uživatel, který je ve skupině Administrators, vytvoří soubor, nestává se vlastníkem on, ale celá skupina Administratorů

»Kompatibilita souborových systémů

- FAT12/FAT16
    - podporovány ve všech OS Microsoft
- FAT32
    - Windows 9x, 2000/XP/2003
    - Sysinternals FAT32 driver pro NT4
- NTFS
    - OS řady Windows NT
    - Sysinternals NTFSDOS pro DOS
    - Sysinternals NTFS pro Windows 9x

»Porovnání systémů

Feature	Description	FAT	NTFS	UDF
Journaling	File systems that support this feature use transactions to commit metadata changes to the file system. In the event of a power failure or operating system crash, the file system quickly rolls back the uncommitted transactions to quickly return the file system back to a consistent state.	X	?	X
Metadata clustering	The file system attempts to store metadata in contiguous locations on the media. Note that metadata clustering is only supported on UDF 2.5 and later on nonincremental-write media.	X	?	?
Directories are B-trees	A B-Tree index–based directory provides more efficient access to directory entries than a linear directory.	X	?	X
Volume mount points	Volume mount points enable administrators to mount a file system to a directory instead of mounting the file system to a drive letter.	X	?	X
Resident file storage	This feature allows small files (typically a few hundred bytes for each file) to be stored within the file system metadata.	X	?	?
File and directory security	**The file system can restrict access to files and directories individually for each user or for a group of users.**	**X**	**?**	**X***
Compression	This feature enables users to store files in a compressed format on the media.	X	?	X
Hard links	A hard link is the file system representation of a file by which more than one path references a single file in the same volume.	X	?	?
Directory symbolic links	This feature is similar to hard links but allows one directory name to point to another directory on the same PC.	X	?	X*
Encryption	This feature enables users to store files in an encrypted format on the media.	X	?	X
Change journal	This feature provides a persistent log of changes made to files on a volume.	X	?	X
Quotas	This feature enables an administrator to limit the amount of disk space a particular user can use on a given volume.	X	?	X
Sparse file support	This feature allows for efficient utilization of disk space for sparse files.	X	?	?
Alternate data stream support	**This feature allows a file to contain multiple streams of user-defined data.**	**X**	**?**	**X*+**
Configurable allocation size	This feature allows the allocation unit size of the file system to be configured.	?	?	X
Unicode naming	The file system supports Unicode file names.	X	?	?
Defect management	The file system supports sparing of bad blocks on the media when the underlying hardware does not provide defect management.	X	X	?
Incremental-write media support	The file system can work with media that needs data to be written incrementally.	X	X	?

ZÁKLADNÍ NÁSTROJE PRO PRÁCI S PAMĚŤOVÝMI MÉDII

» attrib.exe « - nastavení atributů

» diskmgmt.msc « - správa svazků

» chkdsk.exe « - kontrola svazků

» fsutil.exe « - ladění NTFS

» cacls.exe « - práva

» cipher.exe « - šifrování

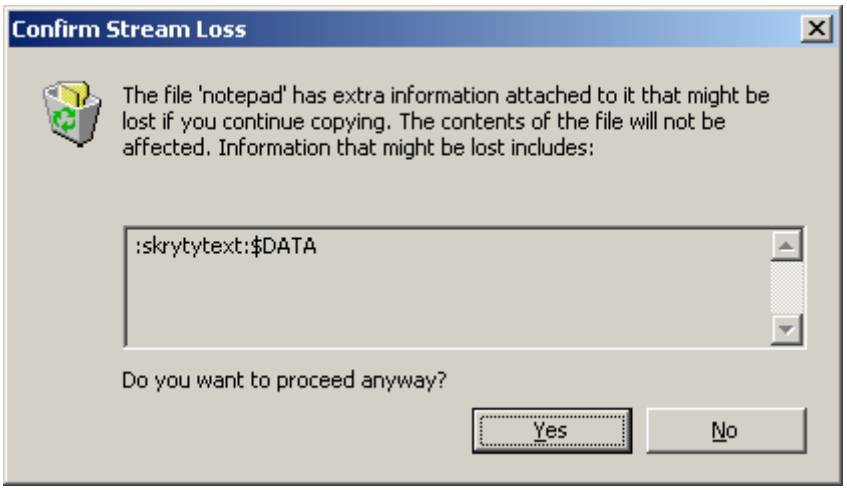
» dfrg.msc « - defargmentace

» defrag.msc « - defragmentace

ALTERNATE DATA STREAM (ADS)

Jak uložit text nebo jinou informaci do ADS existujícího souboru?

type text.txt > notepad.exe:skrytytext
„vepiš obsah souboru „text.txt. do alternativního streamu s názvem ‚skrytytext‘ programu notepad.exe“



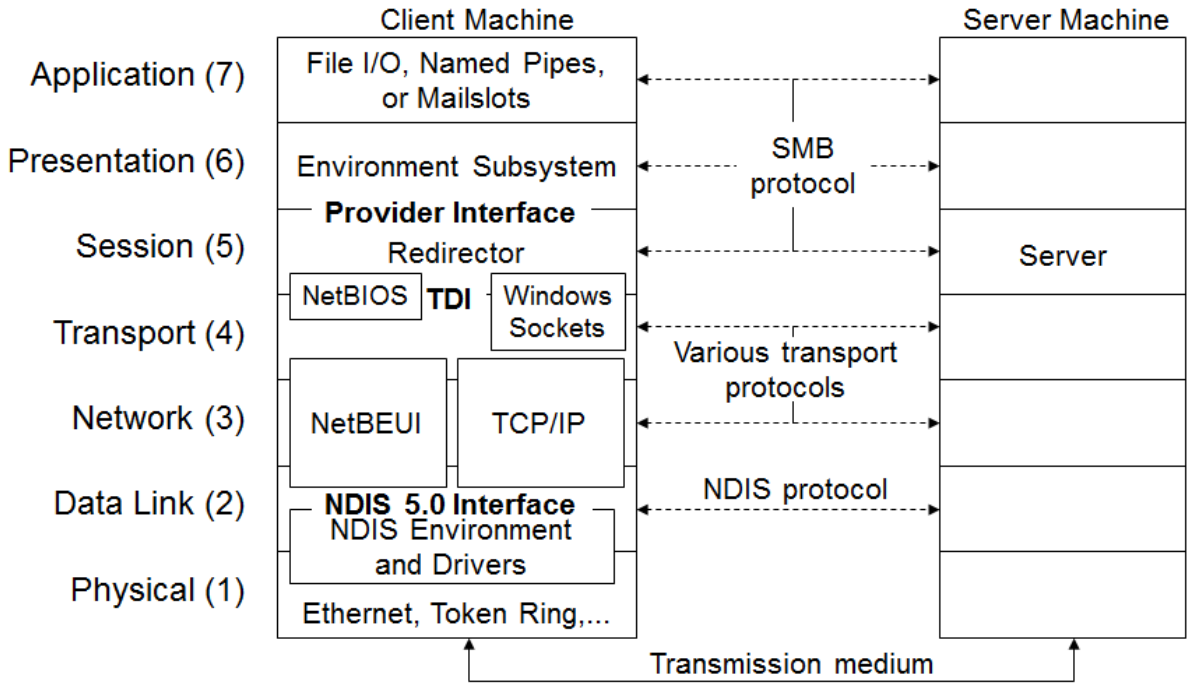
» fsutil « - nastavení parametrů souborového systému

