tiskárny + spooler
sharing
DFS
NTFS práva + práva obecně
kvóty

Radim Němec
Microsoft Certified Professional Systems Engineer

http://www.cs.vsb.cz/navrat

Realizace sdílení prostředků

- Architektura Client-Server
  - Lan Manager
    - služba Server
    - služba Workstation (klient pro přístup k serveru)
  - protokol SMB – Server Message Block
  - nezávislé na transportních protokolech
    - TCP/IP (port 445), NBT (porty 137-139), IPX/SPX
- Bezpečnost
  - autentizace běžnou Windows metodou
    - LanManager (LM), Kerberos
  - přístupová práva nastavena na objektu (permissions)

Uložení informací o shares

- Běžné sdílené adresáře
  - konfigurace Serveru v registrech
    HKLM\System\CurrentControlSet\Services\LanManServer\Parameters
    - podklíč Shares
  - výchozí zabezpečení klíče – modifikace pouze pro Administrators
- Administrativní sdílení
  - ADMIN$, Print$, C$, D$ (přístup jen Administrators)
  - není vidět v průzkumníkovi (ale \\pce322k\d$)
  - důležité i pro některé programy (SMS, instalace, …)
  - lze vypnout v konzoli, ale obnoví se při restartu
  - trvalé vypnutí jen v registrech - AutoShareServer = 0

Bezpečnost sdílení

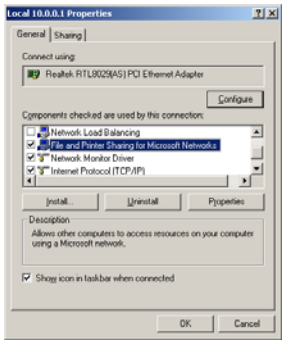
- Kdo může nasdílet složku
  - Administrators, Server Operators a Power Users (ownership nepomůže, ale dá se to změnit)
  - vyžaduje se READ DATA permission na složce
- Anonymous access (NULL Sessions)
  - pokud je povoleno, není nutná autentizace a procesy běžící pod „Local System“ mohou přistupovat k počítači ze sítě
  - velice nebezpečné
  - nastavení v registrech (+ restart Serveru)
    NullSessionShares, NullSessionPipes
    HKLM\System\CurrentControlSet\Control\LSA\RestrictAnonymous

Bezpečnost sdílení

- Bezpečnostní nastavení týkající se sdílení
  - Additional restrictions for anonymous connections
  - LAN Manager authentication level
  - Amount of idle time required before disconnecting session
  - Digital signatures
    - mutual authentication
    - message consistency
  - Send unencrypted password to connect to third-party SMB servers

Vypnutí sdílení

- Služba Server
  - vypnutí služby
  - NET STOP Server
- Odinstalace / vypnutí
  - Control Panel Network Connections
  - File and Printer Sharing for Microsoft Networks
- TCP port filter
  - 445, 137-139
  - nevhodné, vypíná celý NetBIOS



Vypnutí sdílení

- Nevýhody vypnutí služby Server
  - vypne také službu NetLogon
    - nepojede přihlášení ze sítě
  - vzdálené administrativní úkoly nebudou možné

Příkaz NET

- Management z příkazové řádky
  - NET STOP, START, PAUSE, CONTINUE
  - NET STATISTICS SERVER
  - NET STATISTICS WORKSTATION
  - NET USE M: “\\lektor\data 2” heslo /user:”dom\user”
  - NET USE M: /D
  - NET SHARE
  - NET VIEW \\lektor
  - NET CONFIG SERVER, WORKSTATION
  - NET SESSION \\computer /delete
  - NET FILE fileID /close

Příkaz NET

- Sdílení adresáře
  - NET SHARE sharename=d:\data
    /DELETE
    /USERS:number
    /UNLIMITED
    /REMARK:"notice"

Příkaz NET

- Konfigurace služby Server
  - NET CONFIG SERVER
    /autodisconect:minutes (-1, …)
    /srvcomment:"komentář"
    /hidden:yes|no
- Konfigurace služby Workstation
  - NET CONFIG WORKSTATION
    /charcount:bytes
    /chartime:msec

