MS WINDOWS III

Přihlašování

Registr

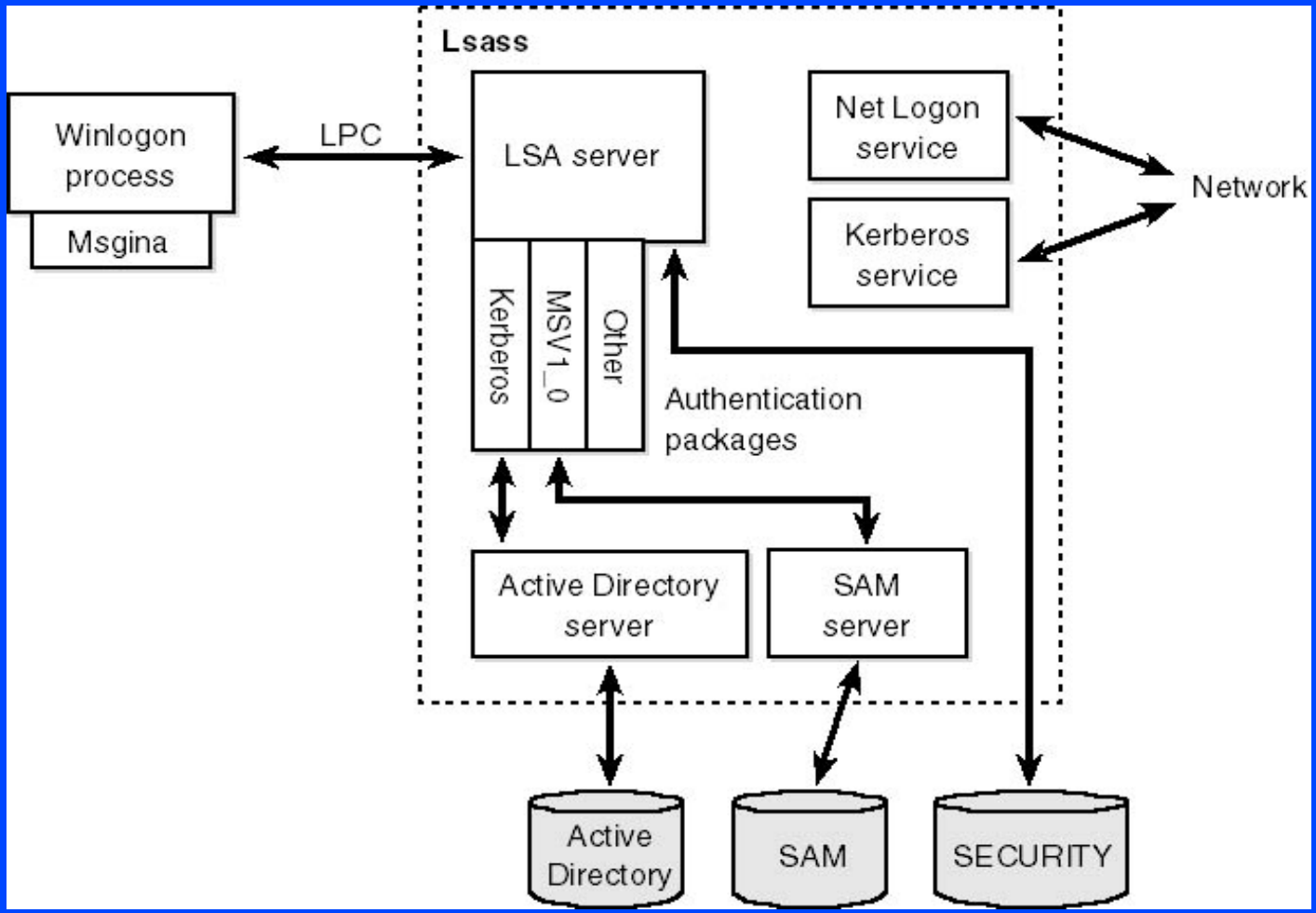
Služby

Správa disků

Souborový systém

PŘIHLAŠOVÁNÍ I

Winlogon, Lsass, autentizační balíčky, DB



PŘIHLAŠOVÁNÍ II

Winlogon
- zabezpečené interakce s uživatelem
- vytvoření viditelné Windows Station (WinSta0) přístupné pouze SIDu tohoto procesu
- vytvoření Desktopů (aplikační, winlogon, scrsvr)

GINA
- získání přihlašovacích údajů
- MSGina x alternativní dll (biometrika, karty...)

