Kerio MailServer 6™

Příručka administrátora

Kerio Technologies

Datum vydání: 5. února 2008

Tento manuál popisuje produkt: *Kerio MailServer* ve verzi *6.5.0*. Změny vyhrazeny.

Aktuální verzi produktu a manuálů naleznete na WWW stránkách `http://www.kerio.cz/kmsdwn`.

Obsah

Kapitola 1

Úvod

1.1 Základní vlastnosti a funkce Kerio MailServeru

Kerio MailServer 6.5 je koncipován jako „bezpečný poštovní server dostupný odkudkoliv“. Zde uvádíme stručný přehled jeho hlavních funkcí a vlastností.

SMTP server

Plnohodnotný SMTP server umožňující provozování několika nezávislých lokálních domén, vytváření virtuálních adres (aliasů), příjem pošty pomocí ETRN atd. Odchozí pošta může být odesílána buď přímo do cílových domén (dle MX záznamů v DNS) nebo odesílána prostřednictvím nadřazeného SMTP serveru (např. u poskytovatele internetového připojení).

POP3 server

POP3 (Post Office Protocol version 3) je protokol, který umožňuje uživatelům stahovat zprávy ze serveru na svůj lokální disk. Je vhodný zejména pro klienty, kteří nemají trvalé připojení do Internetu.

Na rozdíl od protokolu IMAP, POP3 neumožňuje uživatelům manipulovat se zprávami na serveru. Veškeré operace s nimi musí být prováděny na počítači klienta. POP3 umožňuje přístup pouze do uživatelovy složky *INBOX* a nepodporuje veřejné složky.

IMAP server

IMAP (resp. IMAP4 — Internet Message Access Protocol version 4) je protokol umožňující klientům pracovat se svými zprávami na serveru, bez nutnosti stahování na lokální počítač. Uživatel se tak může připojovat k serveru z více různých počítačů a má vždy k dispozici všechny své zprávy (pokud by byly zprávy staženy na lokální disk určitého počítače, nebyly by z ostatních počítačů dostupné).

K téže schránce lze (za určitých podmínek) přistupovat protokoly IMAP i POP3 současně.

NNTP server

NNTP (Network News Transfer Protocol) je protokol umožňující přenos zpráv typu news a zobrazení veřejných složek uživatelům. NNTP server obsahuje archiv všech zpráv e-mailové konference.

WWW rozhraní (Kerio WebMail)
Zabudovaný HTTP server umožňuje vzdálený přístup k uživatelské schránce — čtení a psaní zpráv, událostí a úkolů, správu složek a změnu osobního nastavení. Přitom není třeba žádný poštovní klient ani složité nastavování účtů, pouze WWW prohlížeč. *Kerio WebMail* popisuje samostatná uživatelská příručka *Kerio MailServer, Příručka uživatele*.

Osobní a veřejný adresář
Kerio MailServer umožňuje uchovávání osobního a veřejného adresáře kontaktů (tj. e-mailových adres a dalších informací o osobách). V podporovaném poštovním klientovi či rozhraní *Kerio WebMail* tak má uživatel k dispozici nejen všechny své zprávy, ale také adresy osob s nimiž komunikuje.

Free/Busy server
Free/Busy server zabudovaný do *Kerio MailServeru* je služba, která uživatelům prostřednictvím protokolu HTTP poskytuje informace o zaneprázdněnosti/volném čase ostatních uživatelů, aniž by se zobrazily podrobnosti jednotlivých událostí.

Kalendáře, úkoly a poznámky
Kerio MailServer umožňuje uchovávání osobních i veřejných složek s kalendáři, úkoly a poznámkami. V rozhraní *Kerio WebMail* a aplikaci *MS Outlook* může uživatel díky aplikaci *Kerio Outlook Connector* (kapitola 32.2) spravovat složky s kalendáři, úkoly a poznámkami.

LDAP server
Pro snadný přístup ke kontaktům uloženým na serveru z poštovních klientů obsahuje *Kerio MailServer* jednoduchý LDAP server umožňující přístup k uživatelskému i veřejnému adresáři.

Správa uživatelských účtů, skupin a aliasů přes webové rozhraní
Kerio MailServer umožňuje správu uživatelů pomocí webového rozhraní. To umožňuje zákazníkům poskytovatelů Internetu přistupovat k nastavení uživatelských schránek, skupin a aliasů ve svých doménách.

Vybírání vzdálených schránek
Poštovní server může automaticky vybírat jednu nebo více POP3 schránek na jiných serverech (např. doménový koš u poskytovatele připojení) a zprávy doručovat do vybraných lokálních schránek nebo třídit podle nastavených pravidel.

Bezpečné komunikační cesty
U všech služeb *Kerio MailServeru* má uživatel možnost výběru mezi nechráněným spojením a spojením šifrovaným SSL. Šifrovaným spojením je rovněž možno přenášet odesílané zprávy, jestliže to cílový server podporuje.

Antivirová kontrola

Všechny příchozí zprávy je možno kontrolovat, zda neobsahují viry. V případě nalezení viru je pak možno provést několik akcí — vyjmout infikovanou přílohu nebo vrátit zprávu odesílateli, poslat upozornění, přeposlat původní zprávu správci serveru apod. Antivirová kontrola se provádí externím antivirovým programem (např. AVG, NOD32 apod.). Dále je možno filtrovat určité typy e-mailových příloh (dle přípon souborů — např. `exe`, `com`, `vbs` apod. nebo dle MIME typů — např. `application/x-msdownload`), bez ohledu na to, zda jsou infikovány virem či nikoliv.

Antispamová ochrana

Poštovní server je možno ochránit před zneužitím (rozesílání nevyžádaných zpráv — spamů), a také před příjmem těchto zpráv. Zprávy mohou být rozpoznány a případně také blokovány spamovým filtrem *SpamAssassin*, bayesovským filtrem, databázemi SMTP serverů rozesílajících spam, kontrolou „e-mail policy“ záznamů a v neposlední řadě systémem vlastních pravidel pro nevyžádanou poštu, která lze nastavit v sekci *Filtr spamu*.

Archivace pošty

Kerio MailServer může archivovat všechny zprávy (nebo jen odeslané zprávy), a to buď lokálně, nebo na vzdálený server.

Zálohování uživatelských složek a konfiguračních souborů

Kerio MailServer umí zálohovat uživatelské složky (adresář `store`) a konfigurační soubory mailserveru v nastavených časových intervalech.

Filtrování a notifikace

Každý uživatel si může nastavit celou řadu akcí, které mají být provedeny se zprávou uloženou do jeho schránky (přesun do určené složky, filtrování, notifikace na mobilní telefon, automatická odpověď...). Akce přitom může být aplikována na všechny zprávy, nebo podle adresy odesílatele, příjemce apod.

Plánovač

Správce serveru má úplnou kontrolu nad tím, zda mají být zprávy odesílány okamžitě nebo v plánovaných časech či časových intervalech. Tím je možno optimalizovat cenu připojení (v případě vytáčených linek).

E-mailové konference

V každé lokální doméně je možné zřídit libovolný počet e-mailových konferencí. Členy konference může definovat správce serveru nebo se mohou přihlašovat a odhlašovat automaticky pomocí e-mailu. Konference může být moderována jedním nebo více moderátory — ti pak řídí přihlašování a odhlašování uživatelů, posílání příspěvků atd.

Kerio MailServer umožňuje nastavení archivace e-mailové konference.

Podpora Active Directory a Open Directory

Kerio MailServer plně spolupracuje s *Microsoft Active Directory* a *Apple Open Directory*. Uživatelské účty již není nutné importovat do interní databáze. Přidání či odebrání uživatelského účtu (resp. skupiny) tak stačí provést pouze v systémovém nástroji pro správu *Active Directory* nebo *Open Directory*.

Kerio Outlook Connector

Kerio Outlook Connector je rozšíření aplikace *MS Outlook* využívající otevřené rozhraní MAPI. Slouží ke komunikaci *Kerio MailServeru* a aplikace *MS Outlook*. Umožňuje ukládání různých typů složek (zpráv, kontaktů, kalendářů, úkolů a poznámek) na straně serveru. Zároveň umožňuje mapování a sdílení složek a nastavení pravidel pro třídění pošty.

Kerio Outlook Connector (Offline Edition)

Kerio Outlook Connector (Offline Edition) je rozšíření aplikace *MS Outlook* využívající otevřené rozhraní MAPI. Slouží ke komunikaci *Kerio MailServeru* a aplikace *MS Outlook*. Umožňuje ukládání různých typů složek (zpráv, kontaktů, kalendářů, úkolů a poznámek) na straně serveru. Zároveň umožňuje mapování a sdílení složek a nastavení pravidel pro třídění pošty.

Kerio Outlook Connector (Offline Edition) umožňuje uživatelům, kteří nejsou permanentně připojeni k Internetu pracovat se svou poštou, kalendářem a dalšími groupwarovými nástroji v offline režimu.

Synchronizace IMAP a POP3 účtů v aplikaci MS Outlook

Kerio Synchronization Plug-in je doplněk do aplikace *MS Outlook*, který umožňuje využívat základní funkce týmové spolupráce přes IMAP nebo POP3 účty. *Kerio Synchronization Plug-in* dále umožňuje práci v režimu offline s možností připojit se ke *Kerio MailServeru* a změněná data synchronizovat.

Podpora pro Windows Calendar

Kerio MailServer podporuje aplikaci *Windows Calendar*. Tato podpora umožňuje přihlášení kalendářů a jejich publikaci v *Kerio MailServeru*.

Podpora pro MS Entourage

Kerio MailServer podporuje poštovního klienta *Microsoft Entourage*. Umožňuje mu ukládat na serveru poštovní složky, kontakty a kalendáře. Dále lze díky této podpoře pracovat s *Free/Busy* serverem *Kerio MailServeru*.

Kerio MailServer komunikuje s *MS Entourage* pomocí protokolu WebDAV. Z toho důvodu musí být na serveru spuštěna služba HTTP.

Podpora pro týmovou spolupráci v Apple Mail 10.4

Kerio MailServer podporuje některé funkce týmové spolupráce v aplikaci *Apple Mail 10.4*.

Podpora přihlašování a publikace kalendářů v Apple iCal

Kerio MailServer podporuje přihlašování a publikaci kalendářů ve formátu iCalendar. Podpora umožňuje přihlášení kalendářů z *Kerio MailServeru* do *Apple iCal* a naopak publikaci kalendářů z *Apple iCal* na *Kerio MailServer*.

Podpora pro Apple Address Book

Podpora umožňuje aplikaci *Apple Address Book* vyhledávání v LDAP databázi, kterou používá *Kerio MailServer*. *Apple Address Book* ve verzi pro *Apple Mac OS X 10.3* umožňuje rovněž synchronizaci kontaktů.