Přístup ke sdíleným prostředkům

- \\pce322k\data
  - NetBIOS jméno počítače
  - NetBIOS over TCP/IP = NetBT
  - port 139 = netbios-ssn (NetBIOS Session Service)
  - pokud je NetBIOS zakázán nebo je "objeveno" DNS jméno, použije se TCP/IP
- \\10.0.0.1\data
  - IP adresa počítače
  - TCP/IP port 445 = microsoft-ds
- \\pce322k.vsb.cz\data
  - DNS jméno počítače
  - TCP/IP port 445 = microsoft-ds

Nebezpečný GUEST

- Lokální účet GUEST
  - defaultně vypnut (zakázán)
  - pokud je povolen, uživatelé ze sítě bez účtu jsou ověřeni jako GUEST
- Podmínky přístupu jako Guest
  - přístup ze sítě pomocí lokálního účtu
  - neexistence účtu stejného jména
  - povolený účet GUEST bez hesla
- Nebezpečí účtu
  - GUEST je ve skupinách Guests, Users, Authenticated Users a Everyone
  - ze sítě ve skupině Network

Auditování přístupu ze sítě

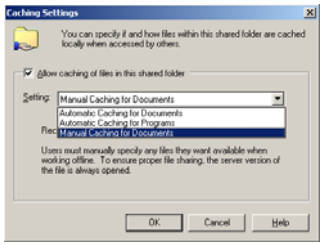
- Sdílení souborů neposkytuje audit
  - zapnout audit na příslušných souborech
  - auditované položky mají

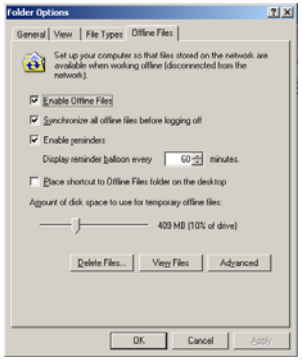
    primary user name: počítač$
    primary domain: doménapočítače

    client user name: jménoklienta
    client domain: doménaklienta

Off-line files

- Přístup k datům off-line
  - synchronizace při pozdějším připojení
  - stavy online / offline





Off-line files

- Módy synchronizace
  - Manual caching for documents
    - manuální označení (pin) souborů které je nutné zpřístupnit off-line
    - při dostupnosti serveru přístup vždy na server
  - Automatic caching for documents
    - automatické zpřístupnění všech otevřených souborů ve složce
    - při dostupnosti serveru přístup vždy na server
  - Automatic caching for programs (Optimize for performance ve Windows 2003)
    - vždy čtení pouze lokální verze

Administrace off-line files

- Reset cache
  - Folder Options / Offline Files
    CTRL+Shift + Delete Files
- Administrativní nastavení
  - gpedit.msc – editor politiky
  - Group Policy / Computer Configuration / Administrative Templates / Network / Offline Files

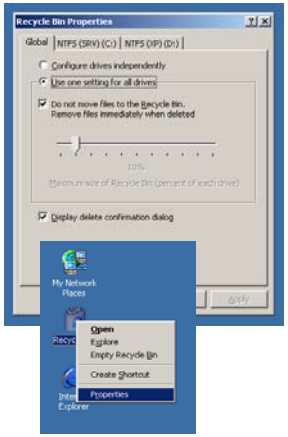
  - Disable user configuration of Offline Files
  - Subfolders always available offline
  - Administratively assigned offline files

Poznámky k off-line files

- Nelze vyvolat „Make available offline“
  - Terminal Services na Serveru Windows 2000
  - lokální složka i při přístupu přes \\pocitac\share
  - Offline files jsou zakázány politikou
  - Novell NetWare server
- Zástupce
  - zástupce souboru je dostupný offline
    => soubor je dostupný offline
  - zástupce složky je dostupný offline
    => složka není dostupná offline

Koš a obnovitelné mazání souborů

- RECYCLER
  - NTFS nepodporuje obnovu souborů
  - mazání v průzkumníkovi pouze přesouvá do koše (SHIFT-DEL maže)
  - nešetří se místo, nutno občas vysypat
  - každý uživatel má vlastní koš (SID) pro ostatní nepřístupný



