

Instalace, konfigurace a správa souborových a tiskových služeb

Souborové služby

Souborové služby jsou jednou z hlavních rolí, které servery odjakživa zastávaly, a jako takové by jí měla být věnována patřičná pozornost.

Operační systém Windows Server 2008 nepřináší novinky ve své podstatě revoluční, ale několik užitečných doplňků a nástrojů zde určitě najdeme. Nadšení z nich však poněkud chladí skutečnost, že tyto „novinky“ jsou v jiných systémech už léta samozřejmostí a je poněkud ostudné, že se stávají součástí operačního systému až nyní.

V tomto oddílu knihy se budeme věnovat právě službám, které slouží ke sdílení dat a tiskáren. Téma sdílení čehokoliv je samo o sobě velice obsáhlé a možná by si zasloužilo samostatnou knihu, přesto se zde však pokusím nastínit alespoň ty nejdůležitější postupy a hotová řešení pro úspěšnou správu.

Instalace role Souborová služba (File Server)

Samotná instalace role Souborové služby (File Server) nepřináší nějaké zásadní výhody. Užitečnost a potenciál této role se zvětšuje až s instalací dalších služeb rolí, které jsou zde dostupné, konkrétně:

- Systém souborů DFS (Distributed File System) včetně komponent Obory názvů DFS (DFS Namespaces) a Replikace distribuovaného systému souborů (DFS Replication).
- Správce prostředků souborového serveru (File Server Resource Manager)
- Services for NFS
- Služba Windows Search

- Souborová služba systému Windows Server 2003 (Windows Server 2003 File Services) a její součástí Služba replikace souborů (File Replication Service) a Služba indexování (Indexing Service)

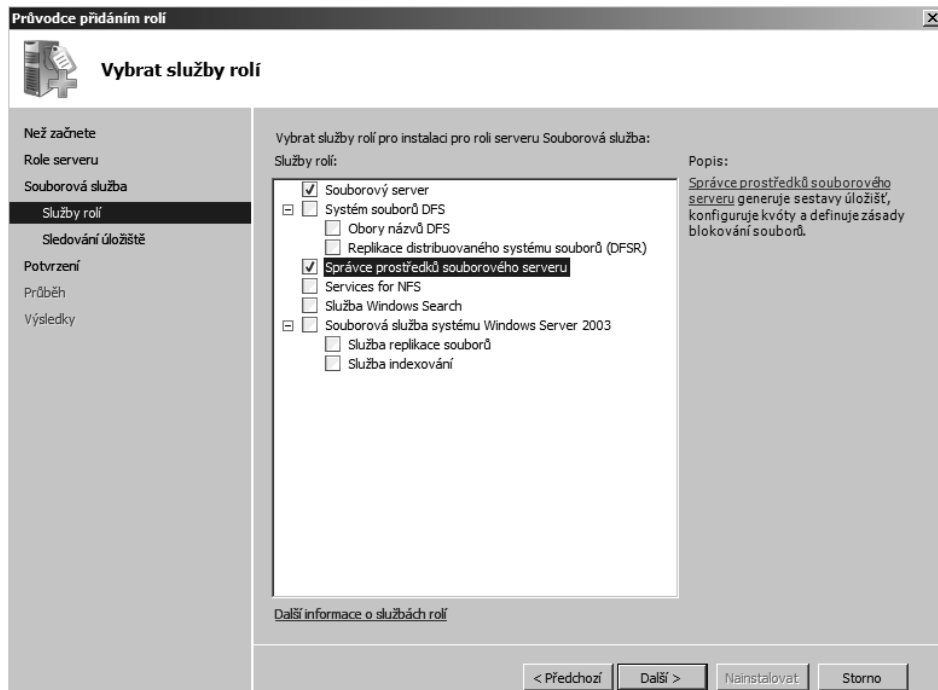
Při instalaci role Souborová služba (File Server) doporučuji rovnou nainstalovat i Správce prostředků souborového systému (File Server Resource Manager). Nic tím nezkažíte, a naopak získáte sadu základních nástrojů pro efektivní správu souborového serveru.

Při instalaci role včetně onoho správce (dále jen FSRM) postupujte takto:

1. Spusťte **Správce serveru** (Server Manager), klepněte na uzel **Role** (Roles) a poté klepněte na odkaz **Přidat role** (Add Roles). Pokud se zobrazí obrazovka **Než začnete** (Before you begin), přečtěte si její text a klepněte na tlačítko **Další** (Next).
2. Na obrazovce **Vybrat role serveru** (Select Server Roles) zaškrtněte položku **Souborová služba** (File Server) a klepněte na tlačítko **Další** (Next). Na tlačítko **Další** (Next) klepněte rovněž na obrazovce **Souborová služba** (File Server).
3. Na obrazovce **Vybrat služby rolí** (Select Server Roles) ponechejte zaškrtnutou položku **Souborový server** (File Server) a dále zaškrtněte všechny služby rolí, které budete potřebovat.

Jak jsem zmínil výše, instalace služby role s názvem **Správce prostředků souborového serveru** (File Server Resource Manager – dále jen FSRM) určitě není od věci, zatrhneme ji tedy rovněž (viz obrázek 5.1).

Jste-li hotovi s výběrem, klepněte na tlačítko **Další** (Next).



Obrázek 5.1 Výběr služeb rolí při instalaci role souborového serveru

4. Jestliže jste v předchozím kroku nainstalovali službu role **Správce prostředků souborového serveru** (File Server Resource Manager), zobrazí se nyní obrazovka **Konfigurovat sledování využití místa** (Configure Storage Using Monitoring).

Na této obrazovce můžete zatrhnout políčka vedle oddílů, jejichž využití má být sledováno a klepnutím na tlačítko **Možnosti** (Options) můžete upřesnit typy sestav, které mají být generovány.

Po nastavení požadovaných voleb klepněte na tlačítko **Další** (Next).

5. Následující obrazovka také souvisí se službou role FSRM. Můžete zde nakonfigurovat zda, komu a přes jaký server SMTP mají být zaslány vygenerované sestavy.

Po nastavení těchto voleb klepněte na tlačítko **Další** (Next).

Na poslední obrazovce průvodce přidáním rolí klepněte na tlačítko **Nainstalovat** (Install).

Instalace nástroje Správce prostředků souborového serveru (File Server Resource Manager)

Jestliže již máte nainstalovanou roli **Souborový server** (File Server) a postrádáte nástroj **Správce prostředků souborového serveru** (File Server Resource Manager – FSRM), můžete jej přidat kdykoliv později, a to následujícím způsobem.

1. Spusťte **Správce serveru** (Server Manager) a v levém panelu rozbalte uzel **Role** (Roles) a klepněte na položku **Souborová služba** (File Server).

V pravém panelu nyní najdete sekci s názvem **Služby rolí** (Role Services) a klepněte na tlačítko **Přidat služby rolí** (Add Role Services).

2. V seznamu služeb rolí zaškrtněte položku **Správce prostředků souborového serveru** (File Server Resource Manager) a klepněte na tlačítko **Další** (Next).

3. Na obrazovce **Konfigurovat sledování využití místa** (Configure Storage Using Monitoring) zaškrtněte oddíl, u kterých chcete sledovat využití místa, a klepněte na tlačítko **Další** (Next).

4. Na obrazovce **Nastavit možnosti sestavy** (Set Report Options) pomocí tlačítka **Procházet** (Browse) můžete změnit výchozí cestu pro ukládání sestav a také povolit odesílání sestav e-mailem (budete potřebovat znát název serveru SMTP).

Po nastavení těchto voleb klepněte na tlačítko **Další** (Next) a následně na tlačítko **Nainstalovat** (Install).

Po úspěšné instalaci by neměl být vyžadován restart (může být v případě, že jste instalovali více komponent najednou) a nástroj FSRM najdete v **Nástrojích pro správu** (Administrative Tools).



Poznámka: V době psaní této knihy se vyskytoval jeden problém spojený s nástrojem FSRM. Když nainstalujete roli serveru Souborová služba na řadiči domény, může přestat fungovat konzola Správa zásad skupiny (Group Policy Management). Konkrétně při pokusu o vytvoření nového objektu zásad skupiny se objeví nepřilíhší informativní chybová hláška a objekt se nepovede vytvořit.

Řešením se ukázalo odstranění nástroje FSRM z řadiče domény, případně následná reinstalace konzoly pro správu zásad skupiny.

Je možné, že problém byl vyřešen formou nějaké aktualizace, tak jako tak bychom však neměli z řadiče domény dělat souborový server (pokud je to možné).



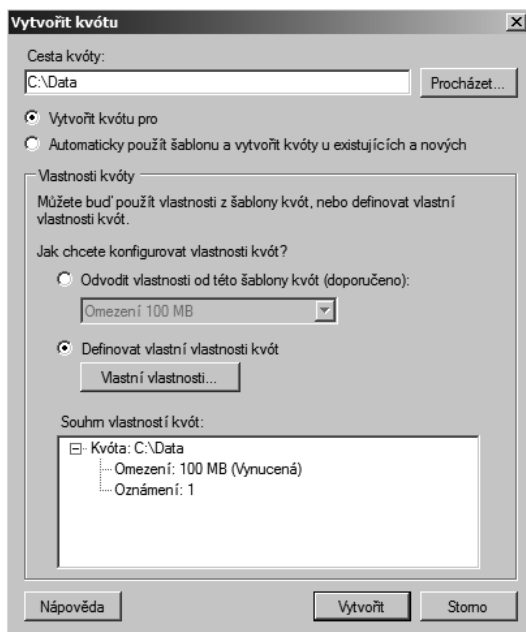
Nasazení kvót pomocí Správce prostředků souborového serveru (File Server Resource Manager)

Jedním z hlavních přínosů nástroje Správce prostředků souborového serveru (File Server Resource Manager – dále jen FSRM) je možnost nasazení kvót na úrovni složky.

Jen pro srovnání – pomocí systému souborů NTFS jsme mohli doposud nastavovat pouze kvóty na úrovni oddílů, což nebylo zdaleka vždy žádoucí. A generovat nějaké sestavy o využití místa na disku s nasazenými kvótami NTFS byla a je kapitola sama pro sebe.

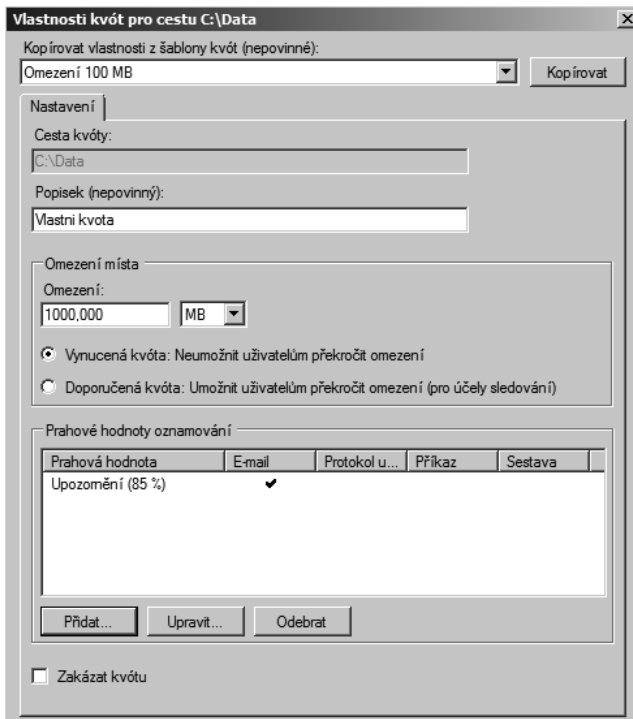
Nástroj FSRM celou situaci značně zjednodušuje. Následující postup popisuje nasazení kvóty na složku.

1. Klepněte na **Start** → **Nástroje pro správu** (Administrative Tools) → **Správce prostředků souborového serveru** (File Server Resource Manager).
2. V levém panelu konzoly rozbalte klepnutím uzel **Správa kvót** (Quota Management), označte uzel **Kvóta** (Quotas), klepněte na něj pravým tlačítkem myši a vyberte z nabídky položku **Vytvořit kvótu** (Create Quota).
3. Pomocí tlačítka **Procházet** (Browse) vyberte složku, na kterou se má kvóta uplatnit.
4. Na obrazovce znázorněné na obrázku 5.2 si vyberte, zda se použije některá z předdefinovaných kvót. Pokud vám tyto šablony z nějakého důvodu nevyhovují, přepněte položku **Odvodit vlastnosti od této šablony** (Derive properties from this quota template) na **Definovat vlastní vlastnosti kvót** (Define custom quota properties).



Obrázek 5.2 Dialogové okno pro vytvoření kvóty

Následně pak klepněte na tlačítko **Vlastní vlastnosti** (Custom Properties) a v dialogovém okně, které můžete vidět na obrázku 5.3, nadefinujte podrobnější vlastnosti kvóty.



Obrázek 5.3 Dialogové okno pro definici vlastních vlastností kvóty

Dialogová okna vlastních vlastností kvóty zavřete klepnutím na tlačítko **OK** a v hlavním dialogovém okně klepněte na **Vytvořit** (Create).

5. Zobrazí se dotaz, zda se má nově vytvořená kvóta uložit jako šablona anebo zda chcete kvótu jen uložit bez vytváření šablony z této kvóty.

Vyberte si jednu z možností a klepněte na tlačítko **OK**.

Tím je kvóta vytvořena a můžete ji spravovat z nástroje FSRM.



Poznámka: Kvóty NTFS a kvóty nástroje FSRM by se neměly kombinovat. Technicky to sice možné je, ale jeden druh kvót potlačí nastavení jiných kvót, takže se ve výsledku stejně použijí jen jedny kvóty.

Blokování ukládání určitých typů souborů

Situace, kdy uživatelé ukládají na souborové servery gigabyty dat, která nemají ve firemním prostředí co dělat, je chronicky známá snad každému administrátorovi (čest výjimkám).

Nástroj Správce prostředků souborového serveru (File Server Resource Manager – dále jen FSRM) přichází s funkcí, která umožňuje blokovat ukládání souborů určitého typu.

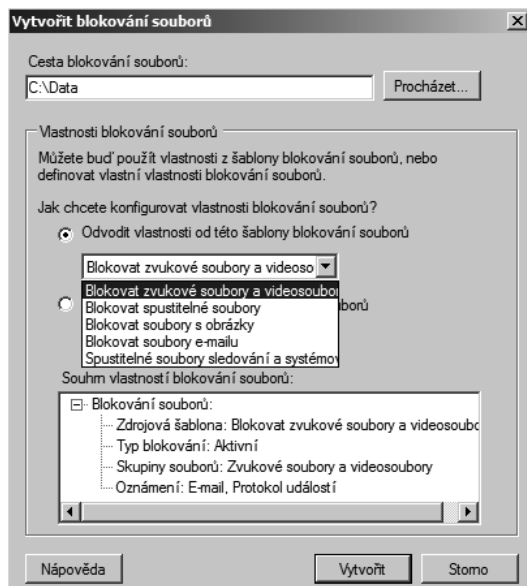
Můžeme tedy zakázat například ukládání souborů typu mp3, avi, mpg, apod. Pokud v tomto okamžiku zajásáte, že už bylo načase něco takového do serverového operačního systému

implementovat, musím vás zklamat. Blokování ukládání souborů hlídá pouze přípony souborů, nikoliv jejich skutečný obsah, což je vcelku neodpustitelné.

Pokud se smíříte s přístupem „lepší něco, než nic“, můžete zablokovat ukládání určitých souborů takto:

1. Klepněte na tlačítko **Start** → **Nástroje pro správu** (Administrative Tools) → **Správce prostředků souborového serveru** (File Server Resource Manager).
2. V levém panelu konzoly rozbalte uzel **Správa blokování souborů** (File Screening Management), klepněte pravým tlačítkem myši na položku **Blokování souborů** (File Screens) a z nabídky vyberte **Vytvořit blokování souborů** (Create File Screen).
3. V dialogovém okně **Vytvořit blokování souborů** (Create File Screen) zadejte pomocí tlačítka **Procházet** (Browse) cestu ke složce, v které bude ukládání souborů zablokováno. Z nabídky **Odvodit vlastnosti od této šablony blokování souborů** (Derive properties from this file screen template) si můžete vybrat typ blokování souborů (viz obrázek 5.4) nebo můžete vytvořit vlastní typ blokování.

Když jste s nastavením hotovi, klepněte na tlačítko **Vytvořit** (Create).