Autentizační balíčky
- vyjmenovány v registru HKLM\System\CurrentControlSet\Lsa

PŘIHLAŠOVÁNÍ III

Doména
- soubor prostředků přístupných uživatelům
- centrální adres. služba (Active Direcory) na DC
- autentizační balíček Kerberos

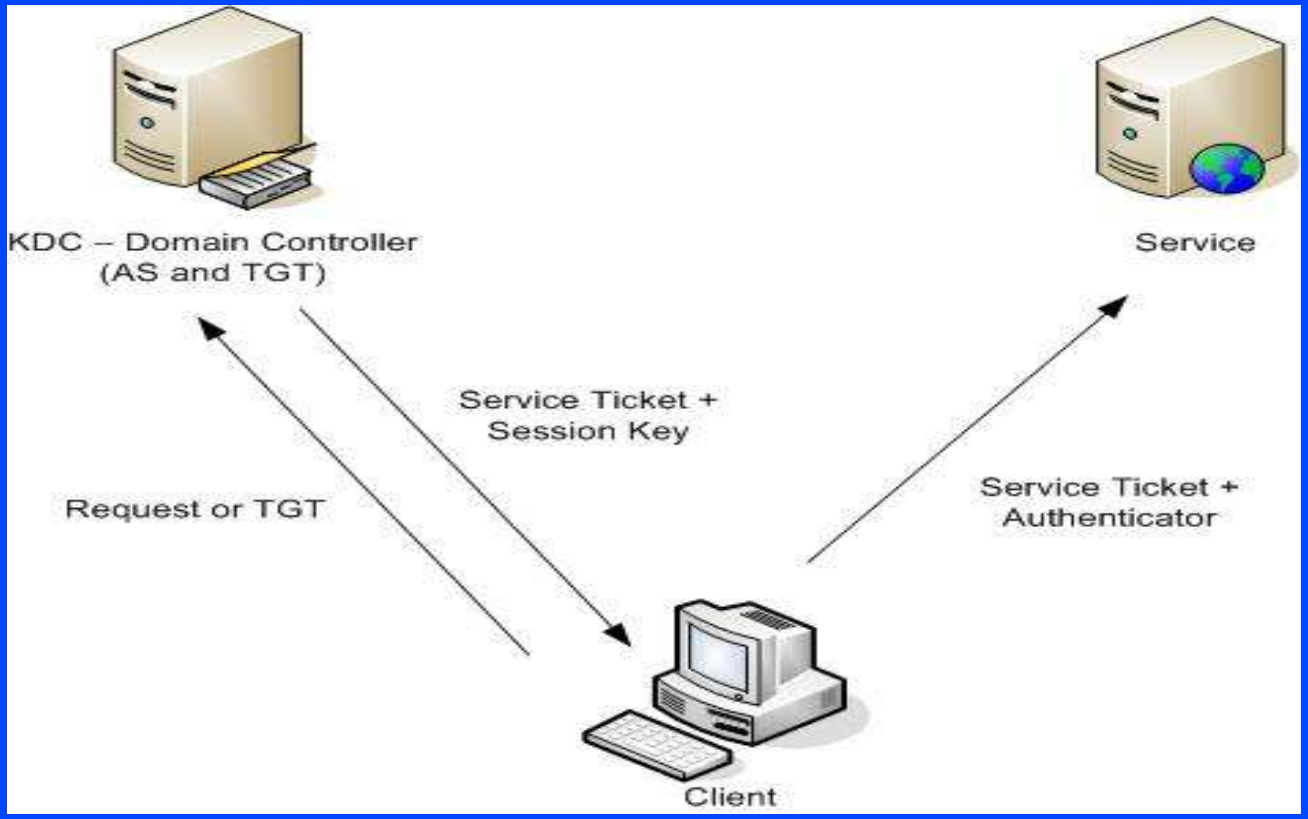
Lokální přihlášení nebo doménové bez DC
- autentizační balíček MSV1_0
- ověření v lokální SAM DB

Přihlášení do Pre-2000 domény
- lokální služba Net Logon komunikuje se vzdálenou Net Logon, vzdálené ověření MSV1_0