Zabezpečení souborového systému

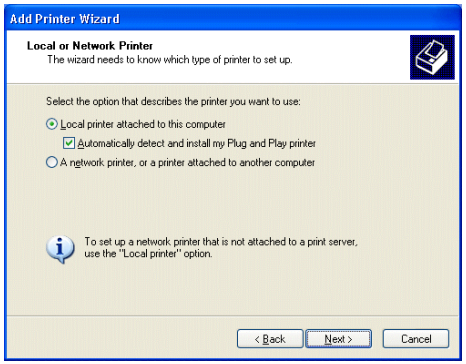
- ACL – Access Control List
- Výchozí zabezpečení
  - pouze NTFS souborový systém
  - administrator – plný přístup
  - Power Users – nebezpečí kvůli instalacím
  - Users – přístup pouze ke svým profilům
- Root systémového oddílu (Windows 2000)
  - výchozí přístup pro Everyone
  - veliké nebezpečí změny loaderu, boot.ini
  - DoS – Denial of Service (zahlcení disku)
  - vytváření nových adresářů

Vlastnosti přístupu k souborům

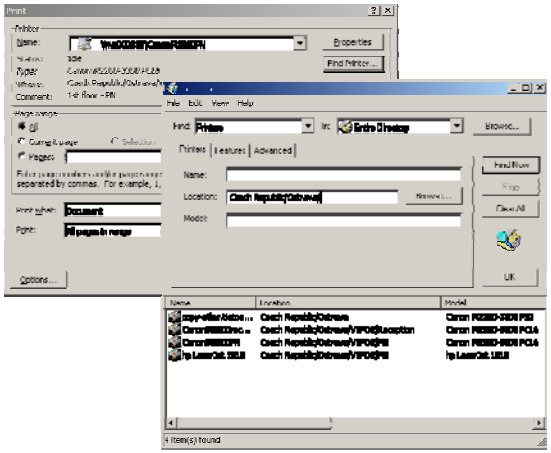
- Kolize
  - spuštěný .EXE soubor (image) nelze smazat ani změnit - jde přejmenovat a jeho místo je pak volné
  - .EXE soubor lze spustit vícekrát za sebou
  - soubor někdo používá (má ho otevřený)
    - i při násilném ukončení procesu dojde k zavření souboru a je opět možné s ním pracovat
  - systémové soubory nelze nahradit (WFP)
    - nesmí existovat kopie v DllCache ani nesmí být dostupná instalační složka (i386, ServicePackFiles)
    - vše se synchronizuje => musíte na to rychle (.BAT)

Printers

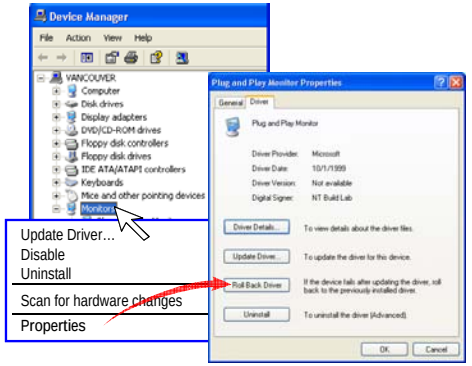
Adding a Local Printer



Find Printer



Driver Rollback

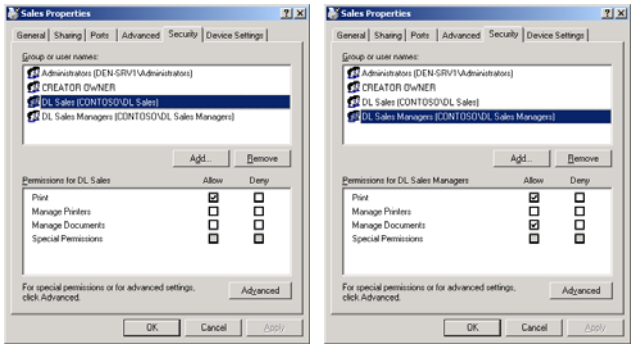


What Are Printer Permissions?

Permission	Allows the user to:
Print	**Connect to a printer and send documents to the printer**
Manage Printers	**Perform the tasks associated with Print permission. The user has complete administrative control of the printer**
Manage Documents	**Manage all aspects of documents that all users submit. The user cannot send documents to the printer or control the status of the printer**

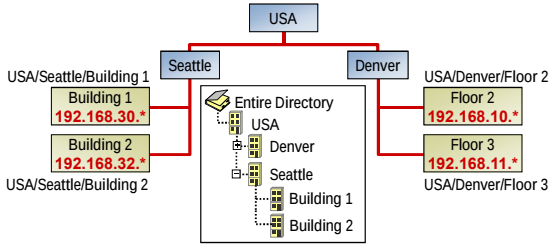
Why Modify Printer Permissions?