SÍŤOVÝ MODEL

- protokol TCP/IP, winsock
- síťové služby a jejich nastavení
  - ***DHCP***
    - Dynamic Host Configuration Protocol
    - používá se pro automatickou konfiguraci počítačů připojených do počítačové sítě
    - standartní protokol pro dynmickou konfiguraci TCP/IP
    - centralizovaná správa IP adres a dalších TCP/IP parametrů (IP adresa, maska, default gateway, DNS, WINS, domain name, ...)
    - autorizace MS DHCP serveru v Active Directory
    - DHCP server přiděluje pomocí DHCP protokolu řadu parametrů (IP adresu, masku sítě, implicitní bránu a adresu DNS serveru) pro komunikaci pomocí IP protokolu
    - platnost těchto údajů je omezená, proto musí být spuštěn i DHCP klient, který jejich platnost prodlužuje
    - příkazy:
      - dhcpcmd
      - netsh dhcp
      - ipconfig
  - ***DNS***
    - Domain Name System
    - hierarchický systém doménových jmen, který je realizován servery DNS a protokolem stejného jména, kterým si vyměňují informace
    - základní resolving protokol pro TCP/IP a CIFS
    - nezbytnou součástí Active Directory; AD integrated zóny
    - podpora dynamických registrací
    - koexistence s WINS
    - zóny:
      - primární
      - sekundární
      - AD integrated
    - forward zóny
    - podpora classless reverse zón
    - příkazy:
      - ipconfig
      - dnscmd
      - nslookup
      - soubor hosts
  - ***WINS***
    - Windows Internet Naming Service
    - MS implementace NetBIOS Name Serveru pro Windows
    - slouží jako name server pro jména počítačů v síťovém prostředí NetBIOS
    - centrální uložiště informací pro NetBIOS
    - většinou mívá počítačová síť více WINS serverů
    - dynamicky aktualizovaná centrální databáze, možnost statických záznamů
    - plná replikace
    - možnost vazby s DNS
    - příkazy:
      - nbtstat
      - soubor imhosts

  - netsh wins
- ***RRAS***
  - Routing and Remote Access Service – „směrování a vzdálený přístup“
  - implementace routeru a serveru pro vzdálený přístup
  - podporuje směrování v síti pomocí protokolů IPv4 a IPv6 a připojení
  - podporuje připojení vzdálených uživaelů nebo prpopojení mezi sítěmi pomocí virtuální privátní sítě (VPN) či telefonického spojení
  - softwarový směrovač
  - směrování se používá pro víceprotokolové služby směrování LAN-to-LAN, VPN, NAT, ...
- ***WSUS***
  - Windows Server Update Services
  - centralizovaná služba pro aktualizace software Microsoft (ekvivalent Microsoft Update)
  - využívá IIS a SQL (MSDE)
  - základní nastavení pomocí Group Policy
  - konfigurace pomocí webového rozhraní
  - silný reporting (Reporting Services)

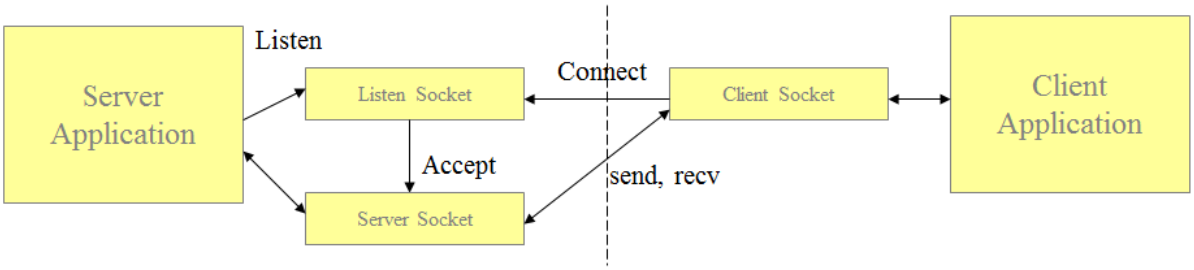
»OSI Model a Win. Networking



»Winsock

- implementace BSD Unix (Berkeley Software Distribution) Sockets společností Microsoft
  - BSD Sockets
    - aplikační programové rozhraní (API), s jehož pomocí lze programovat komunikační apliakce všeho druhu
    - původně vytvořeno pro BSD Unix, ale postupně se rozšířilo i do MacOS, MS Windows a dokonce i PalmPS
    - neomezuje se jen na síťový protokol IP, ale má v oblasti internetových aplikací největší význam

- rozšířené na unixových systémech
- definice Winsock API za pomoci Winsock consortium
- reliable connection-oriented (streams) and unreliable connectionless (datagram) modes



»Implementace TCP/IP v MS Windows

- podpora standartních funkcí
  - podpora více síťových karet s různými typy médií
  - logický multi-homing
  - podpora interního routingu
  - IGMP (IP Multicasting) support
  - detekce duplicitních IP adres
  - více default gateway
  - dead gateway detection
  - automatické zjištění „Maximum Transmission Unit“ (PMTU)
- zlepšení výkonu
  - snížení generovaného broadcastu
  - úsporný kód – nižší nároky na CPU
  - self-tuning
- dostupné služby
  - Dynamic Host Configuration Protocol (DHCP) client and server
  - Windows Internet Name Service (WINS), a NetBIOS name server
  - Domain Name Server (DNS) (od Windows NT 4.0)
  - Point-to-Point Tunneling Protocol (PPTP) pro VPN
  - Dial-up (PPP/SLIP) support
  - TCP/IP network printing (lpr/lpd)
  - SNMP agent
  - Wide Area Network (WAN) browsing support
  - High-performance Microsoft Internet Information Server
  - Basic TCP/IP connectivity utilities, including: finger, FTP, rcp, rexec, rsh, Telnet, and tftp
  - Server software for simple network protocols, including: Character Generator, Daytime, Discard, Echo, and Quote of the Day
  - TCP/IP management and diagnostic tools, including: arp, hostname, ipconfig, lpq, nbtstat, netstat, ping, route, and tracert

»Windows Sockets 2

- přístup k dalším protokolům (nejen TCP/IP)
  - Windows Sockets 2 dovoluje aplikacím používat standartní socket interface pro přístup k množství instalovaných přenosných protokolů
- podpora overlapped I/O with scatter/gather
  - služby pro name resolution nezávislé na protokolu

    - obsahuje standartní set funkcí pro dotazy a práci s mnoha dnešními jmennými službami (DNS, SAP, ...)
- protocol-independent multicast a multipoint
    - aplikace nad Windows Sockets 2 jsou schopny zjistit jaké možnosti multipoint nebo multicast jsou dostupné a používat je
- quality of service
    - obsahuje podporu parametrů QOS jako jsou vyjednání latence a šířky pásma
- další rozšíření
    - shared sockets
    - conditional acceptance
    - exchange of user data at connection setup/teardown

»Utility pro práci s TCP/IP

- arp
- netstat
- ping
- tracert
- MS Network Monitor
- tcpview (utilita 3. strany)
- ethereal (utilita 3. strany)
- nmap (utilita 3. strany)

»Nastavení protokolu TCP/IP

- konfigurace
    - dynamická (DHCP)
    - statická
    - kombinace DHCP + alternativní statická
    - automatická (APIPA – Automatic Private IP Addressing)
- příkaz *netsh* pro commandline nastavení

IMPLEMENTACE SÍŤOVÝCH A BEZPEČNOSTNÍCH SLUŽEB V PROSTŘEDÍ WINDOWS

- OSI model
    - účelem referenčního modelu je poskytnout základnu pro vypracování norem pro účely propojování systémů
    - norma nespecifikuje implementaci (realizaci) systémů, ale uvádí všeobecné principy sedmivrstvé síťové architektury
    - popisuje vrstvy, jejich funkce a služby
- Windows Networking
    - MS-NET
        - redirector zpracovává I/O požadavky na vzdálené soubory, složky, tiskárny a posílá je vzdálenému serveru
        - podpora více redirektorů
    - Active Directory
    - Network Server
        - přijímá a zpracovává SMB požadavky
        - peer-to-peer networking
    - LAN Manager
        - domény
        - sdílení informací o účtech/zabezpečení

    - Server Message Block protocol
        - NetBIOS interface (API)
        - předávání I/O požadavků ve formátu SMB
    - MS-DOS 3.1
    - podpora file-locking a record-locking pro FAT filesystem
    - Microsoft Networks (MS-NET; 1984)
    - uniform naming convention (UNC): ***NET USE X: \\SEVER\SHARE***
- síťové komponenty
    - server, redirector
    - MPR
        - Multiple Provider Router