Kerio Sync Connector for Mac

Kerio Sync Connector for Mac je speciální aplikace, která umožňuje synchronizaci lokálních dat mezi *Kerio MailServerem* a aplikacemi *Apple iCal* a *Apple Address Book*.

Podpora pro CalDAV protokol

Podpora protokolu CalDAV umožňuje připojit si a zobrazit kalendáře uložené v *Kerio MailServeru* v poštovních nebo kalendářových klientech, které protokol CalDAV podporují (například *Apple iCal*). Protokol také podporuje plánování schůzek (Free/Busy a pozvánky) a přihlášení delegovaného kalendáře.

Apple iPhone

Kerio MailServer podporuje zařízení *Apple iPhone*. Díky této podpoře je možné přijímat a odesílat poštu a synchronizovat kalendáře a kontakty s poštovním klientem na desktopu.

Kerio MailServer podporuje spuštění *Kerio WebMail* v *Apple iPhone* jak v plné verzi tak i v omezené verzi určené pro PDA a mobilní zařízení.

Podpora pro BlackBerry

- *Kerio MailServer* umožňuje synchronizaci pošty, kalendáře, kontaktů a úkolů pomocí *NotifyLink* (více viz `http://www.notifycorp.com/`).
- *Kerio MailServer* umožňuje bezdrátový přístup k e-mailu přes *BlackBerry Internet Service*.

Podpora pro ActiveSync

Podpora protokolu *ActiveSync* umožňuje synchronizaci pošty, kalendářů, kontaktů a úkolů mezi *Kerio MailServerem* a mobilními zařízeními (PDA, Smartphone). Synchronizace může probíhat mezi serverem a mobilním zařízením (samozřejmě pouze v případě, že je v mobilním zařízení nainstalována aplikace, která poskytuje synchronizaci přes *ActiveSync*).

Podpora se samozřejmě vztahuje také na synchronizaci mezi desktopovou aplikací (*MS Outlook*) a mobilními zařízeními. Synchronizace bude probíhat mezi desktopovou aplikací a mobilním zařízením.

Upozornění: Aby se synchronizace projevila také na straně serveru, musí být *MS Outlook* doplněn o *Kerio Outlook Connector* nebo *Kerio Synchronization Plug-in*.

Podpora aplikace RoadSync

Kerio MailServer podporuje aplikaci *RoadSync*, která umožňuje přímou synchronizaci pošty, kontaktů a kalendáře v mobilních zařízeních přes protokol *ActiveSync*. O aplikaci a nastavení mobilních zařízení lze příslušné informace nalézt na `http://www.dataviz.com/`.

Migrační nástroje

Kerio MailServer umožňuje jednoduchý převod uživatelských účtů z různých typů poštovních serverů do *Kerio MailServeru* (například *4D* nebo *MS Exchange Server*). Převody jsou prováděny pomocí speciálních utilit, které jsou k dispozici na vyžádání od techniků společnosti *Kerio Technologies*.

1.2 Rychlé nastavení

Kapitola popisuje krok za krokem zjednodušený postup, jak rychle nastavit *Kerio MailServer* tak, aby mohl okamžitě sloužit jako poštovní server pro vaši firmu. Požadovány jsou pouze základní znalosti TCP/IP a funkce internetových poštovních protokolů. Druhým (a posledním) nutným požadavkem jsou informace od vašeho poskytovatele Internetu — typ připojení a způsob doručování pošty pro vaši doménu.

Nebudete-li si jisti některým nastavením v *Kerio MailServeru*, jednoduše vyhledejte příslušnou kapitolu v tomto manuálu. Pokud nevíte, jak a kam je doručována pošta pro vaši doménu, obraťte se na vašeho poskytovatele Internetu.

1. Nainstalujte *Kerio MailServer* a proveďte požadovaná nastavení v konfiguračním průvodci (vytvoření primární domény, jména a hesla administrátora). Přihlaste se ke správě v programu *Kerio Administration Console*.

   Kerio MailServer se standardně instaluje do následujících adresářů:

   - *Mac OS X*

     `/usr/local/kerio/mailserver`

   - *Linux*

     `/opt/kerio/mailserver`

   - *MS Windows*

     `C:\Program Files\Kerio\MailServer`

2. Nastavte služby, které budete chtít využívat. Chcete-li např. provozovat na stejném počítači WWW server, bude zřejmě nutno vypnout službu HTTP/Zabezpečený HTTP,

změnit její port nebo pro standardní port služby vyhradit jednu IP adresu. Více v kapitole 6.1.

3. Vytvořte lokální domény. První vytvořená doména je vždy primární (konfigurační průvodce). Po vytvoření dalších domén je možno jako primární nastavit kteroukoliv z nich. Nevíte-li, kterou doménu zvolit jako primární, zvolte tu, která obsahuje nejvíc uživatelů. Nezapomeňte také vyplnit DNS jméno SMTP serveru. Více v kapitole 7.

4. Vytvořte uživatelské účty v jednotlivých doménách. Názvy účtů by měly korespondovat s primárními e-mailovými adresami uživatelů. V názvech účtů nepoužívejte národní znaky. Uživatele můžete také importovat z externích zdrojů. Více v kapitole 13.

5. Vytvořte skupiny a zařaďte do nich uživatele, je-li to třeba (např. pro vytváření skupinových adres). Více najdete v kapitole 14.

6. Definujte aliasy pro uživatele a skupinové adresy, jsou-li potřeba. Více v kapitole 15.3.

7. Nastavte typ internetového připojení: *Online* pro pevnou linku nebo *Offline* pro vytáčené připojení. Více v kapitole 8.

8. Je-li modem připojen přímo k počítači s *Kerio MailServerem*, vyberte také příslušnou RAS linku (položku telefonického připojení). Více opět v kapitole 8.

9. Je-li typ internetového připojení *Offline*, nastavte plánování. V režimu *Online* nastavte plánování v případě, jestliže budete chtít vybírat vzdálené POP3 schránky nebo přijímat poštu pomocí příkazu ETRN. Více v kapitole 9.

10. Budete-li chtít vybírat poštu ze vzdálených POP3 schránek nebo doménových košů, nastavte příslušné účty v sekci *Stahování POP3 schránek*. Mají-li být zprávy ze schránek (typicky doménových košů) tříděny do lokálních schránek, definujte také třídicí pravidla. Více v kapitole 15.4.

11. Má-li být pošta pro konkrétní domény přijímána ze sekundárního serveru pomocí příkazu ETRN, definujte příslušné účty v sekci *Příjem pomocí ETRN*. Více v kapitole 15.5.

12. Nastavte antivirovou kontrolu: v sekci *Antivirus* vyberte modul (plug-in) pro antivirový program, který máte instalován. Nastavte akci, která se má provést při nalezení infikované přílohy. Můžete také nastavit filtrování určitých typů příloh (např. spustitelných souborů). Více v kapitole 17.

13. Běží-li *Kerio MailServer* za firewallem, zpřístupněte potřebné porty. Více najdete v kapitole 26.3.

14. Je-li SMTP server přístupný z Internetu, nastavte antispamovou ochranu, aby nemohl být zneužit k rozesílání nevyžádaných e-mailů. Zároveň můžete nastavit blokování příjmu těchto e-mailů z jiných serverů. Více v kapitole 16.

15. Nastavte zálohování, archivaci poštovních složek a konfiguračních souborů. Více v kapitole 18.2.

16. Vytvořte certifikát serveru pro bezpečnou komunikaci, případně požádejte o jeho vytvoření některou komerční certifikační autoritu. Více v kapitole 10.

Kapitola 2

Instalace

2.1 Systémové požadavky

Minimální hardwarová konfigurace počítače, na který má být *Kerio MailServer* nainstalován (základní licence pro 20 uživatelů):

- CPU 1 GHz
- 512 MB operační paměti RAM
- 50 MB diskového prostoru pro instalaci
- 40 GB diskového prostoru pro schránky uživatelů a zálohy
- Z důvodu bezpečnosti nainstalovaného produktu (zejména jeho konfiguračních souborů) doporučujeme použít souborový systém *NTFS*

Doporučená hardwarová konfigurace počítače, na který má být *Kerio MailServer* nainstalován:

Pro 20 — 100 aktivních uživatelů

- CPU 2 GHz
- 1 GB operační paměti RAM
- 160 GB diskového prostoru pro schránky uživatelů a zálohy

Pro 100 a více aktivních uživatelů

- CPU 2.8 GHz Dual Core
- 2 GB operační paměti RAM
- 200 GB a více diskového prostoru pro schránky uživatelů a zálohy

Poznámky:

1. Aktivní uživatel je uživatel využívající služeb *Kerio MailServeru* několikrát denně (využívá poštovní služby, kalendáře, úkoly, atd.).

2. Tato doporučení jsou platná pouze v případě, že počítač slouží jen jako poštovní server (*Kerio MailServer*, antivirový program, antispam).

3. *Kerio MailServer* je podporován na 32-bitových verzích systémů.

2.2 Konfliktní software

Kerio MailServer běží výhradně na aplikační úrovni a nevykazuje žádné nízkoúrovňové konflikty s jinými programy, s výjimkou antivirového programu, který kontroluje otevírané soubory. Je-li přijat e-mail s infikovanou přílohou, poštovní server si jej uloží do dočasného souboru na disk. Antivirus jej pak může poškodit. Tomu lze předejít tak, že v antivirovém programu zakážete kontrolu adresáře, popř. disku, ve kterém jsou uložena data *Kerio MailServeru* (více viz kapitolu 17).

Dalším rizikem může být konflikt portů (jsou-li v *Kerio MailServeru* zapnuty všechny služby, jsou využívány následující TCP porty: 25, 80, 110, 119, 143, 443, 465, 563, 993 a 995). Z tohoto důvodu se nedoporučuje provozovat na tomtéž počítači současně jiný poštovní, LDAP nebo WWW server. V opačném případě musí správce serveru zajistit, aby ke konfliktům portů nedošlo (např. pokud současně běží *Kerio MailServer* a WWW server, je doporučeno změnit port služby *HTTP* nebo tuto službu zastavit a povolit pouze její zabezpečenou verzi — *Zabezpečený HTTP*). Další možností je vyhrazení jedné nebo více IP adres pro porty, na kterých služby *Kerio MailServeru* poslouchají. O službách a nastavení portů se dozvíte více v kapitole 6.1.

Bude-li *Kerio MailServer* provozován na firewallu nebo v chráněné lokální síti za ním, je třeba si uvědomit, že firewall do značné míry ovlivní chování poštovního serveru, resp. komunikaci s ním (např. nedostupnost některých či všech služeb). Při konfiguraci firewallu je třeba vzít v úvahu, které služby mají být zpřístupněny do Internetu, příp. do lokální sítě, a povolit komunikaci na příslušných portech (viz výše nebo podrobněji v kapitolách 6 a 26.3).