Limit or increase access to a printer for selected users



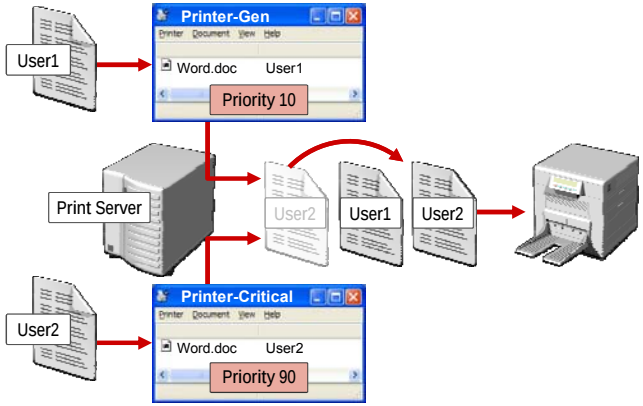
What Are Printer Locations?

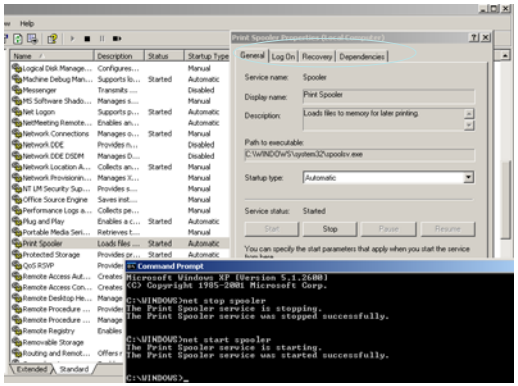
- Each location name corresponds to an IP subnet
- The location attribute for subnet objects and printers must be the same



- Add levels to the location attribute for the printer to better define the physical location

What Are Printer Priorities?

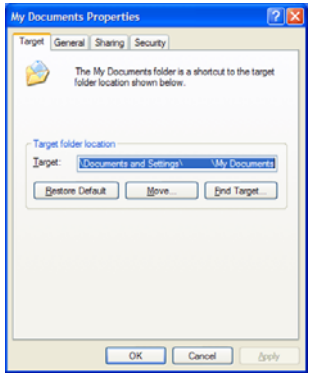




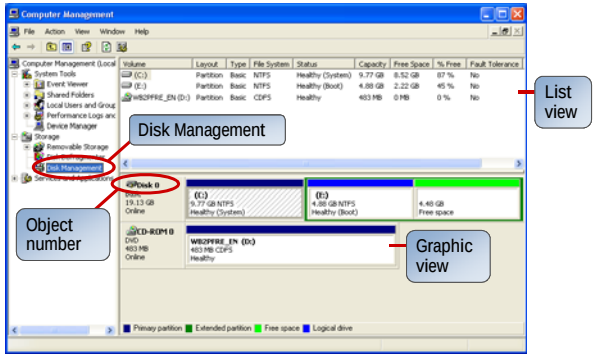
Souborový systém a sdílení

Customizing the My Documents Folder

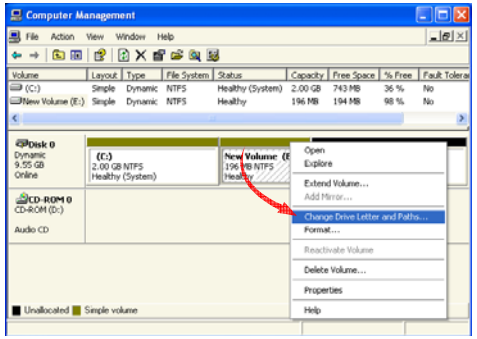
- Changing folder location
- Customizing folder attributes
- Customizing sharing and security properties



Performing Disk-Management Tasks by Using Disk Management



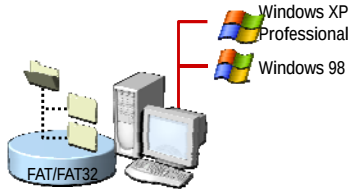
Changing a Drive Letter



Using FAT or FAT32

FAT or FAT32:

- Works well on small disks with simple folder structures
- Supports dual-boot configurations