»Síťová API

- Windows I/O API
    - open, close, read, write s UNC (univerzální konvence) názvy vzdálených souborů
- Windows network (WNet) API
    - procházení souborových systémů peřs standardy LAN Manager, NetWare, VINES, ...
- Windows named pipe and mailslot APIs
    - předávání zpráv mezi aplikacemi
    - broadcasting
- NetBIOS API
    - zpětná kompatibilita pro aplikace MS-DOS, 16bit Windows, OS/2
- Windows Sockets API
    - 16/32 bit UNIXový síťový interface
- Remote Procedure Call (RPC) facility
    - kompatibilní s Distributed Computing Environment (DCE) RPC

»Windows domény

- umožňují sdílení security database (centrální souborová databáze) mezi skupinou počítačů
    - kopie na každém doménovém řadiči (DC)
    - obsahuje uživatelské účty a informace o zabezpečení zdrojů v této oblasti
    - členské stanice používají pro autentikaci doménové řadiče
- dva styly domén:
    - historické NT 4 domény
        - security database je uložena v ***registrech*** (SAM & SECURITY hives)
        - omezená podpora vztahů mezi doménami
        - služba *netlogon* pro autentikaci
    - Windows 2000 Active Directory domény
        - security database je uložena v ***Active Directory***
        - domény Win2000/XP/2003 podporují forests – doménové hierarchie pro lepší škálovatelnost ve velkých firmách
        - autentikace protokolem *Kerberos*

»Síťové komponenty

- redirector a network server
- nástup s MS-NET (assembler)
- kompletně přepsaný kód pro Windows NT/2000
- implementován jako ovladače souborových systémů
- může koexistovat s redirectory / servery jiných dodavatelů (netware)
- implementace v podobě ovladačů znamená

- jsou součástí Windows executive
- přístup k ovladačům interface I/O manageru
- možnost přímého využívání funkcí cache manageru
- vrstvený model I/O manageru odpovídá vrstvám síťových protokolů
- redirector / server mohou pracovat modulárně – nad libovolným protokolem

»Vlastnosti redirector / server

- kompatibilita
  - kompatibilita s existujícími MS-NET a LAN Manager servery (MS-DOS, OS/2, Windows)
  - přístup k vzdáleným souborům, tiskárnám
  - přístup k named pipes
    - API původně vyvinuty firmou Microsoft pro OS/2 LAN Manager
    - obousměrná, reliable connection-oriented komunikace
      - messaging mode pro posílání a příjem celých zpráv
      - ve Windows plně implementovány, omezení Win9x (pouze klient)
- inicializace
  - inicializace ovladače – vytvoření objektu \Device\Redirector
  - registrace rutin pro operace ovladače – operations open, close, read
- spolehlivost
  - obnova konexí k serveru
  - možnost „maskování“ chyb přenosu pokud je možná oprava
  - tabulka otevřených souborů
  - automatické znovuotevření souboru po obnovení spojení
- asynchronní operace
  - rychlý návrat k user-space procesu
  - multithreading

»Resolving síťového názvu

- rozšíření I/O operací o vzdálené (síťové) zdroje
- všechny tyto zdroje jsou ***objekty***
- práci se soubory zprostředkuje Object Manager

»Multiple UNC Provider (MUP)

- MUP driver je aktivován při prvním přístupu aplikace k souboru / zařízení pomocí UNC
- I/O manager otevírá soubor s prefixem |Device|Mup|server|sharename
- MUP driver přijímá požadavek a posílá IRPs asynchronně každému registrovanému ovladači
- je podobný MRP

»Transport Driver Interface

- transportní protokoly jsou implementovány jako ovladače
- Windows poskytují společný programovací interface for redirektory a ostatní síťové ovladače vyšších úrovní
  - Transport Dirver Interface (TDI) umožňuje redirectorům a serverům nezávislost na transportní vrstvě
- jediná verze redirectoru nebo serveru může používat libovolný dostupný transportní mechanismus
- TDI je asynchronní
  - implementuje obecný mechanismsu adresování
  - podpora množství služeb a knihoven
- podporované protokoly

- NetBEUI
  - NetBIOS Extended User Interface
  - jednoduchý síťový protokol vyvinutý firmou IBM pro přímou podporu NetBIOS
- TCP/IP
  - Transmission Control Protocol/Internet Protocol
  - standartní síťový protokol heterogenních systémů (Windows, Unix)
- IPX/SPX
  - Internet Packet Exchange/Sequenced Packet Exchange
  - protokoly používané Novell NetWare
- AppleTalk

»RPC

- Remote procedure call (RPC)
- standart pro síťové programování
- postaven nad dalšími síťovými API (named pipes, Winsock) a poskytuje vývojářům prostředí nezávislé na konkrétních síťových technolgoiích
- používají jej například:
  - remote Registry service
  - tiskové služby
  - messenger

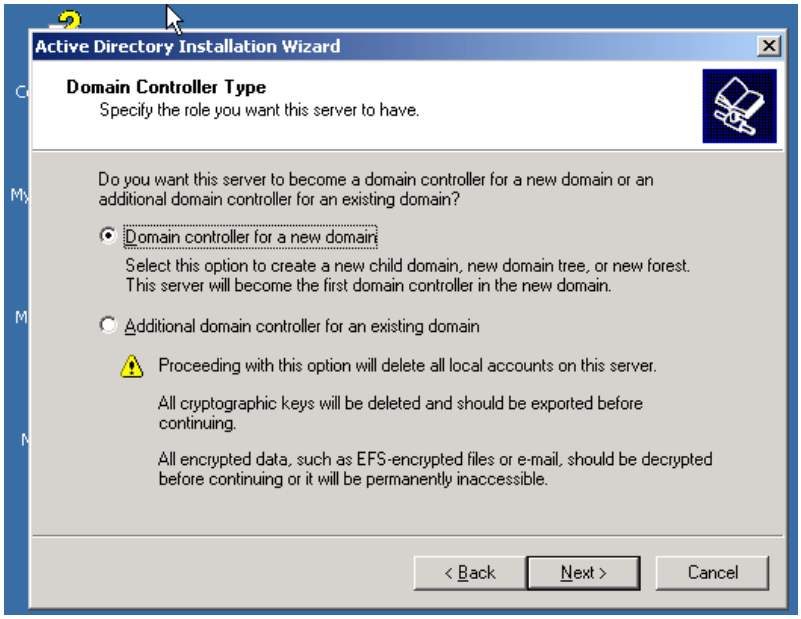
»Windows Firewall

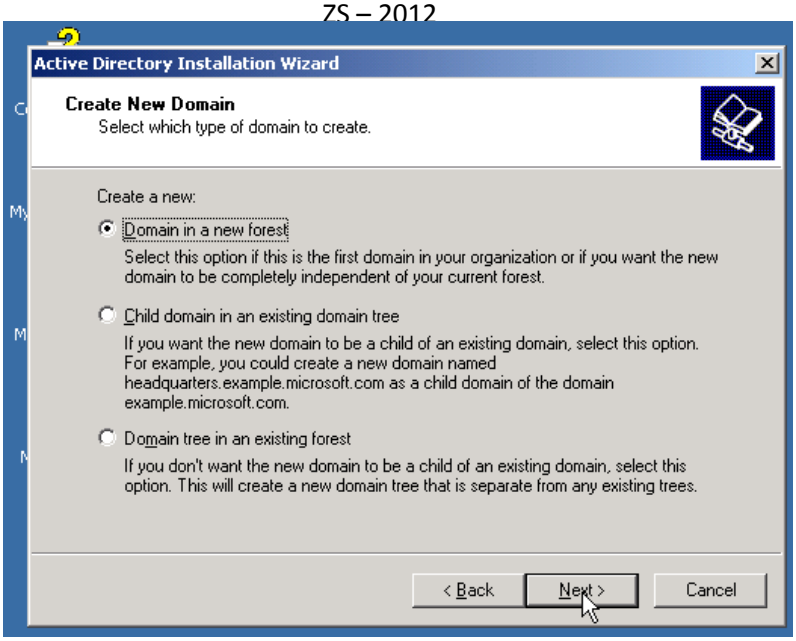
- základní aplikační firewall / packetový filtr
- Windows XP, 2003 – jednosměrný (Windows 2003 RRAS vylučuje použití Windows Firewallu)
- Windows Vista – obousměrný
- konfigurace pomocí Group Policy

