Exchange Server 2003

MARIAN HENČ

- Implementace systému
- Správa a řešení problémů
- Spolupráce s Active Directory
- Instalace a nastavení ve Windows 2000 a Windows Serveru 2003
- Klienti serveru Exchange
- Zálohování a obnovení

EDICE PROFESIONAL

GRADA

Upozornění pro čtenáře a uživatele této knihy

Obsah

Poděkování

Děkuji za spolupráci a cenné rady všem svým kolegům, kamarádům a známým, zejména pak Miroslavu Knotkovi, Petru Šetkovi, Petru Hronovi, Jiřímu Grohmannovi a Filipu Markesovi.

Velký dík patří rovněž Vladimíru Cihlářovi za pomoc při ilustraci obrázků, Tomáši Duškovi ze společnosti *Sunnysoft* za počeštění emulátoru *Pocket PC 2003* a Marku Waldhauserovi ze společnosti *e-Fractal* za seznámení s produktem *SMS Touch*.

V neposlední řadě musím poděkovat své manželce, která se o mě po dobu psaní této knihy pečlivě starala a nepřipustila, abych se zpozdil ani o jediný den.

Zbytek už asi všichni znáte. Za to, co je v této knize dobře, děkuji všem výše jmenovaným, za to, co je špatně, mohu já.

®

Úvod

Poslání knihy

Problematika poštovních serverů *Microsoft Exchange* doposud nebyla v české literatuře dostatečně prezentována. V souvislosti s vydáním předchozí verze *Microsoft Exchange 2000 Server* (dále jen *Exchange 2000*) se na českém trhu neobjevila jediná původní česká publikace, která by detailně mapovala tento produkt, hojně používaný ve firmách fungujících na technologiích společnosti *Microsoft*.

Hlavním posláním této knihy je splatit dluh všem čtenářům, kteří hledali srozumitelnou příručku v českém jazyce, a také těm, kteří nemají tu možnost číst originální anglickou literaturu. Touto knihou také plním slib všem svým studentům a posluchačům, kteří mě často na školeních a konferencích žádali o alternativu k anglickým příručkám dodávaným k výukovým kurzům *Microsoftu* (MOC) a ke knihám MCSE: Training Kit, určeným pro samouky.

Poštovní servery Microsoft Exchange

Microsoft Exchange Server 2003 (dále jen Exchange 2003), známý také pod kódovým označením Titanium, je v pořadí pátou verzí tohoto populárního groupwarového řešení. Samozřejmě do výčtu verzí (4.0, 5.0, 5.5, 2000, 2003) je třeba započítat i předchůdce, a to na tehdejší dobu poměrně pokrokový produkt MS PC Mail (Microsoft Mail for Personal Computing Networking). Tento produkt sice nesdílí s dnešními verzemi jedinou část kódu, ale stál u zrodu aplikačního rozhraní MAPI, které je dodnes používáno při komunikaci s poštovním klientem *Outlook*.

Nová verze doznala oproti serveru *Exchange 2000* mnoha změn. Některé změny jsou přírůstkové povahy (viz i necelé číslo verze Build 6.5), jiné zase zásadním způsobem mění pojetí správy celé organizace.

Exchange 2003 společně s operačním systémem *Windows Server 2003* byl vyvíjen na standardech iniciativy *Microsoft Trustworthy Computing*, jejímž cílem je zlepšit vlastnosti produktů v oblasti zabezpečení, soukromí, spolehlivosti a integrity dat. Základními pravidly této iniciativy, která byla představena v lednu 2002, je zabezpečení při vývoji, zabezpečení ve výchozím stavu, zabezpečení při zavádění a komunikace se zákazníky při udržování zabezpečení a integrity firemního prostředí.

Komu je kniha určena?

Tato kniha je prvním ze dvou svazků věnovaných platformě pro zasílání zpráv *Exchange 2003*. První svazek by měl sloužit jako úvod do implementace a správy poštovního systému *Exchange 2003*, ale i předchozí verze *Exchange 2000* (architektura platformy nebyla zásadně pozměněna) a zároveň by měl posloužit i jako rádce a průvodce v případě řešení problémů (vzhledem k rozsahu ne v kapesním formátu, bohužel ☺).

V prvním svazku si přijdou na své hlavně začínající a mírně pokročilí správci firemních sítí, kteří se chystají nasadit (nebo již provozují) tuto novou verzi poštovního systému do prostředí s adresářovou službou *Active Directory* běžící na operačních systémech *Windows 2000* a *Windows Server 2003*.

První kapitola je věnována přehledu a architektuře systému. Jsou zde popsány rozdíly mezi jednotlivými verzemi systému *Exchange 2003*, jeho závislosti na adresářové službě *Active Directory* a službě *Internet Information Services*. Úvod kapitoly je zasvěcen novinkám serveru *Exchange 2003*, které ocení zejména správci znalí serveru *Exchange 2000*.

Druhá kapitola pojednává o instalaci systému *Exchange 2003*. Kromě samotné instalace jsem se zde snažil klást důraz zejména na její plánování, přípravu a postinstalační kroky, jež bývají ve firmách často opomíjeny, a z toho v budoucnu mnohdy plynou problémy. Kapitola se také věnuje automatizaci instalací systémů *Exchange* v případě hromadného zavádění velkého počtu serverů.

Třetí, nejrozsáhlejší kapitola popisuje jednotlivé činnosti správy poštovního systému. Jmenujme např. správu úložišť dat, příjemců, seznamů adres, směrování atd. Tato kapitola by se měla stát těžištěm a určitým středobodem této knihy, protože mapuje nejčastější činnosti správců serverů *Exchange*.

Klientům systému *Exchange 2003* je vyhrazena čtvrtá kapitola, věnovaná jednotlivým možnostem přístupu do poštovní schránky uživatele. Kromě klasických způsobů (MAPI, POP3, IMAP4) jsou zde popsány i přístupy z mobilních zařízení, jakou jsou např. mobilní počítače a telefony, PDA zařízení (*Pocket PC*, *Pocket PC Phone Edition* apod.). Jakýmsi mottem této kapitoly, vyjadřujícím její cíl a současný trend, je „přístup do poštovní schránky odkudkoliv a kdykoliv“.

Zálohování a obnova neodmyslitelně patří k činnostem provozovaným na jakémkoliv sytému. Ani zde nebude tato oblast opomenuta, je jí věnována pátá kapitola. Kromě samotných procesů zálohování a obnovy jsem se zde snažil nastínit také přípravu scénáře na potencionální možnosti havárie systému.

V těchto pěti kapitolách by měl čtenář získat dostatek informací o nasazení a konfiguraci serveru *Exchange*. Z důvodu omezeného rozsahu knihy jsem si dovolil přesunout některé oblasti správy do druhého svazku knihy, který by měl problematiku rozšiřovat a dále prohlubovat. Je určen spíše pokročilým správcům a návrhářům poštovní infrastruktury firmy. Jmenujme např. oblasti věnované veřejným složkám, systémovým zásadám, zabezpečení serverů, antivirům, nevyžádané poště, clusterovým řešením ke zvýšení redundance a vysoké dostupnosti serveru, digitální podepisování a šifrování e-mailových zpráv atd.

Související publikace

Nezbytným předpokladem pro úspěšné zvládnutí správy serveru *Exchange 2003* je dobrá znalost adresářové služby *Active Directory*, buď na operačním systému *Windows 2000* nebo *Windows Server 2003*. Z české literatury doporučuji knihy Michala Osifa *Windows*

2000 Server a Advanced Server – poradce experta (Grada 2001) a *Windows Server 2003 – poradce experta* (Grada 2003).

Styl a struktura publikace

Kniha je psána prostřednictvím podrobného popisu vzniku nové poštovní organizace *Exchange* ve fiktivní firmě. V potaz je brána komplexnost firmy, včetně pobočky připojené přes síť WAN a mobilních uživatelů, kteří se pohybují nejenom po jednotlivých lokalitách firmy, ale přistupují do poštovní schránky odkudkoliv z internetu.

Z důvodu neexistence české lokalizace serveru *Exchange 2003* jsou v publikaci používány anglické termíny s volným českým překladem. U klientských aplikací *Outlook 2003*, *Outlook Web Access* a *Exchange ActiveSync* jsou použity oficiální české překlady.

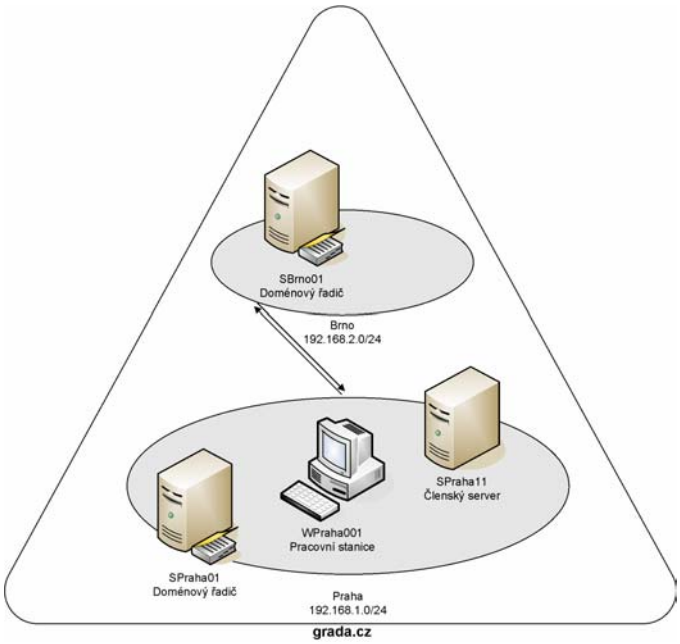
Modelová situace

Jelikož samotná teorie fungování serveru *Exchange 2003* by byla asi dost nudná, pojďme si dále vše prakticky ukazovat přímo na modelovém prostředí fiktivní firmy, jejíž jméno bude jak jinak než **Grada** (jedná se o čistě fiktivní firmu, která kromě jména nemá s firmou Grada Publishing nic společného). Doménová struktura (Forest) firmy se skládá z jedné domény, jejíž jméno je **grada.cz** a kterážto je zároveň názvem celé doménové struktury. Doména i doménová struktura jsou přepnuty na nejvyšší možnou **funkční úroveň Windows Server 2003**. Fyzická topologie firmy je tvořena dvěma pobočkami, a to v Praze a Brně. Pro tyto pobočky byly vytvořeny dvě sítě (Sites), pojmenované **Praha** a **Brno**, na něž jsou navázány IP podsítě **192.168.1.0/24** (Praha) a **192.168.2.0/24** (Brno). V každé síti (Site) je momentálně pouze jeden doménový řadič, a to **SPraha01** v Praze a **SBrno01** v Brně. Oba dva doménové řadiče jsou nainstalovány na operačním systému *Windows Server 2003* a konfigurované jako globální katalogy a servery DNS. Pobočky jsou propojeny pomocí hardwarových směrovačů rychlostí 1 Mb/s, mezi kterými je natažena virtuální privátní síť. Mezi sítěmi je vytvořen objekt spojení sítí (Sitelink) **Praha-Brno**, na kterém jsou nastaveny replikace jednou za hodinu, a to od pondělí do neděle, 24 hodin nepřetržitě.

Jedná se o právě založenou firmu, která si svou infrastrukturu teprve buduje. Firma nemá zatím implementovaný žádný poštovní systém, ale už je rozhodnuta pro nasazení nové verze serveru *Exchange 2003*. Většina zaměstnanců je umístěna na pražské centrále, v Brně je jich prozatím jen několik. Z rozpočtu na IT byly vyhrazeny peníze pouze pro nákup jednoho dalšího serveru. Hlavní IT architekt rozhodl, že tento server bude umístěn na centrále a bude se jednat o členský server pojmenovaný **SPraha11**, na kterém bude nainstalován první server *Exchange 2003*. Na serveru bude instalován *Windows Server 2003 Enterprise Edition* a *Exchange Server 2003 Enterprise Edition*. Tento server bude hostovat poštovní schránky uživatelů jak z Prahy, tak z Brna.

