

Základy souborového systému NTFS

Základy sdílení souborů v síti, mapování jednotek

Přístupová oprávnění souborového systému NTFS

Základy sdílení souborů v síti, mapování jednotek

Smyslem sdílení dat již není šetřit systémové prostředky lokálních počítačů, ale umožnit více uživatelům pracovat na určitém dokumentu. Je-li některá složka sdílena, mohou k ní přistupovat uživatelé ze sítě. Aby se však uživatelé mohli ke složce připojit, musí mít oprávnění, které jim umožní přístup k příslušné sdílené složce.

Základní charakteristiky oprávnění pro sdílení ze sítě:

- **Oprávnění pro sdílení se vztahují na celé složky**, nikoli na jednotlivé soubory. (Jsou méně přesná než dále probíraná oprávnění NTFS.)
- **Oprávnění pro sdílení se vztahuje jen na uživatele přistupující ze sítě**, nikoli pro přístup lokální.
- **Oprávnění pro sdílení je jediný možný způsob zabezpečení na svazky se souborovým systémem FAT.**

Jakmile nabídneme složku ke sdílení, musíme nadefinovat, kdo a jak je schopen a oprávněn využívat obsah této složky, tak i tuto složku samotnou. Rozlišujeme:

- **Úplné řízení** (implicitní oprávnění skupiny Everyone) Měnit oprávnění pro přístup k souborům. Přebírat vlastnictví souborů na svazcích NTFS. Provádět všechny úlohy, které umožňují oprávnění **Změnit a Číst**.
- **Změnit**. Vytvářet složky a přidávat soubory. Měnit data v souborech. Přidávat data do souborů. Měnit atributy souborů. Mazat složky a soubory. Provádět všechny úkoly, které umožňuje oprávnění **Číst**.
- **Číst**. Zobrazovat jména souborů a složek. Zobrazovat data a atributy souborů. Spouštět programové soubory. Přistupovat ke složkám uvnitř složky.
- **Bez přístupu**. Pouze zřídít spojení se sdílenou složkou. Přístup do složky je zakázán a její obsah se nezobrazuje. Toto oprávnění je užitečné pro vysoké zabezpečení. Oprávnění Bez přístupu potlačuje všechna ostatní oprávnění.

Oprávnění je možné přiřadit jak skupině, tak jednotlivým uživatelům. Doporučuje se nastavovat vždy práva pouze pro skupiny uživatelů, nikoli uživatelům samotným.

Pro změnu oprávnění sdílení nutno **splňovat následující kritéria**:

- ◆ Sdílená složka musí být umístěna na svazku naformátovaném na NTFS, FAT nebo FAT32 souborový systém.
- ◆ Je potřeba mít potřebná oprávnění na úrovni oprávnění NTFS.
- ◆ Nutno být členem skupiny *Administrators* nebo *Power Users*.

Postup při zapnutí sdílení (viz obr.):

1. Vyberte složku.
2. Klikněte pravým tlačítkem myši.
3. Vyberte volbu **Vlastnosti**.
4. V okně vlastnosti vyberte záložku **Sdílení**.
5. Vyberte položku **Sdílet tuto složku**.
6. Vyplňte pole **Název sdílené položky**.
7. Klikněte na **OK** pro potvrzení volby.
8. Sdílení se na složce projeví vizuálně tím, že na ikonce složky přibude **obrázek ruky**.

Zapnutí sdílení.



Sdílení zapnete pomocí pravého tlačítka na složce, kterou chcete sdílet v síti s ostatními uživateli.



Připojení sdílených složek

Poté, co se zapne sdílení konkrétní složky, je nutno ji připojit ze vzdáleného počítače. Způsobů je několik:

■ **Pomocí ikony Místa v síti.** Pomocí této ikony lze najít počítač, na kterém je sdílená složka umístěna a tuto následně připojit přes pravé tlačítko.