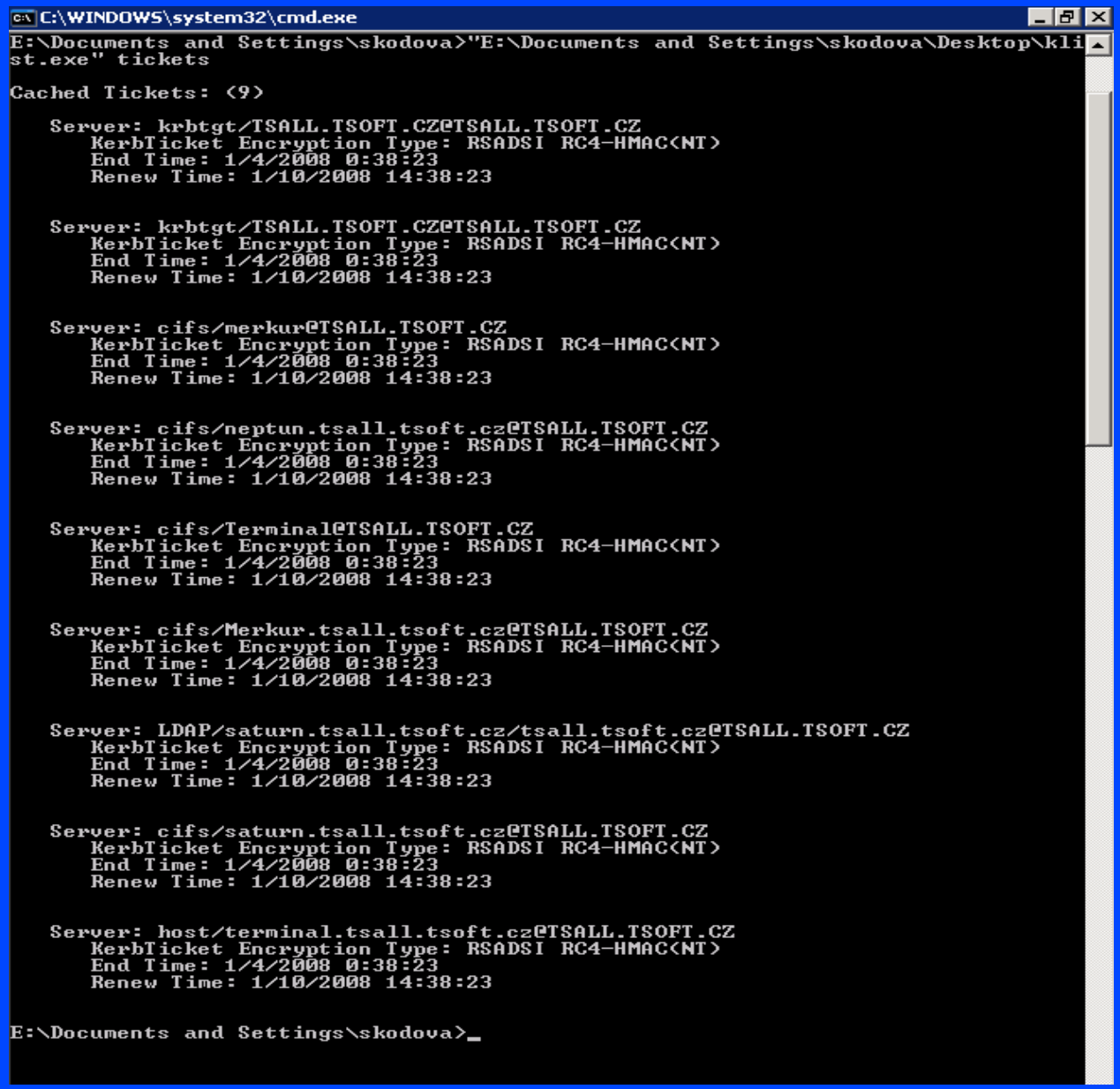
PŘIHLAŠOVÁNÍ IV

Kerberos

- verze 5, RFC 1510
- lokální balíček komunikuje s Kerberos na DC
- nástroj klist



PŘIHLAŠOVÁNÍ V



PŘIHLAŠOVÁNÍ VI

Dokončení přihlášení

- úspěšná autentizace
- získání privilegií a příslušnosti ke skupinám
- ověření lokál. privilegií (interactive přihlášení...)
- připojení dalších SID (everyone, interactive...)
- vytvoření access tokenu
- předání handle Winlogonu
- Userinit.exe
- Explorer.exe

REGISTR I

- konfigurace a řízení OS
- systémová a uživatelská nastavení
- statická i dynamická data
- jednotné rozhraní (GUI, programové)
- struktura a notace podobná logickým diskům
- klíče, podklíče, hodnoty, data
- kořenové klíče
- výchozí hodnoty
- 11 typů hodnot (reg_dword, reg_binary, reg_sz, reg_link...)