Obrázek 5.4 Dialogové okno pro vytvoření blokování souborů

Vytváření přehledů o úložišti dat

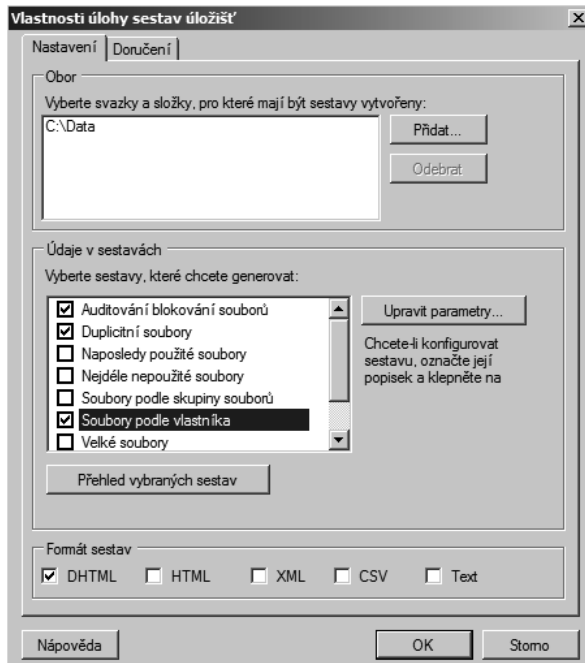
Nástroj Správce prostředků souborového serveru (File Server Resource Manager) umožňuje vytvářet mnoho různých přehledů o využití diskového prostoru, např. dle vlastníka, duplicitní soubory, dle velikosti atd.

Tyto sestavy mohou být generovány automaticky v daných intervalech anebo je můžete vytvářet kdykoliv a zjistit tak informace o aktuálním využití diskového prostoru.

Okamžitý přehled získáte takto:

1. Klepněte na tlačítko **Start** → **Nástroje pro správu** (Administrative Tools) → **Správce prostředků souborového serveru** (File Server Resource Manager).
2. V levém panelu konzoly klepněte pravým tlačítkem na položku **Správa sestav úložišť** (Storage Reports Management) a vyberte **Generovat sestavy** (Generate Reports Now).
3. Klepnutím na tlačítko **Přidat** (Add) vyberte složku nebo svazek, pro které chcete sestavu vygenerovat a ve spodní části dialogového okna zaškrtněte typ nebo více typů přehledů, které chcete vytvořit (viz obrázek 5.5).

V tomtéž dialogovém okně pak zvolte formát sestavy a klepněte na tlačítko **OK**.



Obrázek 5.5 Nastavení pro vygenerování přehledu využití diskového prostoru

4. Zobrazí se dotaz, zda chcete přehled vygenerovat okamžitě nebo jej necháte zpracovat na pozadí a později odeslat e-mailem.
Vyberte zde požadovanou možnost a klepněte na tlačítko **OK**.

Nasazení služby DFS

Služba DFS (Distributed File System – Distribuovaný systém souborů) slouží k efektivnější organizaci, sdílení a synchronizaci dat na souborových serverech. Poskytuje centralizovanou strukturu složek, které se mohou fyzicky nacházet na mnoha serverech napříč sítí, aniž by uživatel musel přesně vědět, kde která data jsou.

Kromě výše uvedeného systém DFS také může poskytovat řešení pro redundanci dat. Pokud několik serverů obsahuje kopii identických dat, nemusí výpadek jednoho z těchto serverů nutně znamenat nepřístupnost dat pro uživatele, neboť tento může přistupovat k datům na jiném serveru, aniž by o tom věděl.



Službu DFS můžete nainstalovat dvěma způsoby: Buď zároveň s instalací role Souborová služba (File Service) (viz řešení *Instalace role Souborová služba* na začátku této kapitoly) nebo ji můžete přidat jako službu role (pokud je již role Souborová služba nainstalována bez DFS).

Při instalaci DFS jako služby role postupujte takto:

1. Spusťte **Správce serveru** (Server Manager), rozbalte uzel **Role** (Roles) a klepněte na položku **Souborová služba** (File Services).
2. V pravé části okna konzoly klepněte na tlačítko **Přidat služby rolí** (Add Role Services). Na obrazovce **Vybrat služby rolí** (Select Server Roles) zaškrtněte položku **Systém souborů DFS** (Distributed File System) a klepněte na tlačítko **Další** (Next).
3. Na další obrazovce můžete začít konfigurovat obor názvů. Budeme se jím však zabývat v dalším řešení, můžete tedy přepnout volbu na **Vytvořit obor názvů později pomocí modulu Snap-in Správa systému souborů DFS v součásti Správce serveru** (Create a namespace later using the DFS Management snap-in in Server Manager) a klepnout na tlačítko **Další** (Next).

Na následující obrazovce klepněte na tlačítko **Nainstalovat** (Install) a po dokončení instalace na tlačítko **Zavřít** (Close).



Vytvoření oboru názvů DFS

Hlavním účelem oboru názvů systému DFS je sjednocení různých fyzických úložišť dat do jediné logické struktury, ve které se uživatelé mohou snadno orientovat.

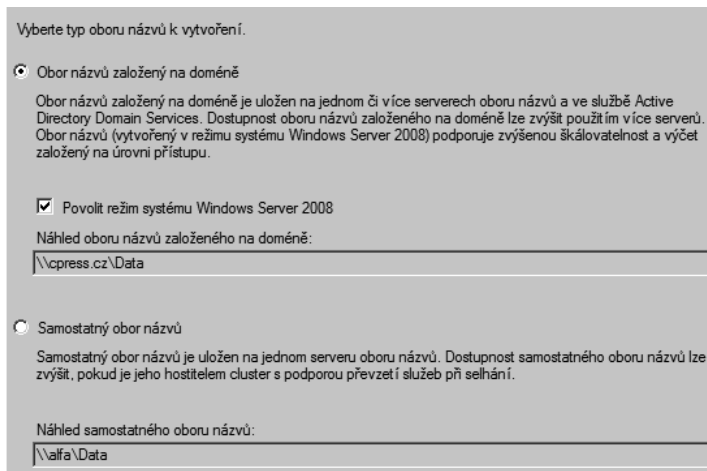
Obor názvů systému DFS tedy uživatelé uvidí ve formě sdílené složky obsahující více podsložek.

Při vytvoření nového oboru názvů postupujte takto:

1. Klepněte na tlačítko **Start** → **Nástroje pro správu** (Administrative Tools) → **DFS Management**.
V levém panelu konzoly klepněte pravým tlačítkem myši na uzel **Obory názvů** (Namespaces) a vyberte položku **Nový obor názvů** (New Namespace), načež se spustí **Průvodce novým oborem názvů** (New Namespace Wizard).
2. Na obrazovce **Server oboru názvů** (Namespace Server) zvolte server, který bude hostitelem oboru názvů DFS. Obor názvů může být hostován více servery, a to z důvodu zajištění vyšší dostupnosti.
Po zadání názvu klepněte na tlačítko **Další** (Next).
3. Na další obrazovce zadejte název oboru názvů. Tento název pak budou uživatelé používat pro přístup k datům v systému DFS, takže pokud vytvoříme například obor názvů s názvem *Data* v doméně *cpress.cz*, budou uživatelé zadávat cestu `\\cpress.cz\data`.
Po zadání názvu klepněte na tlačítko **Další** (Next).
4. Na obrazovce **Typ oboru názvů** (Namespace Type) zvolte, zda se má použít obor názvů založený na doméně nebo samostatný obor názvů (viz obrázek 5.6).
Obor názvů založený na doméně se snadněji škáluje a také poskytuje jednodušší formu odolnosti vůči selhání, můžete tedy vybrat například tento typ oboru názvů a v ideálním případě povolit režim Windows Server 2008.

Poté klepněte na tlačítko **Další** (Next) a na následující obrazovce zkontrolujte nastavení a klepněte na tlačítko **Vytvořit** (Create).

Po úspěšném vytvoření oboru názvů můžete průvodce ukončit klepnutím na tlačítko **Zavřít** (Close).



Obrázek 5.6 Výběr typu oboru názvů

Přidání složky do oboru názvů DFS

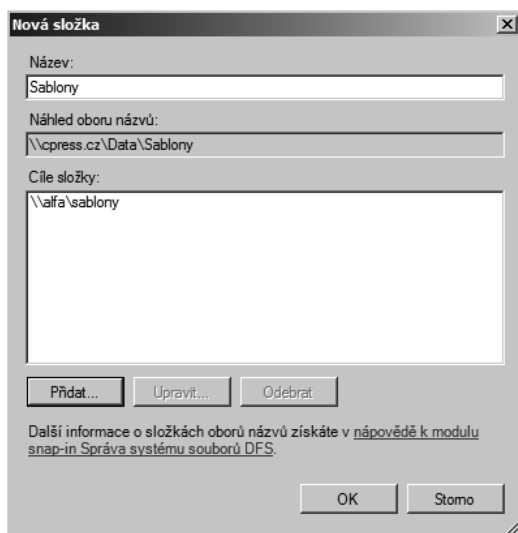


Jak bylo uvedeno dříve, jedním z účelů systému DFS je konsolidace fyzických úložišť dat do jednotného oboru názvů, ve kterém mohou figurovat sdílené složky z mnoha různých serverů.

Následující postup popisuje, jak do oboru názvů DFS přidat sdílenou složku.

1. Klepněte na tlačítko **Start** → **Nástroje pro správu** (Administrative Tools) → **DFS Management**.
2. V levém panelu konzoly rozbalte uzel **Obory názvů** (Namespaces), klepněte pravým tlačítkem myši na obor názvů, do kterého chcete přidat složku a vyberte možnost **Nová složka** (New Folder). Zobrazí se dialogové okno, které můžete vidět na obrázku 5.7. Zde zadejte název složky, pod kterým bude dostupná v oboru názvů systému DFS. Poté klepněte na tlačítko **Přidat** (Add) a zadejte název UNC ke sdílené složce na serveru a klepněte na tlačítko **OK**. Tímto krokem jste přidali tzv. cíl složky, tedy fyzické umístění sdílené složky.
3. Když je složka vytvořena, má ve výchozím stavu jeden cíl složky. Těchto cílů však můžete nadefinovat více a docílíte tím synchronizace dat v uvedených složkách mezi různými servery.

Pokud tedy chcete přidat další cíl složky, rozbalte v levém panelu konzoly uzel **Obory názvů** (Namespaces), dále rozbalte konkrétní obor názvů, vyberte v něm složku, které chcete přidat cíl složky, klepněte na ni pravým tlačítkem myši a zvolte **Přidat cíl složky** (Add Folder Target).



Obrázek 5.7 Dialogové okno pro přidání složky do oboru názvů systému DFS

V dialogovém okně **Nový cíl složky** (New Folder Target) pak zadejte cestu UNC ke sdílené složce, která se má stát dalším cílem složky.

4. Zobrazí se dotaz, zda chcete vytvořit skupinu replikace (viz obrázek 5.8). Chcete-li data mezi různými cíli složek skutečně synchronizovat, klepněte na tlačítko **Ano** (Yes). Spustí se průvodce replikací složek, kterému se budeme věnovat v následujícím řešení.



Replikace složek v systému DFS

Pokud máte v oboru názvů DFS vytvořenou složku, která obsahuje více cílů složek, bude vhodné zajistit synchronizaci obsahu těchto sdílených složek mezi jednotlivými servery.

Výsledkem pak bude mechanismus, kdy budete moci například měnit soubory na jednom serveru, a tato změna bude replikována na ostatní servery, takže bude zajištěna integrita dat.

Replikaci cílů složek nastavíte takto:

1. V konzole DFS Management rozbalte v levém panelu uzel **Obory názvů** (Namespaces), dále pak rozbalte konkrétní obor názvů a označte klepnutím složku, jejíž cíle složky chcete replikovat.
2. V pravém panelu konzoly přepněte na záložku **Replikace** (Replication) a klepněte na odkaz **Průvodce replikací složek** (Folder Replication Wizard).

Na první obrazovce průvodce pak zkontrolujte název skupiny replikace a replikované složky a klepněte na tlačítko **Další** (Next).

Průvodce vyhodnotí cíle složky a vypíše, zda jsou všechny cíle připraveny pro členství v replikační skupině. Je-li na této obrazovce vše v pořádku, klepněte na tlačítko **Další** (Next).

3. Na obrazovce s názvem **Primární člen** (Primary Member) vyberte z rozbalovací nabídky server, z kterého se bude obsah složky replikovat na ostatní členy replikační skupiny (pokud již nějaký obsah složek v okamžiku vytváření replikační skupiny existuje).

Po určení primárního člena klepněte na tlačítko **Další** (Next).

4. Vyberte replikační topologii a klepněte na tlačítko **Další** (Next).

Na následující obrazovce určete, jak a případně kdy mají jednotliví členové replikační skupiny replikovat data. Pokud to technické zázemí umožňuje, bude vhodné ponechat výchozí nastavení.

Chcete-li však z nějakého důvodu naplánovat replikační rozvrh jinak, přepněte na možnost **Replikovat během zadaných dnů a časů** (Replicate during specified days and times), klepněte na tlačítko **Upravit plán** (Edit Schedule) a v dialogovém okně s rozvrhem nastavte požadované časy replikace.

Po zadání těchto údajů klepněte na tlačítko **Další** (Next), na poslední obrazovce průvodce zkontrolujte zadané informace a klepněte na tlačítko **Vytvořit** (Create).

Bylo-li vše v pořádku, měl by průvodce vygenerovat potvrzení o úspěšnosti provedených akcí. Klepněte na tlačítko **Zavřít** (Close) a pokud se objeví dialogové okno s informací o zpoždění replikací, klepněte na tlačítko **OK**.

Sdílení dat v síti

Sdílení dat bylo vždy v operačních systémech Windows vcelku jednoduchou záležitostí (někdy až moc) a nejinak je tomu i ve Windows Server 2008.

V porovnání s předchozí verzí operačního systému došlo ve sdílení dat k několika málo změnám, které se mohou jevit jako vcelku zanedbatelné, avšak z hlediska správy a zabezpečení svůj význam rozhodně mají.

Následující hotová řešení popisují základní postupy pro sdílení a zabezpečení dat s přihlédnutím k novinkám ve Windows Server 2008.

Vytvoření sdílené složky

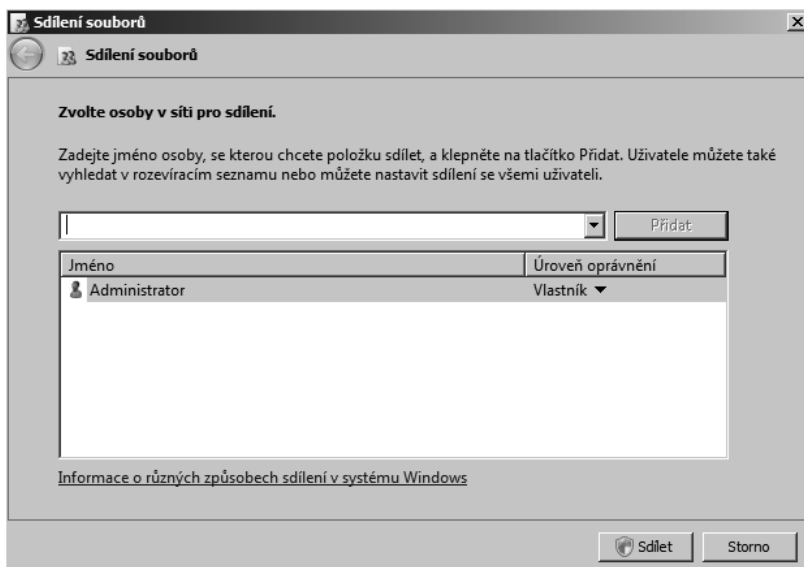
Složka se stane sdílenou v okamžiku, kdy k ní umožníme přístup po síti, a to zpravidla dalším uživatelům systému.

V operačním systému Windows Server 2008 doznala tato prostá operace dvou zásadních změn: První z nich jsou dialogová okna pro sdílení, která se mohou zdát na první pohled poněkud nepřehledná, a druhou je nastavení výchozích oprávnění pro sdílení – již zde není nastaveno oprávnění ke čtení pro skupinu *Everyone*, ale v seznamu řízení přístupu figuruje pouze vlastník složky.