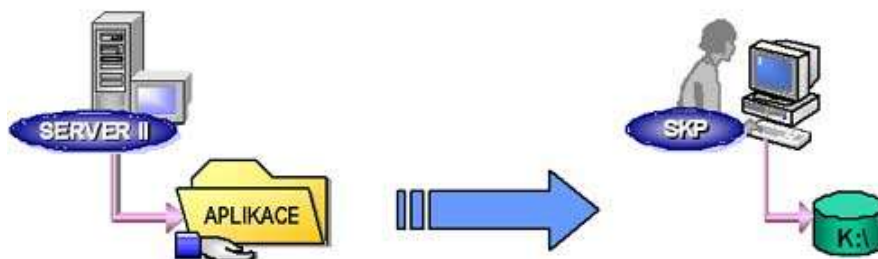
- **Pomocí příkazu Spustit v nabídce Start.** Po otevření nabídky *Start* a zvolení *Spustit*, do tohoto pole se vepíše název počítače a případně i název sdílené složky, Nutno však držet tuto syntaxi: **\\jménoPC**
- **Pomocí volby Připojit síťovou jednotku**
 - ◆ pravým tlačítkem myši se klikne na ikonu *Místa v síti* umístěné na ploše
 - ◆ vybere se volbu *Připojit síťovou jednotku*
 - ◆ v tomto okně se nastaví písmeno připojované složky pro její reprezentaci
 - ◆ do pole *Cesta* se napíše nebo pomocí tlačítka *Procházet* vloží síťová cesta ke sdílené složce (v případě že použijete tlačítko *Procházet* stačí znát název počítače, kde je složka umístěna a nikoli síťovou cestu).
 - ◆ Zatrhne se volba *Znovu připojit při přihlášení*. Spojení s touto složkou bude automaticky navázáno při každém přihlášení do počítače
 - ◆ klikne se na *Dokončit* pro potvrzení připojení složky.
 - ◆ Připojená složka bude reprezentována vybraným písmenem v seznamu místních složek.

Mapování sdílených složek

Připojení písmene jednotky k síťovému počítači nebo složce se provede takto:

Mapování sdílených složek.

Mapování je dočasné či trvalé připojení sdílené složky, která je reprezentována pomocí jednotky označené písmenkem.



- ◆ Spustit program *Průzkumník* Windows.
- ◆ V nabídce *Nástroje* vybrat příkaz *Připojit síťovou jednotku*.
- ◆ V roletovém menu *Jednotka* vybrat písmeno jednotky pro připojení ke sdílenému prostředku
- ◆ V roletovém menu *Složka* zadat server a sdílený název prostředku ve formátu `\\název_serveru\název_sdílené_položky`

Lze také použít tlačítko *Procházet* a prostředek vyhledat.

Pro opětovné připojení ke sdílené jednotce při každém přihlášení, zaškrtnout políčko *Znovu připojit při přihlášení*.

Připojené jednotky jsou dostupné pouze v případě, že je dostupný i hostitelský počítač.

Připojené jednotce lze přiřadit jiné písmeno jednotky odpojením a opětovným připojením jednotky.

Nevýhody sdílení

Oprávnění na úrovni sdílení má **dvě základní nevýhody**, díky kterým není vhodné pro zabezpečování složek obsahujících citlivé informace.

První nevýhodou je, že sdílená složka s nastavenými oprávněními pro jednotlivé skupiny a uživatele je přístupná s právem *Úplné řízení* z lokálního počítače při lokálním přihlášení uživatele. Toto by šlo zabezpečit zakázáním lokálního přihlašování na počítači.

Druhá, dalo by se říci **závažnější, nevýhoda** je možnost přístup do zabezpečené složky přes složku jí nadřazenou.

Z důvodu těchto nevýhod je dobré **kombinovat sdílení oprávnění na úrovni složek se sdílením na úrovni NTFS**, které je z hlediska bezpečnosti více spolehlivé. Proto pro nabídnutí struktury složek nebo složky samotné je vhodné používat sdílení, pro nabídnutí složek ke sdílení a oprávnění nastavit až na úrovni NTFS.

Přístupová oprávnění souborového systému NTFS

Přístupová oprávnění systému NTFS slouží k určení uživatelů nebo jejich skupin, kterým chceme povolit přístup k určitým souborům či složkám. Přístupová oprávnění lze použít pouze na pevných discích naformátovaných souborovým systémem NTFS (nikoli souborovým systémem FAT nebo FAT32).

- Oprávnění je platné jak pro uživatele pracující s daty na místním disku, tak i pro uživatele přistupující přes síť.
- Oprávnění je možné nastavit pro složky i pro jednotlivé soubory.
- Přístupová oprávnění lze i odepřít.

Rozlišujeme tedy:

- **Oprávnění k souborům** - zahrnují *Úplné řízení, Měnit, Číst a spouštět, Číst a Zapisovat*.
- **Oprávnění ke složce** - navíc zahrnují ještě oprávnění *Zobrazovat obsah složky*.

Přehled oprávnění NTFS k složkám a souborům

- ◆ **Úplné řízení** - Všechna nižší oprávnění s možností změny oprávnění a vlastnictví.
- ◆ **Měnit** - Všechna nižší oprávnění, možnost mazání a provedení změn ve složkách a souborech.
- ◆ **Číst a spouštět** - Čtení dokumentů a spouštění programů.
- ◆ **Zobrazovat obsah složky** - Zobrazení složek a souborů. Tento typ oprávnění není definován pro soubory.
- ◆ **Číst** - Zobrazení složek a souborů. Možnost zobrazení obsahu, atributů a oprávnění.
- ◆ **Zapisovat** - Vytváření nových složek a souborů. Možnost provádění změn v souborech.