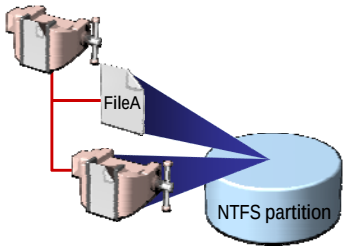
Using NTFS

NTFS Provides:

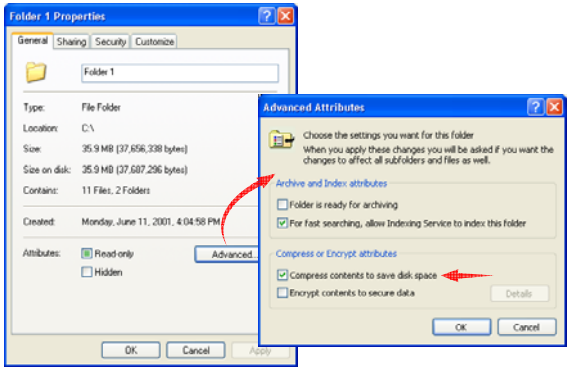
- Improved reliability by identifying and not using bad sectors
- Enhanced security by using EFS and file permissions
- Improved management of storage growth
- Support for large volume sizes

Defining Compressed Files and Folders

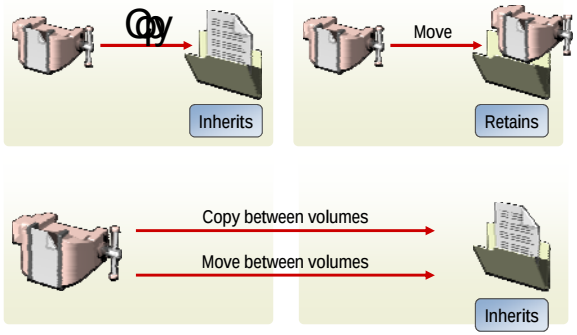
- NTFS files and folders have a compression state
- When accessed, files are automatically uncompressed
- Space allocation is based on uncompressed file size
- Compressed files and folders can be designated by color



Compressing Files and Folders

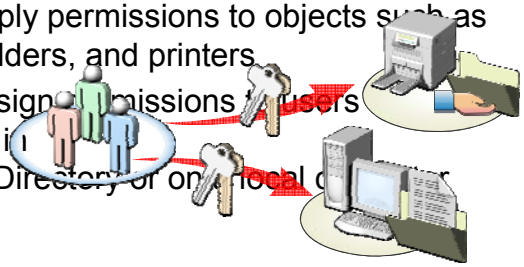


Copying and Moving Compressed Files and Folders



What Are Permissions?

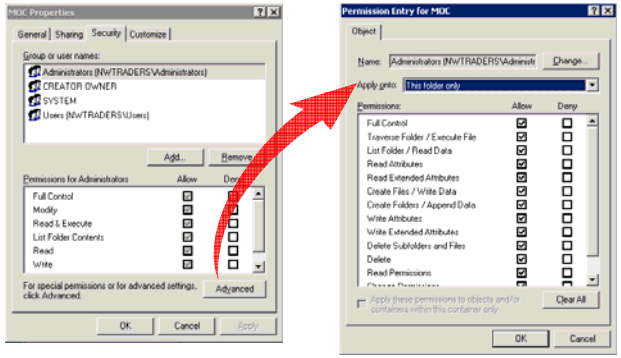
- Permissions define the type of access granted to a user, group, or computer for an object
- You apply permissions to objects such as files, folders, and printers
- You assign permissions to users, groups in Active Directory or on local computer



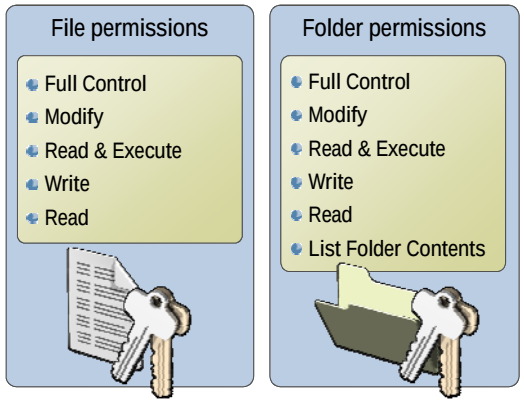
What Are Standard and Special Permissions?