Při sdílení složky postupujte takto:

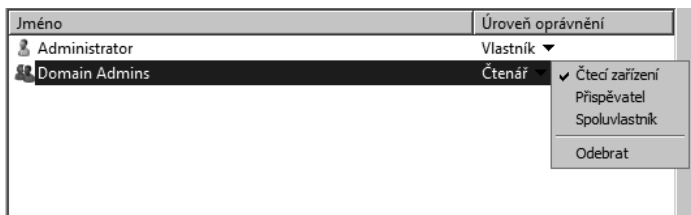
1. V okně Průzkumníka označte složku, kterou chcete sdílet, klepněte na ni pravým tlačítkem myši a zvolte položku **Sdílet** (Share).
2. Zobrazí se dialogové okno s výchozími oprávněními (viz obrázek 8.5), kde můžete klepnout na tlačítko **Sdílet** (Share), čímž složku nasdílíte s použitím výchozích oprávnění.

Nebo v tomto dialogovém okně zadejte název skupiny či uživatele a klepněte na tlačítko **Přidat** (Add). Takto zadaná skupina nebo uživatel získá oprávnění ke čtení, pokud neučíté jinak.



Obrázek 5.8 Dialogové okno pro nasdílení složky. Zde jsou vidět výchozí oprávnění.

Jestliže se rozhodnete dát přístup ke sdílené složce další skupině nebo uživatelům, klepněte pak vedle jejich názvu v seznamu na drobnou šipku dolů a vyberte z nabídky jednu z úrovní oprávnění (viz obrázek 5.9).



Obrázek 5.9 Seznam možných oprávnění ke sdílené složce

Když jste s nastavením oprávnění spokojeni, klepněte na tlačítko **Sdílet** (Share) a od tohoto okamžiku bude složka sdílená.

Publikování sdílené složky v Active Directory

Dokud ve vaší síti existuje jen několik málo serverů a sdílené složky se počítají v řádu desítek, mohou se v nich uživatelé orientovat ještě poměrně snadno.

Nezřídka jsou však v síti stovky sdílených složek a v takovém případě již hledání „té pravé“ může být poněkud složitější.

Naštěstí existuje možnost tzv. publikovat sdílenou složku v Active Directory, díky čemuž budou moci uživatelé prohledat celou síť a vybrat si potřebnou složku, nebo dokonce vyhledat složku pomocí klíčových slov.

Při zveřejnění složky v Active Directory postupujte takto:

1. Klepněte na tlačítko **Start** → **Nástroje pro správu** (Administrative Tools) → **Správa počítače** (Computer Management).
2. V levém panelu konzoly rozbalte uzel **Systémové nástroje** (System Tools) → **Sdílení složky** (Shared Folders) → **Sdílené položky** (Shares).
3. V pravém panelu pak vyberte sdílenou složku, kterou chcete publikovat, klepněte na ni pravým tlačítkem myši a zvolte **Možnosti** (Properties).

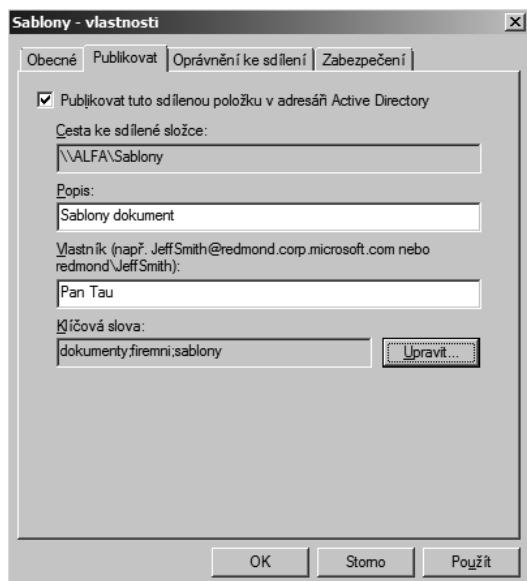
V dialogovém okně s vlastnostmi sdílené složky přepněte na záložku **Publikovat** (Publish) a zaškrtněte možnost **Publikovat tuto sdílenou položku v adresáři Active Directory** (Publish this share in Active Directory) (viz obrázek 5.10).

Do pole **Popis** (Description) můžete zadat nějakou srozumitelnou popisnou informaci, která bude uživatelům nápomocná při hledání konkrétní složky.

V poli **Vlastník** (Owner) se také vyplatí zadat jméno osoby, která je zodpovědná za přidělování oprávnění k přístupu do dané složky. Uživatelé se tak na tuto osobu budou moci obracet se svými požadavky o přístup (jen jeden z příkladů využití).

V poli **Klíčová slova** (Keywords) pak můžete zadat klíčová slova, která budou pro danou složku charakteristická, tedy např. *nástroje*, *administrace*, *obnova*. Uživatel pak bude moci vyhledávat složky na podobném principu jako v internetovém vyhledávači – zadá klíčová slova a bude mu zobrazen seznam složek, které splňují kritéria vyhledávání.

Klepnutím na tlačítko **OK** dialogové okno zavřete a tím je složka publikována.



Obrázek 5.10 Dialogové okno s vlastnostmi pro publikování sdílené složky v Active Directory

Zajištění sdílené složky

Sdílení složky samo o sobě obsahuje několik dílčích akcí, které je třeba provést a také několik kritérií, která bychom měli při sdílení vzít v potaz (na prvním místě funkčnost a bezpečnost).

V operačním systému je k dispozici nová administrativní konzola s názvem **Správa sdílených složek a úložišť** (Share and Storage Management), z které můžete spustit průvodce zajištěním složky. Ten se vás postupně zeptá na všechny informace, které by měl mít systém k dispozici pro efektivní sdílení složky a budete tak mít jistotu, že jste žádný krok nevynechali.

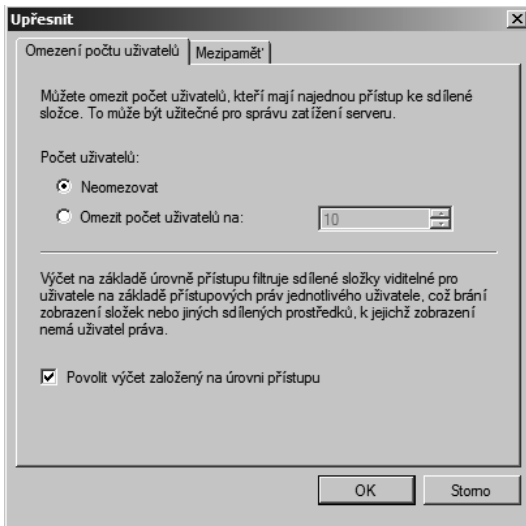
1. Klepněte na tlačítko **Start** → **Nástroje pro správu** (Administrative Tools) → **Správa sdílených složek a úložišť** (Share and Storage Management). V panelu akcí klepněte na tlačítko **Zajistit sdílenou složku** (Provision Storage), načež se spustí průvodce zajištěním sdílené složky.
2. Na první obrazovce průvodce klepnutím na tlačítko **Procházet** (Browse) vyberte složku, se kterou chcete pracovat (nemusí být v tomto okamžiku ještě sdílená), a klepněte na tlačítko **Další** (Next).
3. Na obrazovce **Oprávnění NTFS** (NTFS Permissions) rozhodněte, zda chcete měnit stávající oprávnění NTFS nastavená na dané složce nebo je ponecháte tak, jak jsou. Každopádně jejich alespoň letmá kontrola vás nebude stát mnoho času a protože složku zajišťujeme z důvodu vyššího zabezpečení, je na místě kontrolu provést.
Po nastavení oprávnění NTFS klepněte na tlačítko **Další** (Next).
4. Na obrazovce **Protokoly sdílení** (Share Protocols) vyberte, zda se pro sdílení složky použije protokol SMB nebo NFS (pro operační systémy Windows i pro koexistenci s Linuxovými servery bude vhodný protokol SMB).
Na této obrazovce také zadejte název sdílení, tedy název, pod kterým se bude složka zobrazovat v síti ostatním uživatelům.
Po nastavení těchto vlastností klepněte na tlačítko **Další** (Next).
5. Nyní se objeví obrazovka se zdánlivě nepodstatnými nastaveními, avšak je zde skryto jedno tlačítko, které se může ukázat jako velice užitečné.
Na obrazovce **Nastavení protokolu SMB** (SMB Settings) můžete zadat popis sdílené složky, důležitější nastavení však najdete v dialogovém okně, které se zobrazí po klepnutí na tlačítko **Upřesnit** (Advanced), (viz obrázek 5.11).

Ve výchozím stavu je zde povoleno neomezené množství uživatelů připojených v jednom okamžiku, ale pokud je například tato složka umístěna na serveru se slabším diskovým subsystémem, může se hodit možnost počet uživatelů omezit.

Ono výše zmíněné užitečné nastavení se skrývá v podobě nenápadného zaškrťovacího tlačítka s názvem **Povolit výčet založený na úrovni přístupu** (Enable access-based enumeration).

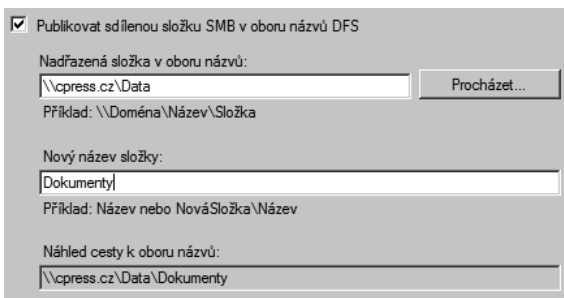
Když jej zaškrtnete, uvidí uživatelé přistupující k této sdílené složce pouze ty podsložky a soubory, k nimž mají oprávnění NTFS pro čtení. Ostatní položky ve složce zůstanou skryty a nebudou tak v uživatelích vyvolávat někdy nežádoucí zvědavost.

Nastavte tedy možnosti dle svých preferencí, zavřete dialogové okno klepnutím na tlačítko **OK** a poté klepněte na tlačítko **Další** (Next).



Obrázek 5.11 Dialogové okno pro upřesnění nastavení protokolu SMB

6. Následující obrazovka slouží k nastavení oprávnění SMB. Vyberte zde jedno z předdefinovaných oprávnění nebo zvolte možnost **Uživatelé a skupiny mají vlastní oprávnění ke sdílení** a klepnutím na tlačítko **Upřesnit** (Advanced) nadefinujte vlastní oprávnění. Poté klepněte na tlačítko **Další** (Next).
7. Další dvě obrazovky jsou určeny pro nastavení kvót a blokování ukládání souborů. Protože je jim věnován prostor v jiných řešeních v této kapitole, nebudeme se zde jimi zabývat a přeskočíme je klepnutím na tlačítko **Další** (Next) (dvakrát).
8. Máte-li nasazen v síti systém souborů DFS, umožňuje obrazovka s názvem **Publikování v oboru názvů DFS** publikovat aktuální složku tak, aby byla dostupná v rámci systému DFS. V takovém případě zadejte název nadřazené složky systému DFS a nový název této sdílené složky určený pro publikování (příklad viz obrázek 5.12). Po zadání názvů klepněte na tlačítko **Další** (Next).



Obrázek 5.12 Zadání názvů pro publikování složky v systému DFS

7. Nyní už jen zkontrolujte zadané údaje, klepněte na tlačítko **Vytvořit** (Create) a v případě úspěšného dokončení zavřete průvodce tlačítkem **Zavřít** (Close).

Zabezpečení pomocí oprávnění SMB

Z důvodu lepší kontroly nad tím, kdo má přístup k jakým objektům souborového systému, se může při vyhodnocování udělení přístupu použít kromě oprávnění NTFS ještě další mechanismus. Tím jsou oprávnění protokolu SMB (tedy protokolu používaného pro přístup ke sdíleným složkám po síti).

Pokud tedy máme takovýto „dvojitý metr“, která oprávnění definitivně určují, zda uživatel bude nebo nebude mít přístup k požadované složce či souboru?

Obecně lze na tuto otázku odpovědět takto: pokud se při vyhodnocení přístupu vyhodnocují oprávnění NTFS a oprávnění SMB, použijí se ta více restriktivní.

Následující příklad by měl snad vše vysvětlit (velmi zjednodušeně):

Mějme například uživatele Josefa, který chce pracovat s dokumenty uloženými na serveru ve sdílené složce s názvem Data.

Na této sdílené složce jsou nastavena oprávnění SMB tak, že Josef má přístup pro čtení. Oprávnění NTFS na téže složce jsou nastavena tak, že Josef má plný přístup (tedy měnit, mazat, zapisovat, číst, atd.).

V souladu s výše uvedeným principem se použijí ta restriktivnější oprávnění, takže v konečném důsledku bude Josef moci dokumenty ve sdílené složce pouze číst.

Fungovalo by to i obráceně: kdyby na složce Data měl Josef plná oprávnění SMB a NTFS oprávnění jen pro čtení, opět by mohl dokumenty jen číst.

Chceme-li tedy, aby nějaký uživatel nebo skupina uživatelů mohla provádět s daty nějaké operace, musíme se ujistit, aby byla správně nastavena jak oprávnění pro sdílení (SMB), tak oprávnění NTFS.

Když tento princip ještě zjednoduším – aby uživatel mohl něco dělat s daty, musí projít dvěma pomyslnými „sítí“. Pokud neprojde libovolným z nich, nebude mu oprávnění k provedení dané operace uděleno.

Mějte však na paměti, že **oprávnění pro sdílení (SMB) se aplikují pouze na uživatele, kteří k datům ve sdílené složce přistupují po síti, tzn. pomocí síťové cesty UNC** (např. `\\server\data`)!

Občas tedy může být poněkud matoucí, že pokud jste přihlášení na nějakém počítači a „proklikáte“ se ke složce přes např. **Počítač** → **Místní disk (C:)** → **Název sdílené složky**, tak přístup mít budete, zatímco když se z téhož počítače pokusíte přistoupit do téže složky pomocí síťové cesty (`\\server\data`), přístup nebude udělen. Ujistěte se tedy, že máte povolen konkrétní typ přístupu jak v oprávněních SMB, tak i v oprávněních NTFS.

Výčet založený na úrovni přístupu

Toto nastavení již bylo zmíněno v postupu nazvaném *Zajištění sdílené složky*, ale pro případ, že byste potřebovali povolit či zakázat výčet založený na úrovni přístupu jednoduše a rychle, bez sáhodlouhého průvodce, můžete to udělat takto:

1. Klepněte na tlačítko **Start** → **Nástroje pro správu** (Administrative Tools) → **Správa sdílených složek a úložišť** (Share and Storage Management).

2. V seznamu sdílených složek vyberte tu, na které chcete výčet povolit. Klepněte na ni pravým tlačítkem myši a vyberte možnosti **Vlastnosti** (Properties).
3. V dialogovém okně s vlastnostmi sdílené složky klepněte na tlačítko **Upřesnit** (Advanced). Ve spodní části dialogového okna pak povolte položku **Povolit výčet založený na úrovni přístupu** (Enable Access Based Enumeration).

Výpis sdílených složek pomocí grafického rozhraní

Mít přehled o sdílených složkách je jednou ze svatých povinností každého administrátora. Mohou totiž představovat atraktivní a někdy i velmi snadno průchozí bod pro případného útočníka. Uvedu zde tedy několik příkladů, jak můžeme získat seznam sdílených složek, a to jak na místním, tak i vzdáleném počítači:

1. Klepněte na tlačítko **Start** → **Nástroje pro správu** (Administrative Tools) → **Správa počítače** (Computer Management).
2. V levém panelu pak rozbalte uzel **Systémové nástroje** (System Tools) → **Sdílené složky** (Shared Folders) → **Sdílené položky** (Shares).

Takto uvidíte seznam všech sdílených složek na tomto počítači, a to včetně těch, které jsou skryté nebo tzv. administrativní.

Výpis sdílených složek pomocí příkazového řádku

Pro zobrazení sdílených složek místního počítače můžete použít starý dobrý příkaz *net share*. Ten slouží ke sdílení složek, ale zadán takto bez parametrů vám poskytne výpis složek sdílených na místním počítači.

Pokud byste chtěli dosáhnout téhož s použitím PowerShellu, tak zadejte tento příkaz (v prostředí PowerShellu):

```
PS C:\> get-wmiobject win32_share
```

Pro výpis sdílených složek vzdáleného počítače bychom tento příkaz trochu pozměnili:

```
PS C:\> get-wmiobject win32_share -computer nazev_pocitace
```

Kromě těchto možností, které máme k dispozici přímo v operačním systému, pak doporučuji vynikající a jednoduchý nástroj *ShareEnum* od společnosti Sysinternals. *ShareEnum* je součástí balíku Sysinternals Suite, ale lze jej stáhnout i samostatně. Jak balík, tak samostatnou aplikaci můžete stáhnout na této adrese:

<http://technet.microsoft.com/en-us/sysinternals/bb842062.aspx>

Celá sada má pouhých 9,8 MB a nástroje v ní jsou k nezaplacení (a paradoxně zdarma), přičemž tyto nástroje jsou podporovány i Microsoftem (který ostatně firmu Sysinternals koupil).