Slučování oprávnění

Oprávnění pro soubory je důležitější než oprávnění pro složky. Správce tak může některé soubory znepřístupnit před neoprávněnými uživateli, aniž by musel vytvářet novou složku.

V případě členství ve více skupinách a členství ve skupině s odepřeným přístupem bude mít uživatel přístup také odepřen. **Odepřený přístup má nejvyšší možnou důležitost!** (V praxi se lze setkat spíše s promyšleným přidělováním práv a s odepřením pouze ve zvláštních případech nebo jako dočasné řešení).

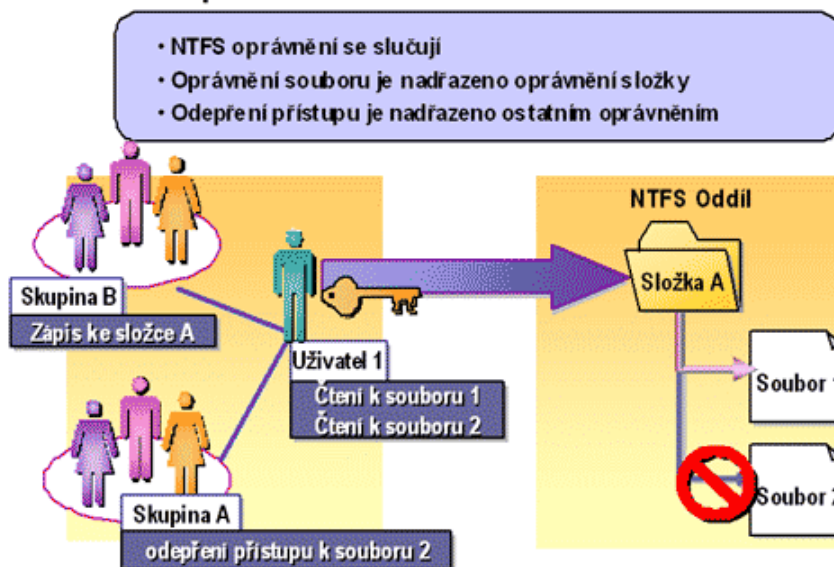
Efektivní práva jsou výsledkem součtu práv uživatele a skupiny - v případě několika skupin s různými oprávněními se uživatelský účet může objevit v několika skupinách určených k jedné sdílené složce. Výsledkem je součet oprávnění (nebo právo vyšší, zahrnující nižší oprávnění).

Analýza obrázku v prezentaci. Uživatel 1 je členem obou skupin, A i B. Dále je nutno si uvědomit, jaká přístupová oprávnění mají nastaveny jednotlivé skupiny a vlastní uživatel.

Jaká budou efektivní oprávnění k souboru 1 pro uživatele? Samozřejmě, že čtení. Jak bylo řečeno, oprávnění k souborům mají přednost před oprávněními ke složkám.

Jaká budou efektivní oprávnění k souboru 2 pro uživatele? Uživateli bude odepřen přístup a se souborem nebude moci pracovat. Důvodem je pak jeho členství ve skupině A, která má odepřen přístup. Odepření přístupu má nejvyšší prioritu.

Slučování oprávnění



Dědění oprávnění

Dědění oprávnění

- 1 Oprávnění se dědí od nadřazené složky při vytváření či kopírování objektu v rámci jednoho oddílu NTFS.
- 2 Oprávnění se dědí od nadřazené složky při přemístění objektu mezi různými oddíly NTFS.
- 3 Oprávnění se **NE**dědí od nadřazené složky při přemístění objektu v rámci jednoho oddílu NTFS.

Nastaví-li se oprávnění pro nadřazenou složku, budou nové soubory a podsložky vytvořené v této složce dědit tato oprávnění. Při kopírování se vytvářejí nové soubory, proto oprávnění vzniká od nadřazené složky. Při přesouvání se soubory přesouvají i s oprávněním, to neplatí při přesunu mezi oddíly, ale pouze v rámci jednoho oddílu.