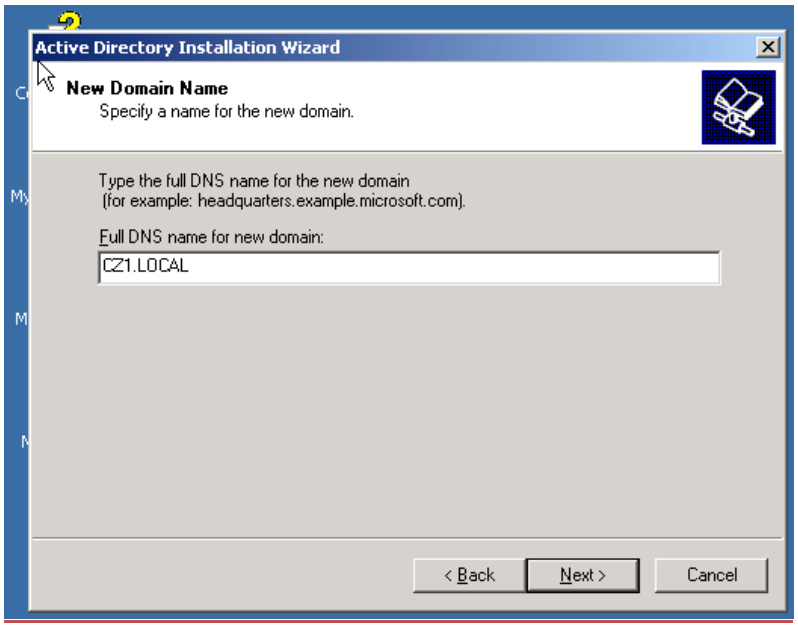
ACTIVE DIRECTORY

»Instalace AD

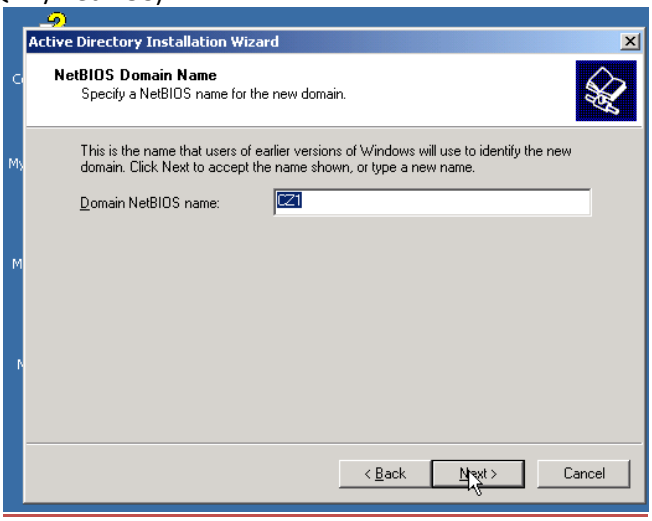
» dcpromo « - instalační průvodce

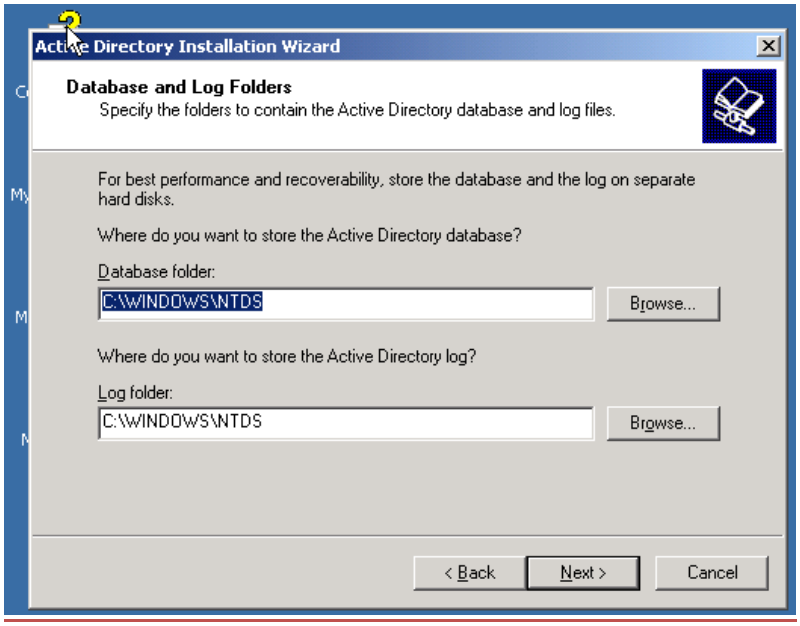




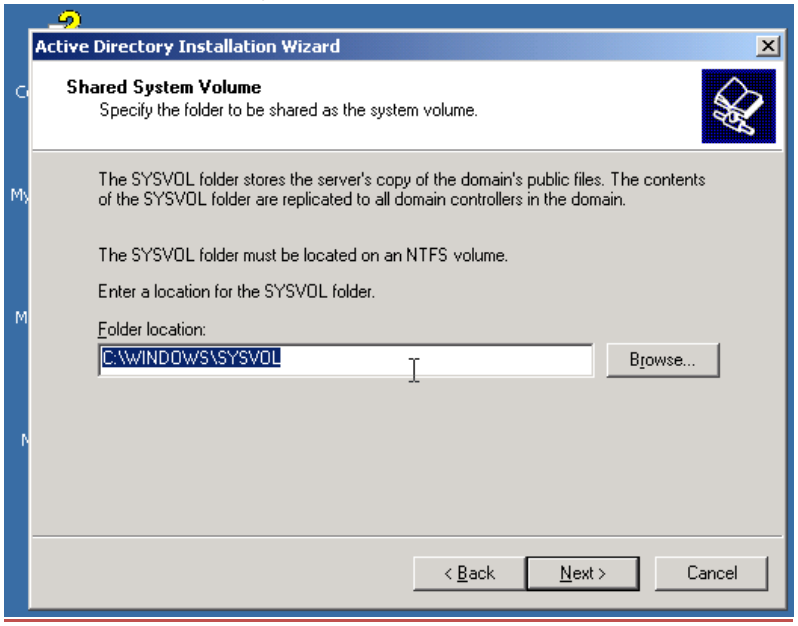


DNS, název domény (FQDN/NetBIOS)