ShareEnum je vynikající v tom, že umožňuje zadat rozsah adres IP nebo název domény, poté prohledá všechny dostupné počítače z tohoto rozsahu a vygeneruje přehledný seznam sdílených složek na všech počítačích, a to dokonce včetně oprávnění (která odsud z jednoho místa můžete rovnou změnit).

Mapování síťového disku pomocí grafického rozhraní

Namapování síťového disku znamená, že na místním počítači si připojíme sdílenou složku jiného počítače a tato složka se nám bude jevit podobně jako místní disk (bude dostupná prostřednictvím písmene jednotky).

Způsobů pro mapování je několik:

1. Spustíte **Průzkumníka Windows** (Windows Explorer), v jeho okně pak klepněte na nabídku **Nástroje** (Tools) → **Připojit síťovou jednotku** (Map Network Drive).
2. Zobrazí se dialogové okno, ve kterém můžete vybrat písmeno jednotky, které bude použito pro síťový disk, a také zde zadejte síťovou cestu UNC ke sdílené složce, tedy např. `\\server\složka`.

Můžete také použít tlačítko **Procházet** (Browse), jenž vám umožní zobrazit počítače v síti a jejich sdílené složky. Tato funkce však bude pracovat jen tehdy, máte-li povoleno **Zjišťování sítě** (Network Discovery) v **Centru síťových připojení a sdílení** (Network and Sharing Center).

V případě potřeby můžete pomocí tohoto nástroje pro mapování nastavit, aby se při připojování vzdálené sdílené složky použila oprávnění jiného uživatele, než je ten aktuálně přihlášený. Stačí klepnout na odkaz **Připojit se pomocí jiného uživatelského jména** (Connect using a different user name).

Mapování síťového disku pomocí příkazu nebo skriptu

U mapování síťových disků je často žádoucí, aby k němu docházelo automaticky, a to v okamžiku přihlášení uživatele.

Můžete tedy použít např. následující příkaz, ať už zadaný v příkazovém řádku nebo umístěný v dávkovém souboru, který se vykoná při přihlášení:

```
C:\>net use x: \\server\složka
```

Písmeno *x*: zde znamená písmeno jednotky, které se použije a za písmenem následuje síťová cesta UNC ke sdílené složce.

Pokud byste chtěli zakomponovat mapování síťových disků do přihlašovacího skriptu v jazyce VBScript, můžete použít třeba tuto konstrukci:

```
Dim oNetwork
Set oNetwork = CreateObject("WScript.Network")
oNetwork.MapNetworkDrive "X:", "\\server\složka"
```

Zabezpečení přístupu k datům pomocí oprávnění NTFS

Správa oprávnění pro přístup k prostředkům nás provází operačními systémy už řadu let. Nedá se říci, že by se s příchody nových verzí měnilo zabezpečení dat mílovými kroky. Spíše se vždy jedná o drobné až kosmetické změny, které ale na hlavních principech nic nemění.

Tyto principy, resp. potřeby z hlediska správy datových úložišť a umožnění přístupu k těmto datům na víceuživatelských systémech bychom mohli shrnout asi do této podoby:



1. Možnost ukládat data (dnes už tento bod může vyvolat pobavený úsměv, ale ti z vás, kteří stejně jako já neměli svého času jiné úložiště pro své drahocenné bajty než operační paměť RAM o velikosti 24 kB, 48 kB, 64 kB, 128 kB a později pak na svých Amigách s 512 MB až 1 MB jistě chápou, o čem je řeč.)
2. Možnost ukládat data dlouhodobě – také si s nutnou dávkou nostalgie povzdechnu nad tím, že dnes koupíte 1 DVD o kapacitě 4,7 GB za několik korun, zatímco má první disketa o kapacitě 880 kB stála kolem 50 Kčs a její kapacita pro mne byla téměř ekvivalentem nekonečných virtuálních světů.
Dnes, kdy terabajtové disky stojí méně než trošku kvalitnější boty, už rozhodně nikdo kvůli pár gigabajtům ronit slzy nebude. A modlit se, aby náhodou nedošlo k výpadku proudu, protože máte ve svém ZX Spectru právě napsaný program, který potřebujete ještě pár hodin používat a nemáte jej kam uložit, také ne.
3. Dát data k dispozici jen těm subjektům, které jsou tzv. ověřeny a autorizovány.

Zabezpečení pomocí oprávnění NTFS obecně

Oprávnění NTFS jsou jedním ze základních pilířů zabezpečení dat na platformě operačních systémů firmy Microsoft.

Někdo na ně nadává, někdo jimi opovrhuje, ale velmi mnoho lidí je vůbec neumí používat. Velmi často se setkávám s problémy typu „uživatel se dostane tam, kam by neměl“ nebo naopak „uživatel se nedostane tam, kam by měl“.

Přitom je tento systém zcela jednoduchý a transparentní, stačí se řídit pravidly a postupy uvedenými v následujícím textu.

Principy oprávnění NTFS

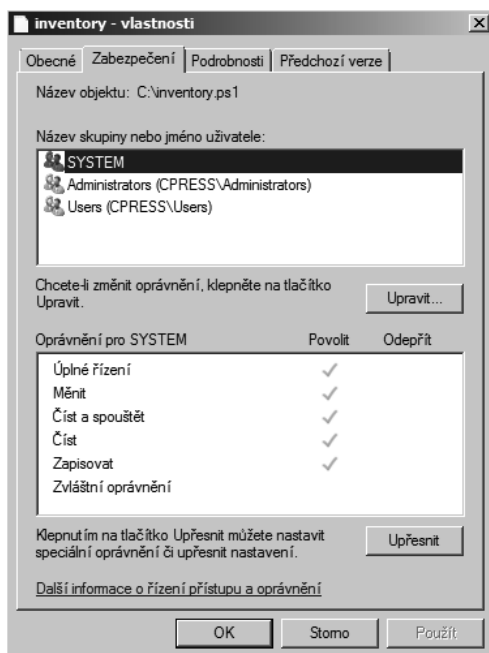
1. Pokud nejsou oprávnění konfliktní, jsou kumulativní.
To znamená, že jestliže je např. uživatel členem skupiny A, která má oprávnění pro zápis a tento uživatel je také členem skupiny B, která má oprávnění jen pro čtení, výslednými oprávněními tohoto uživatele bude součet všech oprávnění získaných skrze členství v různých skupinách – tedy čtení i zápis.
2. Explicitní odepření některého oprávnění má vždy nejvyšší prioritu.
V praxi to znamená, že pokud je uživatel členem libovolného množství skupin, které mají nějaké oprávnění uděleno (např. smí číst) a tentýž uživatel je členem byť i jediné skupiny, která má explicitně odepřené oprávnění (deny – odepřít), pak toto odepření přístupu „přebije“ všechna povolení přístupu.
Je to z toho důvodu, že jak už název napovídá – explicitní odepření přístupu je něco, co nevznikne samo o sobě, ale musí jej někdo nastavit. Nikdy se nepoužívá jako výchozí oprávnění, a proto je považováno za směrodatnějšího než běžná, automaticky udělená oprávnění.
3. Oprávnění NTFS jsou děděna.
Vytvoříme-li někde soubor nebo složku, pak tento objekt zdědí nastavení oprávnění NTFS od nadřazené složky.
Chceme-li pak tato zděděná oprávnění změnit, musíme dědičnost na daném objektu vypnout.

Změna oprávnění NTFS a vypnutí dědičnosti

Princip nastavování a používání oprávnění NTFS se oproti předchozím systémům nikterak nezměnil. Dialogová okna vypadají trošku odlišně a možná méně intuitivně.

Následující postup popisuje změnu oprávnění NTFS a vypnutí dědičnosti z nadřazené složky.

1. Klepněte pravým tlačítkem myši na objekt (soubor nebo složka), na kterém chcete změnit oprávnění. Z místní nabídky vyberte možnost **Vlastnosti** (Properties) a přepněte na záložku **Zabezpečení** (Security).
2. Měl by se vám naskytnout podobný pohled jako na obrázku 5.13.



Obrázek 5.13 Záložka Zabezpečení dialogového okna Vlastnosti souboru nebo složky

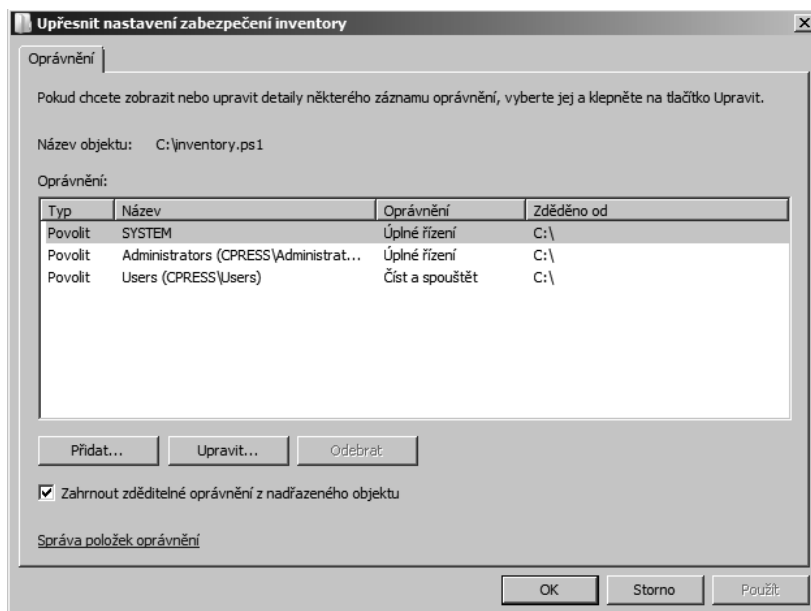
Na tomto obrázku vidíme vždy dvě důležité informace: V horní části je seznam objektů zabezpečení (jinými slovy uživatelů, počítačů nebo skupin), kterým byla na zkoumaném objektu udělena nějaká oprávnění. Kdo není uveden v tomto seznamu, nebude mít k danému objektu žádný druh přístupu (samozřejmě může být členem skupiny uvedené v seznamu, potom by přístup mít mohl).

Spodní část dialogového okna pak zobrazuje, jaká oprávnění byla nahoře vybranému objektu zabezpečení přidělena. Na obrázku 5.13 tedy vidíme, že např. skupina SYSTEM má oprávnění typu **Úplné řízení** (Full Control) a může tedy se zkoumaným souborem dělat vše, co se jí líbí.

Všimněte si jedné věci: ve spodní části dialogového okna ve sloupci **Povolit** (Allow) jsou zaškrťovací políčka sice zaškrtnutá, ale zneprístupněná (zašedlá). Znamená to snad, že uživatel, který toto dialogové okno zobrazil, nemá možnost měnit oprávnění?

Nikoliv. Znamená to toliko skutečnost, že tato oprávnění byla zděděna z nadřazené složky a pokud je chcete upravit, je zapotřebí vypnout dědičnost, což je popsáno v následujícím kroku.

3. Klepněte na tlačítko **Upřesnit** (Advanced) a v dalším okně na **Upravit** (Edit). Zobrazí se dialogové okno (viz obrázek 5.14), kde zrušte zaškrtnutí v poli s názvem **Zahrnout zděditelné oprávnění z nadřazeného objektu** (Include inheritable permissions from the object's parent).



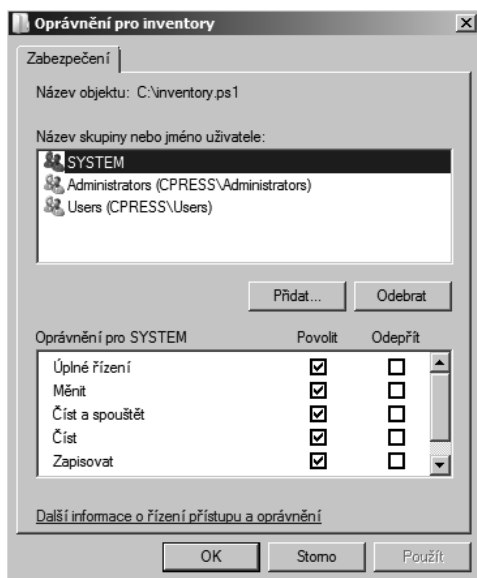
Obrázek 5.14 Zaškrťovací políčko pro vypnutí dědění oprávnění

4. Po zrušení zaškrtnutí budete dotázáni, zda chcete stávající oprávnění **Kopírovat** (Copy) či **Odebrat** (Remove).

Pokud vyberete **Kopírovat** (Copy), budou na objektu ponechána stávající oprávnění a vy budete mít možnost je pozměnit podle potřeby.

Vyberete-li však možnost **Odebrat** (Remove), budou odebrána všechna stávající oprávnění a budete je muset sami nadefinovat. V tomto případě postupujte tedy raději s určitou dávkou opatrnosti, abyste si například nesmazali poněkud delší a složitější seznam řízení přístupu, který byste pak pracně museli vytvářet znovu.

5. Nyní klepnutím na tlačítko **OK** (dvakrát) zavřete dialogová okna tak, abyste viděli ono výchozí – tedy vlastnosti objektu, resp. záložka **Zabezpečení** (Security). Zde pak klepnutím na tlačítko **Upravit** (Edit) můžete povolit, odebrat či odeprít přístup pro jednotlivé skupiny nebo uživatele (viz obrázek 5.15).



Obrázek 5.15 Dialogové okno pro udělení, odebrání či odepření oprávnění uživatelům nebo skupinám

Poznámka: Z obrázku 5.15 může být patrné, že správa oprávnění se řídí třístavovou logikou. Jak bylo dříve uvedeno, oprávnění lze povolit, odebrat (jinými slovy nepovolit) či odepřít. Jaký je rozdíl mezi nepovolením a odepřením oprávnění?

Dost značný. Vzpomínáte na základní pravidla, kterými se řídí zabezpečení systému souborů NTFS? Pokud někomu pouze neudělíme oprávnění, může tento uživatel nebo skupina získat přístup pomocí členství ve skupině, která toto oprávnění má povoleno.

Pokud však někomu oprávnění výslovně odepřeme (Deny), tak tento uživatel nebo skupina nebude mít dané oprávnění za žádných okolností, ani jej nezíská členstvím v nějaké skupině (i kdyby to byla skupina Super-Omni-Mega-Administrators).

Udělení přístupu prostřednictvím oprávnění NTFS

Předchozí postup možná poněkud komplikovaně (zato však důkladně) popsal postup pro změnu oprávnění NTFS.

Chcete-li prostě a jednoduše udělit nějaké oprávnění uživateli nebo skupině, zde je stručný postup:

1. Klepněte pravým tlačítkem myši na souboru či složce, ke kterým chcete udělit oprávnění a z místní nabídky vyberte možnost **Vlastnosti** (Properties). V dialogovém okně pak přepněte na záložku **Zabezpečení** (Security).
2. Klepněte na tlačítko **Upravit** (Edit) a v dialogovém okně, které se nyní zobrazí, můžete pomocí tlačítek **Přidat** (Add) a **Odebrat** (Remove) přidávat či odebrat objekty zabezpečení, tedy uživatele a skupiny.

Ve spodní části dialogového okna pak můžete zaškrtnutím a rušením zaškrtnutí nastavovat jednotlivá oprávnění.

Zjištění skutečných oprávnění NTFS

Pravidla, kterými se řídí systém oprávnění NTFS, jsou sice prostá, avšak jejich nasazení v praxi může vyústit v někdy poněkud nepřehlednou a složitou situaci.

Například uživatel si stěžuje, že se nemůže dostat do nějaké složky, a administrátor se dušuje, že uživateli přístup nastavil.