Standard Permissions

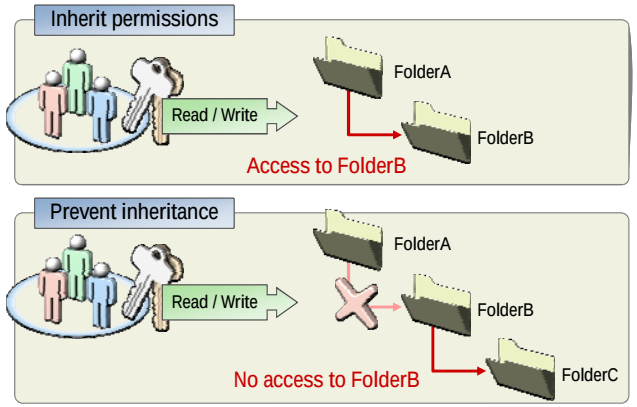
Special Permissions



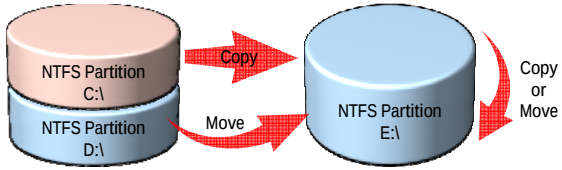
NTFS File and Folder Permissions



What Is NTFS Permissions Inheritance?

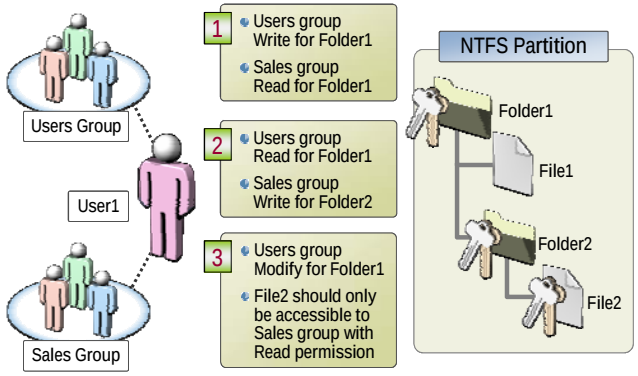


Effects on NTFS Permissions When Copying and Moving Files and Folders



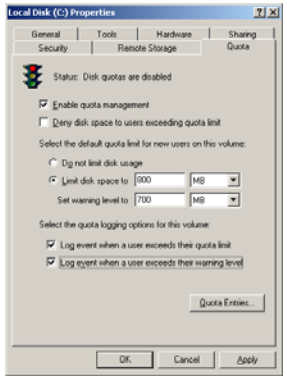
- When you copy files and folders, they inherit the permissions of the destination folder
- When you move files and folders within the same partition, they retain their permissions
- When you move files and folders to a different partition, they inherit the permissions of the destination folder

Applying NTFS Permissions

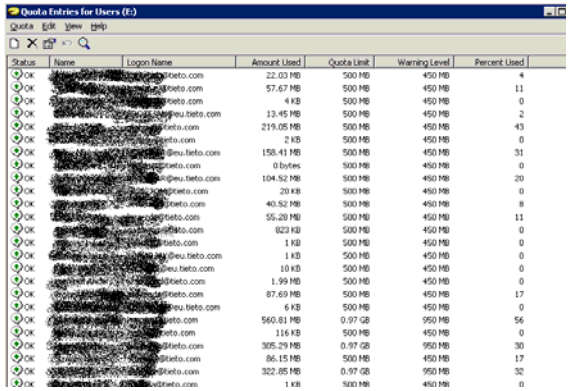


Disk Quotas

- Can be set globally or individually for each user
- Can prevent storing data for users under space limit



Disk Quotas 2



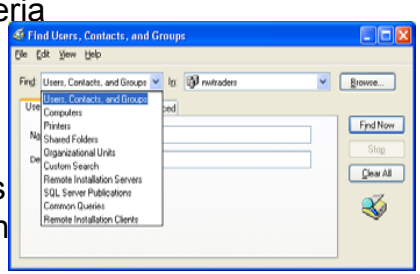
Security Identifiers and Access Control Entries

- A computer or user account is assigned a unique security identifier (SID)
  - A SID is verified when a user attempts to establish a connection with a domain resource
  - A SID is created for each account
- Each directory object, or resource, is protected by access control entries (ACE)
- Users logging on to the local computer may access domain resources; they will be prompted for a valid domain user name and password