Pro pojmenování serverů v naší fiktivní firmě byla zvolena konvence **SSíťXX**, kde **S** značí, že se jedná o typ objektu server, a **XX** je pořadové číslo určující zároveň, zdali se jedná o doménový řadič (01-10), nebo členský server (11 a výše). Číslování bylo zvoleno z důvodu zajištění odlišení serverů v případě přidávání dalších serverů stejné kategorie do jedné sítě.

Pro pojmenování stanic byla zvolena konvence **WSíťXXX**, kde **W** značí, že se jedná o typ objektu pracovní stanice a **XXX** je pořadové číslo. Protože daná firma se může v budoucnu rozrůst o více stanic, bylo zvoleno trojmístné pořadové číslo.



Modelové prostředí fiktivní firmy Grada používané dále v této knize

1. Přehled a architektura serveru Exchange 2003

1.1 Novinky oproti serveru Exchange 2000

Vzhledem k tomu, že knihu mohou číst i správci předchozí verze, zmíním na tomto místě zásadní změny a novinky, které se objevily v serveru *Exchange 2003*. Tyto novinky či zdokonalení budu dále rozebírat v následujících kapitolách (popř. se objeví v druhém svazku knihy). Začínajícím správcům serveru *Exchange 2003* doporučuji přeskočit rovnou na kapitolu 1.2.

Seznam novinek a změn je volně převzat z dokumentu Microsoft Exchange Server 2003 Getting Started Guide.

1.1.1 Novinky v oblasti mobilní komunikace

Do serveru *Exchange 2003* byly zařazeny dvě nové služby podporující přístup do poštovní schránky uživatele z mobilních zařízení, jakými jsou např. zařízení založena na platformě *Pocket PC 2002/2003* a *Windows Mobile 2003* a dále mobilní telefony s wapovým prohlížečem. Jedná se o webové aplikace *Exchange ActiveSync* a *Outlook Mobile Access*, které byly dříve dostupné pouze pomocí produktu *Microsoft Mobile Information Server 2002*.

Aplikace *Exchange ActiveSync* zajišťuje synchronizaci složek **Doručená pošta**, **Kalendář** a **Kontakty** mezi serverem *Exchange 2003* a mobilním zařízením na platformě *Pocket PC 2002* a vyšší. Jedná se většinou o synchronizaci „vzduchem“, přes bezdrátové sítě Wi-Fi či sítě mobilních operátorů. Po synchronizaci jsou data na mobilním zařízení dostupná ve stavu offline. Oproti serveru *Mobile Information Server 2002* je zde jedna nová funkce, a to notifikace up-to-date. Tato funkce umožňuje pomocí zprávy SMS probudit mobilní zařízení a vynutit jeho synchronizaci se serverem *Exchange 2003*, ve chvíli, kdy se ve schránce uživatele objeví nová e-mailová zpráva.

Aplikace *Outlook Mobile Access* umožňuje přístup do schránky uživatele přes mobilní prohlížeč založený na protokolu WAP. Uživatelé se tak mohou dostat do složek **Doručená pošta**, **Kalendář**, **Kontakty** a **Úkoly**. Prohlížeč mobilního zařízení musí podporovat jeden z jazyků HTML (např. Casio Cassiopeia E-200), XHTML (např. Sony Ericsson T68i), nebo CHTML (např. Panasonic P504i). *Outlook Mobile Access* nabízí přístup k serveru *Exchange 2003* i z nepodporovaných zařízení, která nejsou na oficiálním seznamu zařízení firmy *Microsoft* (neprošla jejich testovacími laboratořemi).

1.1.2 Novinky v oblasti správy

V oblasti správy doznal *Exchange 2003* mnoha zjednodušení a urychlení práce, což ocení hlavně správci znalí předchozí verze, kteří se potýkali s občasnými prodlevami v konzole **Exchange System Manager**. Tato konzola prodělala nejedno vylepšení, i když to na první pohled není patrné. Nejpříjemnější změnou, na kterou bych rád upozornil, je možnost vy-

volání průvodce **Exchange Tasks Wizard** u uživatele nebo vícera uživatelů (vybraných pomocí přidržení kláves CTRL nebo SHIFT) přímo z konzoly **Exchange System Manager**, což považuji v předchozí verzi za velký nedostatek. V serveru *Exchange 2000* tato možnost chyběla, a uživatelé tak museli být spravováni z konzoly **Active Directory Users and Computers** (Uživatelé a počítače služby Active Directory). V dalších odstavcích jsou stručně popsány nejdůležitější změny.

Volume Shadow Copy (Podpora služby Stínová kopie svazku)

Exchange 2003 může při zálohování a obnově využívat kromě starého zálohovacího rozhraní z *Windows 2000* také nové rozhraní ze systému *Windows Server 2003*. Toto nové rozhraní využívá službu *Stínová kopie svazku*, která vytváří zrcadlenou kopii disku na začátku procesu zálohování. Skutečná záloha je poté vytvořena ze zrcadlené kopie (a ne přímo z disku, na kterém probíhají změny), a tím pádem normální operace mohou pokračovat v běhu. Záloha takto reflektuje stav svazku v momentě, kdy byl započat proces zálohování, i když se data v jeho průběhu změnila. Všechna data v záloze jsou interně konzistentní k danému bodu v čase. Aplikace jsou notifikovány o začátku procesu zálohování a mohou se na něj připravit vyčištěním mezipaměti a souborů transakčních protokolů. Proces zálohování a obnovy databáze serveru *Exchange 2003* je takto mnohonásobně rychlejší než v předchozích verzích (blíže kapitola 5.2).

Query-based Distribution Groups (Dynamické distribuční skupiny)

Dynamická distribuční skupina má stejnou funkci jako standardní distribuční skupina známá ze serveru *Exchange 2000* (která je zachována i u serveru *Exchange 2003*), ale liší se správou členství. Na rozdíl od standardní distribuční skupiny, jejíž členství je statické, dynamická distribuční skupina umožňuje specifikaci členů pomocí dotazů protokolu LDAP (např. pomocí atributů u účtu uživatele). To urychluje a zjednodušuje správu distribučních skupin. Na druhou stranu, tento nový typ skupiny sice snižuje náklady na správu, ale daleko více zatěžuje procesor, jelikož pokaždé, když je do dynamické distribuční skupiny poslána e-mailová zpráva, je vůči *Active Directory* spuštěn dotaz LDAP na členství ve skupině (blíže kapitola 3.6.7).

V globálním seznamu adres nelze zobrazit členy distribuční skupiny. Členství se generuje v době, kdy je e-mailová zpráva poslána.

Konzola Exchange System Manager

Konzola **Exchange System Manager** doznala následujících vylepšení:

- Zjednodušení filtrů pro vyhledávání, zdokonalené řazení podle sloupců a lepší manipulace s vícero frontami a zprávami.
- Fronty jsou centralizovány podle serveru místo podle virtuálního serveru, což znamená, že všechny fronty na serveru lze zobrazit z jediného místa.

- Zvýšený výkon z hlediska výčtu front a zobrazení všech front ve výchozím nastavení.
- Zobrazeny jsou nyní všechny systémové fronty, což usnadňuje řešení problémů.
- Funkce **Enable Forms Based Authentication** (Povolit formulářovou autentizaci) na úrovni virtuálních serverů HTTP, umožňující prostřednictvím uživatelského rozhraní snadno povolit či zakázat soubory cookie pro ověřování.
- Možnost přesunout soubory protokolů a dat fronty. V předchozí verzi *Exchange 2000* bylo možné přesouvat soubory protokolů trasování pouze ručně prostřednictvím nástrojů pro změny v adresářích (**ADSI Edit**, **LDP**) a článků znalostní databáze společnosti *Microsoft*. Nyní soubory protokolů pro sledování zpráv lze přesunout přímo v konzole **Exchange System Manager**, stejně jako data fronty MTA (Message Transfer Agent) X.400 a data fronty SMTP (Simple Mail Transfer Protocol).

Bližší informace o přesunutí souborů protokolů trasování jsou uvedeny v článku Q317700 „XADM: How to Change the Location of the Message Tracking Logs" znalostní databáze společnosti Microsoft *(**http://support.microsoft.com**).*

- Možnost získat další informace o akcích v clusterech. V rámci clusterů lze zobrazit informace o stavu virtuálních serverů a o převzetí služeb při selhání.
- Zařazení nových tříd objektového modelu WMI (Windows Management Instrumentation) k ovládání serveru *Exchange 2003* pomocí skriptů.

Nástroj Move Mailbox

Nyní je možno přesunovat vícero poštovních schránek paralelně spuštěním několika instancí průvodce **Exchange Task Wizard**. Schránky takto lze přesouvat na jiný server nebo do jiné databáze poštovních schránek. Přesun schránky je možno také naplánovat a před započetím samotného procesu přesunu lze zprávy ve schránkách zkontrolovat, zdali nejsou porušené. Přesunovat schránky ve více instancích je užitečné například při migracích velkého počtu uživatelů ze serverů *Exchange 5.5* na servery *Exchange 2003* nebo při konsolidacích serverů *Exchange*.

Queue Viewer (Prohlížeč front)

Nyní je možno sledovat data fronty X.400 a SMTP z jednoho místa, a to přímo z nástroje **Queue Viewer** (Prohlížeč front). Lze také nastavit obnovovací interval front a sledovat dodatečné informace o dané frontě. **Prohlížeč front** zahrnuje nové funkce jako např. **Disable Outbound Mail** (Pozastavit odchozí poštu), která správcům umožňuje v případě potřeby pozastavit všechny odchozí e-mailové zprávy ve všech frontách SMTP. **Prohlížeč front** nyní také zobrazuje skryté fronty, jako např. fronty pro nezdařené pokusy o znovuodeslání zprávy.

***Disable Outbound Mail** nepozastavuje data fronty MTA ani systému.*

Stav linky (Link State)

Došlo ke dvěma vylepšením stavu linky:

- Stav linky zůstává beze změny, pokud neexistuje alternativní cesta. Neexistuje-li alternativní cesta pro linku (nebo směrování), bude server *Exchange* považovat cestu za dostupnou.
- Byla zavedena střídavě dostupná připojení (tzv. oscilující připojení). *Exchange 2003* zdokonaluje směrování kódu stavu linky kontrolou fronty stavů linek. Pokud existuje několik konfliktních změn stavů konektorů (oscilace – střídavě dostupný/nedostupný), bude server *Exchange 2003* považovat konektor za dostupný. Místo neustálých změn stavu linky je vhodnější nechat k dispozici střídavě dostupný konektor.

Public Folders Referrals (Odkazy veřejných složek)

Exchange 2003 poskytuje pro **odkazy veřejných složek** bohatší rozhraní než v předchozích verzích. Rozhraní je možno využít k vytvoření seznamu konkrétních serverů, mezi nimiž jsou odkazy povoleny. Např. odkazy lze omezit na jednu směrovací skupinu, nebo jenom povolit odkazy mezi danými servery v dané směrovací skupině.

Správa veřejných složek

Uživatelské rozhraní veřejných složek bylo vylepšeno o nové záložky:

- **Content** (Obsah) – zobrazuje obsah veřejné složky pomocí aplikace *Outlook Web Access*.
- **Find** (Najít) – prohledává jednotlivé položky v rámci vybrané veřejné složky nebo hierarchie veřejných složek.
- **Status** (Stav) – obsahuje informace o stavu veřejné složky, serveru složky, databázi složek, velikosti složky, počtu položek ve složce a času posledního přístupu.
- **Replication** (Replikace) – zobrazuje údaje týkající se replik veřejné složky.

Replikace veřejných složek

Nyní je možno manuálně spustit replikaci, aniž bych musel čekat na přednastavený replikační interval. Tímto způsobem lze replikovat pouze hierarchii složek (např. pokud jsem vytvořil novou složku a chci, aby se ihned zreplikovala na všechny servery) nebo obsah složky.

Public Folder Migration Tool (Nástroj na migraci veřejných složek)

Nástroj **Microsoft Exchange Public Folder Migration Tool** (pfMigrate.wsf) je ve skutečnosti skript využívající prostředí *Windows Script Host 2.0*. Skript vytváří repliky veřejné složky na novém serveru a poté, co se data zreplikovala, odstraňuje repliky ze zdrojového serveru. Jakákoliv replika se chová jako primární vůči datům, která obsahuje, a jakýkoliv server může být odstraněn ze seznamu replik.