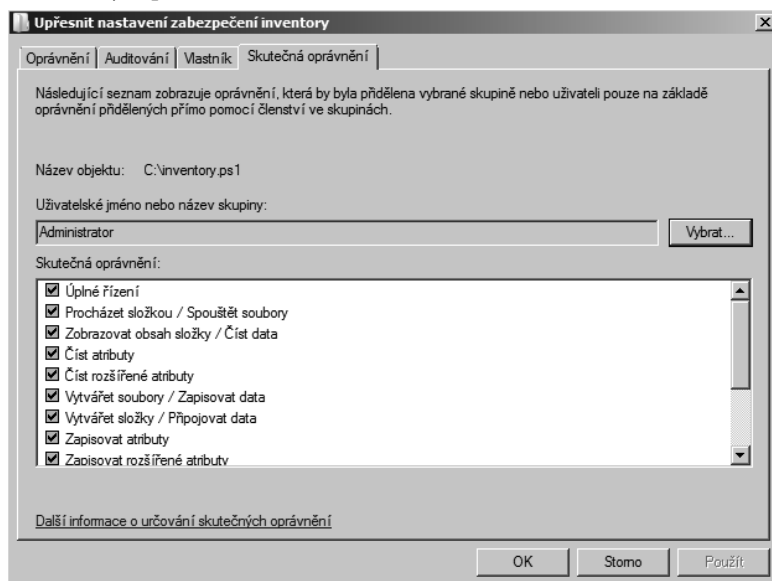
V okamžiku, kdy používáte desítky nebo stovky skupin zabezpečení a struktura dat na souborovém serveru má mnoho úrovní, přičemž někde se používá dědění, někde je dědění vypnuto, uživatel je členem desítek skupin, z nichž některá má taková, jiná zase onaká oprávnění – inu, zjistit, co skutečně může inkriminovaný uživatel se soubory dělat, by byla detektivní práce.

Naštěstí však existuje nástroj v podobě Skutečných oprávnění, který dokáže zobrazit výslednou sadu oprávnění udělených konkrétnímu uživateli či skupině. Používá se takto:

1. Klepněte pravým tlačítkem myši na soubor nebo složku, na kterých chcete zjistit efektivní oprávnění a vyberte možnost **Vlastnosti** (Properties). Následně pak přepněte na záložku **Zabezpečení** (Security).
2. Klepněte na tlačítko **Upřesnit** (Advanced) a přepněte na záložku **Skutečná oprávnění** (Effective permissions).

Nyní klepněte na tlačítko **Vybrat** (Select), zadejte název uživatele nebo skupiny a dialogové okno pro zadání názvu zavřete klepnutím na tlačítko **OK**.

Zobrazí se přehled skutečných oprávnění, tedy výsledek zohledňující veškeré členství ve skupinách a veškeré povolení, nepovolení a odeprání přístupu. Jinými slovy – toto je definitivní a rozhodující přehled (viz obrázek 5.16).



Obrázek 5.16 Přehled skutečných oprávnění nastavených na konkrétním souboru pro konkrétního uživatele

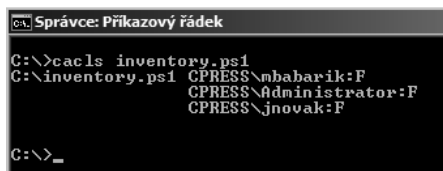
Zjištění a nastavení oprávnění pomocí příkazového řádku

V operačním systému Windows Server 2008 najdeme dva nástroje příkazového řádku pro nastavování nebo zjišťování oprávnění NTFS: *cacls.exe* a *icacls.exe*. *Cacls.exe* byl dostupný už ve starších verzích systému Windows a *icacls.exe* je vlastně jeho novější verzi a náhradou zároveň.

Tuto informaci vám ostatně potvrdí i výpis nápovědy k příkazu *cacls.exe*, kde je uvedeno, že *cacls.exe* se již nepoužívá a místo něj máte používat *icacls.exe*.

Přesto však můžeme příkaz *cacls.exe* používat i nadále. Jeho možnosti jsou sice vcelku skromné, ale podívejme se alespoň na základní použití:

Například chceme-li zobrazit aktuálně nastavená oprávnění na souboru s názvem *inventory.ps1*, použijeme nejjednodušší formu zápisu tohoto příkazu (příkaz i jeho výstup viz obrázek 5.17).

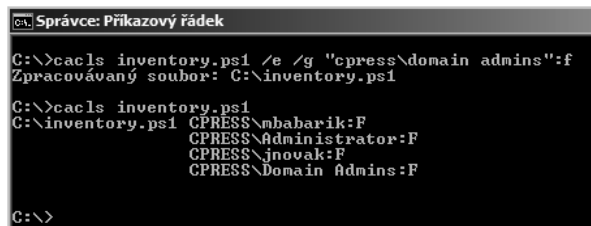


```

C:\>cacls inventory.ps1
C:\inventory.ps1 CPRESS\mbabarik:F
                  CPRESS\Administrator:F
                  CPRESS\jnovak:F
C:\>_
  
```

Obrázek 5.17 Výstup příkazu *cacls.exe*

Když bychom pak chtěli tato oprávnění změnit, mohli bychom použít zápis jako na obrázku 5.18. V uvedeném příkladu jsou skupině *Domain Admins* udělena oprávnění pro plné řízení (Full Control). Že byla oprávnění změněna, můžeme vidět na dalších řádcích ve výpisu.



```

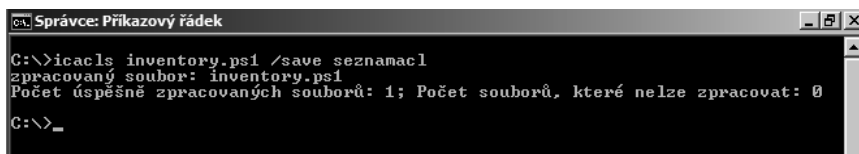
C:\>cacls inventory.ps1 /e /g "cpress\domain admins":f
Zpracovávaný soubor: C:\inventory.ps1
C:\>cacls inventory.ps1
C:\inventory.ps1 CPRESS\mbabarik:F
                  CPRESS\Administrator:F
                  CPRESS\jnovak:F
                  CPRESS\Domain Admins:F
C:\>
  
```

Obrázek 5.18 Změna oprávnění pomocí příkazu *cacls.exe* a jejich následné ověření

Nástroj *icacls.exe* nabízí poměrně široké a zajímavé možnosti využití. Umí například uložit seznam řízení přístupu do souboru a tento později použít pro obnovu nastavení oprávnění nebo nastavení těchto oprávnění na mnoha dalších souborech (hromadě).

Nápověda k příkazu *icacls.exe* je trochu delší než u jeho předchůdce, ale určitě doporučuji ji pročíst. Zde si uvedeme několik typických příkladů použití příkazu *icacls.exe*.

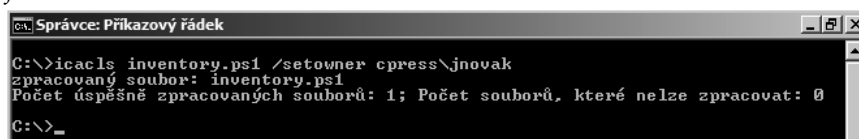
Příkaz uvedený na obrázku 5.19 uloží seznam řízení přístupu (ACL), který je nastaven na souboru *inventory.ps1* do souboru s názvem *seznamacl*. Tento seznam můžete později obnovit pomocí parametru */restore*.



```
ca: Správce: Příkazový řádek
C:\>icacls inventory.ps1 /save seznamacl
zpracovaný soubor: inventory.ps1
Počet úspěšně zpracovaných souborů: 1; Počet souborů, které nelze zpracovat: 0
C:\>_
```

Obrázek 5.19 Export seznamu řízení přístupu do souboru

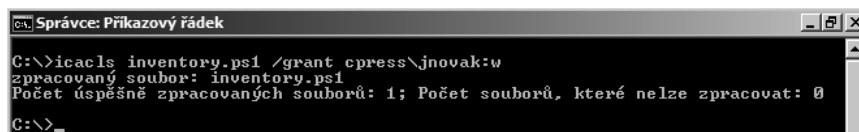
Příkaz na obrázku 5.20 nastaví, že vlastníkem souboru *inventory.ps1* se stane uživatel *cpress\jnovak*.



```
ca: Správce: Příkazový řádek
C:\>icacls inventory.ps1 /setowner cpress\jnovak
zpracovaný soubor: inventory.ps1
Počet úspěšně zpracovaných souborů: 1; Počet souborů, které nelze zpracovat: 0
C:\>_
```

Obrázek 5.20 Nastavení vlastníka souboru

Obrázek 5.21 pak znázorňuje udělení oprávnění k zápisu (w) na souboru *inventory.ps1* uživateli *cpress\jnovak*.



```
ca: Správce: Příkazový řádek
C:\>icacls inventory.ps1 /grant cpress\jnovak:w
zpracovaný soubor: inventory.ps1
Počet úspěšně zpracovaných souborů: 1; Počet souborů, které nelze zpracovat: 0
C:\>_
```

Obrázek 5.21 Příklad pro udělení oprávnění k zápisu

Převzetí vlastnictví souboru nebo složky

Občas se stane, že je odstraněn uživatelský účet, který jako jediný má přístup k nějakému souboru či složce. V takovém případě by k těmto datům nikdo neměl přístup, nikdo by je nemohl smazat či jinak modifikovat (ani administrátor).

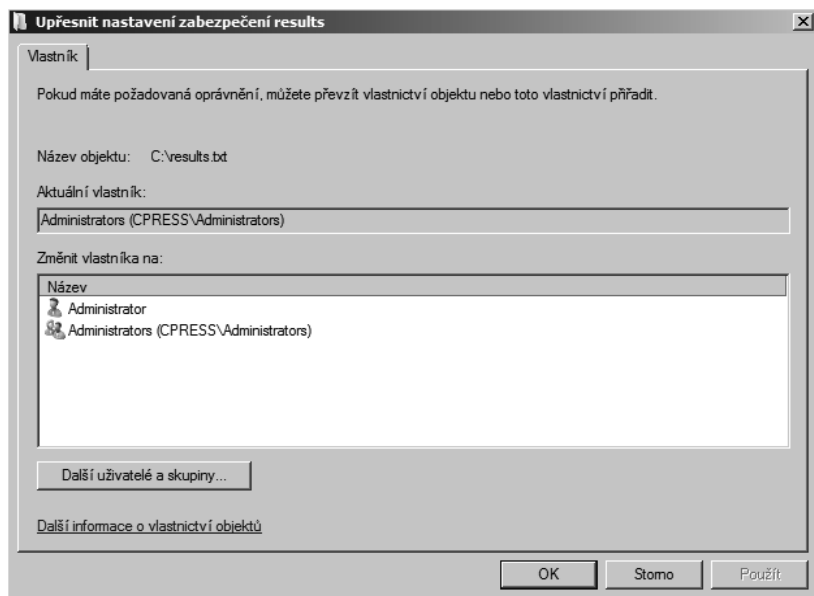
I když třeba administrátor nemá žádná oprávnění ke čtení nebo změně dat, může tzv. převzít vlastnictví souboru nebo složky. Jakmile se pak stane vlastníkem, může sám sobě nebo jinému uživateli přidělit taková oprávnění, jak uzná za vhodné.

Ono vlastnictví může být administrátorem také rovnou „přehozeno“ na jiného uživatele. Tento postup se hodí např. tehdy, když z firmy odchází zaměstnanec a nahradí jej někdo jiný. Správce jednoduše nastaví oprávnění tak, že se vlastníkem dat původního zaměstnance stane zaměstnanec nový.

Převzetí vlastnictví můžete provést takto:

1. Klepněte pravým tlačítkem myši na soubor nebo složku, jejíž vlastnictví chcete změnit a vyberte možnost **Vlastnosti** (Properties). V dialogovém okně vlastností pak přepněte na záložku **Zabezpečení** (Security).
2. Klepněte na tlačítko **Upravit** (Advanced) a přepněte na záložku **Vlastník** (Owner). Zde uvidíte aktuálního vlastníka. Chcete-li jej změnit, klepněte na tlačítko **Upravit** (Edit) a vyberte ze seznamu nového vlastníka (viz obrázek 5.22). Jestliže zde nevidíte požadovaného uživatele nebo skupinu, klepněte na tlačítko **Další uživatelé a skupiny** (Other users and groups).

Po výběru nového vlastníka můžete dialogová okna s oprávněními a vlastnostmi pozavírat.



Obrázek 5.22 Výběr nového vlastníka souboru

Tiskové služby

Implementace tiskových služeb v operačním systému Windows Server 2008 je vcelku povedená a dá se říci, že správu tiskáren a tiskového serveru zvládne každý, a to i bez nějakých expertních znalostí.

Následující text se zabývá výhradně správou serverové strany tiskového řešení a co se týká klientských počítačů, jsou zde uvedeny pouze informace pro hromadné nasazení tiskáren.

Stejně jako u každého jiného tématu i zde nemohu vzhledem k rozsahu knihy uvést všechny možnosti nastavování tiskáren. Nicméně snad shledáte následující hotová řešení užitečnými pro běžnou instalaci a správu.

Instalace role Tiskové služby

Aby server s operačním systémem Windows Server 2008 mohl plnohodnotně vykonávat funkci tiskového serveru, je nutné na něj nejprve nainstalovat roli **Tiskové služby** (Print Services).

1. Spustíte **Správce serveru** (Server Manager), v levém panelu označíte uzel **Role** (Roles) a následně v pravém panelu klepněte na odkaz **Přidat role** (Add Roles).
2. V průvodci můžete přeskočit úvodní stránku a na stránce s výběrem rolí zatrhněte **Tiskové služby** (Print Services). Klepněte dvakrát na tlačítko **Další** (Next) a na obrazovce s výběrem služeb rolí zatrhněte ty služby, které budete potřebovat a opět klepněte na tlačítko **Další** (Next) a **Nainstalovat** (Install).

- Po dokončení instalace klepněte na tlačítko **Zavřít** (Close). Neměl by být vyžadován restart.

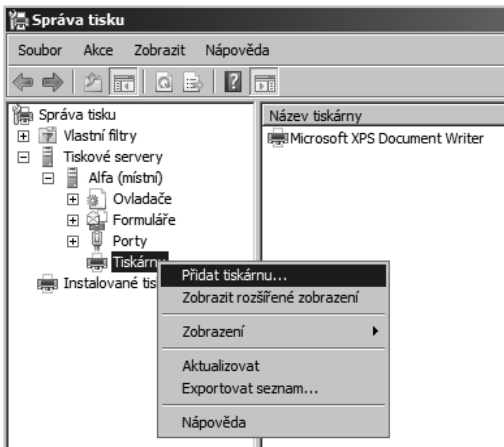
Nyní můžete pro správu tiskového serveru a tiskáren použít konzolu s názvem **Správa tisku** (Print Management), kterou najdete v **Nástrojích pro správu** (Administrative Tools).

Instalace tiskárny na tiskový server

Chcete-li přidat k tiskovému serveru další tiskárnu, která bude „spadat do jeho pole působnosti“, a bude tedy podléhat správě a nastavením provedeným na tomto serveru, postupujte takto:

- Klepněte na tlačítko **Start** → **Nástroje pro správu** (Administrative Tools) → **Správa tisku** (Print Management).

V konzole pak rozbalte uzel **Správa tisku** (Print Management) → **Tiskové servery** (Print Servers) → **Název serveru** → **Tiskárny** (Printers) (viz obrázek 5.23).



Obrázek 5.23 Tlačítko pro přidání tiskárny v konzole Správa tisku

- Klepněte pravým tlačítkem na uzel **Tiskárny** (Printers) a vyberte z místní nabídky položku **Přidat tiskárnu** (Add printer). Zobrazí se dialogové okno (viz obrázek 5.24), kde si můžete vybrat z několika možností.

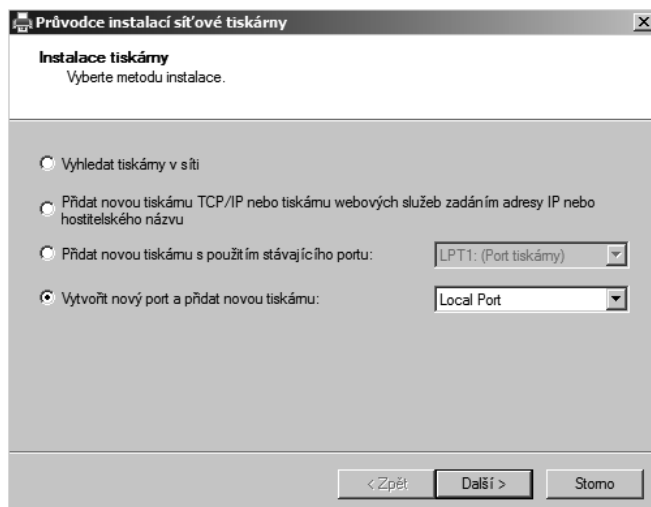
Vyhledat tiskárny v síti – tuto možnost použijte, pokud je přidávaná tiskárna síťová, tzn., podporuje komunikaci pomocí TCP/IP a chcete ji vybrat ze seznamu

Přidat novou tiskárnu TCP/IP nebo tiskárnu webových služeb zadáním adresy IP nebo hostitelského názvu – jestliže znáte název nebo adresu IP síťové tiskárny, která je již připojená k síti, můžete zvolit tuto možnost.