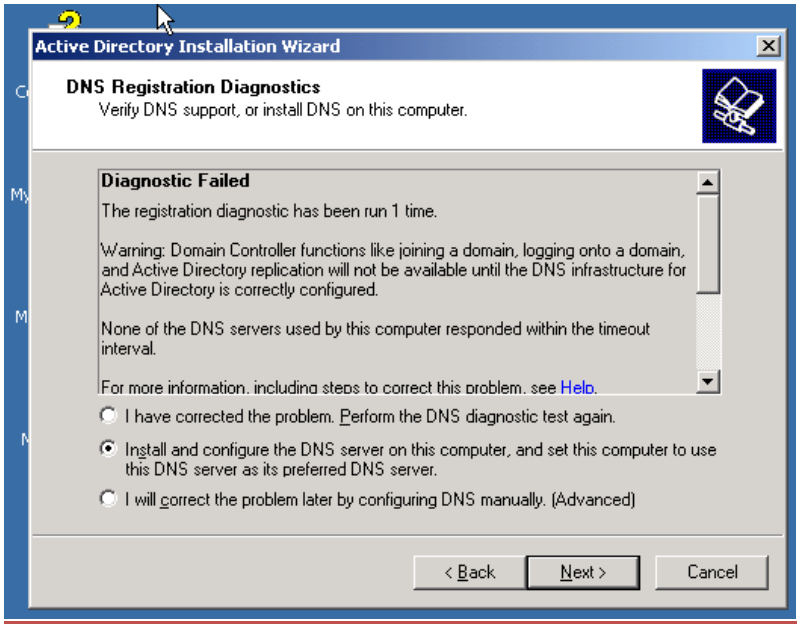


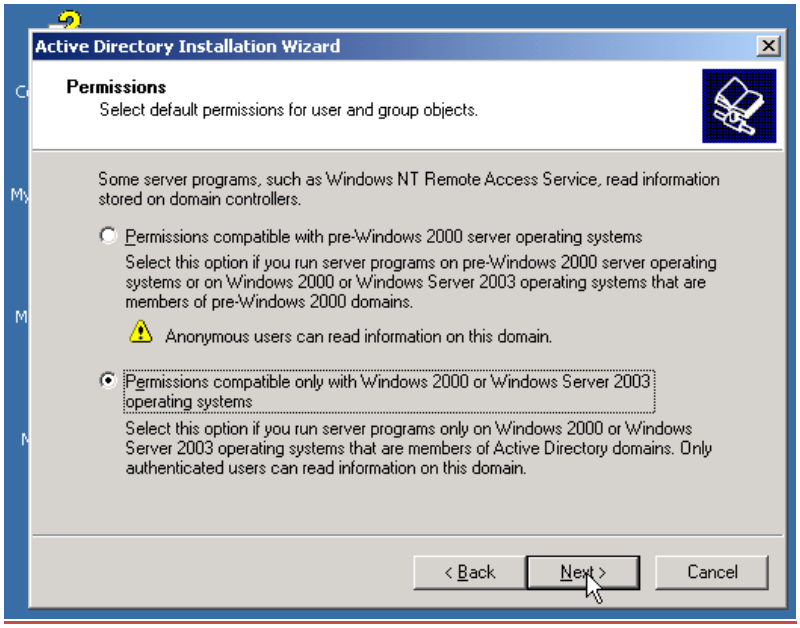


Umístění NETLOGON a AD – extra oddíl, RAID

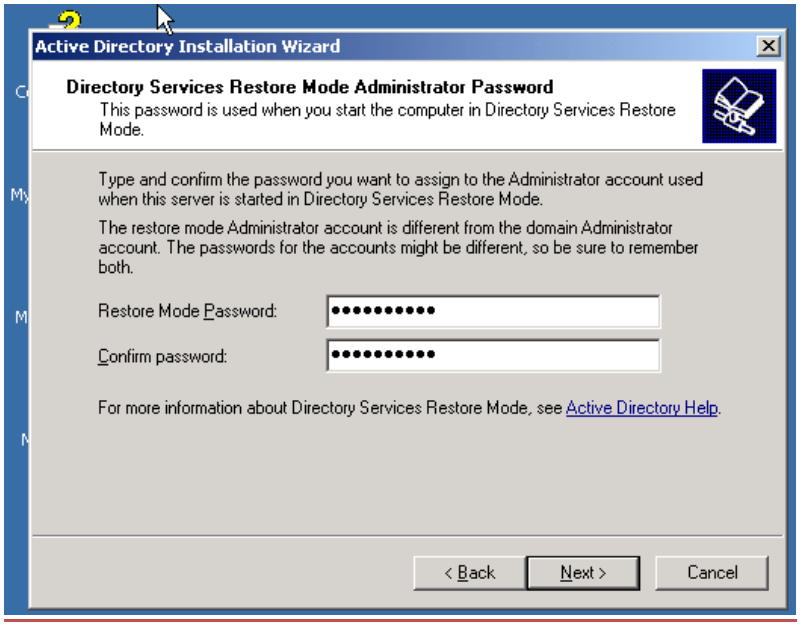


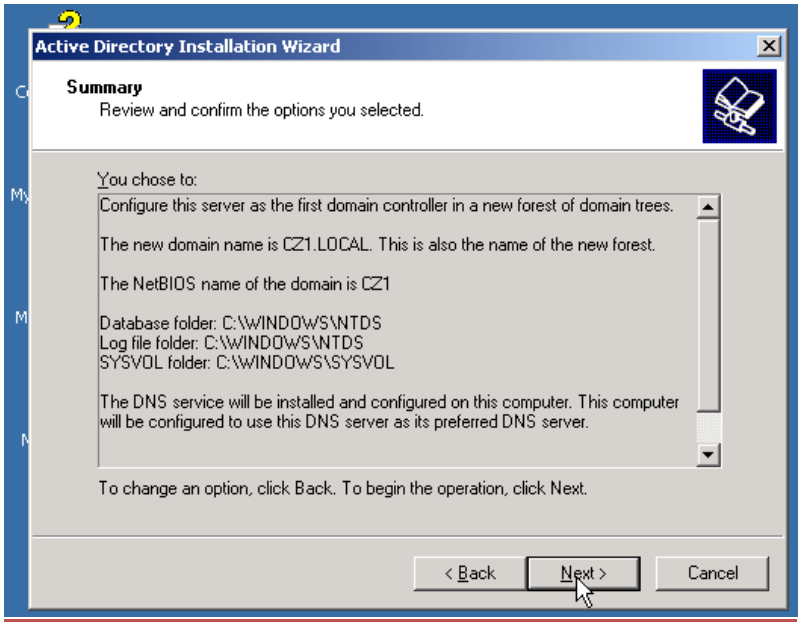
Automatická instalace DNS

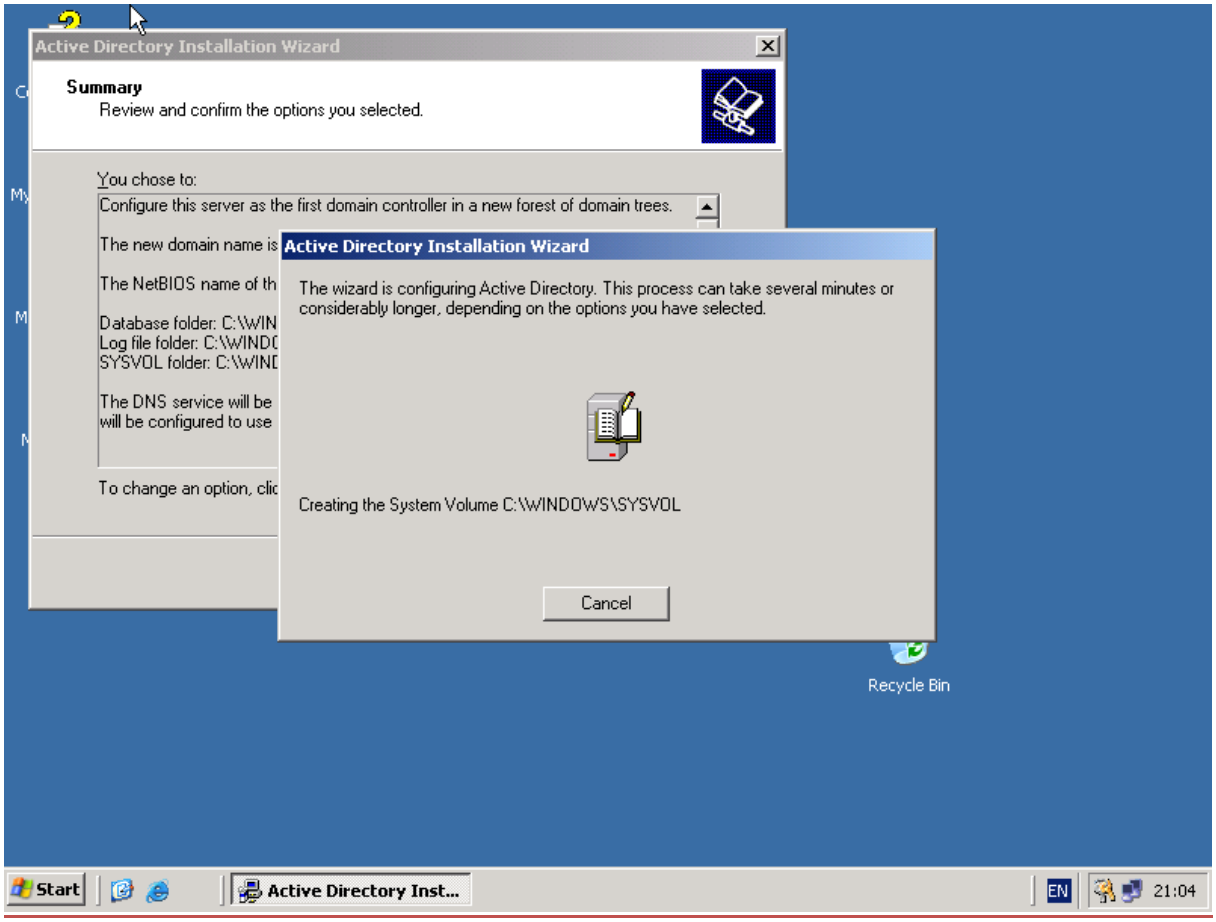




AD restore password







- Active Directory je implementací adresářové struktury Lightweight Directory Access Protocol (LDAP) v prostředí MS Windows
- jádrem Active Directory je replikovaná databáze obsahující objekty, které reprezentují zdroje definované aplikacemi v síti Windows
    - soubor *ntds.dit*
- Active Directory podporuje následující API:
    - LDAP C API
    - Active Directory Service Interfaces (ADSI) COM interface
    - Messaging API (MAPI)
    - Security Account Manager (SAM) APIs
        - MSVI_0 – legacy LanManager auth.
        - Kerberos aut.
    - Windows NT 4 networking APIs (Net APIs)
- umožňuje administrátorům nastavovat politiku, instalovat programy na skupinu počítačů nebo aplikovat kritické aktualizace v celé organizační struktuře
- své informace a nastavení ukládá v centrální organizované dazabázi