Ještě před spuštěním samotného nástroje je možné vygenerovat zprávu o tom, kolik veřejných složek má být zreplikováno. Po spuštění nástroje je možné vygenerovat stejnou zprávu a určit, zdali veřejné složky byly úspěšně zreplikovány.

Konzola Message Tracking

Exchange 2003 vylepšuje možnosti sledování zpráv dvěma způsoby:

- Z důvodu větší flexibility a správy je možné změnit umístění souborů protokolů pomocí konzoly **Exchange System Manager**. Není již nutné používat nástroje pro modifikaci změn v *Active Directory* (např. **ADSI Edit**, **LDP**) jako u předchozí verze.
- Možnost sledování zpráv až za fázi kategorizace, kdy je adresa příjemce ověřena v *Active Directory* a je určena cesta, kudy bude zpráva odeslána. Nyní je možno sledovat zprávu ve fázi postkategorizace a během směrování.

Nástroj EXCHDUMP

EXCHDUMP je užitečný nástroj příkazového řádku, který sbírá informace o konfiguraci serveru *Exchange* z mnoha zdrojů, jako např. z *Active Directory*, metabáze *IIS* a registru. Nástroj generuje zprávu, která obsahuje údaje o konfiguraci pomocí vybraných přepínačů **/HTTP**, **/SERVER**, **/RPC**.

1.1.3 Novinky v oblasti výkonu a škálovatelnosti

Potlačení posílání zpráv Mimo kancelář do distribučních seznamů

Pokud uživatel není uveden na řádku **To** (Komu) nebo **Cc** (Kopie), zpráva **Mimo kancelář** není odeslána. To zabraňuje odesílání zprávy **Mimo kancelář** členům distribučních seznamů, kteří obvykle nechtějí, aby jim tyto zprávy byly doručovány. Tato změna také snižuje zatížení procesoru na serverech *Exchange*.

Ukládání členů distribučních seznamů do mezipaměti

Exchange 2003 využívá mezipaměť k vyhledání členů distribučního seznamu před samotným posláním zprávy. Tato mezipaměť byla optimalizována a výsledkem je snížení zátěže na server při vyhledávání členství, což se odráží asi v 60% úspoře z hlediska počtu dotazů služby *Active Directory*.

Výkonnost aplikace Outlook při synchronizaci

Exchange 2003 zvyšuje výkon synchronizačního procesu aplikace *Outlook* u klientů přepnutých do **režimu serveru Exchange s mezipamětí** (Cached Exchange Mode). Klienti s aplikací *Outlook* přepnutou do tohoto režimu dosahují následujících výhod:

- Lepší výkon klienta díky snížení počtu notifikací o změnách.
- Detekce nativního formátu zprávy (např. HTTP), ve kterém se má zpráva synchronizovat, a zaslání zpráv klientovi pouze v tomto formátu.
- Vylepšené podmínky pro synchronizaci hierarchie vnořených složek.
- Speciální zprávy určující počet a velikost e-mailů, jež jsou posílány na klienta a umožňují uživateli vybrat si, které e-maily si stáhne.
- Komprese dat provedená serverem *Exchange 2003* vedoucí ke snížení celkového objemu informací posílaných mezi aplikací *Outlook* a servery *Exchange 2003*.
- Optimalizace komunikace mezi klientem a serverem vedoucí ke snížení celkového počtu žádostí o data ze serveru (bez ohledu na to, jestli je aplikace *Outlook* přepnuta do **režimu serveru Exchange s mezipamětí**).

Tyto změny snižují celkovou zátěž na procesor serveru *Exchange*. Jinými slovy, server zpracovává nižší množství dat díky nižšímu množství požadavků ze strany klientů.

Výkonnost služby Outlook Web Access

Vylepšení výkonu aplikace *Exchange 2003 Outlook Web Access* (dále jen *Outlook Web Access*) zahrnuje rychlejší zobrazení schránek uživatelů a možnosti konfigurace pro rychlejší odezvu, zejména na pomalých linkách. To plyne hlavně ze sníženého počtu bajtů posílaných ze serveru do prohlížeče klienta.

Po zapnutí **formulářové autentizace** (Forms Based Authentication) si uživatelé mohou při přihlašování vybrat, jakou verzi aplikace *Outlook Web Access* budou používat: zdali verzi **Premium,** nebo **Basic** (Základní) (blíže kapitola 4.5.

- Verze **Premium** dává k dispozici všechny funkce aplikace *Outlook Web Access*. Tato volba vyžaduje, aby klienti používali prohlížeč *Microsoft Internet Explorer 5* a vyšší. Uživatelé používající prohlížeč *Internet Explorer 6* (a vyšší) a připojující se přes rychlou linku by měli využít verze **Premium**, aby dosáhli celkového zvýšení výkonu. Pokud je server *Exchange 2003* instalován na systému *Windows Server 2003*, je možno také využít vestavěnou kompresi GZIP (data jsou ze serveru do prohlížeče posílána komprimovaně), která byla také přidána do prohlížeče *Internet Explorer 6* a vyššího.
- Verze **Basic** dává k dispozici pouze část funkcí obsažených ve verzi **Premium** (např. neobsahuje volbu **Show/Hide Preview Pane** (Zobrazit/Skrýt náhled), volby kontextové nabídky, dvouřádkový náhled na e-mailovou zprávu, kontrolu pravopisu atd.). Pro „svižnější“ práci s aplikací *Outlook Web Access* na pomalých linkách je doporučeno používat verzi **Basic**, i když to může být na úkor snížení funkčnosti.

Outlook Web Access Basic funguje v jakémkoliv prohlížeči na jakékoliv platformě, což určitě potěší správce heterogenních sítí, ve kterých se používají i jiné operační systémy než Microsoft Windows.

Sledování výkonnosti klientské aplikace Outlook

Servery *Exchange 2003* mohou sbírat informace o aktuálním výkonu aplikace *Outlook*. Servery zaznamenávají prodlevy a chyby protokolu RPC (Remote Procedure Call) pozorované na klientských stanicích s aplikací *Outlook*. Tato data jsou přeposílána na server *Exchange* pro účely řešení potíží s dostupností serverů a z důvodu pozdějších rozborů a analýz.

1.1.4 Novinky v oblasti spolehlivosti

Podpora až osmi uzlů clusteru

Na serveru *Exchange 2003* byla představena podpora clusterů až o osmi uzlech. Clustery o osmi uzlech je možné vytvořit pouze na systémech *Windows Server 2003 Enterprise Edition* a *Windows Server 2003 Datacenter Edition*. Omezením, které je nutno vzít v potaz, je fakt, že cluster o třech až osmi uzlech musí obsahovat alespoň jeden pasivní uzel – jedná se o tzv. konfiguraci active/passive. Pouze cluster o dvou uzlech lze instalovat v konfiguraci active/active.

Pro vytvoření clusteru lze použít Exchange 2003 pouze ve verzi Enterprise.

Microsoft nicméně doporučuje nasadit servery *Exchange* v konfiguraci active/passive z následujících důvodů:

- Clustery active/passive se daleko lépe škálují. Instalace dalšího pasivního uzlu je obdobná jako instalace stand-alone serveru *Exchange*.
- Clustery active/passive jsou daleko více spolehlivější. Při selhání jsou virtuální servery *Exchange* vždy převzaty „čerstvým“ pasivním uzlem.
- Clustery active/active mají limit 1900 simultánních připojení k uzlu, který hostuje virtuální servery *Exchange*.

Zkrácení doby pro převzetí clusteru při selhání

Hierarchie závislostí služeb serveru *Exchange* byla pozměněna, a to tak, že služby protokolů (POP3, IMAP4 atd.) již nejsou závislé na službě **Microsoft Exchange Information Store**. To umožňuje správcům uvést úložiště *Exchange* do stavu online či offline nezávisle na protokolech, a zkrátit tak dobu nutnou pro převzetí clusteru při selhání (Cluster Failover). Navíc, pokud zdroj (Resource) úložiště *Exchange* selže a má být znovu nastartován, nemusí čekat na žádný další zdroj, než bude uveden do stavu online.

Pokud je použita kombinace serveru *Exchange 2003* a operačního systému *Windows Server 2003*, pak je také zkrácena doba, po kterou *Exchange* detekuje, který uzel je volný pro převzetí virtuálních serverů *Exchange* při selhání, což se projeví ve zkrácení doby výpadku serveru.

Nástroj Mailbox Recovery Center

Pomocí nástroje **Mailbox Recovery Center** je možné hromadně napojit vícero odpojených poštovních schránek ke správným účtům uživatelů v *Active Directory*. Nástroj skenuje databázi poštovních schránek a rozpozná všechny odpojené schránky a automaticky je spáruje s účty uživatelů v *Active Directory*. Nástroj lze takto využít v některých scénářích obnovy serveru *Exchange* po havárii. Jeho hlavní výhodou je zkrácení doby výpadku havarovaného serveru.

*V Resource Kitu pro Exchange 2000 existoval nástroj **MBCONN**, který plnil podobnou funkci jako **Mailbox Recovery Center**.*

Recovery Storage Group (Skupina úložišť pro obnovení)

Skupina úložišť pro obnovení (Recovery Storage Group) je speciální typ skupiny úložišť (pátá skupina), která může koexistovat vedle standardních čtyřech skupin úložišť. Skupina poskytuje dočasné umístění a prostor pro obnovu databáze poštovních schránek. Poté je možné z obnovené databáze zkopírovat jednotlivé zprávy či celou schránku do původního umístění (pomocí nástroje **ExMerge**). Odpadá tak problém z předchozí verze, kdy bylo třeba nejprve postavit novou organizaci *Exchange* (nejlépe v testovacím labu), v ní zálohu obnovit a pak pomocí souborů **.pst** zprávy přetáhnout na server v původní organizaci. Tato nová skupina značně zkracuje dobu obnovy a nevyžaduje žádný dodatečný hardware (obnova je prováděna v rámci stejného serveru *Exchange* či jiného serveru ve stejné administrativní skupině).

Dle mého názoru se jedná o jednu z nejužitečnějších funkcí v nové verzi serveru Exchange 2003, která bude podrobněji rozebrána v kapitole 5.3.2.

Error Reporting (Zasílání zpráv o chybách)

Tato funkce umožňuje správcům snadněji zasílat zprávy o chybách firmě *Microsoft*, která tyto zprávy sbírá a údaje využívá ke zlepšení funkčnosti svých produktů do budoucna (vývoj nových záplat a aktualizací *Service Pack*). Pokud se při správě serveru v konzole **Exchange System Manager** nebo v konzole **Active Directory Users and Computers** (Uživatelé a počítače služby Active Directory) vyskytne chyba, pak je zobrazeno okno s chybovým hlášením a správce je vybídnut k zaslání chyby firmě *Microsoft* (viz obr. 2.71). Chyba je zasílána přes protokol HTTPS v 10–50kilobajtových souborech.

Vše je integrováno s aplikací *Dr. Watson 2.0*, která zaznamenává chyby konzoly **Exchange System Manager**, služeb **System Attendant**, **DSMx**, **Exchange Management**, **Exchange Setup** a **Exchange Store**.

Nástroj pro zasílání chyb je možné nastavit tak, aby posílal chybová hlášení automaticky firmě *Microsoft*. Tato funkce je užitečná, pokud si správce nepřeje být přerušován při administraci ihned při výskytu chyby (např. kontroluje pravidelně **Prohlížeč událostí** nebo o dané chybě ví).

Vylepšení používání a sledování paměti

Používání virtuální paměti v systému *Windows Server 2003* ve spojení s úložištěm serveru *Exchange* snižuje fragmentaci a přináší vyšší dostupnost na serverech zpracovávajících požadavky velkého počtu uživatelů.

Správa virtuální paměti serverů v clusteru byla také pozměněna. Při zpětném převzetí clusteru na původní uzel je nastartován nový proces služby úložiště, tím pádem je tomuto procesu alokován nový „čerstvý" blok virtuální paměti.

1.1.5 Novinky v oblasti zabezpečení a služeb

Filtrování příjemců u příchozí pošty (Recipient Filtering)

Tento filtr může blokovat zprávy určené neexistujícím příjemcům pomocí náhledů do *Active Directory*. Takto lze filtrovat e-maily adresované uživatelům, kteří nejsou v *Active Directory* nebo kterým odesílatel nemá oprávnění zprávu poslat. Jakákoliv příchozí zpráva vyhovující těmto kritériím je zamítnuta a server SMTP vrátí během relace chybu 550 5.x.x.