Přidat novou tiskárnu s použitím stávajícího portu – pokud již na serveru existuje port, můžete na něj připojit tiskárnu (např. na porty LPT a COM).

Vytvořit nový port a přidat novou tiskárnu – ta pravá volba, když potřebujete vytvořit úplně nový port a na něj nainstalovat novou tiskárnu. Jinými slovy: instalace tiskárny od nuly.

Vyberte tedy jednu z požadovaných možností a klepněte na tlačítko **Další** (Next). V tomto postupu použijeme poslední volbu, tedy **Vytvořit nový port a přidat novou tiskárnu** (Create new a new port and add a new printer).



Obrázek 5.24 Možnosti pro přidání nové tiskárny na tiskový server

3. Zadejte název portu (cokoliv, např. PRN1) a klepněte na tlačítko **OK**.
4. Vyberte, zda chcete použít některý z již nainstalovaných ovladačů, ovladač doporučený průvodcem nebo zcela nový ovladač (zde použijeme tuto volbu) a klepněte na tlačítko **Další** (Next).
5. Bude zobrazen seznam mnoha typů tiskáren. Jestliže je vaše tiskárna uvedena v tomto seznamu, můžete ji ze seznamu vybrat a klepnout na tlačítko **Další** (Next). Ale obecně bude určitě lepší dodat systému aktuálnější ovladače (volba **Z diskety** (Have Disk)).
6. Nyní zadejte název tiskárny (ideálně by měl reflektovat typ tiskárny nebo její umístění, aby ji uživatelé snadno našli a rozpoznali) a určete, zda má být sdílená.

Pokud ano, zadejte název, pod kterým bude sdílená tiskárna vidět v síti, a pokud je to žádoucí, zadejte také umístění tiskárny a její popis (ten je asi žádoucí vždy).

Umístění tiskárny by mělo odpovídat struktuře Active Directory, konkrétně lokalitám a podsítím. Podrobněji na toto téma později v této kapitole.

Po zadání těchto informací klepněte dvakrát na tlačítko **Další** (Next) a poté na tlačítko **Dokončit** (Finish).



Vytvoření fondu tiskáren

Tzv. fondy tiskáren slouží zejména k rozložení zátěže tam, kde je zapotřebí zpracovávat velké množství tiskových úloh v omezeném čase.

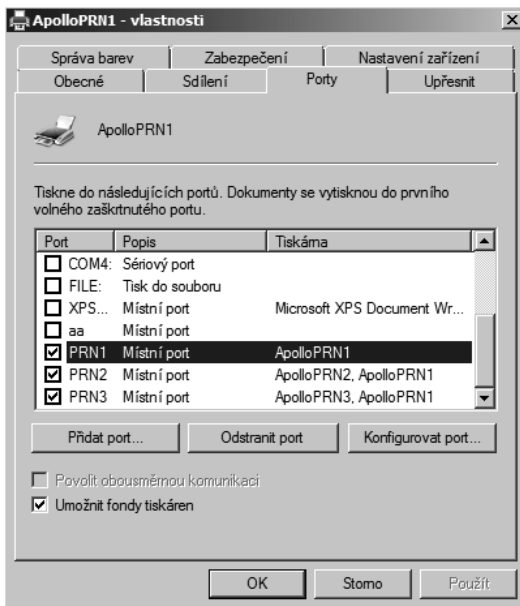
Fondy se v praxi používají tak, že uživatel vidí v síti jednu sdílenou tiskárnu, která však reprezentuje několik fyzických tiskáren připojených k serveru. Uživatel odešle tiskovou úlohu na sdílenou tiskárnu a tiskový server rozhodne, které fyzické tiskárně tuto úlohu přidělí.

Základním předpokladem pro vytvoření fondu tiskáren je tiskový server a několik tiskáren připojených k tomuto serveru. Tyto tiskárny by měly být shodného typu nebo alespoň používat shodné ovladače.

Také je důležité (i když ne nezbytně nutné), aby tiskárny patřící do jednoho fondu tiskáren byly umístěny v jedné místnosti. Uživatelé totiž nebudou vědět, která fyzická tiskárna jejich úlohu realizovala, a kdyby měli hledat své výtisky v několika kancelářích nebo dokonce budovách, jistě by nadšením nejásali.

Při vytvoření fondu tiskáren postupujte takto:

1. Klepnutím na tlačítko **Start** → **Nástroje pro správu** (Administrative Tools) → **Správa tisku** (Print Management) spusťte konzolu pro správu tisku. Přidejte tiskárny, které mají být součástí fondu tiskáren, na tiskový server. V tomto okamžiku bude mít každá z nich svůj port.
2. V konzole **Správa tisku** (Print Management) rozbalte uzel **Správa tisku** (Print Management) → **Tiskové servery** (Print Servers) → **Název Serveru** → **Tiskárny** (Printers). Klepněte pravým tlačítkem na jednu z tiskáren fondu a z místní nabídky vyberte možnost **Vlastnosti** (Properties).
3. V dialogovém okně s vlastnostmi tiskárny přepněte na záložku **Porty** (Ports) a zaškrtněte políčko **Umožnit fondy tiskáren** (Enable printer pooling). Potom v tomtéž okně zaškrtněte všechny porty tiskáren, které mají patřit do fondu (viz příklad na obrázku 5.25).



Obrázek 5.25 Umožnění fondu tiskáren a přidání portů do fondu

Všimněte si, že tiskárny ApolloPRN2 a ApolloPRN3 mají za svým názvem ještě ApolloPRN1. Toto je název, pod kterým bude fond tiskáren dostupný uživatelům.

Nyní je fond tiskáren připraven k použití. Stačí, aby si uživatelé na klientských stanicích přidali tuto virtuální sdílenou tiskárnu, a mohou na ni začít odesílat tiskové úlohy.



Vypis CD: 05 / 2

Instalace tiskárny na klientský počítač pomocí skriptu

V operačním systému Windows Server 2008 je několik možností pro mapování sdílených tiskáren tiskového serveru na uživatele nebo počítače: pomocí přihlašovacího nebo spouštěcího skriptu, pomocí zásad skupiny a pomocí předvoleb zásad skupiny. Podívejme se na všechny tyto postupy.

První způsob je asi nejméně pohodlný a vyžaduje alespoň minimální znalost skriptovacího jazyka, jakým je např. VBScript. V něm by mapování tiskárny mohlo vypadat třeba takto:

```
Dim oNetwork
Set oNetwork = CreateObject("WScript.Network")
oNetwork.AddWindowsPrinterConnection "\\server\tiskarna"
```

V praxi a zejména při nasazení na rozlehlelé síti jsou tyto skripty však mnohem delší a složitější. Můžeme například použít jeden přihlašovací skript v objektu zásad skupiny propojeném na celou doménu, přičemž v tomto skriptu dojde k vyhodnocení členství uživatele ve skupinách a podle toho se tomuto uživateli tiskárny namapují.

Kromě toho by měl solidní skript také prohledat klientský počítač na již existující připojené tiskárny a samozřejmě by také měl být schopen ošetřit případné chyby při mapování (např. nedostatečná oprávnění uživatele na tiskárně, nedostupná síťová cesta, atd.).

Ve výsledku by tedy výše uvedený mini-skript mohl mít s přehledem 200 řádků. A co si budeme nalhávat, není to zrovna nejpřehlednější a nejflexibilnější systém (i když na druhou stranu vše je napsáno na jednom místě).



Instalace tiskárny na klientský počítač pomocí zásad skupiny

Tato metoda je vhodná zejména tam, kde struktura organizačních jednotek věrně odráží geografické rozložení organizace. Abych byl konkrétnější – dejme tomu, že sedí vždy několik uživatelů v kanceláři a my máme pro každou takovou skupinku uživatelů vytvořenou organizační jednotku.

Nebo jiná varianta: máme organizační jednotky vytvořené podle geografického rozmístění počítačů.

Taková struktura organizačních jednotek však není ideální a je použitelná jen na nevelkých a nepříliš dynamických sítích nebo naopak u movitějších firem, které dávají uživatelům k dispozici velkokapacitní tisková zařízení umístěná v uživatelům známých místnostech.

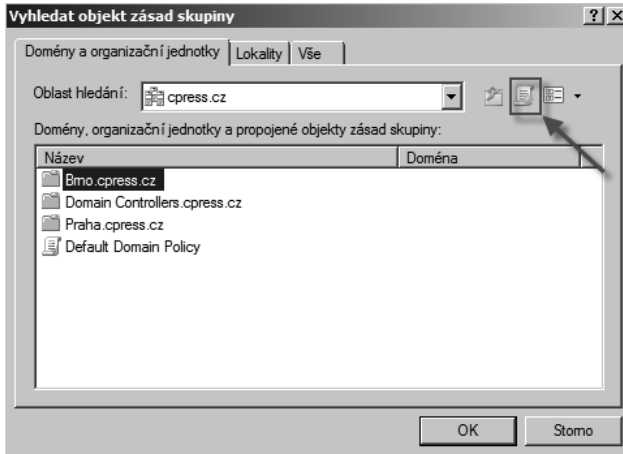
Pro instalaci tiskáren pomocí zásad skupiny existují dva odlišné postupy, oba však vedou k identickému výsledku a liší se pouze v tom, jak je „naklikáte“. Můžete to zkusit třeba takto:

1. Klepněte na tlačítko **Start** → **Nástroje pro správu** (Administrative Tools) → **Správa tisku** (Print Management).

V levém panelu konzoly rozbalte uzel **Správa tisku** (Print Management) → **Tiskové servery** (Print Servers) → **Název serveru** → **Tiskárny** (Printers).

2. Vyberte tiskárnu, kterou chcete instalovat na klientské počítače, klepněte na ni pravým tlačítkem a vyberte možnost **Instalovat se zásadami skupiny** (Deploy with Group Policy). Nyní musíte určit, v kterém objektu zásad skupiny bude tato instalace tiskárny definována. Klepněte tedy na tlačítko **Procházet** (Browse) a zobrazí se dialogové okno **Vyhledat objekt zásad skupiny** (Browse for a Group Policy Object).

Zde můžete procházet doménovou strukturu a vybrat existující objekt zásad skupiny nebo vytvořit nový pomocí tlačítka vyznačeného na obrázku 5.26.



Obrázek 5.26 Dialogové okno pro vyhledání nebo vytvoření objektu zásad skupiny. Tlačítko označené šipkou slouží pro vytvoření objektu zásad.

V tomto příkladu vytváříme nový objekt zásad skupiny poklepáním na organizační jednotku *Brno.cpress.cz* a klepnutím na vyznačené tlačítko s názvem **Vytvořit nový objekt zásad skupiny** (Create New Group Policy Object). Objekt je pojmenován *Tiskárny – Brno*.

Až objekt najdete nebo vytvoříte, klepněte na tlačítko **OK**.

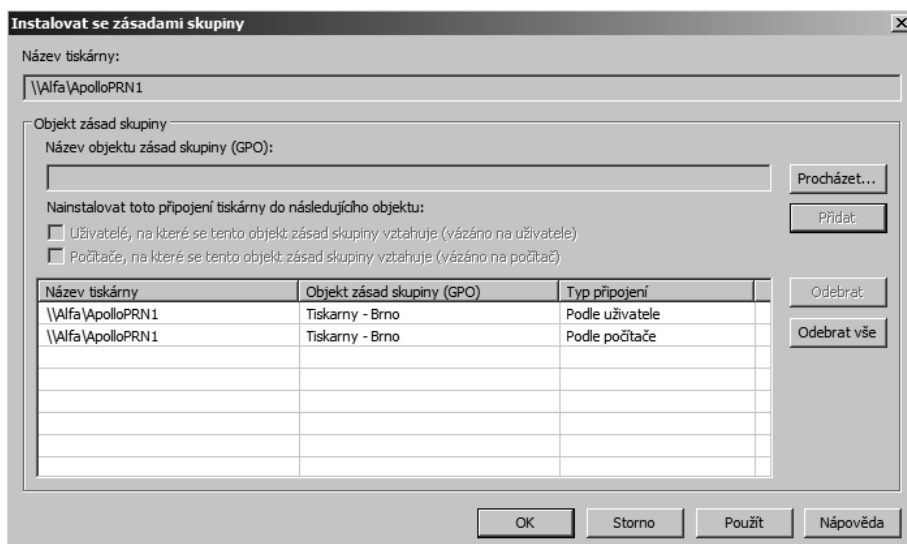
3. Nyní je třeba rozhodnout, zda se bude tiskárna mapovat na počítač nebo uživatele. Pokud jsou uživatelé i jejich stanice v jedné organizační jednotce, tak je vcelku jedno, kterou možnost zaškrtnete.

Pokud jsou však uživatelské účty v jiné organizační jednotce, než jsou účty počítačů, je třeba tuto skutečnost zohlednit a vybrat správnou volbu (tzn., pokud jsme objekt zásad skupiny vytvořili v organizační jednotce uživatelů, tak zde zatrhneme volbu pro uživatele. A vice versa.).

Pokud si nejste jisti a nechcete nebo nemůžete situaci blíže prozkoumat, přinejhorším zaškrtněte obě volby.

Když jste s nastavením hotovi, klepněte na tlačítko **Přidat** (Add), přičemž výsledné dialogové okno by mělo vypadat podobně jako na obrázku 5.27.

Pokud jsou cílovými stanicemi počítače s operačními systémy Windows Vista nebo Windows Server 2008, tak by postup byl tímto krokem dokončen.



Obrázek 5.27 Seznam tiskáren instalovaných prostřednictvím zásad skupiny

Jestliže jsou ale na cílových počítačích starší operační systémy, než ty výše uvedené, bude nutné udělat ještě několik dalších úkonů, aby se instalace tiskáren provedla korektně:

4. Na serveru klepněte na tlačítko **Start** → **Nástroje pro správu** (Administrative Tools) → **Správa zásad skupiny** (Group Policy Management).

Zde v doménové struktuře najdete objekt zásad skupiny, který provádí mapování tiskárny (v našem případě to byl objekt s názvem *Tiskárny - Brno* propojený s organizační jednotkou *Brno* domény *cpress.cz*), klepněte na něj pravým tlačítkem a vyberte možnost **Upravit** (Edit).

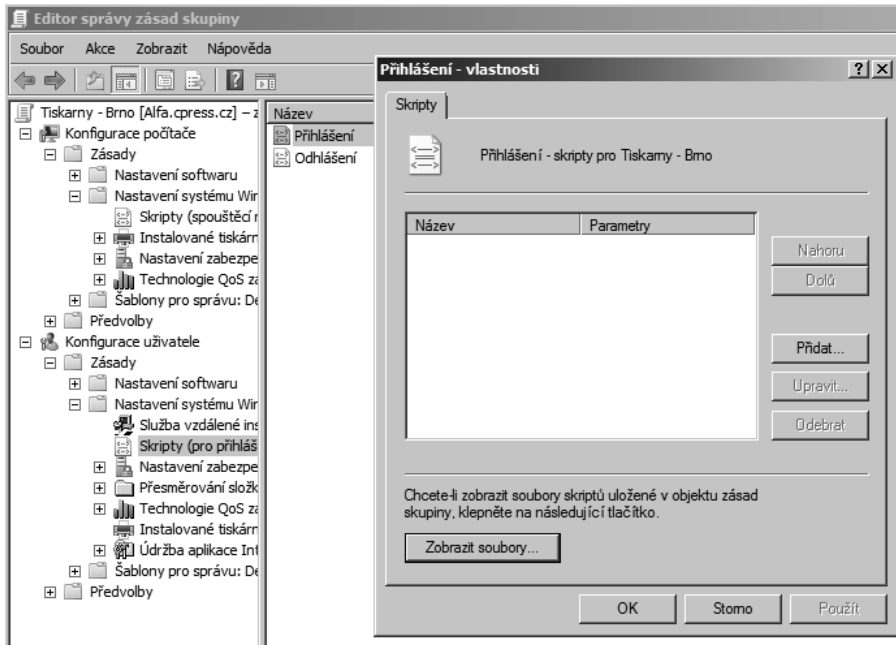
5. V levém panelu editoru zásad skupiny pak rozbalte uzel **Konfigurace uživatele** (User Configuration) (nebo **Konfigurace počítače** (Computer Configuration)), podle toho, pro koho se tiskárny instalují) → **Zásady** (Policies) → **Nastavení systému Windows** (Windows Settings) → **Skripty (pro přihlášení nebo odhlášení)** (Scripts (Logon/Logoff)), respektive hovoříme-li o nastavení pro počítače, pak **Skripty (spouštěcí nebo ukončovací)** (Scripts (Startup/Shutdown)).