- vyžaduje instalaci služby DNS
- je založena na standartních internetových protokolech
- jednoznačně definuje strukturu sítě
- organizuje skupiny počítačů a domén
- organizační jednotky
    - nejnižší forma seskupování objektů v Active Directory
    - máme doménu firma.cz a OU následně můžeme vytvořit na základě jednotlivých oddělení této firmy; a tato oddělení pak dále členit na podřízená OU

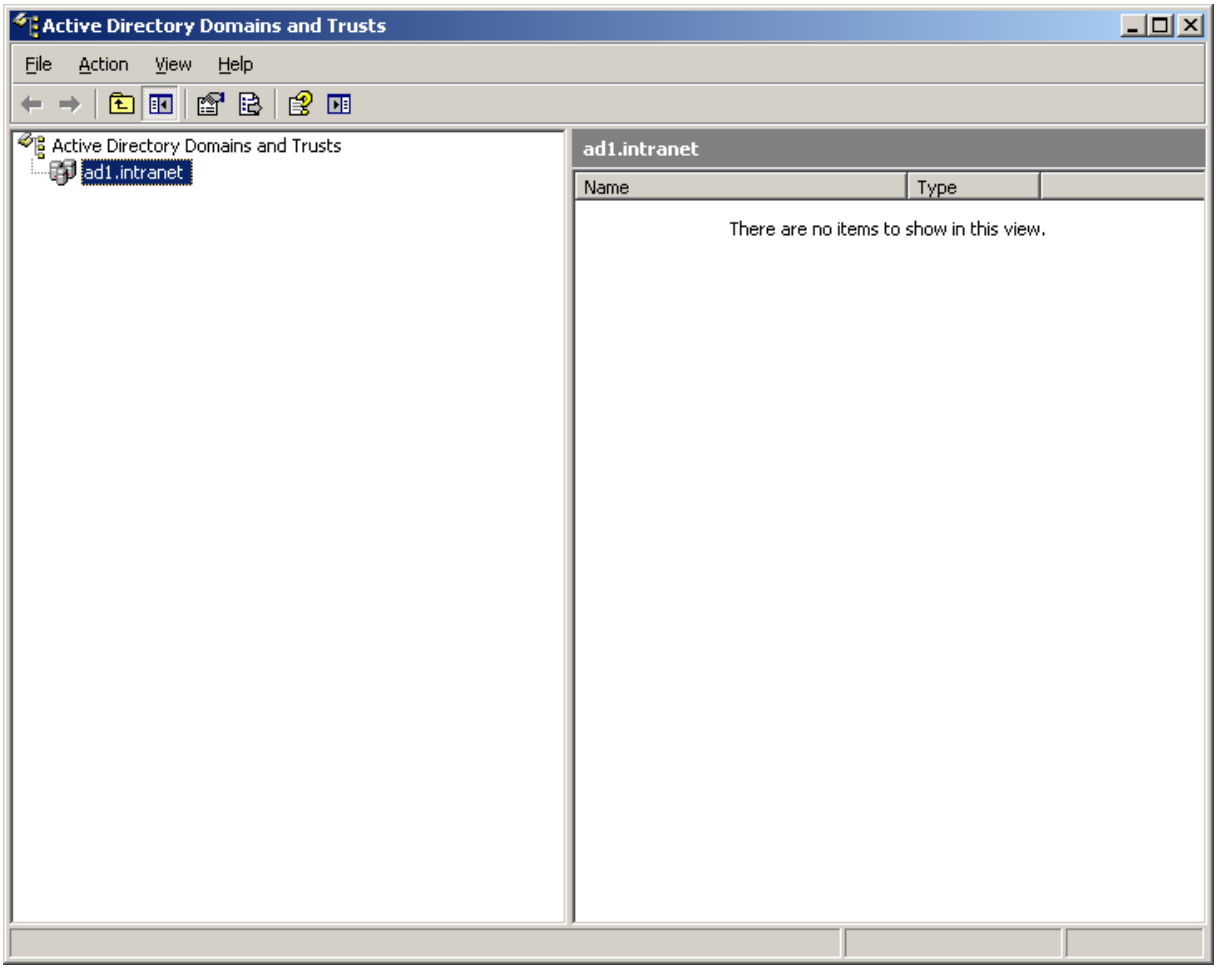
- skupinová politika může být uplatňována na úrovni organizační jednotky
- může být vnořená až do hloubky 12 úrovní
- OU jsou definovány uvnitř domén
- Vlastnosti OU se dědí pouze v rámci domény (nikoliv mezi doménami)

»FSMO

- Flexible Single Master Operations Roles
- specializované doménové řadiče

»AD Domains and Trusts

- nastavení vztahů důvěryhodnosti (trusts) mezi doménami
  - umožňuje uživatelům jedné domény přistupovat k prostředkům jiné domény
  - v rámci *forest* jsou vytvořeny automaticky
  - ruční vytvoření je potřeba pro:
    - Trust mezi Win 2000 a NT4 doménami
    - Trust mezi doménami v rámci různých forests
  - Domain Naming FSMO
  - netdom.exe