REGISTR II

- zabezpečení pomocí security descriptorů
- sada souborů s příponou .dat (hive)
- některé hive nestálé (pouze v paměti)
- spravovány Konfiguračním správcem
- možnost ručního připojování
- možnost síťového přístupu
- vnitřní reprezentace pomocí bloků a buněk
- nástroj regedit – vždy zálohovat (export)
- jiné nástroje pro kontrolovanou úpravu obsahu
- nástroj regmon – monitoring přístupu

REGISTR III

Soubory registru

HKEY_LOCAL_MACHINE\SYSTEM	\Windows\System32\Config\System
HKEY_LOCAL_MACHINE\SAM	\Windows\System32\Config\Sam
HKEY_LOCAL_MACHINE\SECURITY	\Windows\System32\Config\Security
HKEY_LOCAL_MACHINE\SOFTWARE	\Windows\System32\Config\Software
HKEY_LOCAL_MACHINE\HARDWARE	Volatile hive
HKEY_LOCAL_MACHINE\SYSTEM\Clone	Volatile hive
HKEY_USERS\<security ID of username>	\Documents andSettings\<username>\Ntuser.dat
HKEY_USERS\<security ID of username>_Classes	\Documents and Settings\<username>\Local Settings \Application Data\Microsoft\Windows\Usrclass.dat
HKEY_USERS\.DEFAULT	\Winnt\System32\Config\Default

REGISTR IV

Kořenové klíče – H=handle, K=Key

HKCU (Current User) – podklíč HKU
- AppEvents (zvuky a události)
- Console (příkazový řádek)
- Control Panel (myš, klávesnice, regionál. nast...)
- Environment (proměnné)
- Printers, SW...

HKU (Users)
- právě užívané profily

HKCR (Classes Root) – podklíč HKLM a HKCU
- registrované přípony
- COM objekty

REGISTR V

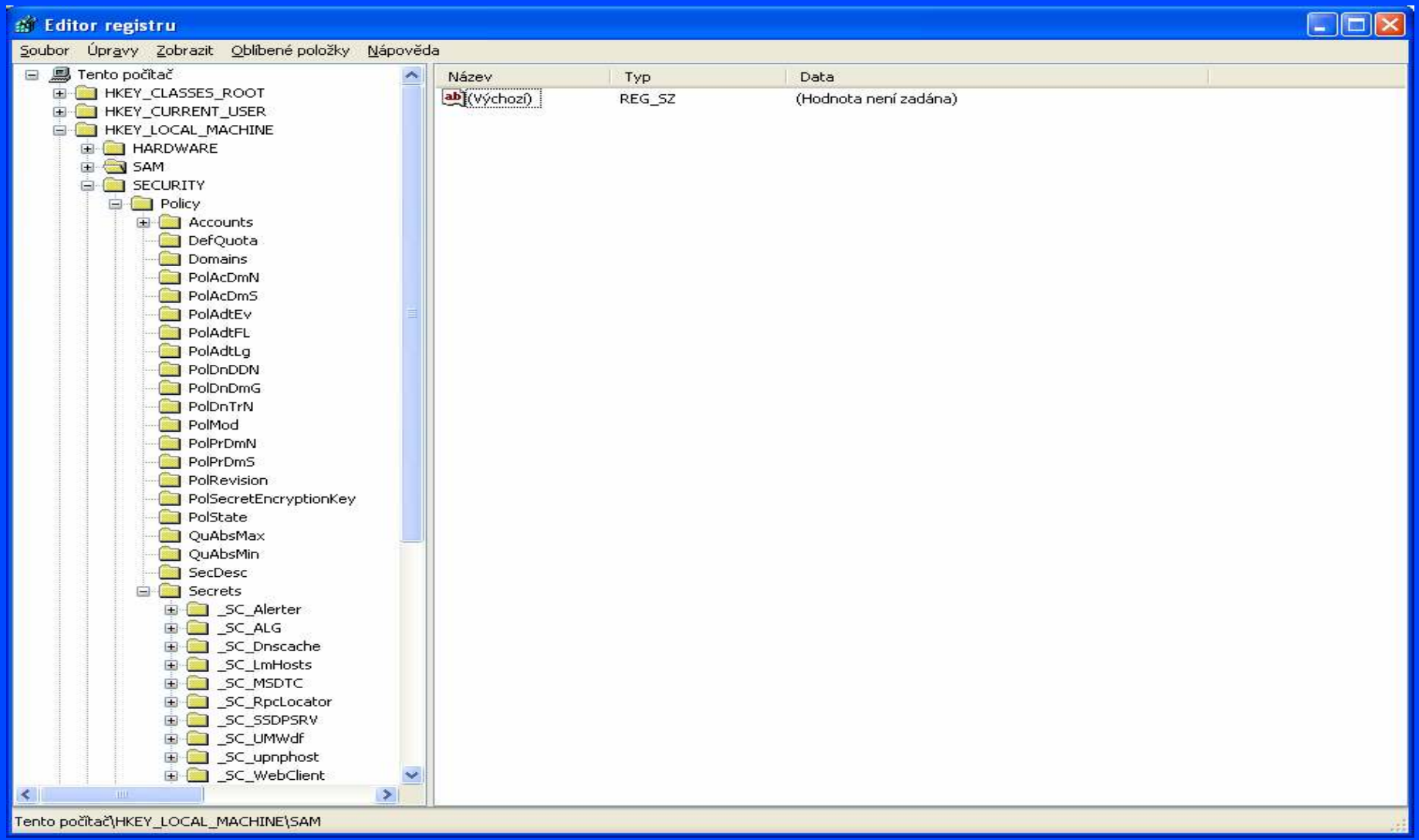
HKLM (Local Machine)
- Hardware (konfigurace a ovladače)
- SAM (bezpeč. DB, podklíč Security, šifrováno)
- Security (bezpečnostní nastavení, šifrováno)
- Software (konfigurace SW vč. Windows)
- System (konfigurace, služby...)