Poklepejte na položku **Přihlášení** (Logon), resp. **Po spuštění** (Startup).

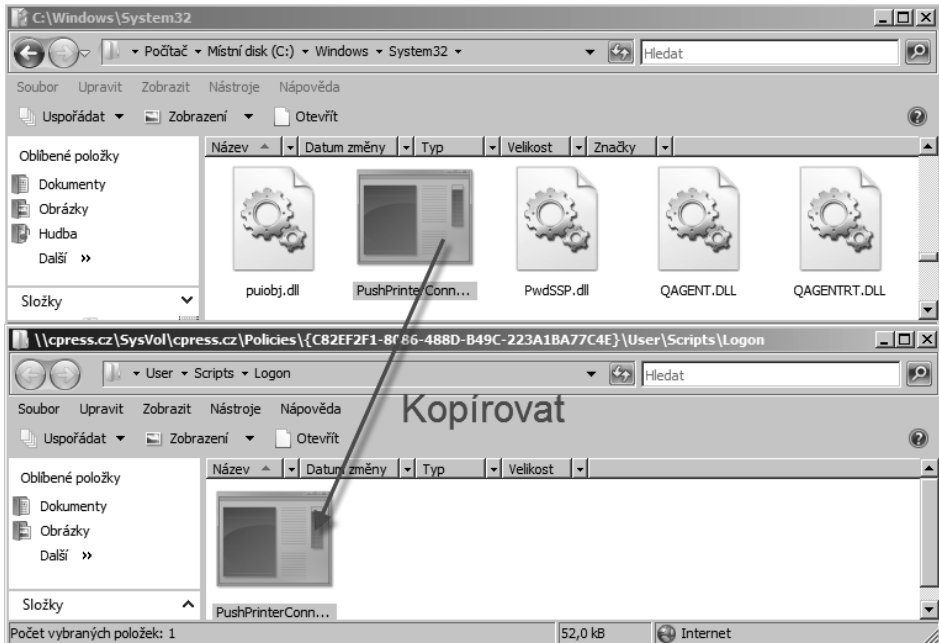
6. V dialogovém okně skriptu pro přihlášení nebo po spuštění klepněte na tlačítko **Zobrazit soubory** (Show Files) (vše by mělo být zřejmé z obrázku 5.28), načej se zobrazí okno Průzkumníka v umístění, kam jsme se v tomto případě potřebovali dostat (poněkud delší cesta ke složce).

Otevřete si další okno průzkumníka a v něm najdete soubor *PushPrinterConnections.exe* umístěn ve složce *%windir%\system32* (tedy např. *C:\Windows\System32*).

Tento soubor zkopírujte do prvního okna Průzkumníka, tedy toho, které se otevřelo po klepnutí na tlačítko **Zobrazit soubory** (Show Files) (náznorněji viz obrázek 5.29).



Obrázek 5.28 Editor správy zásad skupiny

Obrázek 5.29 Zkopírování souboru *PushPrinterConnections.exe* do složky s objektem zásad skupiny pro instalaci tiskáren

Tento soubor umožňuje starším operačním systémům instalovat tiskárny např. právě formou nastavení v zásadách skupiny.

Tento komplikovaný krok jsme provedli z toho důvodu, aby soubor byl dostupný klientským počítačům společně s objektem zásad skupiny a aby si jej klienti mohli automaticky stáhnout a použít při instalaci tiskáren.

Po zkopírování můžete obě okna Průzkumníka zavřít.

7. V dialogovém okně **Přihlášení – Vlastnosti** (Logon – Properties) klepněte na tlačítko **Přidat** (Add) a do pole **Název skriptu** (Script name) napište *PushPrinterConnections.exe*, což sice není soubor skriptu, ale systému je to srdečně jedno a prostě tuto aplikaci spustí, až to bude zapotřebí.

Po zadání názvu příkazu klepněte dvakrát na tlačítko **OK** a poté můžete zavřít **Editor správy zásad skupiny** (Group Policy Management Editor).

To už je skutečně vše. Tento postup bych s nepatrným množstvím nadsázky okomentoval slovy „mnoho povyku pro nic“.

Poznámka: Tato metoda funguje skutečně jen pro Windows Vista a Windows Server 2008 (a zřejmě bude fungovat i pro Windows 7). Ve Windows XP SP3 je nutné použít aplikaci *PushPrinterConnections.exe*.



Instalace tiskárny na klientský počítač pomocí předvoleb zásad skupiny

Předvolby zásad skupiny jsou skvělou novinkou v operačním systému Windows Server 2008 a kromě mnoha dalších věcí je můžeme použít také pro hromadnou instalaci tiskáren na klientské počítače.

Postup je výrazně jednodušší než ten předchozí a také se mnohem lépe spravuje i později po prvotním nasazení.

Jako zásadní výhody tohoto systému bych vyzvedl fakt, že díky předvolbám můžeme instalovat tiskárny podle organizačních jednotek, ale díky tzv. cílení na úrovni položky (item-level targeting) máme možnost nesrovnatelně podrobnější správy, takže např. můžeme definovat jeden objekt zásad skupiny na nějakou organizační jednotku nebo klidně na celou doménu, přičemž díky předvolbám budeme schopni určit, že se konkrétní tiskárna nainstaluje jen uživatelům nebo na počítače, které splňují nějaká kritéria (např. členství ve skupině zabezpečení, adresa IP z nějakého rozsahu a mnoho dalších).

Kromě výše uvedeného je zde příjemný také fakt, že tento způsob instalace tiskáren funguje i bez použití aplikace *PushPrinterConnections.exe* a zprovozníte jej tedy na všech počítačích s operačním systémem Windows Vista, Windows Server 2008 a Windows XP se Service Packem 3 (nebo alespoň nainstalovanými *Rozšířeními předvoleb zásad skupiny pro klientskou část pro systém Windows XP*). Více informací o této aktualizaci naleznete v článku znalostní databáze firmy Microsoft na adrese <http://support.microsoft.com/?kbid=943279>. Jsou tam také odkazy na stažení potřebných souborů).

Rozhodnete-li se použít tento způsob instalace tiskáren, postupujte takto:

1. Klepněte na tlačítko **Start** → **Nástroje pro správu** (Administrative Tools) → **Správa zásad skupiny** (Group Policy Management).

V levém panelu rozbalte doménovou strukturu tak, abyste viděli organizační jednotku, pro kterou chcete provést instalaci tiskáren, klepněte na ni pravým tlačítkem a vyberte možnost **Vytvořit objekt zásad skupiny v této doméně a propojit jej sem** (Create a GPO in this domain, and Link it here).

Pokud vás až tak nezajímají organizační jednotky jakožto kritérium pro instalaci tiskáren, můžete vytvořit nový objekt zásad skupiny a propojit jej přímo s doménou.

2. Klepněte na takto vytvořený objekt zásad skupiny pravým tlačítkem a vyberte možnost **Upravit** (Edit).

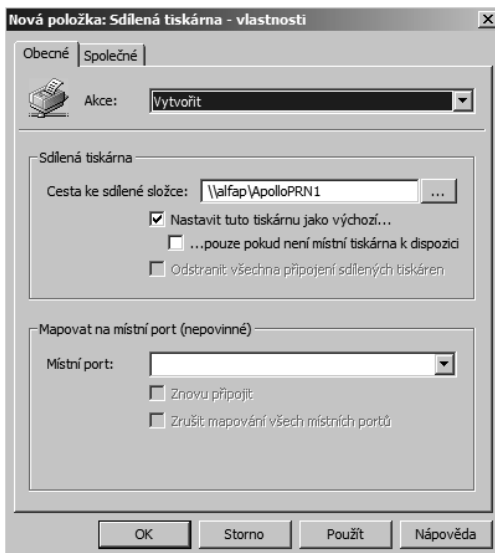
Nyní opět záleží na tom, zda chcete tiskárny instalovat pro počítače nebo uživatele. Podle svého uvážení tedy rozbalte uzel **Konfigurace uživatele** (User Configuration) (resp. **Konfigurace počítače** (Computer Configuration)) → **Předvolby** (Preferences) → **Nastavení ovládacích panelů** (Control Panel Settings).

3. Označte položku **Tiskárny** (Printers), klepněte na ni pravým tlačítkem a vyberte možnost **Nová položka** (New) → **Sdílená tiskárna** (Shared Printer).

Na výběr jsou kromě sdílené tiskárny i další možnosti jako **Tiskárna TCP/IP** (TCP/IP Printer) (vhodná pro instalaci tiskáren s vlastním síťovým rozhraním a adresou IP) anebo **Místní tiskárna** (Local Printer) (např. pokud plošně nasazujete tiskárny k mnoha stanicím pomocí místního připojení).

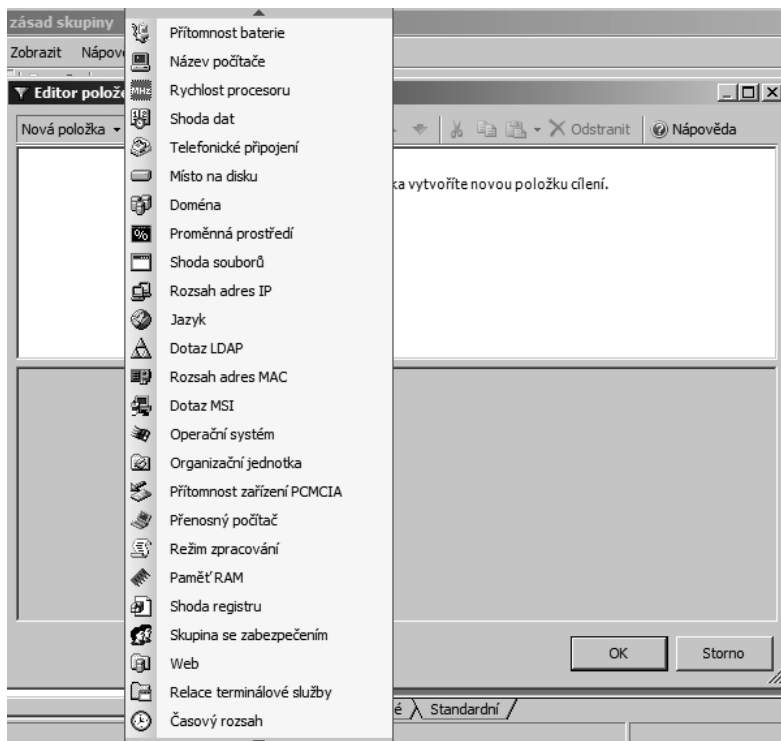
4. V dialogovém okně s vlastnostmi nové tiskárny vyberte v seznamu s názvem **Akce** (Action) možnost **Vytvořit** (Create).

Do pole **Cesta ke sdílené složce** (Share Path) zadejte síťovou cestu UNC ke sdílené tiskárně, tedy např. `\\alfa\ApolloPRN1`. Pokud chcete, můžete zde definovanou tiskárnu nastavit jako výchozí nebo ji nastavit jako výchozí pouze v případě, že místní tiskárna není k dispozici (viz obrázek 5.30).



Obrázek 5.30 Nastavení instalace tiskárny pomocí předvoleb zásad skupiny

5. V tomto místě by instalace tiskárny mohla skončit. Chcete-li však z předvoleb zásad skupiny „vyždímat“ maximum, přepněte na záložku **Společné** (Common), zaškrtněte položku **Cílení na úrovni položky** (Item-level Targeting) a klepněte na tlačítko **Cílení** (Targeting).
6. V dialogovém okně **Editor položek cílení** (Targeting Editor) klepněte na tlačítko **Nová položka** (New Item) a z obsáhlého seznamu si vyberte kritérium, podle kterého chcete mapování provádět (pro inspiraci viz seznam kritérií na obrázku 5.31).

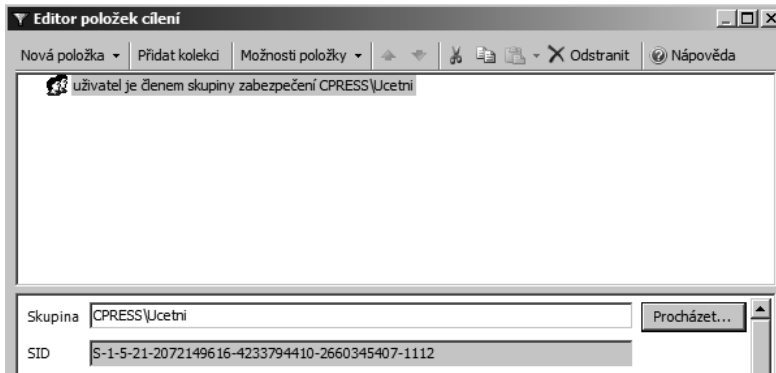


Obrázek 5.31 Část seznamu kritérií, podle kterých můžeme provádět cílení na úrovni položky

Například bychom zde mohli vybrat kritérium **Skupina se zabezpečením** (Security Group) a klepnutím na tlačítko **Procházet** (Browse) bychom vybrali skupinu, pro jejíž členy se má instalace tiskárny provést (na obrázku 5.32 instalujeme tiskárnu pro členy skupiny *Účetní* z organizační jednotky *Brno*).

Nyní už jen dvakrát klepněte na tlačítko **OK**, pozavírejte okna editorů a dílo je dokonáno.

Pokud byste chtěli, můžete v jednom objektu GPO (např. propojeném na celou doménu) definovat mnoho instalací tiskáren, kdy každý se může instalovat podle jiných kritérií. Veškeré informace pro správu instalace tiskáren byste takto měli přehledně na jednom místě a případné budoucí změny jsou otázkou několika klepnutí myši.



Obrázek 5.32 V případě uvedeném na tomto obrázku by se tiskárna instalovala pouze pro členy skupiny *Účetní*.

Přesunutí tiskové úlohy z jedné tiskárny na druhou

Občas se stane, že je na jednu tiskárnu posláno větší množství tiskových úloh a v nejnevhodnější okamžik dojde k nějaké poruše – zasekne se papír, dojde toner nebo jiné podobné „radvánky“.

V takové situaci někdy nemůžeme čekat, až se problém s konkrétní tiskárnou vyřeší, ale potřebujeme uživatelům umožnit dokončení jejich tiskových úloh. Naštěstí můžeme tisknuté dokumenty přeměřovat na jinou tiskárnu (podmínkou je, aby používala stejný ovladač, jako tiskárna původní).

Při přesunu tiskové úlohy postupujte takto:

1. Klepněte na tlačítko **Start** → **Nástroje pro správu** (Administrative Tools) → **Správa tisku** (Print Management).
V levém panelu konzoly rozbalte uzel **Správa tisku** (Print Management) → **Tiskové servery** (Print Servers) → **Název serveru** → **Tiskárny** (Printers).
2. Klepněte pravým tlačítkem na tiskárnu, z níž chcete dokumenty přesunout a vyberte položku **Vlastnosti** (Properties).
Nyní přepněte na záložku **Porty** (Ports) a zaškrtněte port tiskárny, na kterou mají být dokumenty přesunuty. Pokud jsou tiskárny nastaveny pro použití ve fondu tiskáren, tak může dojít k tomu, že budete mít zaškrtnuto více portů. V takovém případě se ujistěte, že jste zrušili zaškrtnutí portu u původní tiskárny (té, z které přesunujete dokumenty).

Nastavení exkluzivity pro používání tiskárny specifickou skupinou uživatelů

Ve větších firmách nebo organizacích mohou existovat velmi různorodé skupiny uživatelů, které mají rovněž různorodé požadavky na zpracování tiskových úloh.

Manažeři mohou například potřebovat tisknout kratší prezentace, zato však rychle a kvalitně, zatímco účetní potřebují tisknout obsáhlé přehledy a uzávěrky o stovkách stránek a nepotřebují tisk v nejvyšší kvalitě a v barvě.