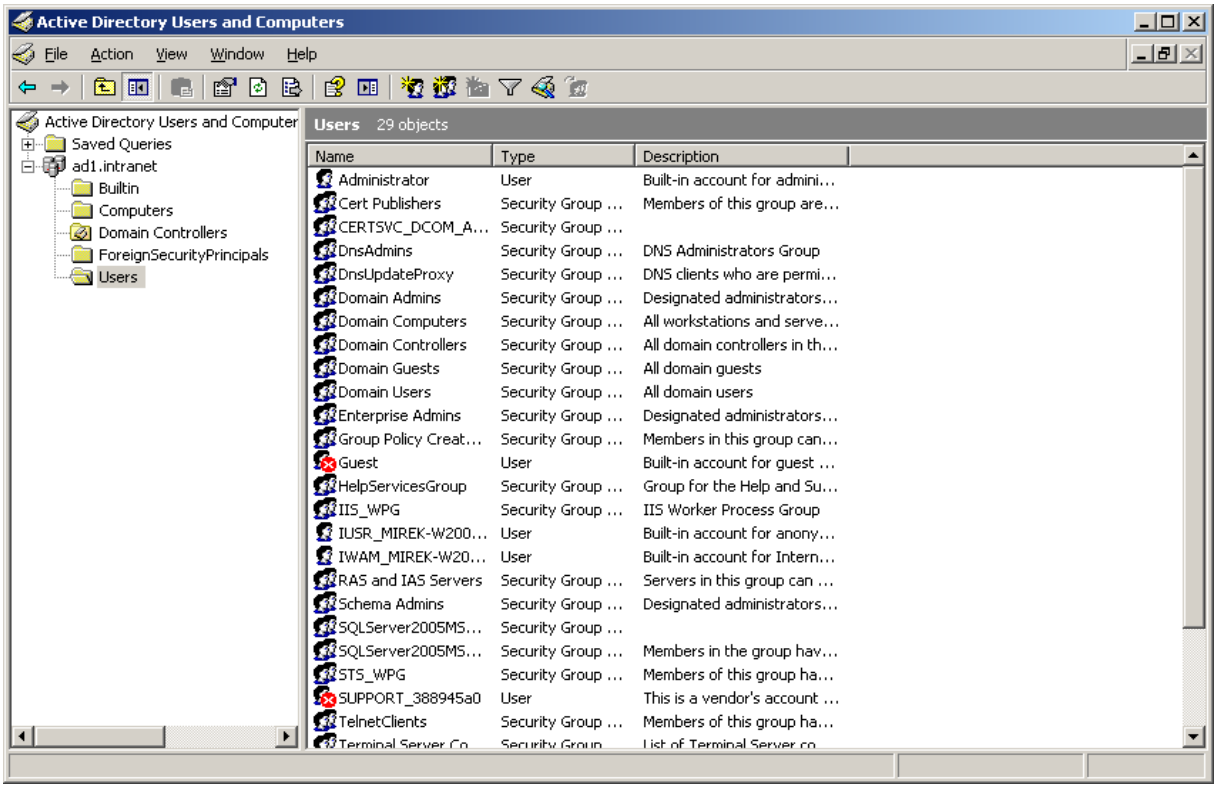


»AD Sites and Services

- nastavení replikace v rámci LAN a mezi LAN a WAN
- specifikace Group Policies

»AD Users and Computers

- základní nástroj pro běžnou správu uživatelů, skupin, počítačů, tiskáren v AD (organizačních jednotek)
- hierarchická struktura
- FSMO role domény



»Správa AD

- správa uživatelů a skupin
  - přístupová práva a další omezení
  - logon scripty
  - roaming profiles
  - home directory
- správa počítačů
- sdílení a publikování prostředků v AD (sdílené složky a tiskárny)
- Group Policies

GROUP POLICIES

Politiky = nástroje pro centralizovanou správu – vynucení nastavení OS Windows.

- první náznak ve Win 3.11
- Windows NT doména
  - skupinové politiky vytvářené pomocí *.adm* a *poledit.exe*
  - ukládané v netlogon
  - Windows NT – *ntconfig.pol*
  - Windows 9x – *config.pol*
- Windows 2000 AD
  - integrace s AD

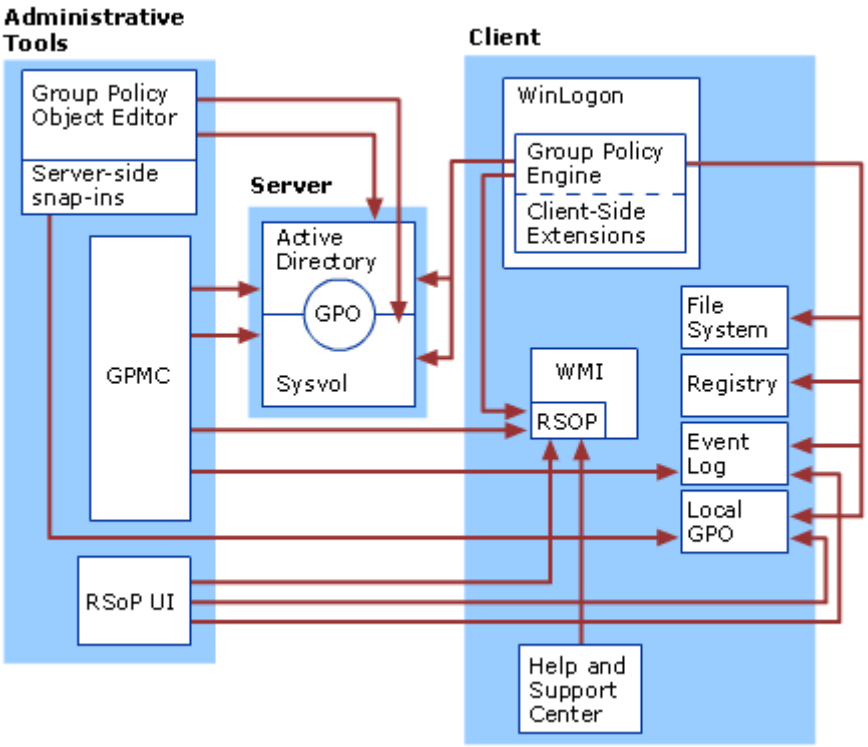
- aplikace na OU (hierarchie politik)
- RSOP
- WMI filtry

- lokální politiky (možnost použití bez AD)

»Konfigurovatelná nastavení

- registry
  - nastavení registru dle administrativních šablon GPO Editoru
- security
  - definice nastavení zabezpečení pro local computer, doménu, síť, ...
- instalace software
  - deployment aplikací jako assigned (instalace vynucená administrátorem) nebo published (aplikace je poskytnuta administrátorem, uživatelé mohou zvolit instalaci)
  - možnost aktualizace, odinstalace
- scripty
  - specifikace scriptů spouštěných po zapnutí / před vypnutím počítače a při přihlášení / odhlášení uživatele
- nastavení IE
  - správa a customizace Microsoft Internet Exploreru na OS Microsoft Windows 2000 a novějších
- folder redirection
  - přesměrování speciálních složek na síť

»Architektura Group Policy



Computer policies = nastavení POČÍTAČE případně všech uživatelů PC; aplikuje se po startu.
User policies = nastavení UŽIVATELE; aplikuje se po přihlášení.

»Instalace SW

- automatická instalace SW ve formátu msi
- computer
  - assigned
    - automatická instalace po zapnutí PC
- user
  - assigned
  - published
    - instalace „na vyžádání“ – program je dostupný k uživatelské instalaci v Control Panel/Add or Remove