Správce serveru může tento filtr také využít k blokování zpráv posílaných na existující e-mailovou adresu v rámci organizace. Toto lze využít např. k zabránění posílání e-mailů z internetu do velkých distribučních seznamů typu **info@firma.cz**, **zamestnanci@firma.cz**.

Seznamy povolených a blokovaných IP adres v reálném čase (Realtime Block Lists)

Server *Exchange 2003* dokáže filtrovat relaci SMTP pomocí seznamů blokovaných IP adres v reálném čase (tzv. Real-time Block Lists (RBL), někdy také nazývané Black Lists či Blackhole Lists). Na internetu existuje velké množství poskytovatelů těchto seznamů RBL, na které se server *Exchange* může napojit při kontrole příchozí zprávy a zkontrolovat, zdali se zdrojová IP adresa, ze které zpráva přichází, nevyskytuje na některém z těchto seznamů. Nejznámější poskytovatelé RBL jsou např. **relays.ordb.org** nebo **sbl.spamhaus.org**.

Je možné nastavit vícero RBL seznamů a určit prioritu pořadí, ve které bude filtr na zprávu aplikován. Pokud je IP adresa na RBL seznamu nalezena, na příkaz RCPT TO odpoví server SMTP odesílateli chybovým hlášením 550 5.x.x a popř. textem, jejž nadefinuje správce.

Omezení distribučních seznamů

U distribučních seznamů je nyní možné nastavit funkci **From Authenticated Users Only** (Pouze od autentizovaných uživatelů). Po zapnutí této funkce nemohou být zprávy do distribučního seznamu posílány anonymně, ale pouze autentizovaně (odesílatel se musí vůči serveru SMTP nejprve autentizovat pomocí uživatelského jména a hesla a teprve poté e-mail odeslat). Správci mohou také určit, kteří uživatelé mají či nemají oprávnění odesílat zprávy do distribučního seznamu.

Autentizace Kerberos

Aplikace *Outlook 2003* nyní může používat protokol Kerberos k autentizaci uživatelů vůči serverům *Exchange 2003*. Kerberos je bezpečný protokol s dvojím ověřováním, kde se ověřuje jak identita uživatele, tak síťových služeb pomocí vystavování identifikačních dat ve formě jedinečného klíče zvaného Ticket (lístek). Pokud je virtuální server *Exchange* vytvářen na serveru s operačním systémem *Windows Server 2003* nebo *Windows 2000 SP3* (nebo vyšším), pak je protokol Kerberos zapnut ve výchozím stavu.

K zajištění autentičnosti ověřovacích údajů (uživatelské jméno, heslo, doména, popř. uživatelský certifikát, v angličtině tzv. credentials) využívá server *Exchange 2003* delegaci Kerberos při posílání pověření uživatele mezi serverem *Exchange* front-end (např. server s webovými aplikacemi *Outlook Web Access* a *Outlook Mobile Access*) a serverem *Exchange* back-end (např. server držící databáze poštovních schránek).

Pokud jsou v síti použity doménové řadiče s operačním systémem *Windows Server 2003*, uživatelé se mohou nechat autentizovat i na doménových řadičích v důvěryhodných doménových strukturách, umožňujíce tak existenci uživatelských účtů a serverů *Exchange* v jiných doménových strukturách. Jedná se o tzv. **autentizaci mezi doménovými strukturami** (Cross-Forest Authentication), pomocí které je možno vytvořit obousměrné tranzitivní vztahy důvěryhodnosti mezi dvěma a více doménovými strukturami. Tohoto typu autentizace se dá vyžít při implementaci scénáře Account Forest/Resource Forest, kdy v jedné doménové struktuře se nacházejí účty uživatelů a v druhé jsou vytvořeny poštovní schránky, které jsou navázány na tyto účty.

Ochrana soukromí v aplikaci Outlook a Outlook Web Access

Ve výchozím stavu je zablokován externí obsah e-mailové zprávy (tzv. Web Beacons), který se stahuje dodatečně při otevření zprávy v aplikacích *Outlook 2003* a *Outlook Web Access*. Jedná se hlavně o e-maily posílané ve formátu HTML, kde objekty obrázků nejsou přibaleny ke zprávě a musí být dodatečně staženy při čtení zprávy. Tato nová bezpečnostní funkce zabraňuje odesílatelům nevyžádané pošty (Spammers) ve zpětném ověřování platnosti e-mailové adresy. Výchozí nastavení lze pozměnit tak, že nebude blokován externí obsah u e-mailů, jejichž odesílatelé jsou na seznamu **Safe Senders** (bezpeční odesílatelé, tzv. White List), popř. kdy externí obsah je stahován z důvěryhodných internetových zón (zóna **Důvěryhodné servery** v prohlížeči *Internet Explorer*).

Antivirové rozhraní API

Antivirové aplikační programové rozhraní (VSAPI – Virus Scanning API) nyní umožňuje antivirovým výrobcům instalovat a spouštět své programy na serverech *Exchange*, které nedrží poštovní schránky uživatelů, což jsou např. servery sloužící jako brána SMTP či bridgehead servery. *VSAPI* verze 2.5 obsahuje vylepšené funkce, které umožňují mazat zprávy a zasílat odesílateli notifikace o zablokování zavirované zprávy.

Autentizace Kerberos mezi doménovými strukturami na úrovni protokolu SMTP

Exchange 2003 zabraňuje podvržení totožnosti odesílatele zprávy. To je zajištěno vyžádáním autentizace před přeložením jména odesílatele na jméno zobrazené v globálním seznamu adres (Global Address List). Pro správnou funkčnost překladu kontaktů z jiné organizace na jména v *Active Directory* je potřeba zprovoznit autentizaci protokolu Kerberos mezi doménovými strukturami na úrovni konektorů SMTP, kdy příchozí pošta je autentizována pomocí účtu z protější doménové struktury.

Zabezpečení clusterů

Model oprávnění clusteru se změnil. Zvláštní oprávnění pro manipulaci s virtuálními servery *Exchange* závisí jednak na režimu, do kterého je organizace přepnuta (nativní nebo smíšený), jednak na topologii. Hlavní změnu v modelu oprávnění prodělala služba *Windows Cluster Service*, která již nevyžaduje oprávnění **Exchange Full Administrator** při vytváření, modifikaci či mazání virtuálního serveru *Exchange*.

Další změnu zaznamenaly protokoly IMAP4 a POP3. Prostředky protokolů IMAP4 a POP3 již nevznikají při vytváření virtuálního serveru *Exchange*. Tyto dva protokoly nejsou totiž potřeba na všech serverech *Exchange*.

Pokud je vyžadován zabezpečený kanál mezi serverem front-end a servery back-end v clusteru, je nyní možné použít protokol IPSec. Tato konfigurace je plně podporována, pokud server *Exchange 2003* běží na operačním systému *Windows Server 2003*.

Průvodce Internet Mail Wizard

V serveru *Exchange 2003* je implementována nová verze průvodce konfigurace internetové pošty (*Internet Mail Wizard*). Tento průvodce zjednodušuje proces konfigurace příchozí a odchozí pošty. Průvodce je primárně spíše určen pro malé a střední firmy, jejichž prostředí není příliš komplexní.

Protokolování služby ArchiveSink

Služba *ArchiveSink* slouží k archivaci příchozí a odchozí pošty na serveru *Exchange*. Nová verze má zdokonalené protokolování všech zpráv a podrobností týkající se příjemců. Při zapnutí funkce archivace je možno zapnout také protokolování zpráv. *ArchiveSink* si pak vytváří dodatečný soubor ve formátu XML pro každou archivovanou zprávu. Tento soubor obsahuje informace o zprávě, jako je identifikátor zprávy (Internet Message Identifier), předmět zprávy a seznam všech příjemců zprávy (včetně skryté kopie).

Diagnostické protokolování a kódy doručování zpráv

Exchange 2003 má následující vylepšení v oblasti zpráv o nedoručení (NDR):

- Vznikla nová kategorie pro protokolování notifikací o stavu doručení zprávy, která tyto notifikace umožňuje diagnostikovat.
- Byly zde také přidány nové kódy pro notifikace o stavu doručení zprávy, které pomáhají při řešení problémů se směrováním zpráv.

Omezení relayingu

Relaying (povolení posílání zpráv přes server SMTP) nyní může být omezen jen na určité uživatele či skupiny uživatelů pomocí standardního seznamu přístupových práv (Discretionary Access Control List, tzv. DACL). Možnosti povolení relayingu na konkrétní IP adresu, doménu a podsíť jsou stále k dispozici. Toto omezení je užitečné ve chvíli, kdy správce potřebuje povolit posílaní e-mailů do internetu pouze určité skupině uživatelů a zbytku tuto možnost zakázat.

Zabezpečení distribučního seznamu

Na serveru *Exchange 2003* je možno nastavit, kdo může posílat e-mail do daného distribučního seznamu, čehož je dosaženo pomocí restrikcí na určité uživatele či skupiny uživatelů přes standardní seznam oprávnění DACL. Tato nová funkce zabezpečuje interní distribuční seznamy před nevyžádanou poštou od nedůvěryhodných odesílatelů z internetu. Zabezpečení seznamů funguje pouze tehdy, pokud je na bráně či bridgehead serveru instalován *Exchange 2003*.

Oprávnění na veřejných složkách pro neznámé uživatele

Složky, které obsahují v seznamu řízení přístupu (ACL) neznámé uživatele, jejichž jméno nemůže být přeloženo na bezpečnostní identifikátor (Security ID), tyto uživatele vynechávají.

Replikace databází veřejných složek

Servery držící databázi veřejných složek si synchronizují obsah s dalšími místními servery, a to i tehdy, když obsah místních serverů není kompletní. Správce může použít klíč v registru, kde je určen první server, který bude použit v procesu backfillingu (proces, kdy s server, který neobsahuje všechny aktualizace, stahuje chybějící aktualizace z jiného serveru). Při určování serveru, jenž bude použit jako zdroj backfillingu, *Exchange* nejprve vytváří seznam všech serverů, které mají alespoň část obsahu, a poté seznam roztřídí následovně:

1. Podle nejnižších nákladů na transport, kdy servery ve stejné síti (Site) mají vyšší prioritu než servery ve vzdálených sítích.
2. U serverů se stejnými náklady na transport probíhá třídění znovu podle nejnovější verze serveru *Exchange*. V předchozích verzích (*Exchange 5.5* a *Exchange 2000*) měly

prioritu servery s novější verzí serveru *Exchange* bez ohledu na náklady na transport, což mělo za následek, že aktualizace se stahovaly neefektivně např. ze vzdálené sítě se serverem *Exchange 2000*, a ne z místní se serverem *Exchange 5.5*.

3. U serverů se stejnými náklady na transport a stejnou verzí serveru *Exchange* probíhá třídění znovu podle největšího počtu potřebných aktualizací dostupných na serveru. V předchozích verzích byl vybrán ten server, který obsahoval všechny potřebné aktualizace bez ohledu na náklady na transport. U serveru *Exchange 2003* bylo toto chování pozměněno, a to tak, že některé aktualizace jsou stahovány ze serveru s nejnižšími náklady na transport (ten, kterých jich obsahuje nejvíc) a zbytek je stahován z jiných serverů s vyššími náklady.

1.1.6 Co bylo odstraněno oproti serveru Exchange 2000

Ačkoliv většina věcí, o kterých se v této části knihy bavíme, jsou novinky, které přibyly na serveru *Exchange 2003* nebo byly vylepšeny oproti serveru *Exchange 2000*, je třeba také zmínit funkce, které byly odstraněny nebo přesunuty do jiného produktu firmy *Microsoft*. Následující služby či vlastnosti, na něž jsme byli zvyklí u serveru *Exchange 2000*, v nové verzi serveru *Exchange 2003* chybí:

- Konektory pro *Lotus cc:Mail* a *MS Mail*.
- Služby pro spolupráci v reálném čase.
- Namapovaný disk **M:**.
- Key Management Service.