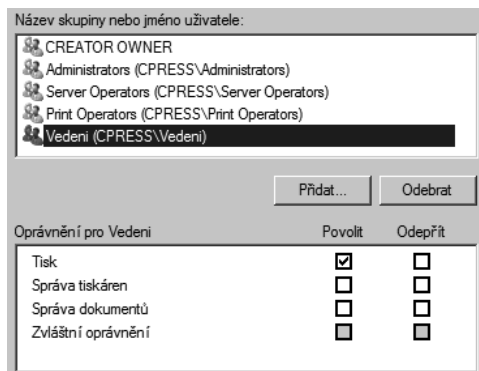
Samozřejmě nějaké zásady používání tiskáren se dají řešit formou dohody nebo vnitropodnikových směrnic, ale abychom vynutili tento systém také po technické stránce, můžeme oprávnění na tiskárnách nastavit tak, aby každý mohl tisknout skutečně jen na té „své“ a nezdržoval tak svými tiskovými úlohami ostatní.

Následující postup ilustruje nastavení oprávnění tak, aby uživatelé ze skupiny *Vedeni* mohli tisknout jen na tiskárnu *ApolloPRN1*, zatímco uživatelé ze skupiny *Ucetni* budou mít k dispozici pouze tiskárnu *ApolloPRN2*.

1. Klepněte na tlačítko **Start** → **Nástroje pro správu** (Administrative Tools) → **Správa tisku** (Print Management).
V levém panelu konzoly rozbalte uzel **Správa tisku** (Print Management) → **Tiskové servery** (Print Servers) → **Název serveru** → **Tiskárny** (Printers).
2. Klepněte pravým tlačítkem na tiskárnu, kterou chcete dedikovat jedné skupině (v našem příkladu tedy tiskárna *ApolloPRN1* pro skupinu *Vedeni*) a vyberte položku **Vlastnosti** (Properties).
3. Přepněte na záložku **Zabezpečení** (Security) a zde odeberte ze seznamu řízení přístupu ty skupiny nebo uživatele, kteří tiskárnu nemají používat (tedy typicky odebereme skupinu *Everyone*).

Místo těchto skupin zde přidejte skupinu, která přístup mít má (samozřejmě těchto skupin může být více) a nastavte pro ni vhodná oprávnění (pokud mají být skutečně jen uživateli této tiskárny, pak postačí oprávnění **Tisk** (Print)).

Na obrázku 5.33 můžete vidět příklad takového nastavení.



Obrázek 5.33 Nastavení oprávnění tiskárny tak, aby ji mohla používat jen skupina *Vedeni* a abychom zachovali přístup pro administrativní skupiny

4. V podstatě totéž bychom pak provedli ve vlastnostech zabezpečení tiskárny *ApolloPRN2* jen s tím rozdílem, že bychom do seznamu řízení přístupu nepřidávali skupinu *Vedeni*, ale *Ucetni*.

Tímto je situace vyřešena. V případě potřeby můžete ještě tyto tiskárny nainstalovat na klientské počítače pomocí jednoho z výše uvedených postupů (v tomto případě je zřejmě ideální instalace tiskáren pomocí předvoleb zásad skupiny).



Poznámka: Výše uvedený postup přiřazení oprávnění je trošku zjednodušen kvůli přehlednosti. Správně bychom měli mít pro každou sdílenou tiskárnu v doméně jednu doménovou místní skupinu a řešit přiřazení oprávnění skrze členství v této skupině.

Abychom situaci vyřešili z hlediska správy korektně, měli bychom přidat uživatelské účty uživatelů z vedení firmy do globální skupiny *G_Vedeni* a tuto skupinu pak přidat jako člena do místní doménové skupiny s názvem např. *DL_ApolloPRN1* (písmena *G* a *DL* zde jsou jen pro přehlednost a představují *G* jako globální skupinu a *DL* jako *Domain Local*, tedy doménová místní).

Upřednostnění tiskových úloh zaslaných specifickou skupinou uživatelů

Dejme tomu, že situace je podobná jako v předchozím řešení jen s tím rozdílem, že se jedná o firmu malou a poněkud chudou na tiskárny.

Máme zde uživatele vedení firmy, kteří potřebují tisknout s co nejmenšími prodlevami krátké a důležité dokumenty a máme zde běžné uživatele, kteří potřebují tisknout dlouhé dokumenty, na které však až tak nespěchají.

Tiskárna je však jen jedna pro všechny a mohou nastávat situace, kdy manažer spěchající na schůzku potřebuje bleskově vytisknout několik málo stránek prezentace a musí čekat hodiny, než se vytisknou dokumenty ostatních uživatelů zařazených ve frontě.

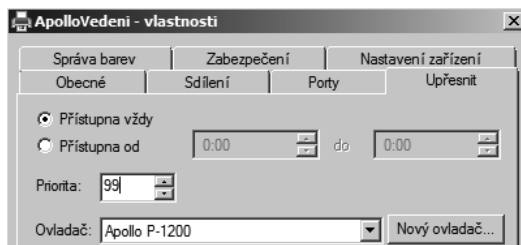
Abychom tomu předešli, můžeme nastavit tiskárny takto:

Výchozí stav je takový, že k serveru je připojena jen jedna fyzická tiskárna a dejme tomu, že ještě nebyla nainstalována na server (začínáme pro zjednodušení od nuly). Máme skupiny *Vedeni* a *Ucetni*, které chceme použít jako kritérium pro to, či tiskové úlohy se mají zpracovávat přednostně.

Nyní je zapotřebí udělat následující kroky:

1. Nainstalujte tiskárnu na server a nasdílejte ji (viz postup *Instalace tiskárny na tiskový server* dříve v této kapitole). Této tiskárně bychom přidělili např. port *PRN4* a tiskárnu samotnou nazveme např. *ApolloVedeni*.
2. Nainstalujte na server druhou tiskárnu, ale tentokrát jí nedávejte její vlastní port, nýbrž v průvodci zadejte, že tiskárna má použít existující port. Konkrétně ten, na kterém jsme nainstalovali první tiskárnu, tedy *PRN4*. Tiskárnu pojmenujte např. *ApolloUcetni*.
3. Na obou tiskárnách nastavte oprávnění přibližně stejným způsobem jako v řešení *Nastavení exkluzivity pro používání tiskárny specifickou skupinou uživatelů*.
4. Nyní v konzole **Správa tisku** (Print Management) klepněte na první tiskárnu (*ApolloVedeni*), vyberte položku **Vlastnosti** (Properties) a v dialogovém okně vlastností přepněte na záložku **Upřesnit** (Advanced).

Zde nastavte prioritu třeba 99 (priorita může být v rozsahu od 1 to 99, přičemž 99 je nejvyšší), viz obrázek 5.34.



Obrázek 5.34 Nastavení vysoké priority tiskárny

5. Otevřete dialogové okno vlastností druhé tiskárny (*ApolloUcetni*) a zde naopak nastavte prioritu nejnižší, např. 1.

Výsledkem tohoto postupu bude to, že ačkoliv máme jen jedno fyzické tiskové zařízení, nainstalovali jsme jej na tiskový server v podobě dvou logických zařízení na jednom portu.

Protože jsme nastavili exkluzivní oprávnění pro přístup skupině *Ucetni* na tiskárnu *ApolloUcetni* a skupině *Vedeni* na tiskárnu *ApolloVedeni* a nastavili jsme tiskárně *ApolloVedeni* nejvyšší prioritu (nebo obecně prostě vyšší, než u dalších logických tiskáren), budou mít tiskové úlohy zasílané členy skupiny *Vedeni* vyšší prioritu a budou se tedy tisknout dříve.

Změna složky pro zařazování tiskových úloh

Vy výchozím stavu jsou tiskové úlohy odesílány na tiskový server, kde jsou v podobě souboru zařazeny do fronty a čekají, až jsou skutečně vytisknuty tiskovým zařízením. Poté mohou být ze serveru smazány, neboť zabírají nezanedbatelné množství místa na disku.

Obsazené místo na disku však není jediným problémem, který se negativně podepisuje na výkonu serveru. Mnohem výrazněji se na celkovém výkonu serveru podepíše nutnost zpracovávat enormní množství požadavků na diskové operace.

Ve výchozím stavu je složka s frontou umístěna na systémovém disku, konkrétně `%windir%\System32\spool\PRINTERS`.

Pokud tedy očekáváte, že váš tiskový server bude značně vytížen zpracováváním tiskových úloh, bylo by vhodné výše uvedené umístění změnit, a to ideálně na jiný fyzický disk, než je ten, na kterém se nachází operační systém.

Změnu umístění provedete takto:

1. Klepněte na tlačítko **Start** → **Ovládací panely** (Control Panel) → **Tiskárny** (Printers).
2. V Průzkumníku klepněte v nabídce **Soubor** (File) na položku **Vlastnosti server** (Server Properties) nebo prostě klepněte kamkoliv na prázdnou plochu v okně Průzkumníka pravým tlačítkem myši a vyberte totéž.
3. V dialogovém okně s vlastnostmi server přepněte na záložku **Upřesnit** (Advanced). Zde uvidíte v poli s názvem **Složka pro zařazování** (Spool Folder) aktuální umístění, ve kterém se ukládají zařazené tiskové úlohy.

V tomto poli tedy zadejte cestu k novému umístění, jak můžete vidět na příkladu na obrázku 5.35.



Obrázek 5.35 Změna umístění složky pro zařazování tiskových úloh

Nastavení a vytvoření vlastní oddělovací stránky

V případě intenzivního využívání tiskáren mnoha uživateli může docházet ke zmatkům, kdy několik lidí pošle na server dokumenty o několika stech stránkách a až jsou dokumenty vytištěny, tito uživatelé se sejdou u tiskárny a hledají, kde začíná a končí cí dokument.

Za tímto účelem máme k dispozici tzv. oddělovací stránky, které jsou vytištěny vždy mezi jednotlivými dokumenty a kromě této své funkce také mohou obsahovat informace o tiskové úloze.

V operačním systému Windows Server 2008 je několik předdefinovaných oddělovacích stránek (najdete je ve složce `%Windir\System32` a mají příponu `.sep`).

Pokud však chcete vytvořit vlastní oddělovací stránku, použijte následující postup.

1. V libovolném textovém editoru vytvořte soubor oddělovací stránky. Tento soubor pojmenujte celkem libovolně, důležité je ale, aby měl koncovku `.sep`. Soubor uložte např. do složky `%Windir\System32`.
2. Takto vytvořený soubor následně editujte tak, aby oddělovací stránka obsahovala požadované informace o tiskové úloze. Příklad takového souboru vidíme na následujících řádcích:

```

\
\U\LNazev uzivatele: \N
\U\LCislo tiskove ulohy: \I
\U\LDatum tisku: \D
\U\LCas tisku: \T
\E

```

Jen stručné vysvětlení:

Znak lomítka („\“) na prvním řádku zde slouží pro určení oddělovače příkazů. Jaký oddělovač zde určíte, takový se musí používat i dále v souboru oddělovací stránky. Vybrat si však můžete libovolný znak.

Konstrukce na začátku každého dalšího řádku („\U\L“) zjednodušeně říká tiskárně, aby vytiskla všechny následující znaky až po první oddělovač příkazů nalezený na řádku (v tomto příkladu je jím ono lomítko).

Co znamenají další písmena na řádcích 2 – 5 je asi zřejmé z doprovodného textu. *N* vypíše název uživatele, *I* číslo úlohy, *D* datum a *T* čas tisku. Není to zrovna kvantum informací, ale aspoň něco.

Poslední řádek soubor pak obsahuje písmeno *E*, které zde znamená *Eject*, tedy vysounout (v našem případě spíš vytisknout tuto stránku).



- Nyní, když máme oddělovací soubor připraven, můžeme jej nastavit pro konkrétní tiskárnu.

V konzole **Správa tisku** (Print Management) najdete tiskárnu, pro kterou chcete nastavit oddělovací stránku, klepněte na tiskárnu pravým tlačítkem a vyberte možnost **Vlastnosti** (Properties).

Přepněte na záložku **Upřesnit** (Advanced) a klepněte na tlačítko **Oddělovací stránka** (Separator Page).

V dialogovém okně pak klepněte na tlačítko **Procházet** (Browse) a najdete soubor obsahující oddělovací stránku.


Klepněte dvakrát na tlačítko **OK** a tím je oddělovací stránka připravena k použití.

Přesunutí tiskáren i tiskových front na jiný tiskový server

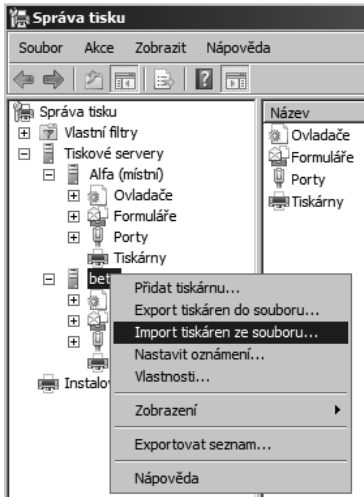
Může nastat situace, kdy potřebujete migrovat tiskárny nainstalované na jednom tiskovém serveru na jiný tiskový server.

To by samo o sobě nebyl až takový problém, ale pokud jsou tyto tiskárny už nakonfigurovány, jsou pro ně vytvořeny tiskové fronty a proces ručního odebrání a následné instalace na nový server by byl příliš pracný, můžeme využít poměrně jednoduchou možnost migrace, jako v následujícím příkladu, kde je popsána migrace tiskáren z tiskového serveru *Alfa* na tiskový server *Beta*.

- Na stávajícím tiskovém serveru (Alfa) klepněte na tlačítko **Start** → **Nástroje pro správu** (Administrative Tools) → **Správa tisku** (Print Management). Rozbalte strukturu v levém panelu tak, abyste viděli jednotlivé tiskové servery (tedy **Správa tisku** (Print Management) → **Tiskové servery** (Print Servers)).
- Označte server, ze kterého chcete migrovat tiskárny (v našem případě server *Alfa*), klepněte na něj pravým tlačítkem a vyberte možnost **Export tiskáren do souboru** (Export printers to a file). Zadejte umístění, do kterého bude uložen soubor s exportovanými tiskárnami.
- Nyní v konzole pro správu tisku klepněte pravým tlačítkem na tiskový server, na nějž chcete tiskárny migrovat a vyberte možnost **Import tiskáren ze souboru** (Import printers from a file) (viz obrázek 5.36). Poté pomocí tlačítka **Procházet** (Browse) vyberte soubor s tiskárnami a v průvodci klepněte na tlačítko **Další** (Next).

 **Poznámka:** Pokud v konzole pro správu tisku nevidíte cílový server, můžete jej sem přidat klepnutím pravým tlačítkem myši na položku **Správa tisku** (Print Management) ☒ **Přidat či odebrat servery** (Add/Remove Servers).

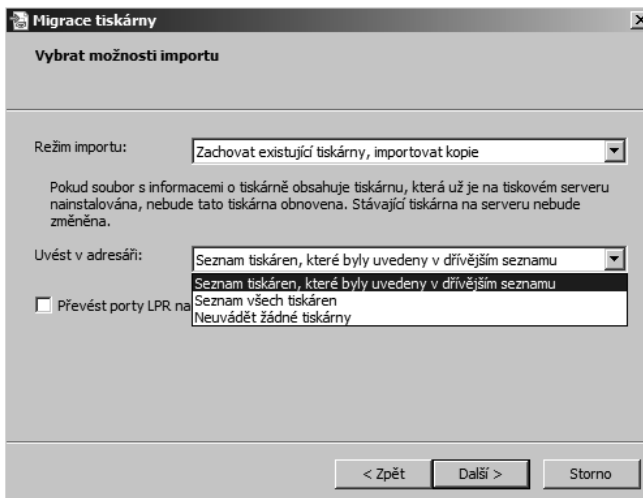
- Na obrazovce s výpisem importovaných tiskáren klepněte na tlačítko **Další** (Next). Následně vyberte režim importu, tzn., jak se má systém zachovat, pokud již tiskárna na cílovém serveru existuje (můžeme k ní vytvořit kopii nebo přepsat původní tiskárnu).



Obrázek 5.36 Import tiskáren ze souboru na cílový tiskový server.
Všimněte si, že oba servery můžeme spravovat z jedné konzoly

Na této stránce také pomocí rozbalovacího seznamu určete, zda mají být v adresáři zveřejněny všechny importované tiskárny, ty, které byly uvedeny v adresáři původně, nebo se nebudou zveřejňovat žádné tiskárny (viz obrázek 5.37).

Po zadání těchto voleb klepněte na tlačítko **Další** (Next) a poté **Dokončit** (Finish).



Obrázek 5.37 Režim importu tiskáren