HKCC (Current Config) – podklíč HKLM
- aktuální hardwarový profil

HKPD (Performance Data)
- výkonnostní čítače aplikací a systému
- přístupný pouze programově

REGISTR VI

regedit spuštěný pod účtem Local System (at)



SLUŽBY I

- spouštění procesů nespojených s int. uživatelem
- často serverová část aplikace
- jako daemon v Unixu

Správce služeb (Service Control Manager, SCM)
- services.exe
- registrace služeb
- komunikace se službami (řízení, hlášení stavu)
- informace o mapování síťových disků

Řídící program (Service Control Program, SCP)
- obsluha služeb (start, stop, přerušit...)
- výchozí nebo vlastní

SLUŽBY II

Služba
- min. jeden spustitelný program
- kód pro komunikaci se SCM
- registrace v SCM pomocí CreateService
- zápis parametrů každé služby do registru

Parametry služeb
- vlastní nebo společný proces
- zobrazované jméno, popis
- cesta k programu
- typ spouštění
- spouštěcí účet
- chybový kód, závislosti...

SLUŽBY III

Hostování
- v SCM – běžné vestavěné služby
- v Lsass – bezpečnostní služby
- v Svchost – generický proces pro služby
- v SrvAny – jakýkoliv program
- tasklist /svc

Spouštěcí účty
- výchozí Local system (velká privilegia)
- lze nastavit na běžný uživatelský účet

Interaktivita
- ve výchozím stavu není
- lze nastavit (asociace s WinSta0) i zakázat

SPRÁVA DISKŮ I

Disk
- fyzické zařízení

Sektor
- adresovatelný blok disku, pevná velikost

Oddíl (partition)
- souvislá oblast sektorů, tabulka oddílů

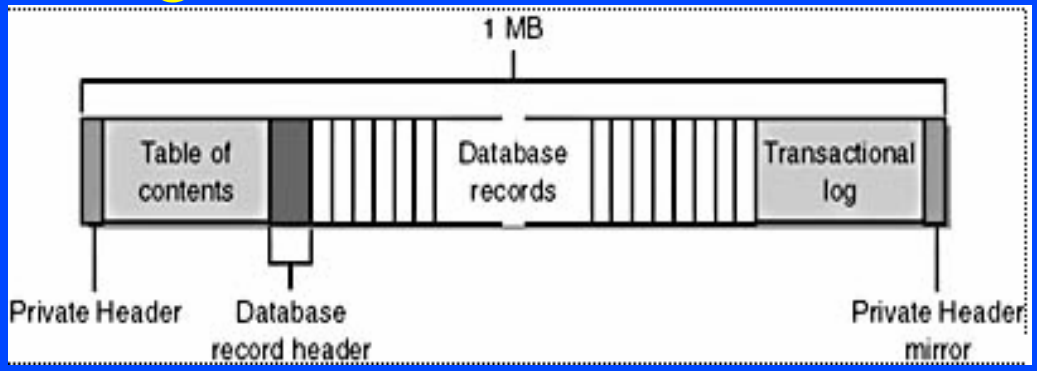
Základní disk (basic)
- běžné dělení na oddíly, rozšířené oddíly