Search Types

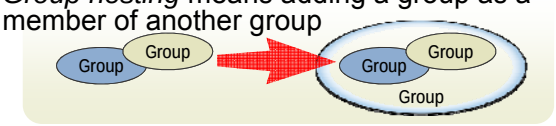
Basic query criteria include:

- Object type
- Location
- General values associated with the object, such as name and description



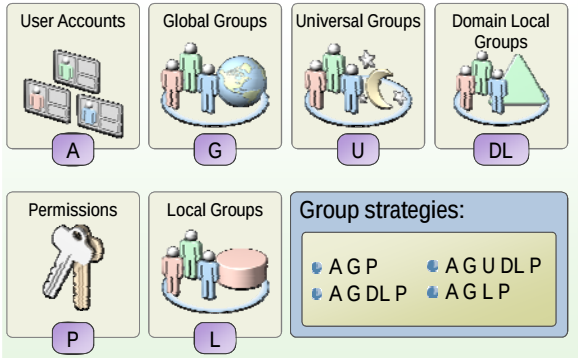
What Is Group Nesting?

- *Group nesting* means adding a group as a member of another group

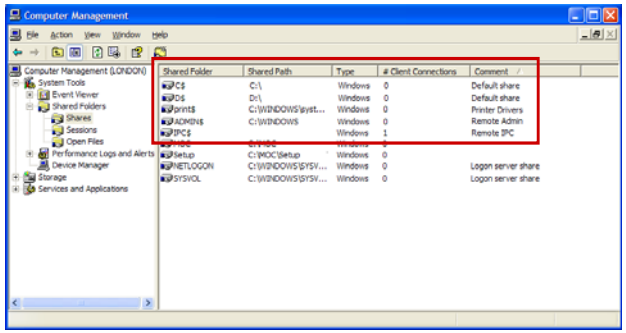


  - Nest groups to consolidate group management
  - Nesting options depend on the domain functional level

Group Strategies



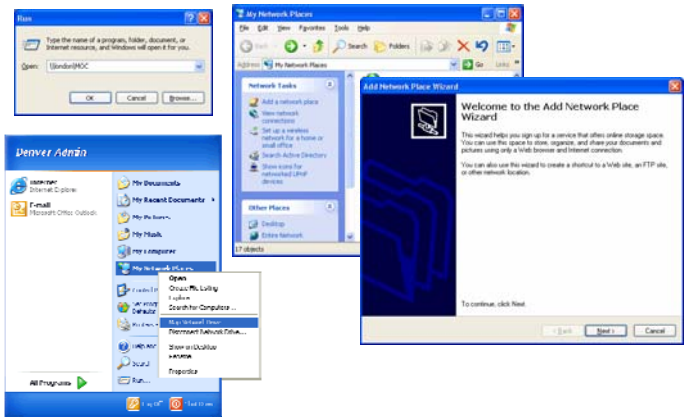
What Are Administrative Shared Folders?



Shared Folder Permissions

Permission	Description
Read (Default, applied to the Everyone group)	**Allows you to view data in files and attributes** **Allows you to view file names and subfolder names** **Allows you to run program files**
Change (Includes all Read permissions)	**Allows you to add files and subfolders** **Allows you to change data in files** **Allows you to delete subfolders and files**
Full Control (Includes all Read and Change permissions)	**Allows you to change NTFS file and folder permissions**

Methods to Connect to Shared Folders

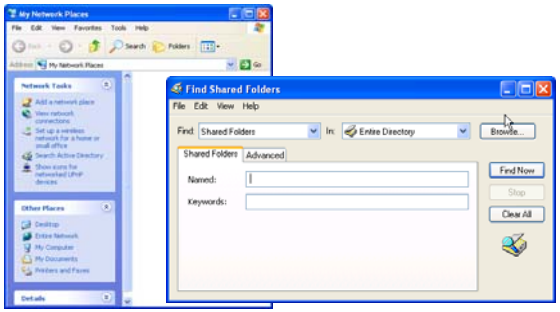


What Are Published Shared Folders?