2.3 Nastavení firewallu

Kerio MailServer je obvykle nainstalován v lokální síti chráněné firewallem. Kromě vlastní konfigurace poštovního serveru tedy musíme provést doplňující nastavení firewallu.

Má-li být poštovní server přístupný z Internetu, je třeba ve firewallu otevřít (tzv. mapovat) některé porty. Každý mapovaný port znamená potenciální problém se zabezpečením. Namapujeme tedy porty jen pro služby, které chceme zpřístupnit z Internetu.

Pokud bude server doručovat poštu přímo přes DNS MX záznamy, potom je třeba namapovat port 25, což je standardní port pro službu SMTP. Toto nastavení je potřebné vždy, když je na server nasměrován MX záznam pro danou doménu. Na port SMTP serveru se může legálně připojit libovolný SMTP server v Internetu, chce-li odeslat e-mail do některé z jeho domén.

Dále bude třeba namapovat porty, na které se budou připojovat uživatelé mimo lokální síť. Protože se zde zvyšuje bezpečnostní riziko, doporučujeme mapovat pouze služby zabezpečené SSL/TLS šifrováním. Nastavení znázorňuje tabulka 2.1.

Služba (standardní port)	**Odchozí spojení**	**Příchozí spojení**
SMTP (25)	povolit	povolit
SMTPS (465)	povolit	povolit
POP3 (110)	povolit	zakázat
POP3S (995)	povolit	povolit
IMAP (143)	povolit	zakázat
IMAPS (993)	povolit	povolit
NNTP (119)	povolit	zakázat
NNTPS (563)	povolit	povolit
LDAP (389)	povolit	zakázat
LDAPS (636)	povolit	povolit
HTTP (80)	povolit	zakázat
HTTPS (443)	povolit	povolit

Tabulka 2.1 Služby, které je třeba povolit na firewallu

2.4 Instalace

Kerio MailServer může být nainstalován na některém z následujících operačních systémů:

Microsoft Windows

Přechod na *Kerio MailServer 6.5.0* doporučujeme provádět z verze *Kerio MailServer* 6.3 nebo 6.4.

Kerio MailServer je možné instalovat na následující verze operačního systému *Microsoft Windows*:

- Windows 2000 (SP4)
- Windows XP (SP2 nebo SP1)
- Windows 2003 (SP2 nebo SP1)
- Windows Vista (Business, Enterprise nebo Ultimate edice)

Kerio MailServer je třeba instalovat pod uživatelem, který má nastavena uživatelská práva k administraci systému.

Kerio MailServer je podporován na 32-bitových verzích systémů.

Kerio MailServer je instalován pomocí aplikace *Windows Installer*. Po spuštění instalačního programu se zobrazí průvodce pro nastavení základních parametrů serveru. Podrobný popis tohoto průvodce najdete v kapitole 2.5.

Kerio MailServer je standardně instalován do adresáře:

```
C:\Program Files\Kerio\MailServer
```

Toto standardní umístění lze v průběhu instalace podle potřeby změnit (viz dále).

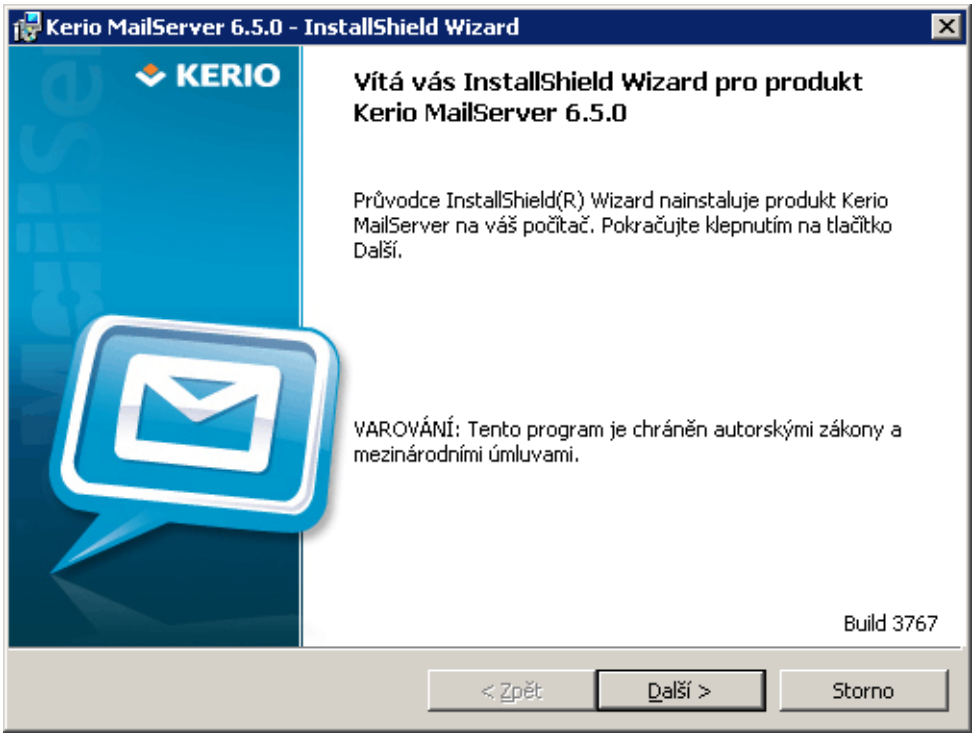
Pro případ řešení nějakého problému je celý průběh instalace *Kerio MailServeru* zaznamenáván do speciálního souboru `C:\WINDOWS\kms_setup.log`, kde lze najít příčiny problémů nebo neúspěšné instalace.

Instalaci *Kerio MailServeru* proveďte následovně:

1. Dvojitým kliknutím spusťte instalační soubor *Kerio MailServeru*. Tento soubor lze získat na produktových stránkách společnosti *Kerio Technologies* (`http://www.kerio.cz/kmsdwn/`).

2. Instalátor se zeptá, v jaké lokalizaci chceme instalaci spustit. Vybereme v nabízeném menu příslušný jazyk (na výběr máme z následujících lokalizací: anglická, německá, italská, ruská a česká) a odsouhlasíme tlačítkem *OK*.

3. Po spuštění instalačního souboru se objeví uvítací stránka průvodce, kde zatím není třeba provádět žádná nastavení (viz obrázek 2.1). Při spuštění uvítací stránky instalátor automaticky zjistí, zda je pro instalaci dostatek volného místa na disku.



Obrázek 2.1 Úvodní krok průvodce

Pokud se opravdu chystáte *Kerio MailServer* nainstalovat, stiskněte tlačítko *Další*.

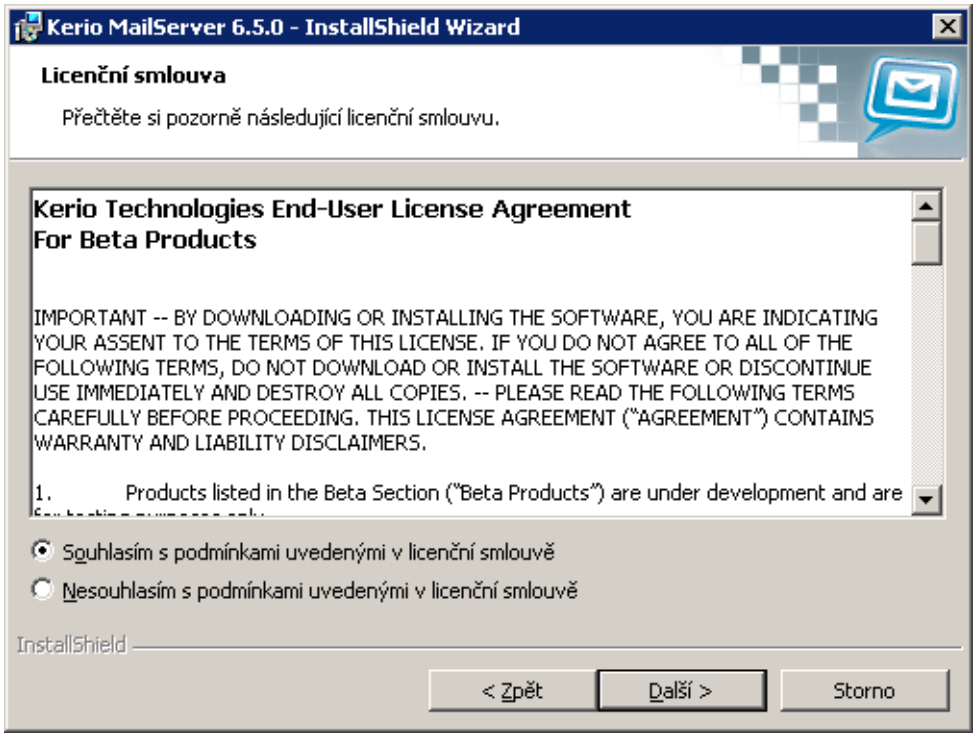
4. Další krok průvodce zobrazuje okno se všemi důležitými novinkami a změnami, které se v nové verzi *Kerio MailServeru* objevily od poslední verze.

   Po pročtení change logu stiskněte tlačítko *Další*.

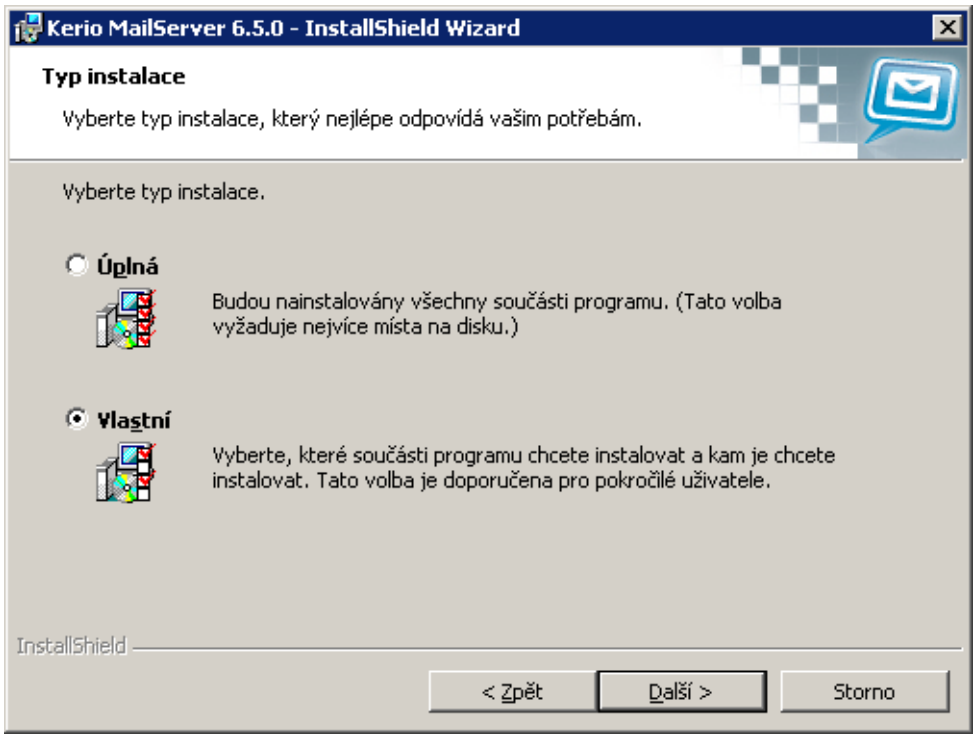
5. Tento krok průvodce zobrazuje licenční podmínky produktu. Aby bylo možno postoupit v instalaci dále, je třeba zvolit možnost *Souhlasím s podmínkami uvedenými v licenční smlouvě* (viz obrázek 2.2).