Dynamický disk (dynamic)
- správce logických disků (LDM od VERITAS)
- databáze LDM na posledním MB disku
- možnost vytváření svazků (volume)

SPRÁVA DISKŮ II

LDM DB

- soukromá hlavička (GUID...)
- tabulka obsahu (16 sektorů)
- hlavička DB (počet záznamů...)
- DB (128B-ové záznamy, až cca 8000 záznamů)
- transakční log



SPRÁVA DISKŮ III

Typy záznamů
- oddíl (příslušnost ke komponentě a disku)
- komponenta (příslušnost ke svazku)
- svazek (GUID, velikost, stav, písmeno)
- disk (GUID)

Jednoduchý svazek
- sektory jednoho oddílu spravované jako samostatná jednotka

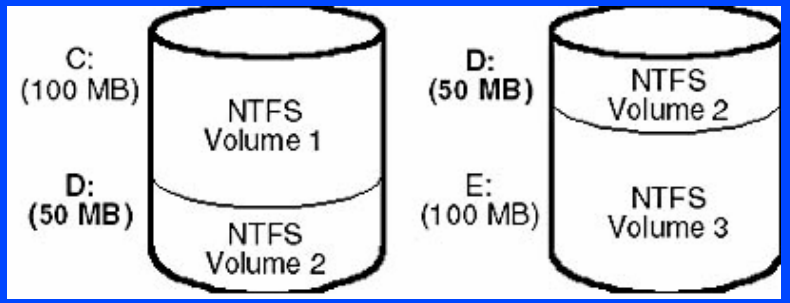
Rozložený svazek
- sektory několika oddílů spravované jako samostatná jednotka

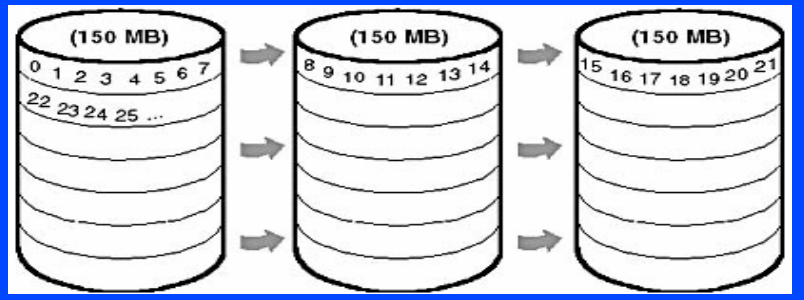
Správa
- Správce disků

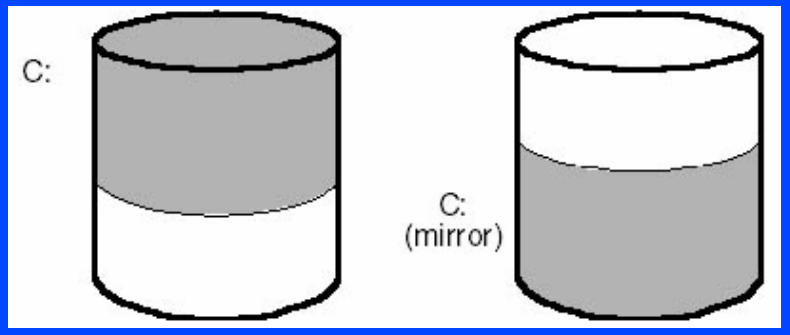
SPRÁVA DISKŮ IV

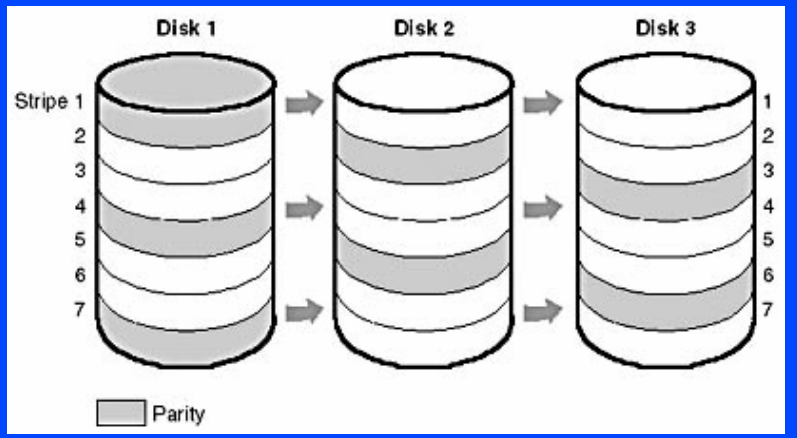
Využití

- rozložený (spanned) svazek - RAID0
- prokládaný (striped) svazek - RAID0
- zrcadlený (mirrored) svazek - RAID1
- prokládaný s paritou svazek - RAID5