Konektory pro Lotus cc:Mail a MS Mail

Komponenty konektorů pro *Lotus cc:Mail* a *MS Mail* nejsou dodávány se serverem *Exchange 2003*. Konzola **Exchange System Manager** ze serveru *Exchange 2003* nepodporuje správu těchto konektorů vytvořených na serveru *Exchange 2000*. Pokud je potřeba tyto konektory spravovat, musí se použít konzola **Exchange System Manager** ze serveru *Exchange 2000 SP3* (nebo vyšší). Před inovací serveru *Exchange 2000* s těmito konektory na server *Exchange 2003* je nutno konektory odinstalovat, jinak operace inovace nedovolí pokračovat dál. Pokud by měly tyto konektory v organizaci zůstat, je třeba zachovat alespoň jeden server *Exchange 2000*, který bude konektory hostovat.

Služby pro spolupráci v reálném čase

Exchange 2000 obsahoval řadu komponent pro spolupráci v reálném čase, jako např. *Instant Messaging*, *Conferencing Server* a *Chat*. Tyto služby nebyly do serveru *Exchange 2003* implementovány. Většina z nich byla zařazena do nového dedikovaného produktu, jehož finální jméno je *Microsoft Office Live Communications Server* (známý také pod kódovým označením *Greenwich* nebo později *Realtime Collaboration Server*). Podobně jako u konektorů, pokud je na serveru *Exchange 2000* přítomna jedna z komponent pro spolupráci v reálném čase, není možné provést inovaci na novou verzi *Exchange 2003*.

Namapovaný disk M:

Server *Exchange 2000* měl databázi úložiště namapovanou jako disk **M:**, přes který bylo možno přistupovat nízkoúrovňově přímo do databáze (např. pomocí *Průzkumníka*). *Exchange 2003* má toto mapování vypnuto. Stále je možné přistoupit přes souborový systém do úložiště, ale je třeba použít přímou cestu **\\.\BackOfficeStorage\Jmenny_Prostor**. Např. pokud bychom chtěli přistoupit do databáze poštovních schránek na serveru *Exchange* v doméně **grada.cz**, příkaz bude vypadat následovně:

```
dir \\.\BackOfficeStorage\grada.cz\mbx
```

Důvodem pro odstranění mapování disku **M:** bylo v některých případech poškození databáze serveru *Exchange 2000* operacemi ze souborového systému, jako např. skenování disku **M:** pomocí antivirových programů a zálohování celého disku **M:**.

*Na serveru Exchange 2000 se nyní také doporučuje permanentně odstranit mapování disku **M:**. Bližší informace lze nalézt v článku Q305145 „HOW TO: Remove the IFS Mapping for Drive M in Exchange 2000 Server" znalostní databáze společnosti Microsoft (**http://support.microsoft.com**).*

Key Management Service

Služba *Key Management Service* (KMS) zjednodušovala správu infrastruktury veřejného klíče (PKI) při zprovoznění podpory digitálně podepisovaných a šifrovaných zpráv mezi uživateli v rámci organizace. Služba *Key Management Service* poskytovala mechanismus pro automatické přidělení a instalaci uživatelského certifikátu, správu archivace a obnovy klíčů. *Exchange 2003* již komponentu *Key Management Service* neobsahuje, ale dále podporuje standardní implementace PKI pomocí certifikátů X.509v3. Je možné využít řešení PKI zahrnuté do operačního systému *Windows Server 2003* (komponenta *Certifikační služby*), které má už v sobě integrované funkce pro automatické vydávání certifikátů uživatelům a pro archivaci a obnovu klíčů.

1.2 Edice serveru Exchange 2003

Před samotnou instalací je potřeba se rozhodnout pro správnou edici serveru *Exchange 2003*. Je nutno vzít v potaz velikost organizace co do počtu uživatelů, kteří budou mít své poštovní schránky uloženy na serveru *Exchange*, včetně odhadu růstu firmy v blízké budoucnosti, limity na velikost schránek uživatelů a požadavky na vysokou dostupnost a odolnost proti výpadkům.

Hlavní rozdíl mezi těmito dvěma edicemi je v podpoře vytváření vícera databází poštovních schránek a možnosti využití služeb clusteru. Na trhu jsou dostupné dvě edice, a to *Microsoft Exchange Server 2003 Standard Edition* a *Microsoft Exchange Server 2003 Enterprise Edition*.

U serveru Exchange 2000 byla ještě dostupná verze Microsoft Exchange 2000 Conferencing Server.

Rozhodujícím faktorem při výběru je ve většině případů cena. Edice *Enterprise* je mnohonásobně vyšší a pro menší organizace s nižším rozpočtem na informační technologie díky této ceně mnohdy nedostupná. V tabulce 1.1 jsou uvedeny hlavní rozdíly.

Funkčnost	Exchange 2003 Standard Edition	Exchange 2003 Enterprise Edition
Podpora skupin úložišť	1 skupina úložišť	4 skupiny úložišť
Počet databází na skupinu úložišť	2 databáze	5 databází
Velikost databáze	16 gigabajtů (GB)	Maximum 16 terabajtů, omezení dáno pouze hardwarem
Podpora služeb clusteru	Ne	Ano
Konektor X.400	Ne	Ano

Tab 1.1: Srovnání edicí Exchange 2003 Standard a Enterprise

Znalci předchozí verze serveru Exchange si určitě povšimnou zásadní změny u těchto dvou edicí, a to že zmizelo omezení na konfiguraci topologie serverů front-end/back-end. Nyní je možno nakonfigurovat i Exchange 2003 Standard Edition jako server front-end.

1.3 Licencování

Licencování serveru *Exchange* se během let několikrát změnilo. Cena edice *Standard* se postupně snižuje, zatímco cena edice *Enterprise* vzrůstá. V době psaní této knihy stála serverová licence edice *Standard* 699 USD a edice *Enterprise* 3999 USD.

Licencování klientů bylo také pozměněno. Pro přístup do poštovní schránky je kromě přístupové licence *Exchange CAL* stále nutná přístupová licence *Windows CAL*, protože poštovní schránka je vázána na uživatelský účet. Na rozdíl od předchozí verze *Exchange 2000* si nyní firma může vybrat mezi dvěma licenčními režimy *Exchange CAL*:

- *Přístupová licence pro zařízení (Device CAL)*. Přístupová licence pro zařízení je vhodná tam, kde se více zaměstnanců střídá u jednoho počítače nebo veřejného terminálu.
- *Přístupová licence pro uživatele (User CAL)*. Přístupová licence pro uživatele je vhodná tam, kde jeden zaměstnanec přistupuje do své poštovní schránky z více zařízení (PC, laptop, PDA, mobilní telefon).

Cena obou přístupových licencí *Exchange 2003 CAL* je stejná u obou edicí. V době psaní této knihy byla cena této přístupové licence 67 USD. Zvolení správného způsobu licencování může ušetřit spoustu peněz.

Kromě přístupových licencí *Exchange 2003 CAL* je také možno zakoupit *licenci pro externí připojení* (External Connector – EC). *Licence pro externí připojení* je volitelná licence pro externí uživatele, kteří nejsou zaměstnanci dané firmy, ale mají v této firmě vytvořenou poštovní schránku, do níž přistupují. Tato licence umožňuje přístup neomezeného počtu externích uživatelů, jako jsou např. obchodní partneři, dodavatelé, zákazníci apod., bez nutnosti nákupu individuálních přístupových licencí *Exchange 2003 CAL*. Tento typ licence je dostupný pouze přes multilicenční programy

Každá z přístupových licencí *Exchange 2003 CAL* také zahrnuje licenci pro aplikaci *Microsoft Office Outlook 2003* a *Microsoft Entourage X for Mac*. Za používání aplikace *Outlook 2003* již tedy není nutno platit žádné dodatečné poplatky.

Bližší informace o licencování serveru Exchange 2003 *lze nalézt na adrese* ***http://www.microsoft.com/exchange/howtobuy/enterprise.asp***.

1.4 Active Directory

Jelikož *Exchange 2003* nelze nainstalovat samostatně bez adresářové služby *Active Directory*, pojďme si nejprve v krátkosti zopakovat základní fakta o této službě.

V minulosti na operačních systémech *Windows NT* byly objekty účtů uživatelů, skupin a počítačů ukládány do SAM (Security Accounts Manager) databáze. Adresář SAM databáze a jeho přístupová rozhraní byly značně omezeny co se týče funkčnosti a bylo obtížné tuto databázi dále rozšiřovat a modifikovat. Aby vůbec mohly aplikace jako *Exchange 5.5* a *SQL Server* fungovat, byla na podporu těchto aplikací vyžadována oddělená adresářová služba.

U operačního systému *Windows 2000* tato omezení zmizela díky nové adresářové službě zvané *Active Directory*, do které byly začleněny některé koncepty známé z adresáře *Exchange 5.5* (identifikátory GUID, přístup přes protokol LDAP atd.). *Active Directory* je plně škálovatelná a rozšiřitelná databáze vystavěná na principech adresářových služeb LDAP (Lightweight Directory Access Protocol). Poskytuje uživatelům a službám distribuovaný přístup k objektům odkudkoliv v organizaci pomocí serverů zvaných globální katalogy (popsáno dále).

Active Directory je databázovým systémem fungujícím na replikovaném multi-master modelu. *Active Directory* je vystavěna na technologii *Joint Engine Technology (JET)*, která je propojena s další technologií zvanou *Extensible Storage Engine (ESE)*. *ESE* je transakční databázový systém, který využívá protokolární soubory k zápisu změn v databázi, což zajišťuje vyšší spolehlivost a rychlost obnovy při haváriích systému.

Ti z vás, kdo se setkali se serverem Exchange 5.5*, si určitě vzpomenou, že měl svůj adresář také vystavěn na technologii ESE. Implementace ESE v* Active Directory *je ale daleko sofistikovanější, i když svého předchůdce nezapře.*

Hlavní vlastnost, která byla v nové verzi *ESE* vylepšena, je odstranění limitů na velikost databáze. *ESE* umožňuje růst databáze *Active Directory* až do enormní velikosti 70 TB, čímž je zajištěno ukládání až několika miliónů objektů. Těmito objekty mohou být např.

uživatelé, skupiny, počítače, domény atd. Každý objekt je složen ze sady atributů, které definují tento objekt v adresářové službě – např. objekt uživatele má atributy jako jméno, příjmení, uživatelské jméno, heslo atd.

Schopnost uložit nespočetně mnoho objektů a atributů, znásobená možností rozšířit adresář o nové objekty a atributy, dává *Active Directory* univerzální využitelnost. Tato mnohostranná využitelnost umožňuje integrovat do *Active Directory* další aplikace jako např. *Exchange 2000*, *2003*, *Microsoft ISA Server 2000*, *Microsoft Office Live Communications Server* a další. Tyto aplikace dále nevyžadují žádnou vlastní adresářovou službu a mohou se plně spolehnout na *Active Directory*, která má již zabudované mechanismy replikací mezi doménovými řadiči. Na rozdíl od serverů *Exchange 4* a *5* se databáze *Active Directory* replikuje na úrovni atributu.

Architektura *Active Directory* využívá dvou topologií, které jsou na sobě navzájem nezávislé. Jednak se bavíme o logické topologii, která je složena z doménové struktury (Forest), doménových větví (Trees) a domén propojených vztahy důvěryhodnosti. Tato logika je založena na systému DNS (Domain Naming System), který je známý jako systém používaný pro překlad jmen na internetu. Domény lze dále členit na organizační útvary. Ve vícedoménovém prostředí hrají významnou úlohu servery konfigurované jako globální katalogy. Globální katalog obsahuje nejčastěji prohledávané informace ze všech domén, a usnadňuje tak prohledávání objektů a jejich atributů v šíři celé doménové struktury. Logická topologie slouží k efektivnějšímu způsobu seskupování objektů za účelem jejich správy a umožňuje neomezenou škálovatelnost tohoto modelu.

Naprosto jiné pojetí přináší fyzická topologie. Zde se bavíme o sítích (Sites), IP podsítích a doménových řadičích. Sítě jsou kolekce počítačů fyzicky ležících na jedné IP podsíti. Sítě (Sites) se většinou mapují na existující IP podsítě (jedné i více) jednotlivých lokalit firmy. Sítě (Sites) vytváříme za účelem zefektivnění replikací mezi těmito lokalitami, které jsou většinou propojeny pomalými linkami WAN.