   Po odsouhlasení licenčních podmínek klikněte na tlačítko *Další*.

6. V tomto dialogu je třeba zvolit typ instalace (viz obrázek 2.3):



Obrázek 2.2 Licence



Obrázek 2.3 Dialog pro výběr typu instalace

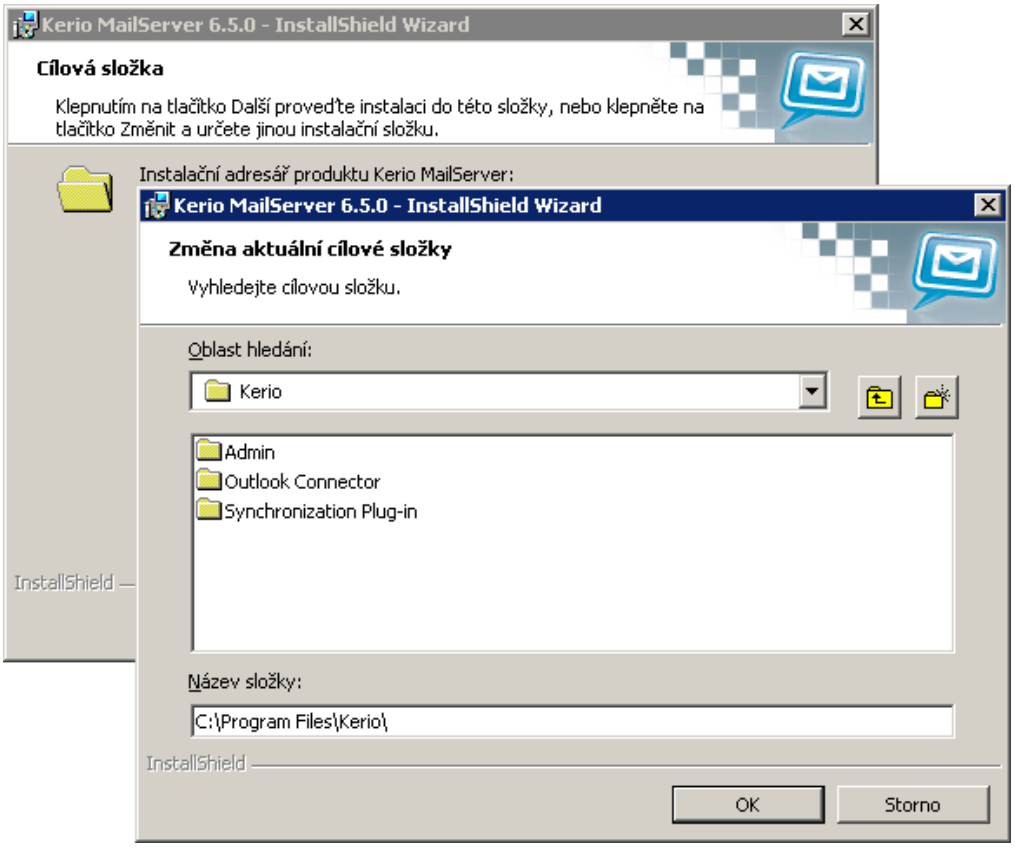
- *Úplná* — po výběru této možnosti se nainstalují všechny součásti *Kerio MailServeru* včetně manuálu ve dvou jazykových mutacích.

  Tuto volbu doporučujeme zejména těm uživatelům, kteří instalují *Kerio MailServer* poprvé.

- *Vlastní* — umožňuje výběr součástí pro *Kerio MailServer* a jazyk, ve kterém se bude zobrazovat nápověda ke *Kerio MailServeru*.

7. Tento krok průvodce vám umožní zvolit adresář, kam bude *Kerio MailServer* nainstalován. Jak je vidět na obrázku 2.4, standardně je mail server instalován do složky

   `C:\Program Files\Kerio\`

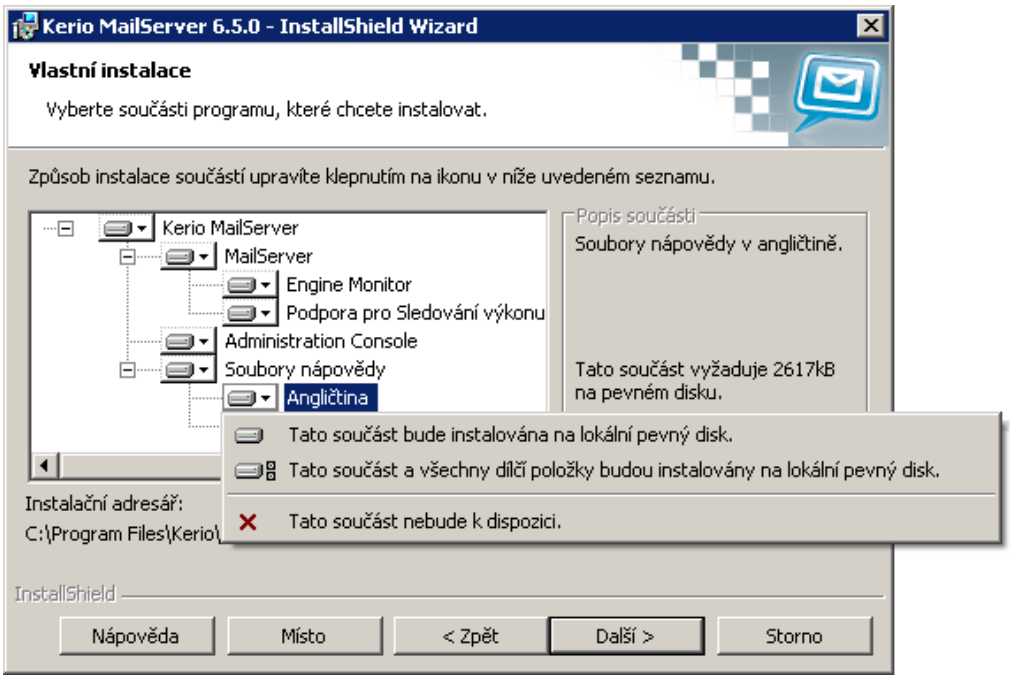


Obrázek 2.4 Dialog pro výběr umístění instalace Kerio MailServeru

Po výběru vhodného adresáře opět klikněte na tlačítko *Další*.

8. Další okno průvodce se zobrazí pouze v případě, pokud byla v předchozím kroku zvolena *Vlastní* instalace. Pokud jste zvolili *Úplnou* instalaci, tento krok přeskočte.

   Vlastní instalace umožňuje nainstalovat pouze některé komponenty *Kerio MailServeru*. Tento typ instalace využijeme zejména v případě, že buď potřebujeme ušetřit místo na disku, a tak vynecháme z instalace nápovědu, nebo například pokud potřebujeme nainstalovat pouze *Kerio Administration Console* na počítač určený pro vzdálenou správu.



Obrázek 2.5 Nastavení konkrétních částí instalace

Součásti instalace:

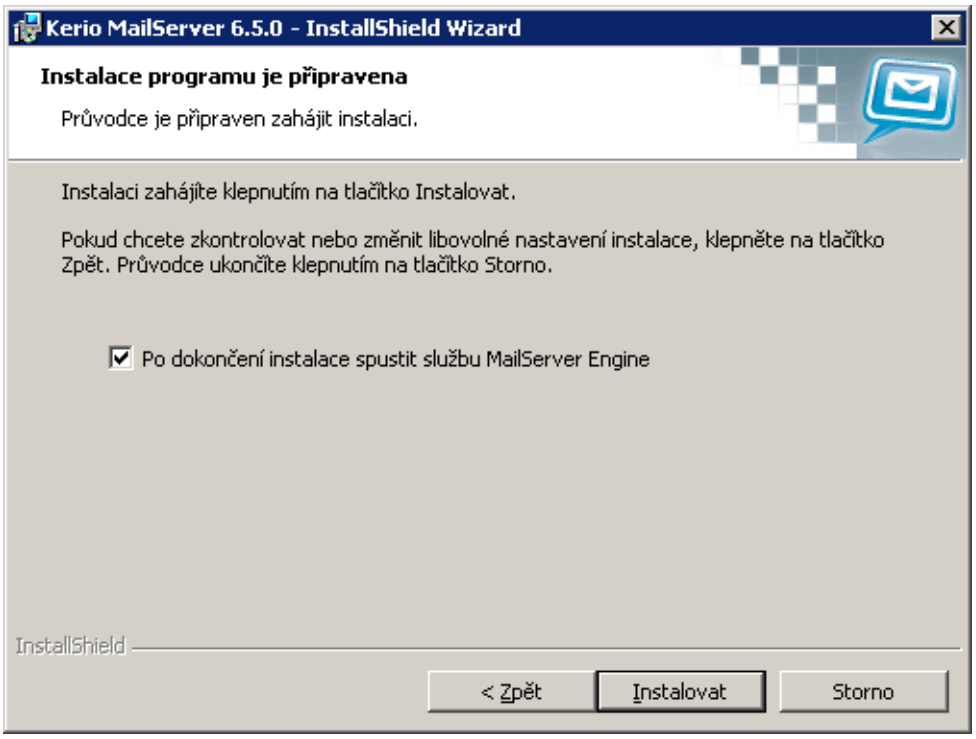
- *MailServer* — vlastní výkonný program (*Kerio MailServer Engine*), který realizuje všechny služby a funkce. Běží skrytě na pozadí (ve Windows 2000, Windows XP a Windows Vista jako služba, v systémech typu Unix jako daemon).

  Ke *Kerio MailServer Engine* doporučujeme nainstalovat ještě následující dvě součásti:

  - *Engine Monitor* — o této součásti se dozvíte více v kapitole 4.1.
  - *Podpora pro Sledování výkonu* — o této součásti se dozvíte více v kapitole 22.9.