Pokud nechceme, aby se oprávnění dědila, vybere se

při nastavování zvláštních oprávnění pro nadřazenou složku v seznamu *Použit pro možnost Jen tato složka*. V případech, kdy chceme zabránit dědičnosti oprávnění jen u určitých souborů nebo složek, klepneme pravým tlačítkem myši na soubor nebo podsložku, která nemá oprávnění dědit, klepneme na příkaz *Vlastnosti*, potom na kartu *Zabezpečení* a zrušíme zaškrtnutí políčka *Umožnit přenos dědičných oprávnění z nadřazeného objektu na tento*. Jsou-li zaškrťovací políčka stínovaná, dědí soubor nebo složka oprávnění z nadřazené složky. Dědičná oprávnění je možné změnit dvěma způsoby:

- Provedte změny v nadřazené složce. Soubor nebo složka budou oprávnění dědit.
- Zaškrtnutím opačného oprávnění (Povolit nebo Odepřít) přepište zděděná oprávnění.

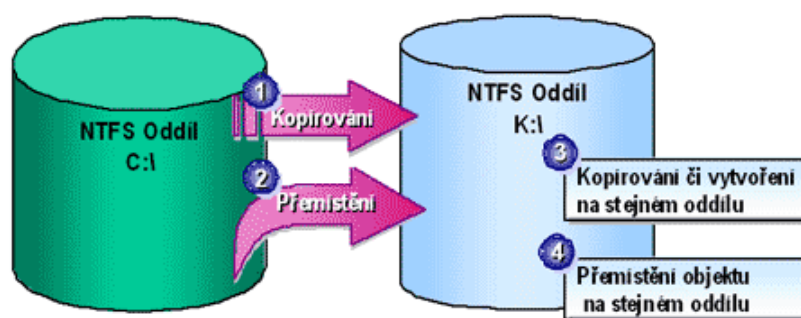
Zrušíme zaškrtnutí políčka *Umožnit přenos dědičných oprávnění z nadřazeného objektu na tento*. Nyní můžete provádět změny v oprávněních nebo odstraňovat uživatele či skupiny

ze seznamu oprávnění. Soubor nebo složka však již nebudou dědit oprávnění z nadřazené složky.

Jestliže není u oprávnění zaškrtnuto políčko Povolit ani Odepřít, získali pravděpodobně uživatel nebo skupina oprávnění prostřednictvím členství ve skupinách. Pokud uživatel nebo skupina nezískali oprávnění prostřednictvím členství v jiné skupině, jsou jim oprávnění implicitně odepřena. Chcete-li výslovně povolit nebo odepřít oprávnění, zaškrtněte příslušné políčko.

Dědění oprávnění

- | | | |
|--|---|--|
| <ol style="list-style-type: none"> 1 2 3 4 | <p>Zdělí se oprávnění při kopírování souboru mezi disky C: a K: ?</p> <p>Zdělí se oprávnění při přemístění souboru mezi disky C: a K: ?</p> <p>Zdělí se oprávnění v tomto případě ?</p> <p>Zdělí se oprávnění přemístíme-li soubor v rámci disku K: ?</p> | <p>ANO</p> <p>ANO</p> <p>ANO</p> <p>NE</p> |
|--|---|--|



Analýza všech čtyř konkrétních případů. Pomůckou může být fakt, že objekt dědí oprávnění pokaždé, když vzniká. A skutečně objekt vzniká při kopírování, samozřejmě objekt vzniká při jeho vytvoření, objekt vzniká i při jeho přemístění na jiný NTFS oddíl. A ve všech těchto případech objekt zdělí oprávnění od cílové složky.

V případě č. 1 objekt kopírujeme z disku C: na disk K: Objekt tedy musí na disku K: vzniknout, tudíž si nenes informace o oprávnění a toto oprávnění zdělí od nadřazené složky.

V případě č. 2 objekt přemísťujeme na disk K:.. Odpověď i vysvětlení je totožné jako u případě č. 1.

V případě č. 3 objekt vytváříme či kopírujeme v rámci jednoho, stejného oddílu. Opět objekt musí vzniknout, tudíž oprávnění zdělí.

V případě č. 4, kdy objekt přemísťujeme v rámci stejného oddílu, tento objekt nevzniká, mění se pouze jeho umístění. Počítač soubor nechá, tak jak je, a pouze změní informaci o jeho umístění. Přístupová oprávnění tedy zůstanou zachována, nebudou zděděna.

Avšak **v případě č. 4**, kdy objekt přemísťujeme v rámci stejného oddílu, tento objekt nevzniká, mění se pouze jeho umístění. Počítač soubor nechá, tak jak je, a pouze změní informaci o jeho umístění. Přístupová oprávnění tedy zůstanou zachována, nebudou zděděna.

Literatura:

- [1] Materiály z internetu www.indos.cz
- [2] Pecinovský, J.: Windows 2000 server, Grada Publishing, Praha 2000