1.5 Active Directory a Exchange 2003

Exchange 2003 využívá k ukládání všech svých systémových informací doménovou strukturu (Forest) *Active Directory*. Každý objekt *Exchange 2003* je reprezentován v databázi *Active Directory* a v okamžiku změny replikován v šíři celé doménové struktury změny. Doménová struktura *Active Directory* určuje hranice organizace *Exchange 2003*. V rámci jedné doménové struktury není možné mít více než jednu organizaci *Exchange 2003*.

Active Directory ukládá data *Exchange 2003* do oddílů, jež jsou někdy nazývány jmennými kontexty (Naming Context – NC). *Active Directory* využívá jmenných kontextů k definování mezí pro informace uložené v databázi. Informace uložené v *Active Directory* na každém doménovém řadiči v doménové struktuře jsou rozděleny do tří oddílů: doménový, konfigurační a schéma. Všechny tři oddíly jsou uloženy na doménových řadičích.

- **Doménový oddíl** *Active Directory* obsahuje všechny objekty (jako např. uživatele, skupiny, kontakty a počítače) pro danou doménu. Příjemci systému *Exchange 2003* (Recipients) jsou objekty *Active Directory*. Příjemcem *Exchange 2003* může být uživatel,

skupina nebo kontakt. Doménová část *Active Directory* je replikována pouze na doménové řadiče dané domény, a ne za hranice této domény.

- **Konfigurační oddíl** *Active Directory* obsahuje konfiguraci organizace *Exchange 2003*. Konfigurační oddíl definuje topologii, konektory, protokoly a nastavení služeb *Exchange 2003*. Jelikož *Active Directory* replikuje konfigurační oddíl přes všechny domény v doménové struktuře, konfigurace organizace *Exchange 2003* je takto replikována v šíři celé doménové struktury. Tím je zajištěna komunikace mezi jednotlivými servery *Exchange 2003* v organizaci (jednotlivé servery *Exchange 2003* o sobě navzájem vědí).
- **Oddíl schématu** *Active Directory* obsahuje všechny třídy objektů, které mohou být vytvořeny v *Active Directory*, a stejně tak všechny atributy k těmto třídám. Tato data jsou společná pro všechny domény v doménové struktuře a jsou replikována na všechny její doménové řadiče. V průběhu instalace prvního serveru *Exchange 2003* nebo spuštěním programu *Setup* s přepínačem **/ForestPrep** je schéma rozšířeno o nové atributy pro *Exchange 2003* (většina názvů atributů začíná písmeny **msExch**). Schéma je rozšířeno za použití souborů LDIF (Lightweight Directory Interchange Format), které je možné si prohlédnout v souborech LDIF na instalačním CD-ROM *Exchange 2003* (soubory **Schema0.ldf** až **Schema9.ldf** v adresáři **\Setup\i386\Exchange**).

1.6 Internet Information Services

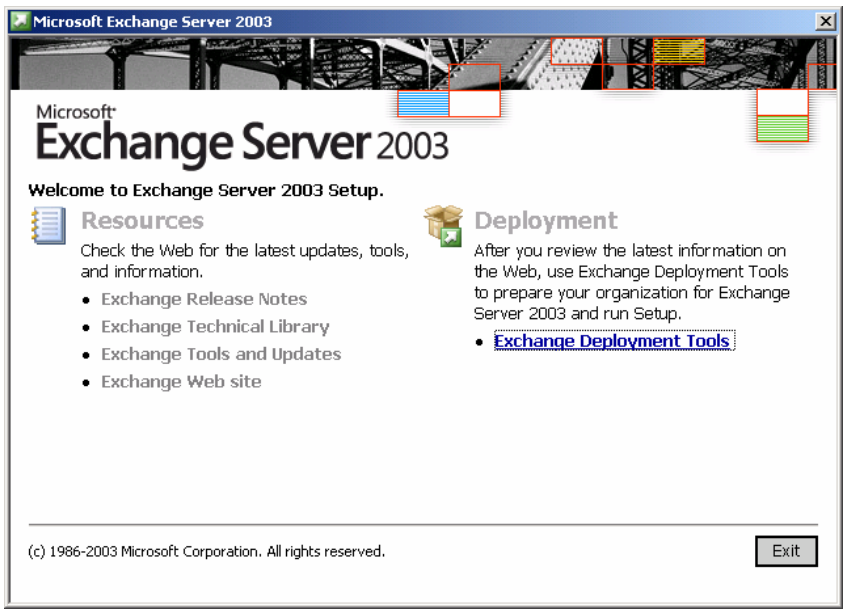
Jednou ze silných stránek serveru *Exchange 2003* je podpora standardních internetových protokolů pro přenos e-mailových zpráv. Ve starších verzích serverů *Exchange* (*4.0, 5.5*) byly tyto komponenty zahrnuty přímo do instalace serveru *Exchange*. Nyní se celá odpovědnost přesunula na službu *Internet Information Services (IIS)*, vestavěnou komponentu operačního systému *Windows 2000* a *Windows Server 2003*. Všechny protokoly serveru *Exchange 2003* jsou hostované v rámci procesu *Internet Information Services* (**Inetinfo.exe**). Po instalaci serveru *Exchange 2003* je rozšířena služba SMTP tak, aby mohla podporovat směrovací funkce organizace *Exchange*.

Subsystémy *Exchange 2003*, jako jsou protokoly a úložiště, nyní mohou být umístěny na oddělených serverech, čímž je zajištěna větší škálovatelnost. Aby toto fungovalo co nejefektivněji, je potřeba rychlé a spolehlivé metody, která by zajišťovala výměnu informací mezi *Internet Information Services* a úložištěm dat serveru *Exchange*. Tato potřeba je zajištěna komponentou zvanou *Exchange Interprocess Communication Layer (ExIPC)*.

2. Instalace serveru Exchange 2003

2.1 Exchange Server Deployment Tools

Exchange 2003 s sebou přináší sadu nástrojů zvaných **Exchange Server Deployment Tools**. Ve skutečnosti se jedná o normativního průvodce, který nás krok za krokem provází správným nasazením serveru *Exchange 2003*. Tohoto průvodce je možné spustit několika způsoby, tím úplně nejjednodušším je nechat si automaticky spustit instalační CD-ROM serveru *Exchange* a ze sekce **Deployment** zvolit položku **Exchange Deployment Tools** (popř. je možné jej spustit přímo z **\Support\Exdeploy\Exdeploy.hta**).



Obr. 2.1: Úvodní obrazovka instalačního CD-ROM serveru Exchange 2003

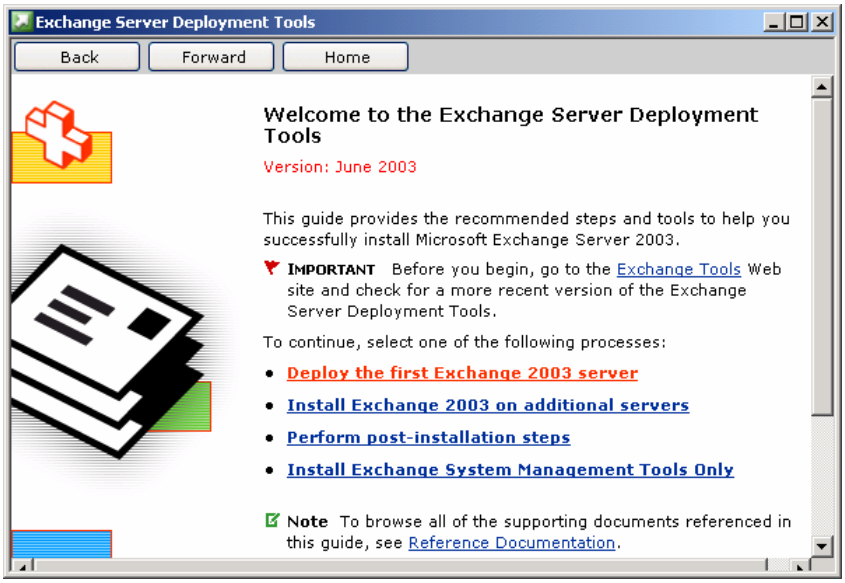
Postup pro instalaci prvního serveru *Exchange 2003* je následující:

1. Na úvodní stránce průvodce je vidět aktuální verze tohoto nástroje (v našem případě Version: June 2003). Doporučuje se používat co nejnovější verzi, kterou je možno si stáhnout z webových stránek firmy *Microsoft*. Klepnutím na položku **Exchange Tools** se dostaneme na stránku **http://www.microsoft.com/exchange/2003/updates**, kde se dá získat i mnoho dalších užitečných nástrojů pro správu serveru *Exchange 2003* (některé z nich budou popsány dále).

   Průvodce nabízí, že nás bude provázet instalací prvního serveru *Exchange*, instalací dalších serverů *Exchange*, postinstalačními kroky, anebo že nám pouze nainstaluje nástroje pro správu systému *Exchange*. Zároveň je zde uveden i důležitý odkaz na refe-

renční dokumentaci, ze které se např. dozvíme, že k tomuto grafickému průvodci existuje i verze pro příkazový řádek (nástroj **Exdeploy.exe**).

Jelikož se v naší organizaci chystáme instalovat první server *Exchange*, z nabídky zvolíme první položku **Deploy the first Exchange 2003 server** (Nasadit první server *Exchange 2003*).



Obr. 2.2: Exchange Server Deployment Tools (1)

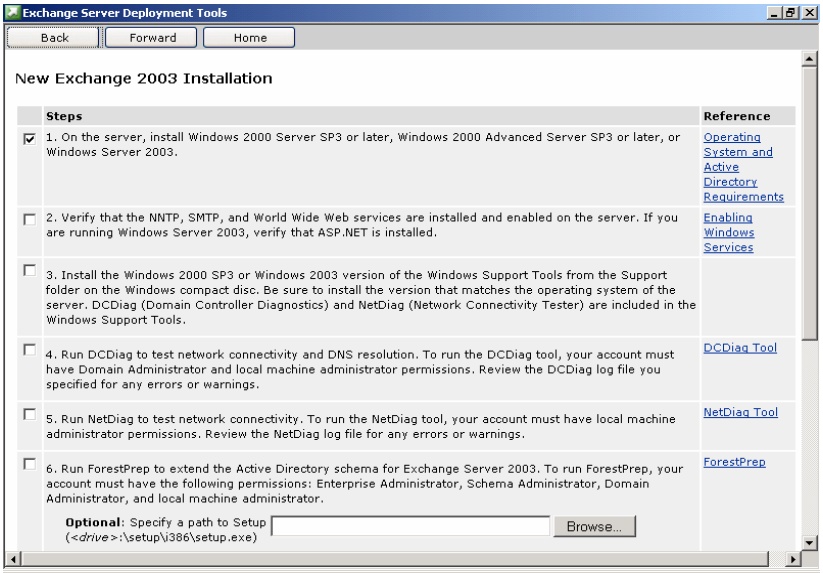
2. Na další obrazovce máme na výběr opět několik voleb. První z nich – **Coexistence with Exchange 5.5** (Koexistence se serverem Exchange 5.5) je možnost instalace serveru *Exchange 2003* do existující organizace *Exchange 5.5*. Tuto položku volíme tehdy, pokud jsme ještě nenasadili *Active Directory Connector*, a nemáme tedy synchronizován adresář serveru *Exchange 5.5* a adresář *Active Directory*.

   Druhá volba – **Coexistence with Mixed Mode Exchange 2000 and Exchange 5.5** (Koexistence se servery Exchange 2000 a Exchange 5.5 ve smíšeném režimu) je určena pro správce, kteří již nasadili server *Exchange 2000* do organizace *Exchange 5.5*, a tím pádem již mají zprovozněný *Active Directory Connector*. Jedná se o totální koexistenci tří verzí serverů *Exchange* v jedné organizaci, a to *Exchange 5.5*, *Exchange 2000* a *Exchange 2003*.

   Třetí volba – **Upgrade from Exchange 2000 Native Mode** (Inovovat ze serveru Exchange 2000 v nativním režimu) je vhodná v okamžiku, kdy je potřeba provést upgrade serveru *Exchange 2000* na verzi *2003*, popř. nainstalovat první server *Exchange 2003* do organizace *Exchange 2000*, která je přepnuta do nativního režimu, a neobsahuje tedy již žádné servery *Exchange 5.5*.