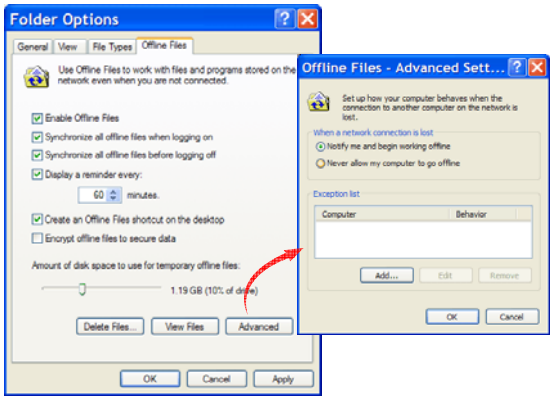
- A published shared folder:
  - Is a shared folder object in Active Directory
  - Can maintain static friendly names
- Clients:
  - Can search Active Directory for published shared folders
  - Do not need to know the name of the server to connect to a shared folder
  - Can search by using keywords if they do not know the exact name of the share

How Published Shared Folders Are Used

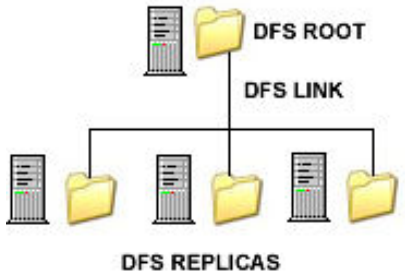
- Administrators can use Active Directory Users and Computers to find shared folders
- Windows XP Professional clients can search Active Directory from My Network Places



Configuring Files and Folders for Offline Use



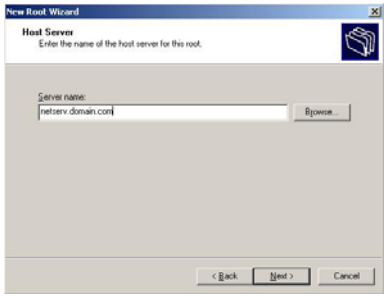
DFS



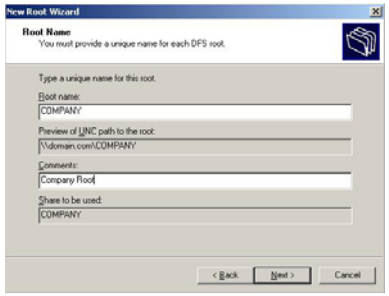
DFS terminology

- **Dfs root:** You can think of this as a share that is visible on the network, and in this share you can have additional files and folders.
- **Dfs link:** A link is another share somewhere on the network that goes under the root. When a user opens this link they will be redirected to a shared folder.
- **Dfs target (or replica):** This can be referred to as either a root or a link. If you have two identical shares, normally stored on different servers, you can group them together as Dfs Targets under the same link.

DFS – new root



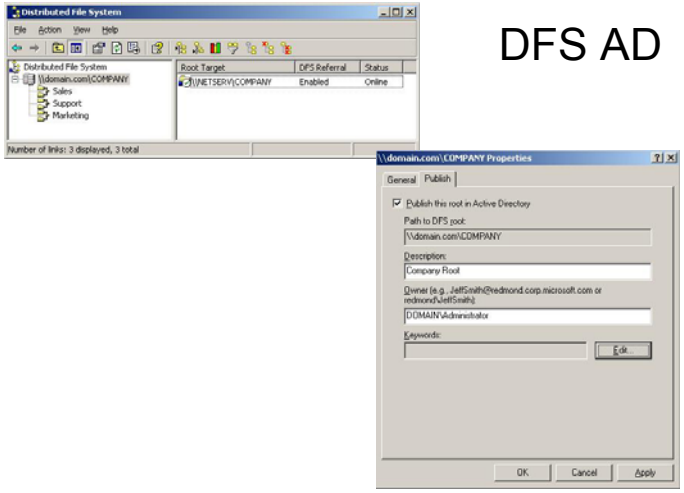
Root properties



Root share

New link

DFS AD



Užitečný sw

- Obsazení disku: TreeSizePro,WinDirStat
- Práva a spousta dalších věcí. : Hyena
- Kopírování: robocopy (MS), Security explorer, Secure copy (Small Wonders)
- Monitoring fs: filemon,diskmon
- Kontrola práv: accesschk, accessenumm, shareenum (MS-SI)
- Otevřené soubory: handle, movefile (MS – SI)
- Přesun: Print migrator (MS)
- Správa: Total Commander, FreeCommander
- Správa hesel: KeePass