- *Administration Console* — rozhraní pro správu *Kerio MailServeru*, lze nainstalovat i samostatně a používat pro vzdálenou správu (více viz kapitolu 5).
- *Soubory nápovědy* — Pokud necháte zaškrtnuty obě volby — *Angličtina* i *Čeština*, nápověda bude zobrazena v jazyce, ve kterém je nastavena *Kerio Administration Console*. Při změně jazyka v *Kerio Administration Console* se automaticky změní také jazyk nápovědy.

9. Další krok průvodce umožňuje nastavit, aby se *Kerio MailServer* spustil automaticky okamžitě po instalaci (volba *Po dokončení instalace spustit službu MailServer Engine*).



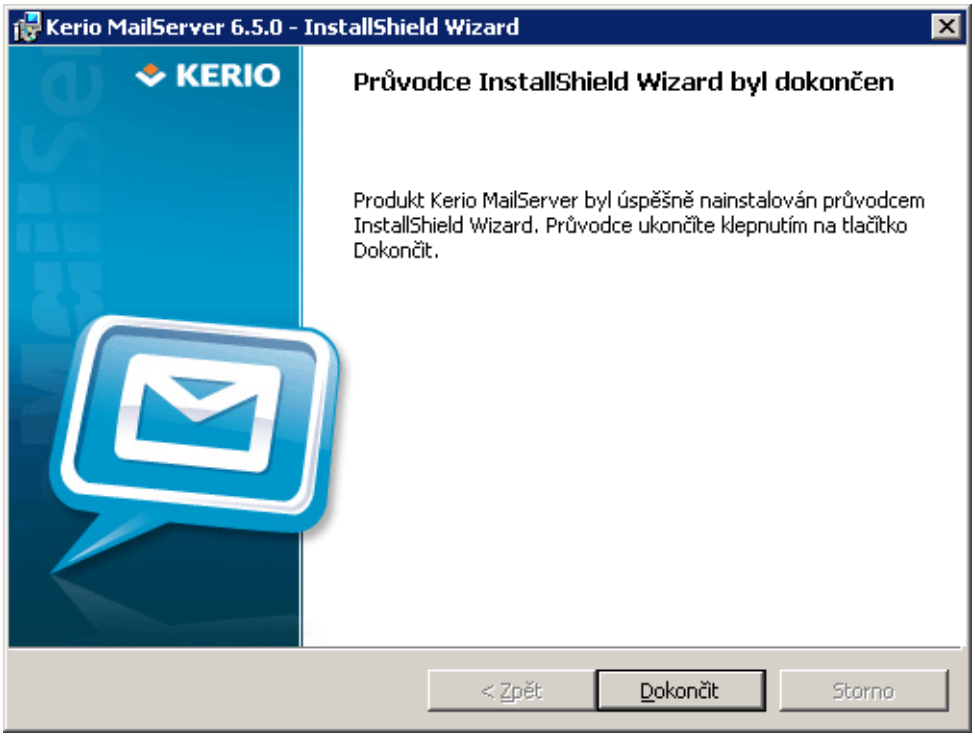
Obrázek 2.6 Odsouhlasení spuštění instalace

Klikněte na tlačítko *Instalovat*. Po provedení tohoto kroku následuje vlastní instalace (tj. zkopírování souborů na pevný disk a nezbytná systémová nastavení).

10. Při samotné instalaci je zobrazen také stav jejího průběhu. Buďte trpěliví, instalace může trvat i několik minut.

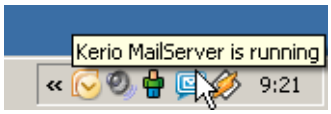
    Po dokončení instalace opět klikněte na tlačítko *Další*. Nyní se spustí vlastní průvodce nastavením základních parametrů serveru (viz sekci 2.5). Průvodce následujte a vyplňte velmi pečlivě.

11. Po vyplnění konfiguračního průvodce se zobrazí závěrečná stránka instalačního průvodce. Celou instalaci ukončíte tlačítkem *Dokončit* (viz obrázek 2.7).



Obrázek 2.7 Instalace na Windows: Závěrečný dialog průvodce

Dále je (volitelně ihned nebo po restartu) spuštěn *Kerio MailServer Engine* (běží jako služba). To znamená, že vlastní výkonné jádro programu, a *Kerio MailServer Monitor* (utilita, která zobrazuje stav *Engine*) jej umožňuje zastavovat, spouštět atd... *Kerio MailServer Monitor* se zobrazuje jako ikona v oznamovací oblasti na nástrojové liště (viz obrázek 2.8).



Obrázek 2.8 Kerio MailServer Monitor na Windows

Ochrana nainstalovaného produktu

Pro zajištění plné bezpečnosti poštovního serveru je důležité, aby neoprávněné osoby neměly žádný přístup k souborům aplikace (zejména ke konfiguračním souborům). Je-li použit souborový systém *NTFS*, pak *Kerio MailServer* při prvním spuštění po instalaci nebo upgradu obnovuje nastavení přístupových práv k adresáři, ve kterém je nainstalován (včetně všech podadresářů — a to i v případě, že cesta je změněna): pouze členům skupiny *Administrators* a lokálnímu systémovému účtu (*SYSTEM*) je povolen přístup pro čtení i zápis, ostatní uživatelé nemají žádný přístup.

Upozornění: Při použití souborového systému *FAT32* nelze soubory *Kerio MailServeru* výše popsaným způsobem zabezpečit. Z tohoto důvodu doporučujeme instalovat *Kerio MailServer* výhradně na disk se souborovým systémem *NTFS*.

Linux

Kerio MailServer je možno instalovat na tyto distribuce:

- *Red Hat 9.0*
- *Red Hat Enterprise Linux 3 / 4 / 5*
- *Fedora Core 4 / 5 / 6 / 7 /8* (na 32-bitových systémech)

  Vyžaduje: libstdc++.so.5 (compat-libstdc++-33 RPM package)

  Fedora Core 5 vyžaduje: compat-gcc-32-3.2.3-56.fc5 a compat-libstdc++-33-3.2.3-56.fc5.
- *SuSE Linux* 10.0, 10.1, 10.2 a 10.3 (32-bit)

  Vyžaduje: libstdc++.so.5 (compat-libstdc++-33 RPM package)

Kerio MailServer je distribuován ve dvou balících RPM (*RedHat Package Manager*) — server a administrační konzole.

Poznámka: Kerio MailServer používá pro instalace standardní program RPM. Všechny parametry pro RPM jsou funkční a *Kerio MailServer* je plně podporuje.

Instalaci je třeba provádět s právy superuživatele (`root`). *Kerio MailServer Engine* se instaluje do adresáře `/opt/kerio/mailserver`, *Kerio Administration Console* do adresáře `/opt/kerio/admin`.

Nová instalace

Instalaci provedeme příkazem:

```
# rpm -i <název_instalačního_souboru>
```

Např.:

```
# rpm -i kerio-kms-6.5.0-1070.linux.i386.rpm
```

U novějších verzí distribucí se při instalaci mohou vyskytnout problémy se závislostmi balíčků. Pokud vaše distribuce odmítne *Kerio MailServer* nainstalovat, stáhněte a nainstalujte balíček `compat-libstdc++`
Bezprostředně po instalaci doporučujeme důkladně pročíst LINUX-README soubor, který najdete v adresáři:

`/opt/kerio/mailserver/doc`

Po instalaci je třeba spustit konfiguračního průvodce, kde lze nastavit doménu a administrátorský účet:

```
cd /opt/kerio/mailserver
./cfgwizard
```

Upozornění: Po dobu, kdy je spuštěn konfigurační průvodce nesmí být spuštěn *Kerio MailServer Engine*.

Spouštění a zastavování serveru

Po úspěšném nastavení konfiguračního průvodce je možno *Kerio MailServer* spustit.

V adresáři `/etc/init.d` se při instalaci vytvoří skript `keriomailserver`, který zajistí automatické spouštění daemona (tj. *MailServer Engine*) po startu systému. Tímto skriptem lze daemon také ručně spustit a zastavit:

```
/etc/init.d/keriomailserver start
```

```
/etc/init.d/keriomailserver stop
```

```
/etc/init.d/keriomailserver restart
```

Poznámka: Kerio MailServer musí být spuštěn pod uživatelem root.

Administrace

Program *Kerio Administration Console* se spouští příkazem `kerioadmin` umístěného v adresáři `/usr/bin`, do kterého je v systému standardně nastavena cesta. Pro jeho spuštění je vyžadováno grafické rozhraní *X Window System*.

Mac OS X

Kerio MailServer podporuje od verze 6.2 systémy Mac OS X jak na procesorech PowerPC, tak na procesorech Intel. Instalační balík *Kerio MailServeru* má tvar univerzálně binárního souboru, který lze spustit na obou platformách.

Instalaci je možno provést na těchto systémech:

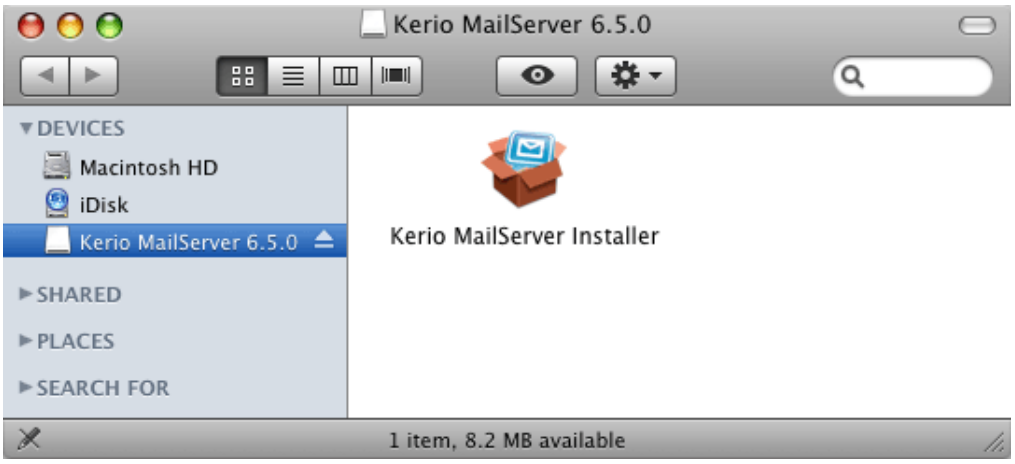
- Mac OS X 10.3.9 Panther na G4 nebo G5, 512 MB RAM, Mac Intel Solo nebo Duo, 512 MB RAM
- Mac OS X 10.4 Tiger na G4 nebo G5, 512 MB RAM; Mac Intel Solo nebo Duo, 512 MB RAM
- Mac OS X 10.5 Leopard na G4 nebo G5, 512 MB RAM; Mac Intel Solo nebo Duo, 512 MB RAM

Doporučeno: G5, 1GB RAM Mac Intel Solo nebo Duo, 1GB RAM

`kerio-kms-6.5.0-1069.mac.dmg`

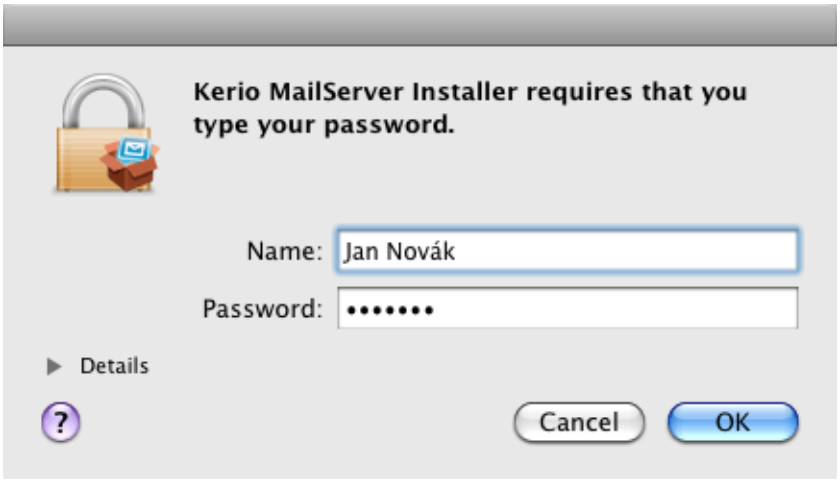
1. Instalační balík `kerio-kms-6.5.0-1069.mac.dmg` otevřeme dvojitým kliknutím na ikonku balíku.