Čtvrtá volba – **New Exchange 2003 Installation** (Instalace nového serveru Exchange 2003) je určena pro vytvoření úplně nové organizace se serverem *Exchange 2003*, kdy ještě není nasazený žádný server *Exchange*. Touto cestou se vydáme my, jelikož se chystáme vytvořit úplně novou poštovní organizaci.

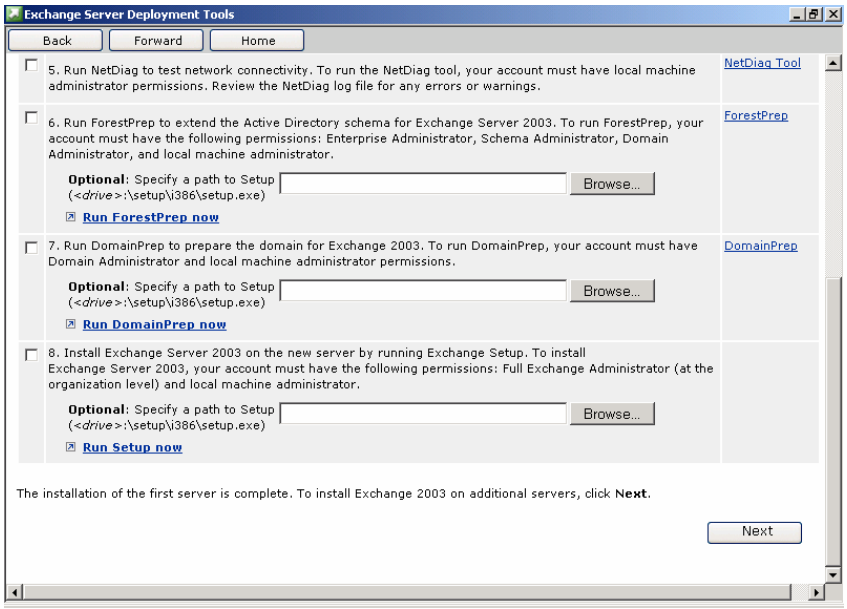
Obr. 2.3: Exchange Server Deployment Tools (2)



Obr. 2.4: Exchange Server Deployment Tools (3)

3. Na další obrazovce průvodce **Exchange Server Deployment Tools** je vidět samotná podstata a krása celého nástroje. Zobrazilo se nám celkem osm kroků k nasazení prvního serveru *Exchange 2003*, které bychom měli projít jeden za druhým přesně ve stanoveném pořadí. Průvodce v podstatě nedává možnost, abychom na něco zapomněli, a zároveň hlídá, jestli vše provádíme podle doporučených praktik. Teoreticky by se dalo říci, že podle tohoto průvodce zvládne instalaci serveru *Exchange 2003* i úplný začátečník (a po tom zákazníci firmy *Microsoft* skutečně prahli, hlavně při inovaci a migraci ze serveru *Exchange 5.5*).
4. Po skončení instalace prvního serveru *Exchange 2003* se můžeme stiskem tlačítka **Next** (Další) přesunout do postinstalační fáze (viz kapitola 2.9).

Zatržítka u jednotlivých kroků mají čistě nápomocný charakter a slouží jako paměťová pomůcka. Postupné zatrhávání jednotlivých kroků není vyžadováno.



Obr. 2.5: Exchange Server Deployment Tools (4)

V dalších kapitolách si jednotlivé kroky postupně projdeme a detailně si vysvětlíme, jak ten který krok správně provést.

2.2 Exchange 2003 a Windows 2000

Server *Exchange 2003* je možno zpětně instalovat na operační systém *Windows 2000* (*Server*, *Advanced Server*, *Datacenter Server*). Bohužel na tomto systému nelze využít všech funkcí, které jsou závislé na operačním systému *Windows Server 2003*. Z nejdůležitějších chybějících funkcí jmenujme:

- Zálohování pomocí služby *Stínová kopie svazku*.
- Přístup k serveru *Exchange 2003* pomocí protokolu *RPC over HTTP* (RPC přes HTTP).
- Replikace vícehodnotových atributů (Multivalue Attributes) na úrovni jednotlivých hodnot.
- Pracovní proces (Worker Process) zabudovaný do *Internet Information Services 6.0*.
- Chybějící zabezpečovací nástroj *IIS Lockdown Tool*, který je nutno doinstalovat odděleně.

2.3 Exchange 2003 a Windows Server 2003

Server *Exchange 2003* instalovaný na operačním systému *Windows Server 2003* (*Standard Edition*, *Enterprise Edition*, *Datacenter Edition*) umožňuje využít všechny nové funkce, které do něj byly zabudovány. Dále je možno říci, že dvojice *Windows Server 2003* a *Exchange 2003* přináší nejvyšší úroveň zabezpečení vystavěnou na iniciativě *Microsoft Trustworthy Computing*.

*Exchange 2003 nelze instalovat na Windows Server 2003 Web Edition, což je speciální edice operačního systému, která je spíše určena pro hostování webových sídel. Tato edice nemůže být použita pro instalaci doménového řadiče (**DCPROMO** je nefunkční), nelze na ni instalovat další aplikace (jmenovitý seznam nejznámějších aplikací firmy Microsoft a dalších firem) a je omezena na deset simultánních připojení Server Mesage Block, obdobně jako operační systémy Windows 2000 Professional či Windows XP Professional.*

Server Exchange 2000 není na operačním systému Windows Server 2003 podporován, proto zde nebudu tuto variantu popisovat.

2.4 Příprava na instalaci

Velkou chybou, které se začínající správci dopouští při své první instalaci serveru *Exchange*, je spuštění instalace bez rozmyslu, jak jsou na to zvyklí u některých jednoduchých aplikací. Ne nadarmo se říká dvakrát měř, jednou řež. Ještě dříve, než spustíme program *Setup* pro započetí instalace, je nutno se na instalaci připravit. Pojďme se nyní podívat, co vše je potřeba zkontrolovat před samotnou instalací.

2.4.1 Hardwarové a systémové požadavky

Server *Exchange 2003* se nám podaří nainstalovat, pouze pokud náš hardware a software splňuje požadavky dané firmou *Microsoft*. V tabulce 2.1 jsou shrnuty minimální a doporučené požadavky na hardwarové komponenty a operační systém. Asi není potřeba upozorňovat, že pro zvýšení spolehlivosti a výkonu serveru *Exchange* je lepší spíše přidat než ubrat (hlavně co se paměti týče). Doporučuji pořídit co nejvýkonnější hardware, který je firma ochotna a schopna koupit.

	Minimální požadavky	Doporučené požadavky
Procesor	Intel Pentium nebo kompatibilní 133 MHz	Intel Pentium nebo kompatibilní 1,6 GHz Více procesorů
Paměť	256 MB doporučené minimum RAM	512 MB RAM
Úložiště	500 MB volného místa pro samotný Exchange 200 MB volného místa pro systémový oddíl Diskové oddíly formátované NTFS Mechanika CD-ROM	Další disky, popř. diskové pole pro soubory databáze a transakčních protokolů
Operační systém	Windows 2000 (Server, Advanced Server, Datacenter Server) Service Pack 3 nebo pozdější Windows Server 2003	Windows Server 2003 Enterprise Edition

Tab. 2.1: Hardwarové a softwarové požadavky pro instalaci serveru Exchange 2003

Ve své podstatě se vychází z požadavků na samotný operační systém (*Windows 2000* a *Windows Server 2003*), ke kterým se přičte nutné minimum ke spuštění a správnému chodu poštovního serveru. Myslím si, že na dnešní dobu nejsou doporučené požadavky nijak nadsazené či přehnané a při dnešních cenách hardwaru ani nijak nákladné na pořízení.

Pro přibližný výpočet nákupu dostatečného hardwaru existují kalkulátory. Microsoft poskytuje kalkulátor zvaný Capacity Planning and Topology Calculator, který je možno stáhnout ze stránek ***http://www.microsoft.com/exchange/techinfo/planning/2000/ExchangeCalculator.asp****. I když se jedná o verzi pro Exchange 2000, pro přibližný odhad se dá využít i u serveru Exchange 2003. Dále existují kalkulátory jednotlivých výrobců hardwaru, které jsou k dispozici online na jejich webových stránkách.*

2.4.2 Požadavky na prostředí Active Directory

Hardware a software jsou sice nutnou podmínkou pro úspěšnou instalaci serveru *Exchange*, ale ne podmínkou postačující. Ještě je nutno zkontrolovat prostředí, do kterého server *Exchange 2003* instalujeme. Jedná se hlavně o ověření přítomnosti a správné funkčnosti adresářové služby *Active Directory*. Instalace prvního serveru *Exchange* je vynikajícím testem, zdali je *Active Directory* správně nainstalována.

Ze všeho nejdříve si musíme ověřit, jestli máme dostatečná oprávnění v *Active Directory*. To zahrnuje kontrolu členství ve správných skupinách, a to u uživatelského účtu, pod kterým hodláme server *Exchange* instalovat. Jedná se hlavně o skupiny **Domain Admins**, **Enterprise Admins** a **Schema Admins**, ale také delegovaná oprávnění na úrovni administrativní skupiny či organizace *Exchange*. Tato problematika bude probrána v další kapitole.

Počítače s operačními systémy *Windows 2000* a *Windows Server 2003*, na které budeme instalovat *Exchange 2003*, musí být součástí *Active Directory*. Jinými slovy, tyto počítače musí být přihlášeny do domény jako členské servery (nemohou zůstat členy pracovní skupiny, jako je např. WORKGROUP).

Dále tyto počítače, na něž se chystám instalovat server *Exchange 2003*, musí být součástí stejné doménové struktury, na kterou bude mapována organizace *Exchange*.

Sice je možné mít více doménových struktur pro podporu organizace Exchange, ale to je nad rámec této knihy. Jedná se o scénář, kdy jedna struktura drží uživatelské účty a druhá poštovní schránky k těmto uživatelským účtům.

Pokud také plánujeme inovaci serveru *Windows 2000* na *Windows Server 2003*, musíme nejprve na *Windows 2000* nainstalovat server *Exchange 2003* a teprve potom inovovat operační systém na *Windows Server 2003*. Pokud dodržíme tuto doporučenou logiku, vyhneme se mnoha zbytečným konfiguracím (jedná se hlavně o dodatečnou konfiguraci služby *Internet Information Services 6.0*), nehledě na to, že *Exchange 2000* nelze instalovat na operační systém *Windows Server 2003*.

Je potřeba se také ujistit, zdali doménové řadiče a servery konfigurované jako globální katalogy mají požadovanou verzi operačního systému. Program *Setup* serveru *Exchange 2003* musí být schopen v dané síti (Site) kontaktovat alespoň jeden server s *Active Directory* na operačním systému *Windows 2000 SP3* (či vyšším) nebo *Windows Server 2003*.

2.4.3 Instalace aktualizace Service Pack a záplat

Obecně bývá doporučeno ihned po instalaci operačního systému aplikovat poslední *Service Pack* (*SP4* u *Windows 2000*, prozatím žádný na *Windows Server 2003*) a dále všechny kritické opravné záplaty, které byly zveřejněny po uvedení *Service Packu*. Existuje mnoho metod, jak aplikovat *Service Pack* a opravné záplaty.

Service Pack lze instalovat následujícím způsobem:

- Buď je už integrován do instalačních souborů operačního systému od výrobce, což bývá uvedeno na instalačním médiu.
- Je možné si jej ručně integrovat do instalačních souborů přiloženým souborem *Service Packu* **Update.exe** s přepínačem **/s**:

```
Update.exe /s <cesta_k_instalačním_souborům>.
```

- Manuálně doinstalovat po instalaci operačního systému.
- Nechat nainstalovat automatizovaně pomocí *Zásad skupin* (Group Policy).
- Využít automatizovanou instalaci pomocí služby *Software Update Services* (platí od října 2003).
- Využít produkt *Systems Management Server 2003* pro automatizované instalace.