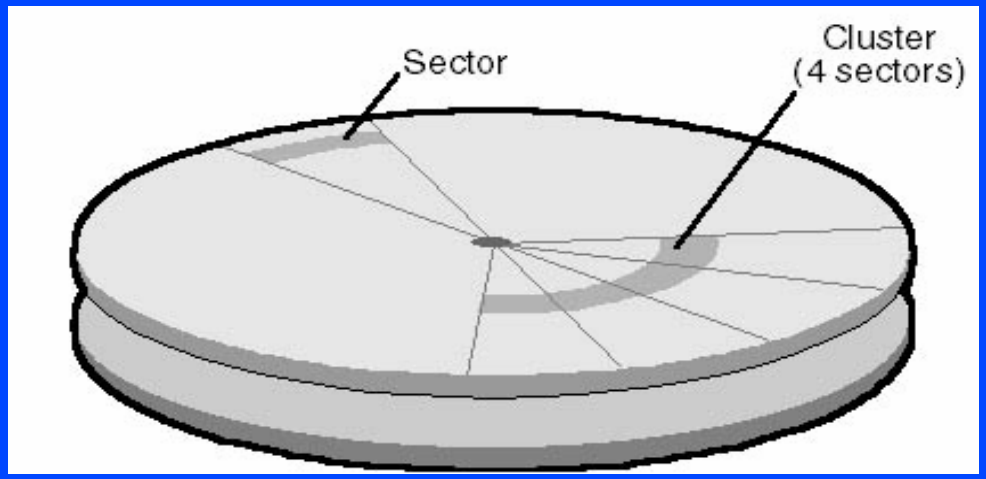


SOUBOROVÝ SYSTÉM I

Souborový systém
- způsob uložení dat v úložišti

Metadata
- data ke správě souborového systému

Cluster
- adresovatelný blok, násobek velikosti sektoru



SOUBOROVÝ SYSTÉM II

Compact Disc File System (CDFS)
- starší, jednoduchý systém pro CD-ROM
- jména kratší než 32 znaků
- max. 8 úrovní vnoření

Universal Disc Format (UDF)
- novější systém pro optické disky
- jména kratší než 255 znaků
- cesta kratší než 1023 znaků

SOUBOROVÝ SYSTÉM III

File Allocation Table (FATxx)

- starší systémy
- xx určuje počet bitů identifikujících cluster

FAT12

- velikost clusteru až 8KB
- velikost svazku až 8KB * 2^12 = 32MB
- disketa

FAT16

- velikost clusteru podle velikosti svazku(až 64KB)
- velikost svazku až 64KB * 2^16 = 4GB

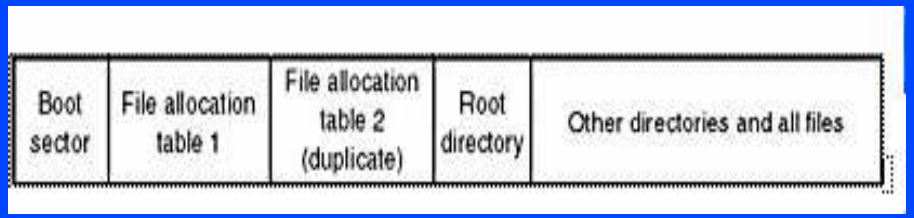
FAT32 (horní 4b rezervovány)

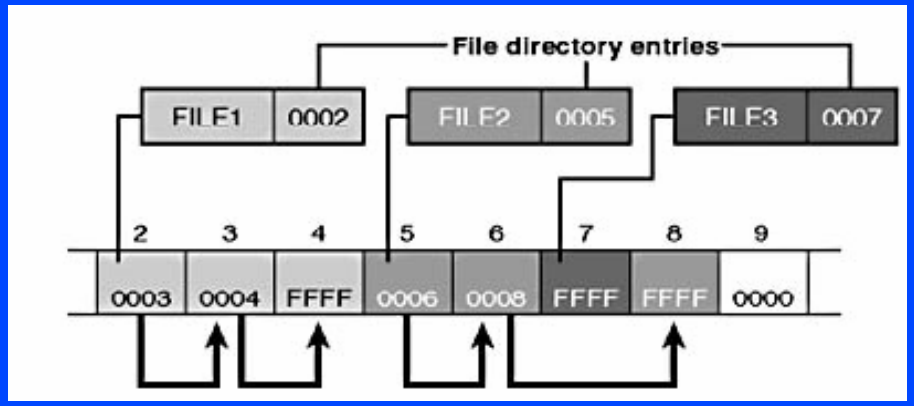
- velikost clusteru podle velikosti svazku(až 32KB)
- vel. svazku až 32KB * 2^28 = 8TB (resp. 32GB)