2. Otevře se *Finder*, který instalační balík otevře jako disk a nabídne spustitelný instalační soubor *Kerio MailServer Installer*, který kliknutím spustíme (viz obrázek 2.9).



Obrázek 2.9 Kerio MailServer Installer

3. *Kerio MailServer* může do systému instalovat pouze uživatel s právem administrace. Před instalací se automaticky otevře okno pro zadání jména a hesla (viz obrázek 2.10). Vyplníme jméno a heslo uživatele, kterému byla přiznána práva k administraci systému. Pouze oprávněný uživatel (člen skupiny *Admins*) může v systému instalovat aplikace.

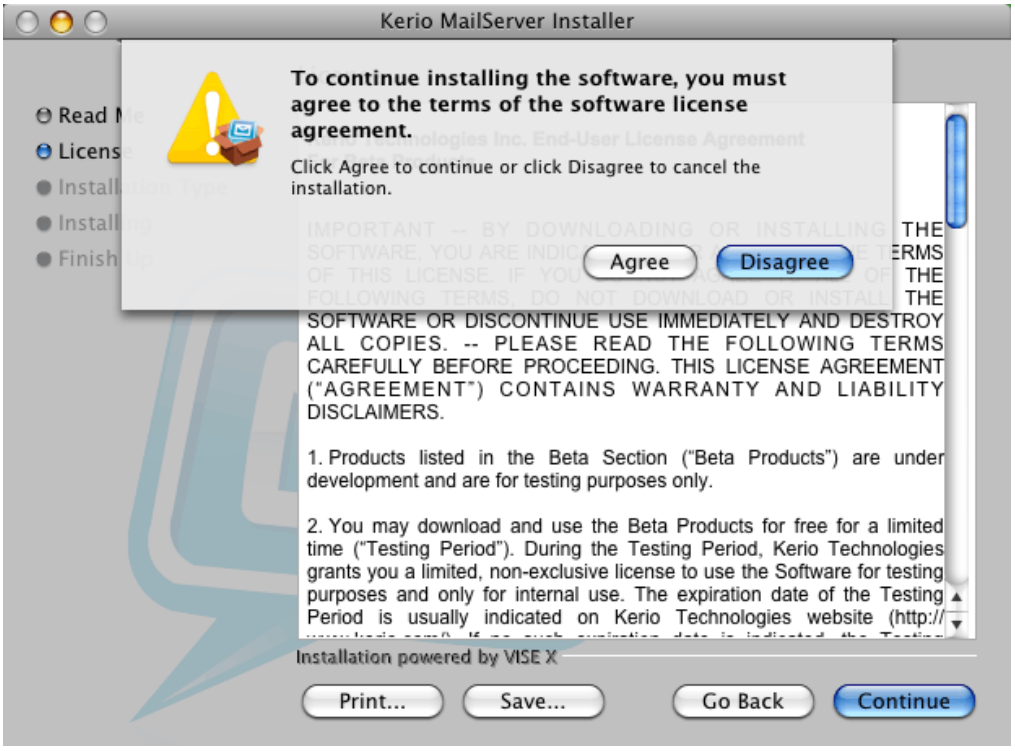


Obrázek 2.10 Ověření uživatele

Tato práva může administrátor přidat každému uživateli v *System Preferences* → *Accounts*.

4. Po úspěšném ověření se otevře standardní průvodce instalací.

5. Průvodce nejprve zobrazí licenční podmínky aplikace. Klikneme na tlačítko *Continue* a odsouhlasíme licenční podmínky tlačítkem *Agree*.

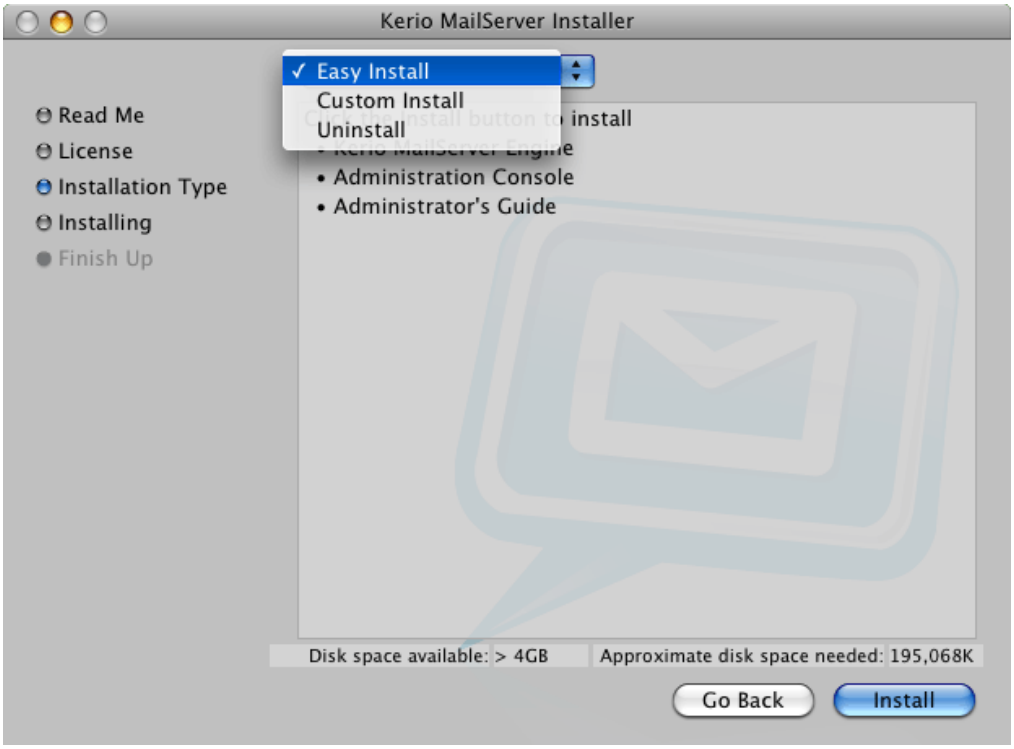


Obrázek 2.11 Licenční podmínky

6. Po odsouhlasení licenčních podmínek se otevře dialog, kde můžeme vybrat typ instalace:

   - *Easy Install* — přednastaveno, instalátor nainstaluje všechny části aplikace.
   - *Custom Install* — můžeme si vybrat jednotlivé komponenty (*Kerio Administration Console*, *Kerio MailServer Engine* a manuál *Administrator's Guide*).
   - *Uninstall* — odinstaluje *Kerio MailServer* ze systému.

   Vybereme vhodný typ instalace (nejjednodušším řešením je typ *Easy Install*, který instaluje všechny komponenty) a klikneme na tlačítko *Install*.



Obrázek 2.12 Instalace-vlastní nastavení

7. Průvodce spustí instalaci.

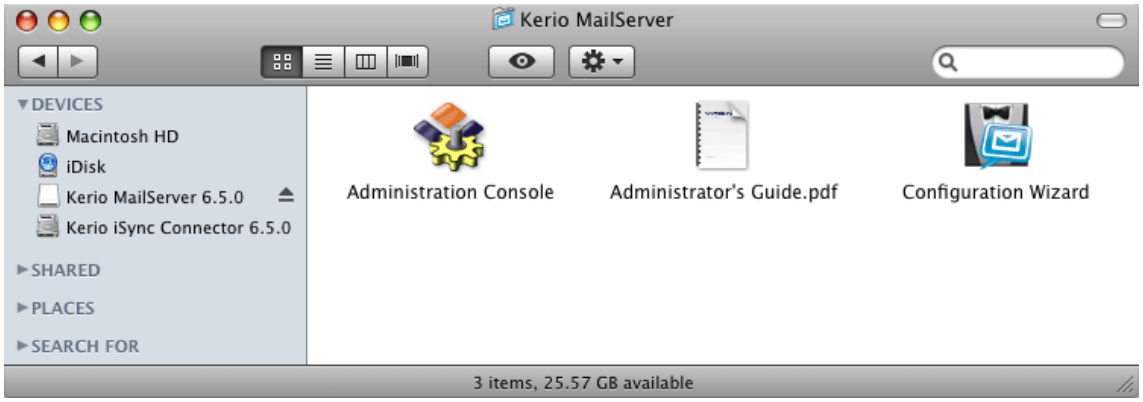
   Kerio MailServer se standardně instaluje do adresáře `/usr/local/kerio/mailserver`

   Podle informací v dialogovém okně bude nainstalována kompletní verze aplikace *Kerio MailServer*, tedy *Kerio Administration Console*, *Kerio MailServer Engine* a manuál *Administrator's Guide*.

8. Po ukončení instalace se automaticky otevře průvodce konfigurací, který nám pomůže nastavit název primární domény a doplnit heslo administrátora, kterým se posléze ověříme při přístupu k administrační konzoli *Kerio MailServeru* (viz kapitolu 2.5).

9. Po vyplnění konfiguračního průvodce se objeví závěrečný dialog instalátoru. Celou instalaci ukončíme pomocí tlačítka *Quit*.

Po ukončení instalačního průvodce se automaticky otevře složka nazvaná *Kerio MailServer*, která obsahuje spustitelný soubor *Administration Console*, příručku administrátora (*Administrator's Guide*) ve formátu *PDF* a *Configuration Wizard* (více viz kapitolu 2.5).