Opravné záplaty je možné instalovat:

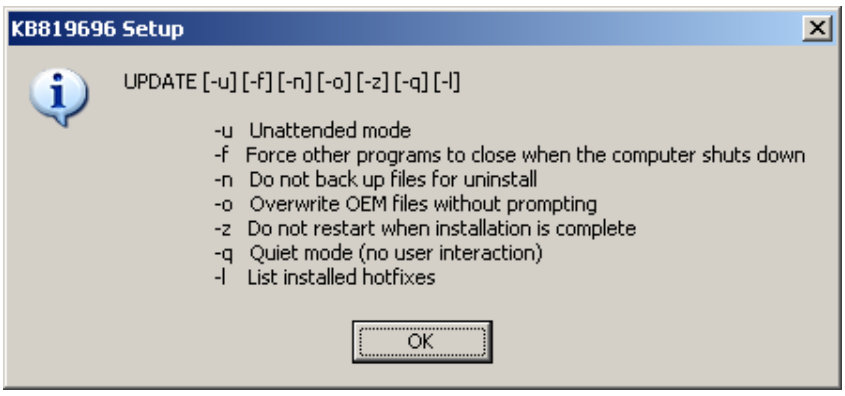
- Ručně jednu po druhé s mezirestarty.
- Automatizovaně všechny najednou pomocí dávky.

- Pomocí služby *Software Update Services*.
- Pomocí produktu Systems Management Server 2003.

Úplně nejpohodlnější způsob instalací jak *Service Packu*, tak opravných záplat, je pomocí služby *Software Update Services (SUS)*. Ta se dá volně stáhnout ze stránek společnosti *Microsoft* a nainstalovat buď na server *Windows 2000*, nebo *Windows Server 2003* (i na doménový řadič). Jedná se o službu synchronizující *Service Packy* a opravné záplaty se servery společnosti *Microsoft* (tzv. *Windows Update Servers*), které jsou poté automatizovaně distribuovány na pracovní stanice a servery (s operačním systémem *Windows 2000* a vyšším). *Service Packy* a záplaty jsou tak stahovány lokálně ze serveru se službou *SUS*, a ne přímo z internetových serverů společnosti *Microsoft*. *SUS* zároveň dává možnost zkontrolovat a schválit záplaty před jejich distribucí, čímž se zamezí mnohonásobným instalacím vadné záplaty, což může mít dalekosáhlé důsledky.

Bližší informace o službě SUS je možné nalézt na stránkách společnosti Microsoft ***http://www.microsoft.com/windowsserversystem/sus/default.mspx****.*

Služba *SUS* je poměrně zajímavým počinem, ale bohužel na ni v této knize nezbývá místo. Pojďme si proto spíše ukázat, jak instalovat záplaty automatizovaně pomocí dávky. I když je doporučeno instalovat záplaty odděleně a pokaždé restartovat systém a zkontrolovat stav serveru, je tohle poměrně dost nepraktické v případě nově nainstalovaného serveru, na kterém nejsou prozatím žádná produkční data. Zde je lepší si záplaty seskupit do jednoho adresáře a spustit je pomocí dávky tak, aby se systém nerestartoval po instalaci každé z nich. To lze zajistit přepínačem **-z**, který po instalaci záplaty potlačí restart operačního systému. Dále je vhodné celou instalaci automatizovat přepínačem **-u** (u *Windows 2000* **-m**), abychom nemuseli procházet jednotlivé obrazovky průvodce instalace záplaty.



Obr. 2.6: Přepínače instalačních souborů opravných záplat

Ve výpisu dávkového souboru je vidět, jak jsem záplaty instaloval já. Jedná se o záplaty dostupné k listopadu 2003.

```
@echo off
setlocal
```

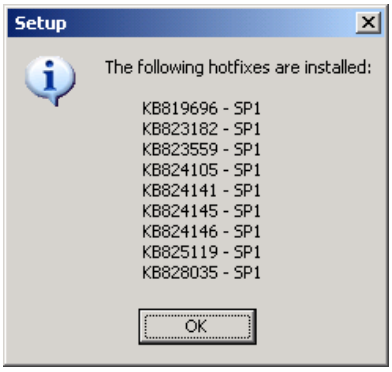
```
set PATHTOFIXES=.
%PATHTOFIXES%\WindowsServer2003-KB819696-x86-ENU.exe -z -u
%PATHTOFIXES%\WindowsServer2003-KB823182-x86-ENU.exe -z -u
%PATHTOFIXES%\WindowsServer2003-KB823559-x86-ENU.exe -z -u
%PATHTOFIXES%\WindowsServer2003-KB824105-x86-ENU.exe -z -u
%PATHTOFIXES%\WindowsServer2003-KB824141-x86-ENU.exe -z -u
%PATHTOFIXES%\WindowsServer2003-KB824145-x86-ENU.exe -z -u
%PATHTOFIXES%\WindowsServer2003-KB824146-x86-ENU.exe -z -u
%PATHTOFIXES%\WindowsServer2003-KB825119-x86-ENU.exe -z -u
%PATHTOFIXES%\WindowsServer2003-KB828035-x86-ENU.exe -z -u
%PATHTOFIXES%\qchain.exe qchainlog.txt
```

Pokud bych si přál, aby celý proces instalace záplaty byl skryt před zraky uživatele, je možné ještě připojit přepínač **-q**. Spuštění utility *QChain* na konci celé dávky je u *Windows 2000 SP3* a vyšších nepovinné a používá se, pouze pokud instalujeme záplatu, která vyšla před prosincem 2002. U těchto starých záplat nastával problém, pokud dvě záplaty obsahovaly různé verze stejného binárního souboru. Takováto aktualizace mohla skončit nainstalováním starší verze binárního souboru. Zde se vše řešilo pomocí utility *QChain*, která zajistila instalaci novějšího binárního souboru.

Bližší informace o utilitě QChain *se nacházejí v článku Q815062 „The Correct File Is Not Installed When You Chain Multiple Hotfixes" znalostní databáze společnosti Microsoft (**http://support.microsoft.com**).*

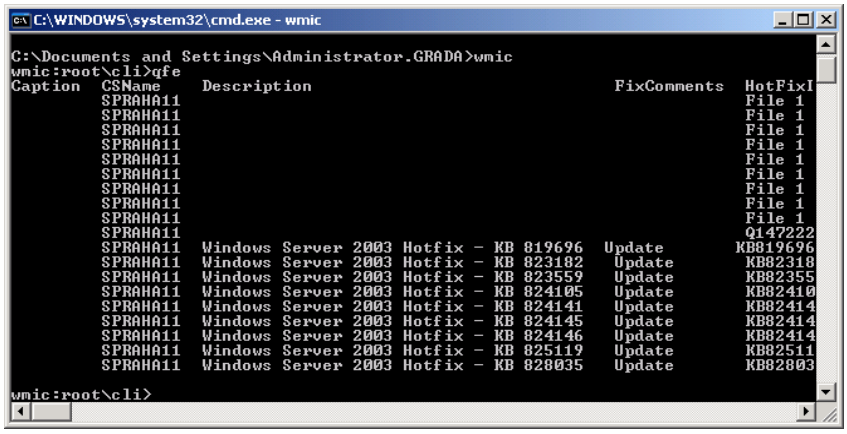
```
---- Old Information In The Registry ------
Source:C:\WINDOWS\system32\SET1D.tmp
Version: 5.2.3790.73
Destination:C:\WINDOWS\system32\user32.dll
Version: 5.2.3790.0

Source:c:\b93bf4bf5f8721fb8e1d
Version:
Destination:
Version:

Source:C:\WINDOWS\system32\SET23.tmp
Version: 6.0.3790.94
Destination:C:\WINDOWS\system32\urlmon.dll
Version: 6.0.3790.0

Source:C:\WINDOWS\system32\SET24.tmp
Version: 6.0.3790.94
Destination:C:\WINDOWS\system32\shdocvw.dll
Version: 6.0.3790.0
```

Kontrolu nainstalovaných opravných záplat lze provést přes panel **Add or Remove Programs** (Přidat nebo odebrat programy), kde jsou vidět pouze záplaty, které nebyly instalovány s přepínačem **-n** (bez zálohy). Daleko efektivnější je použít přepínač **-l** u jakékoliv záplaty a nechat si vypsat seznam záplat, kde je možno vidět, do kterého *Service Packu* budou tyto záplaty zařazeny.



Obr. 2.7: Seznam instalovaných opravných záplat pomocí přepínače -l

Pokud by se vám tato metoda zjištění instalovaných záplat zdála zdlouhavá, doporučuji použít konzolu **WMIC** dostupnou na operačním systému *Windows Server 2003*, kterou lze použít i vůči vzdálenému počítači).



Obr. 2.8: Zjištění instalovaných záplat pomocí konzoly WMIC

2.4.4 Kontrola instalace služeb operačního systému

Posledním krokem před samotnou instalací je kontrola přítomnosti následujících součástí operačního systému:

- .NET Framework,
- ASP.NET,

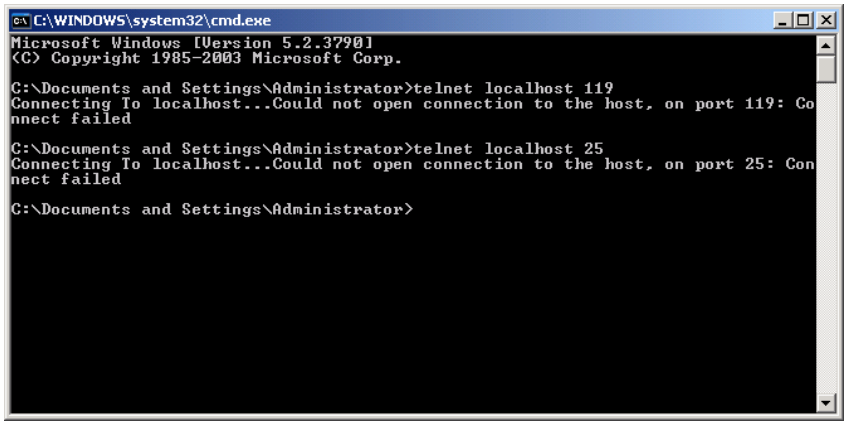
- služby World Wide Web Service,
- služby NNTP Service,
- služby *SMTP Service*.

Pokud by některá z těchto služeb nebyla přítomna, instalační program *Setup* ohlásí chybu a vyzve nás k doinstalování služeb, což je dosti nepříjemné a zbytečné zdržení, jelikož instalátor je nutno stornovat a spustit znovu (nelze jej obelstít doinstalováním služeb na pozadí, zatímco visí v chybové hlášce a nepomůže ani vrácení se v instalátoru na předchozí obrazovku).

Služby *.NET Framework* a *ASP.NET*, které poskytují podporu mobilního přístupu, jsou součástí operačního systému *Windows Server 2003*. Pokud je server *Exchange 2003* instalován na operační systém *Windows 2000*, *Setup* automaticky doinstaluje a nastartuje služby *.NET Framework* a *ASP.NET*, ale služby *SMTP* a *NNTP* musí být již doinstalovány ručně.

Služba NNTP musí být doinstalována před instalací serveru Exchange 2003, i když ji později nebudeme používat (ve skutečnosti je po instalaci vypnuta).

Přítomnost služeb *NNTP* a *SMTP* lze nejrychleji vyzkoušet pomocí programu *Telnet*. V případě, že služby nejsou doinstalovány, *Telnet* s nimi na portech 119 (NNTP), resp. 25 (SMTP) nenaváže spojení.



Obr. 2.9: Ověření přítomnosti služeb NNTP a SMTP pomocí utility Telnet

Při výchozí instalaci Windows 2000 s integrovaným SP4 (a vyšším) není doinstalována žádná komponenta IIS. Proto je nutné kromě NNTP a SMTP také doinstalovat službu World Wide Web Service.

U systému *Windows Server 2003* je nutno všechny služby doinstalovat (kromě komponenty *.NET Framework*, která je již přítomna). Doporučuji dát přednost panelu **Add or Remove Programs** (Přidat nebo odebrat programy) před konzolou **Manage Your Server** (Správa serveru) a její funkcí **Add or remove a role** (Přidat nebo odebrat roli). Konzola **Manage Your Server** (Správa serveru) je sice doporučovaná, jelikož si volá průvodce **Configure Your Server Wizard** (Průvodce konfigurací serveru), ale ten v rámci role aplikačního ser-