SOUBOROVÝ SYSTÉM IV

Tabulka FAT

- kriticky důležitá, dvě kopie na začátku svazku
- záznam pro každý cluster svazku
- alokační řetězce souborů a adresářů





SOUBOROVÝ SYSTÉM V

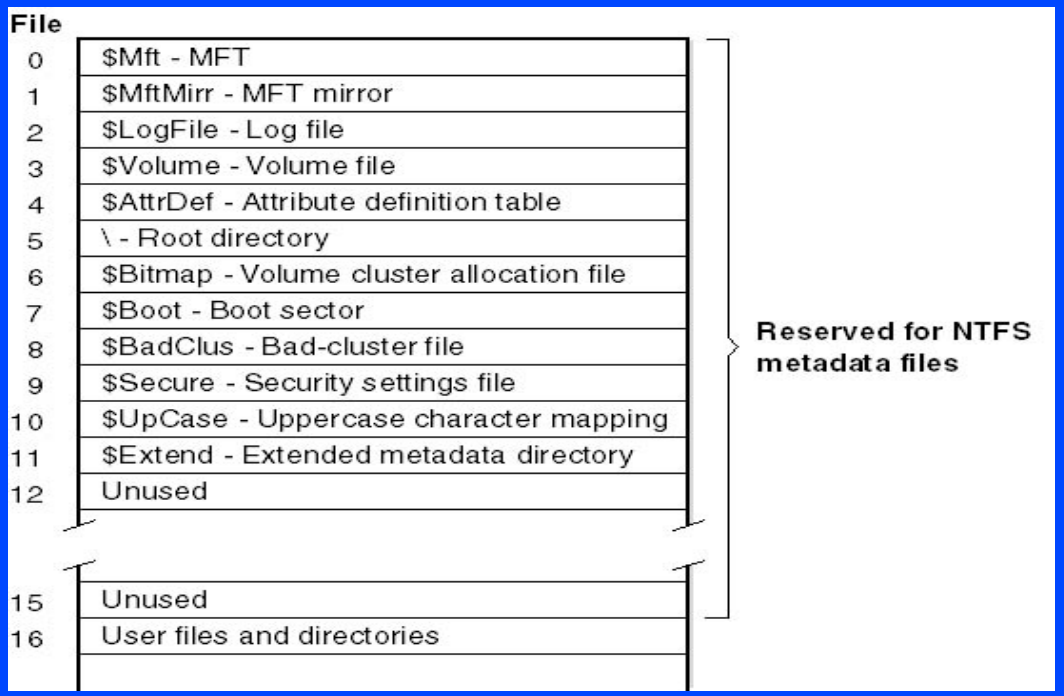
New Technology File System (NTFS)

- nejnovější souborový systém
- 64b identifikace clusteru
- velikost clusteru podle velikosti svazku (až 4KB)
- vel. svazku až 4KB * 2^64 = 16EB (resp. 128TB)
- jméno až 255 Unicode znaků
- cesta až 32767 Unicode znaků
- veškerá data vč. metadat v souborech
- rozšířené vlastnosti
- převod z FAT pomocí convert.exe
- převod do FAT nejde

SOUBOROVÝ SYSTÉM VI

Master File Table (MFT)

- pole 1KB-ových souborových záznamů
- vč. metadat
- souborový záznam – dvojice atribut/hodnota
- rezidentní x nerezidentní atributy



SOUBOROVÝ SYSTÉM VII

Rozšířené vlastnosti

Bezpečnost
- kontrola přístupů jako u objektů
- záložka Zabezpečení ve Vlastnostech souboru

Diskové kvóty
- ve výchozím stavu vypnuty
- na celý svazek

Komprese
- pro aplikace transparentní
- nastavení příznakem
- komprimovaný adresář = komprimovaný obsah

SOUBOROVÝ SYSTÉM VIII

Šifrování (Encrypted File System, EFS)
- transparentní pro aplikace
- ochrana při zcizení disku
- nelze na systémovém disku

Obnovitelnost
- atomické transakce
- záznam změn na metadatech

Defragmentace
- dfrg.msc
- defrag.exe