Obrázek 2.13 Složka Kerio MailServer

Služba *Kerio MailServer* se spustí automaticky při startu počítače. Chcete-li službu zastavit nebo restartovat, musíte spustit *Kerio MailServer Monitor* (*System Preferences* → *Other* → *KMS Monitor*). Pro zastavení nebo spuštění služby je nutné zadat uživatelské jméno (musí být součástí skupiny `Admins`) a heslo. Poté stačí použít tlačítko *Stop Kerio MailServer* (pro zastavení služby) nebo *Start Kerio MailServer* (pro spuštění služby).

Kerio MailServer je možno ovládat také z terminálu nebo SSH klienta následujícími příkazy (s právy uživatele root):

Zastavení Kerio MailServer Engine

```
SystemStarter stop KerioMailServer
```

Spuštění Kerio MailServer Engine

```
SystemStarter start KerioMailServer
```

Restart Kerio MailServer Engine

```
SystemStarter restart KerioMailServer
```

2.5 Průvodce počáteční konfigurací

Instalační program v systémech Windows a Mac OS X automaticky spouští průvodce, který nám pomůže nastavit základní parametry *Kerio MailServeru*. Tohoto průvodce lze vyvolat také kdykoliv později spuštěním programu `cfgWizard.exe` (v tom případě je ale nutno nejprve zastavit službu *Kerio MailServer*). Při spuštění konfiguračního průvodce budou vymazány stávající konfigurační soubory.

V operačním systému Linux je tento průvodce rovněž k dispozici. Po instalaci příslušného RPM balíku je uživatel informován o tom, že může průvodce použít. Tuto informaci zobrazí i samotná služba (daemon) při svém spuštění, jestliže detekuje, že konfigurační průvodce nebyl dosud použit. Konfigurační průvodce je spuštěn příkazem

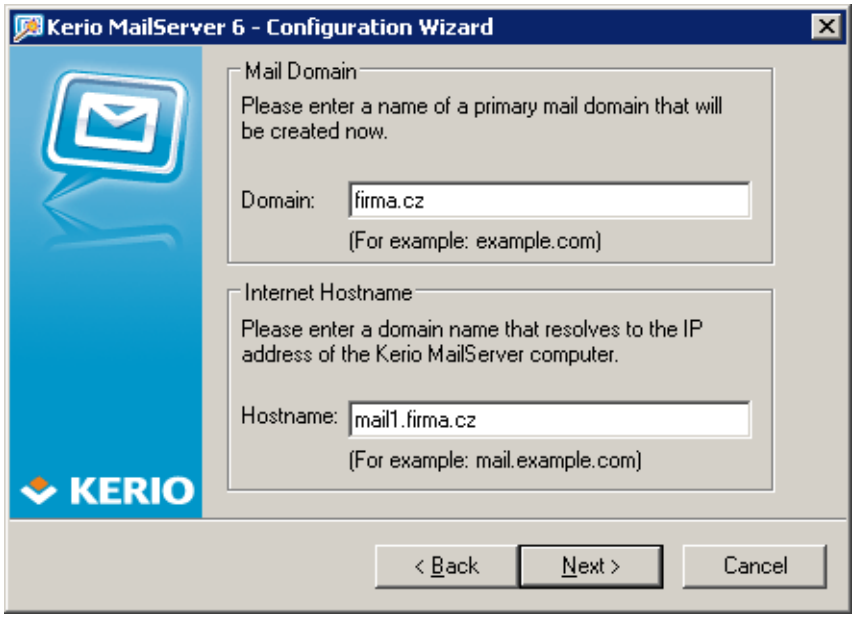
```
cd /opt/kerio/mailserver
./cfgwizard
```

Upozornění: Během nastavování konfiguračního průvodce nesmí být spuštěn *Kerio MailServer*.

Poznámka: Konfigurační průvodce pro všechny platformy je lokalizován pouze do anglického jazyka.

Primární doména a internetové jméno serveru

Aby bylo možno v *Kerio MailServeru* vytvářet uživatelské účty (příp. skupiny atd.), je třeba založit alespoň jednu lokální doménu. Lokální doména, která byla založena jako první, je automaticky primární doménou. Od ostatních lokálních domén se liší pouze tím, že se uživatelé mohou přihlašovat svým uživatelským jménem (v ostatních doménách je nutno použít celou e-mailovou adresu). O funkci a využití domén se dozvíte více v kapitole 7.



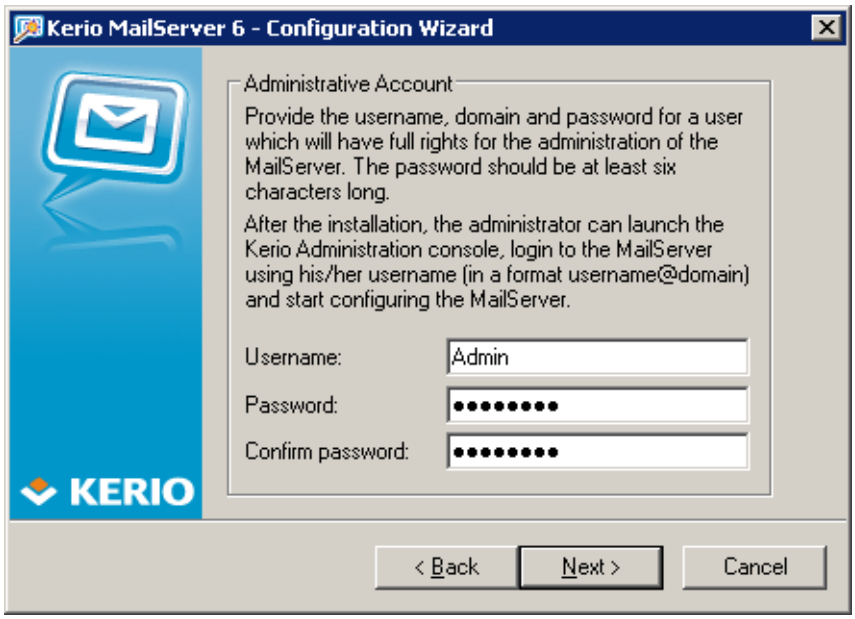
Obrázek 2.14 Průvodce konfigurací — vytvoření domény

Dále je třeba do tohoto kroku průvodce doplnit název serveru, kam je *Kerio MailServer* nainstalován. V položce *Hostname* by mělo být uvedeno internetové DNS jméno počítače, na němž je *Kerio MailServer* spuštěn (typicky název počítače doplněný názvem primární domény — takto je jméno serveru automaticky navrženo konfiguračním průvodcem). Jméno serveru se používá pro identifikaci serveru při navazování SMTP komunikace.

Upozornění: Je-li *Kerio MailServer* umístěn za NAT, je nutné do položky *Internetové jméno serveru* doplnit jméno, které je možné zpětně převést na IP adresu odesílajícího serveru, tj. internetové jméno firewallu.

Nastavení administrátorského hesla

Velmi důležitým krokem pro zajištění bezpečnosti vašeho serveru je nastavení administrátorského hesla. Heslo nesmí zůstat nevyplněno a mělo by obsahovat alespoň 6 znaků.



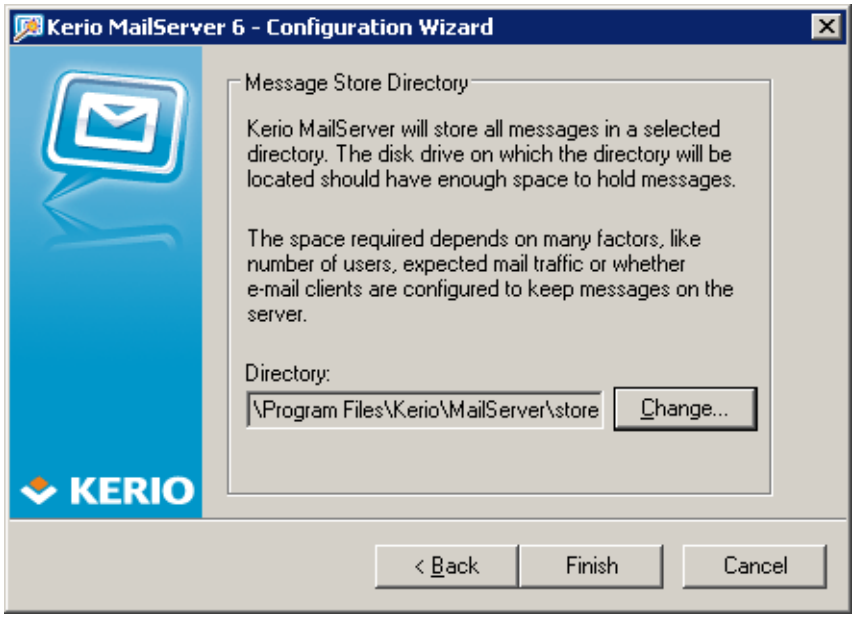
Obrázek 2.15 Průvodce konfigurací — založení administračního účtu

V dialogu pro nastavení účtu je třeba zadat heslo (*Password*) a zopakovat jej pro kontrolu (*Confirm Password*). V položce *Username* můžete změnit jméno administrátora (standardně `Admin`).

Výběr adresáře pro uložení dat

Kerio MailServer za provozu ukládá poměrně značné množství dat na disk (e-mailové zprávy, informace o uživatelských složkách, záznamy...). V některých případech může vzniknout požadavek ukládat data na jiný disk (např. jiný oddíl pevného disku, diskové pole RAID apod.). Adresář pro uložení dat je také možno změnit kdykoliv později v programu *Kerio Administration Console* (více v kapitole 15.6), pak je ale potřeba přesunout soubory, které jsou v něm již uloženy (může to být velmi zdlouhavá operace). To vyžaduje zastavení služby *Kerio MailServer Engine*. Doporučujeme proto vybrat vhodný adresář pro uložení dat již při instalaci — v dialogu konfiguračního průvodce.

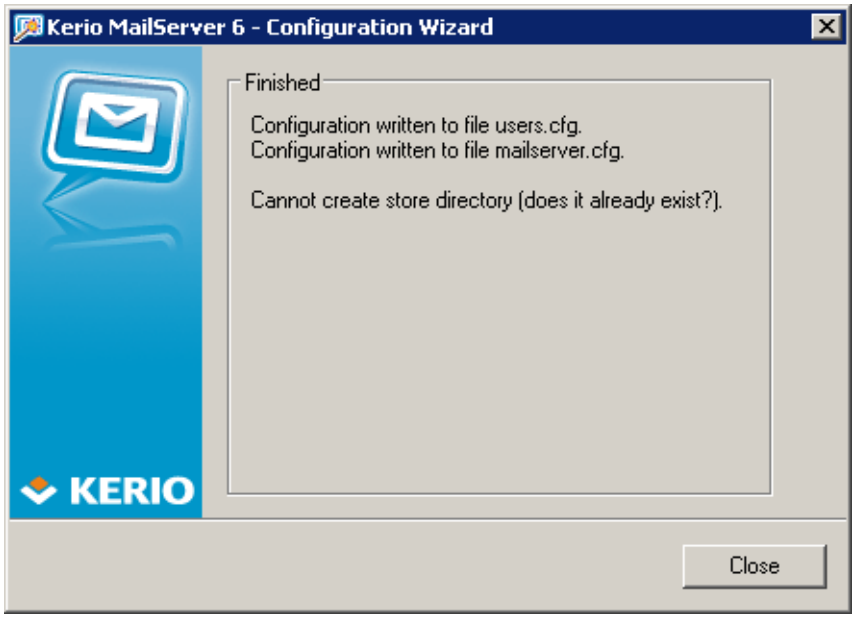
Tlačítko *Change* otevírá standardní systémový dialog pro výběr adresáře.