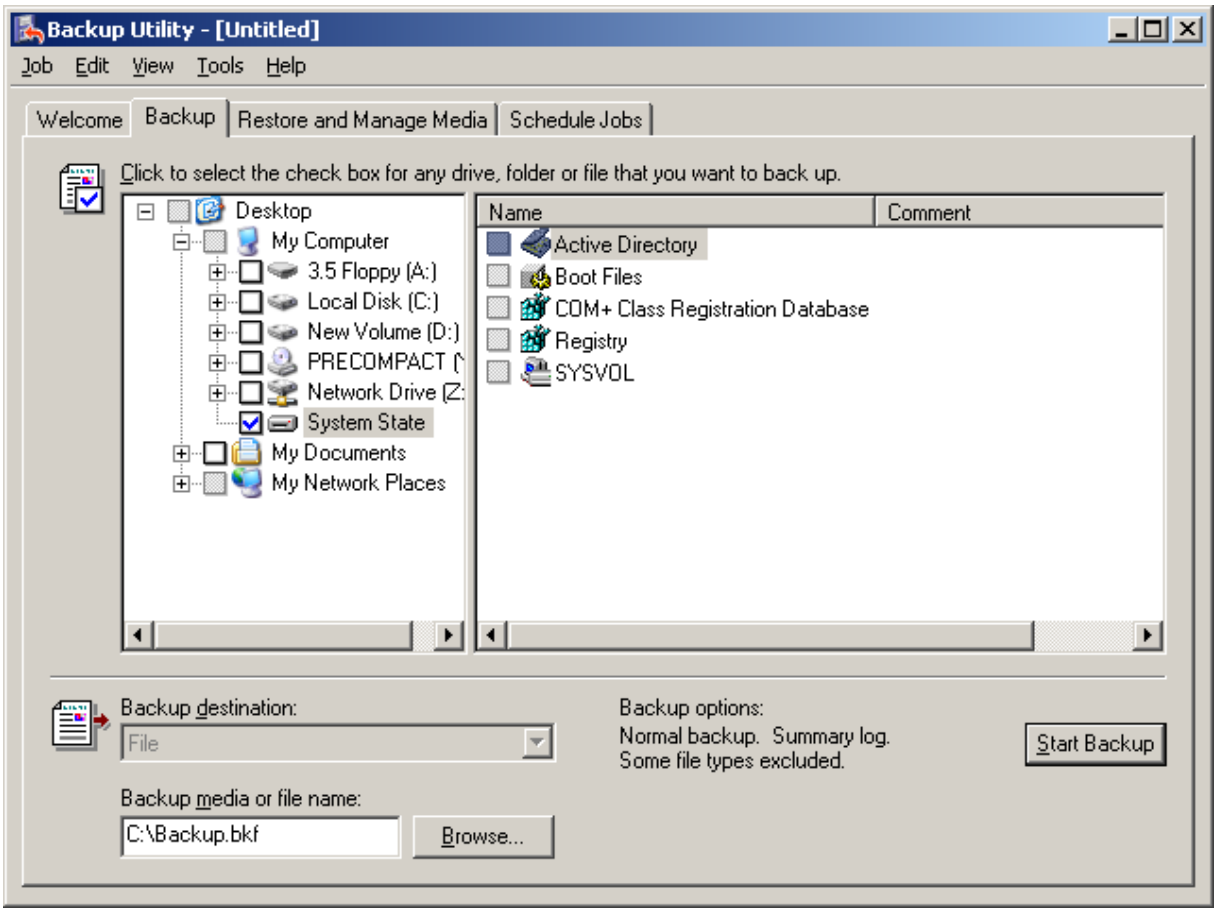
»Ladění

- gpupdate.exe
  - umožňuje ruční refresh GP
- gpresult.exe
  - zobrazí Resultant Set of Policy (RsoP) pro user nebo computer
- GPMC
  - Simulace
- utility:
- regtoADM
- ADM toExcel
- notepad

ŘEŠENÍ KRIZOVÝCH SITUACÍ A SPRÁVA OS

- ntbackup.exe
  - Windows Backup nástroj
  - záloha:
    - filesystému
    - system state
      - nastavení (registry, boot files, com+ database)
      - AD
- safe mode
  - když už nevíme kudy kam a Windows se odmítá spustit korektně, zkusíme přes safe mode (mouzový režim)
- Restore AD
  - Directory Services Restore Mode
    - Primary
      - pád celé domény – není žádný aktivní AD
    - Authoritative
      - po smazání objektů a jeho zreplikování
      - ntdsutil (authoritative restore; restore database/subtree <name>)
    - Normal
- command console
- Windows PE, MS DART
- opravná instalace
- využití virtualizace (snadné přenesední virtuálního stroje)
- Windows Resource Kit

- obsahuje nástroje na řešení nestandartních situací i běžných problémů, nástroje na konfiguraci sítě a bezpečnostních prvků, také nástroje pro Active Directory



»Základní nástroje Windows

- mmc console
  - konzole na správu
  - přidávají se do ní snap-iny
  - vyžaduje Administrative Tools
- WMI nástroje
  - skripty, WMIC
- Event log
- PerfMon
- Debug tools
- Support tools
- Resource Kit
- SFC
  - System File Checker
  - scanuje všechny zabezpečené systémové soubory, mění, nahrazuje, opravuje

»DLL problémy

- cílem je určit, které knihovny jsou chybné, mají nekorektní verzi nebo jsou špatně zaregistrované
- Dependency Walker
- COMExp

- ProcMon\FileMon + nastavení filtrů
- RegShot\InstallRite
- for /f nebo mass copy v případě, že se jedná o širší problém

»Filesystem

- FileMon\Process Monitor
- InstallRite
- Handle\WhoLocksMe
- Streams

»Security

- standart user analyzer
- FileMon\RegMon\ProcMon
- Regular *NIX tools – NetCat or Nmap

»Group Policy

- Event log
- Group Policy logging
- RSOP
  - zjišťuje která nastavení GP jsou platná pro daného uživatele/počítač
- WinPolicies

»Fix implementations

- Application Compatibility Toolkit (5.0)
  - univerzální nástroj od Microsoftu
  - cílem je nejen řešit kompatibilitu ale také poskytnout lepší kontrolu nad systémem
  - nevýhodou je, že většina funkcionality není dobře zdokumentovaná
- GPO

WINDOWS V HETEROGENNÍM PROSTŘEDÍ

- běžné nástroje pro vzdálenou administraci
  - využití běžných nástrojů pro vzdálené ovládání a přenos souborů
    - znakové
      - telnet
      - ssh
    - grafické
      - vnc
      - rdesktop
      - X-window system
    - přenos souborů
      - ftp –s:FileName
      - wget
  - exporty, importy, přenosy textových souborů s dávkovým zpracováním pomocí *cron/Scheduled tasks*
- integrační nástroje
- Services for Unix
  - SFU 3.5
    - finální verze SFU, ke stažení zdarma

        - určena pro Windows 2000, Windows XP Professional a Windows Server 2003 na platformě x86 platforms
        - obsahuje Interix subsystem verze 8.0 (release 3.5) s vícejazykovou podporou a POSIX threadingem
        - podporované verze Unixu: Solaris 7 a 8, Red Hat Linux 8.0, AIX 5L 5.2 a HP-UX 11i
    - SFU přímo obsaženo v:
        - Windows Server 2003 R2
        - Windows Vista Enterprise a Ultimate
- integrace Windows / domény / AD s nejběžnějšími Unix službami
    - Samba
    - Squid

Okruhy témat ke zkoušce:

1. Edice MS Windows - srovnání funkčnosti / omezení , vhodnost nasazení (domácnost, firma a pod.)
2. Scriptování v cmd (přesměrování, roury, proměnné, errorlevel, for, větvení scriptu)
3. Procesy, práce s procesy, nástroje
4. Registry - vlastnosti, práce s registry (zálohování, oprava, scriptování)
5. Nástroje pro správu (MMC, přehled, příklady)
6. Bezpečnost - obecné principy, lokální vs,. síťová, nástroje
7. Filesystémy - typy, vlastnosti, srovnání (Windows x *NIX)
8. Protokol TCP/IP v MS Windows - implementace služeb (DNS, DHCP, NAT….), konfigurace, příkazy pro nastavení / ladění
9. Windows Networking - server, redirector, CIFS/SMB
10. Active Directory - na čem je založeno, co poskytuje, správa (příklady činností při odchodu zaměstnance a jeho náhradě novým a pod.)
11. Group policy - příklady nasazení (instalace SW, restrikce), ladění
12. Zálohování, řešení krizových situací (co, proč, jak je vhodné zálohovat; příklady nestandardního chování počítače/OS a vhodné nástroje na diagnostiku / řešení)
13. Windows v heterogenním prostředí - jak přenášet soubory, sdílet tiskárny, vzdáleně spravovat a pod.