Obrázek 2.16 Průvodce konfigurací — výběr úložiště dat

Dokončení počáteční konfigurace

Poslední dialog průvodce informuje o úspěšném zápisu nastavení do konfiguračních souborů (pouze v operačním systému Windows):



Obrázek 2.17 Informace o úspěšném dokončení konfigurace primární domény

users.cfg
: `users.cfg` je XML soubor obsahující informace o uživatelských účtech, skupinách a aliasech.
Do tohoto souboru bylo konfiguračním průvodcem zapsáno administrátorské jméno a heslo.

mailserver.cfg
: `mailserver.cfg` je XML soubor, který obsahuje všechny ostatní konfigurační parametry *Kerio MailServeru*, jako jsou například konfigurace domén, zálohování, antispamového filtru, antiviru, atd.
Do tohoto souboru byla konfiguračním průvodcem zaznamenána právě založená lokální primární doména, internetové jméno serveru a umístění úložiště zpráv.

2.6 Upgrade a deinstalace

Operační systém Windows

Chcete-li provést upgrade (tj. instalovat novější verzi produktu získanou např. z WWW stránek výrobce), je třeba ukončit *Kerio Administration Console*, ostatní komponenty (*Kerio MailServer Engine* a *Kerio MailServer Monitor*) instalátor *Kerio MailServeru* sám zastaví. Instalační program automaticky rozpozná adresář, v němž je stávající verze nainstalována, a nahradí příslušné soubory novými. Přitom zůstanou zachována veškerá nastavení i uložené zprávy. V tomto případě se nedoporučuje měnit nabízený instalační adresář!

Při upgradu na novou verzi *Kerio MailServeru* postupujte stejným způsobem jako při počáteční instalaci *Kerio MailServeru* (viz kapitolu 2.4).

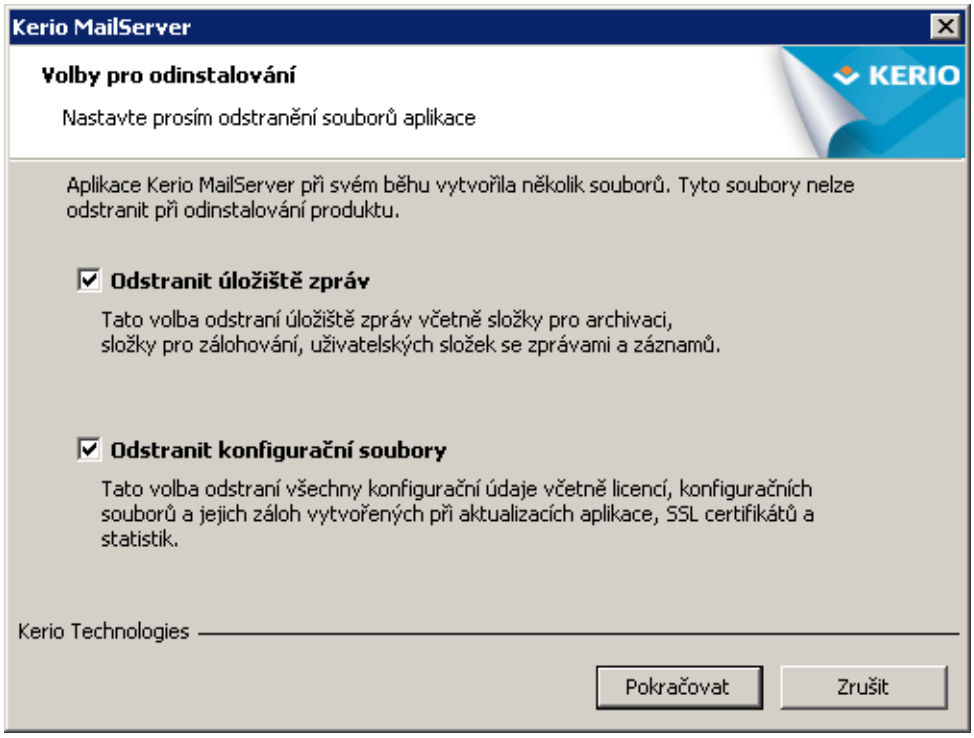
Po úspěšném upgradu na novou verzi se do adresáře, kam je *Kerio MailServer* nainstalován (standardně `C:\Program Files\Kerio`), uloží záloha konfiguračních souborů předchozí verze *Kerio MailServeru* (adresář `UpgradeBackups`).

Program lze odinstalovat průvodcem *Přidat nebo odebrat programy* ve složce *Ovládací panely*:

1. V *Přidat nebo odebrat programy* najděte položku *Kerio MailServer* a stiskněte tlačítko *Odstranit*.

2. Spustí se instalační průvodce *Microsoft Installer*.

3. První krok průvodce zjišťuje, zda chceme smazat *Kerio MailServer* kompletně, tedy i s datovým adresářem a konfiguračními soubory (viz obrázek 2.18):



Obrázek 2.18 Dialog pro odstranění datového adresáře a konfiguračních souborů

- *Odstranit úložiště zpráv* — po zaškrtnutí této volby bude odstraněno datové úložiště *Kerio MailServeru* včetně úložiště pro archivaci a zálohy.
- *Odstranit konfigurační soubory* — po zaškrtnuté této volby budou odstraněny konfigurační soubory (`mailserver.cfg` a `users.cfg`), soubor s licencí, SSL certifikáty, statistiky a záznamy.

Po nastavení dialogu stiskněte tlačítko *Pokračovat*.

4. Při samotné deinstalaci je zobrazen také teploměr se stavem jejího průběhu. Buďte trpěliví, celý proces může trvat i několik minut.

Operační systém Linux

Upgrade na novější verzi

Upgrade provedeme příkazem:

```
# rpm -U <název_instalačního_souboru>
```

Např.:

```
# rpm -U kerio-kms-6.5.0-1070.linux.i386.rpm
```

Oprava instalace stávající verze

Opravu stávající instalace provedeme příkazem:

```
# rpm -U --force <název_instalačního_souboru>
```

Např.:

```
# rpm -U --force kerio-kms-6.5.0-1070.linux.i386.rpm
```

Deinstalace

Kerio MailServer odinstalujeme těmito příkazy:

```
# rpm -e <název_balíku>
```

Tj.:
`# rpm -e kerio-mailserver` (pro standardní *Kerio MailServer*)
`# rpm -e kerio-mailserver-admin` (pro *Kerio Administration Console*)
Poznámka: Při deinstalaci budou odstraněny pouze soubory, které byly obsaženy v původním instalačním balíku a soubory, které nebyly změněny. Konfigurace, zprávy ve schránkách, atd. zůstanou zachovány. Tyto soubory je možno smazat ručně nebo je ponechat pro případnou další instalaci.

Poznámka: Program RPM umožňuje použití i dalších, rozšířených parametrů. Popis a použití těchto parametrů lze najít na manuálové stránce programu RPM. Manuálovou stránku lze spustit následujícím příkazem:

```
man rpm
```

Operační systém Mac OS X

Upgrade

Chcete-li provést upgrade (tj. instalovat novější verzi získanou např. z WWW stránek výrobce), je třeba ukončit *Kerio Administration Console*, ostatní komponenty (*Kerio MailServer Engine* a *Kerio MailServer Monitor*) instalátor *Kerio MailServeru* sám zastaví. Instalační program automaticky rozpozná adresář, v němž je stávající verze nainstalována, a provede nahrazení příslušných souborů novými. Přitom zůstanou zachována veškerá nastavení i uložené zprávy. V tomto případě se nedoporučuje měnit nabízený instalační adresář!

Deinstalace

Pro deinstalaci je také třeba zastavit *Kerio Administration Console*. Program lze odinstalovat pomocí instalátoru *Kerio MailServeru*. To znamená, že stačí kliknout na ikonu instalačního balíku *Kerio MailServeru*, který je momentálně nainstalován, spustit instalaci a v jejím průběhu vybrat jako typ instalace položku *Uninstall*.

Kapitola 3

Registrace produktu a licence

Zakoupený produkt *Kerio MailServer* je třeba zaregistrovat. Registraci *Kerio MailServeru* lze provést v administrační konzoli (kapitola 3.2), případně na WWW stránkách firmy *Kerio Technologies* (kapitola 3.1).

Pokud nebude *Kerio MailServer* řádně zaregistrován, bude se chovat jako zkušební verze. Zkušební verze *Kerio MailServeru* není nikterak funkčně omezena, je omezena pouze časově. Po 30 dnech provozu přestane fungovat *Kerio MailServer Engine*.

Z výše uvedeného zároveň vyplývá, že rozdíl mezi zkušební a plnou verzí *Kerio MailServeru* je pouze v tom, zda si jí zaregistrujete či nikoliv. Každý zákazník má tedy možnost si produkt ve třiceti denní lhůtě vyzkoušet v konkrétních podmínkách. Po registraci již není třeba *Kerio MailServer* znovu instalovat a nastavovat.

3.1 Registrace produktu přes WWW stránky

Registrace přes web je umožněna na produktových stránkách společnosti *Kerio Technologies* (`https://secure.kerio.com/reg`) v menu *Podpora* → *Registrace licencí*. Tento způsob registrace využijete zejména v případě, že *Kerio MailServer* nemá přístup do Internetu.

Registrací získáte licenční klíč (soubor s certifikátem `license.key`), který je třeba importovat do *Kerio MailServeru*. Import licenčního klíče popisuje kapitola 3.3.

Poznámka: Přes web nelze zaregistrovat zkušební verzi *Kerio MailServeru*.

3.2 Registrace produktu pomocí administrační konzole

V *Kerio Administration Console* je možno produkt zaregistrovat na hlavní stránce *Kerio MailServeru* (viz obrázek 3.7). Hlavní stránka *Kerio MailServeru* se zobrazí vždy bezprostředně po spuštění *Kerio Administration Console*. Kdykoli později je možno ji zobrazit kliknutím na *Kerio MailServer* v levém seznamu sekcí uspořádaném do stromové struktury (kapitola 5.2).

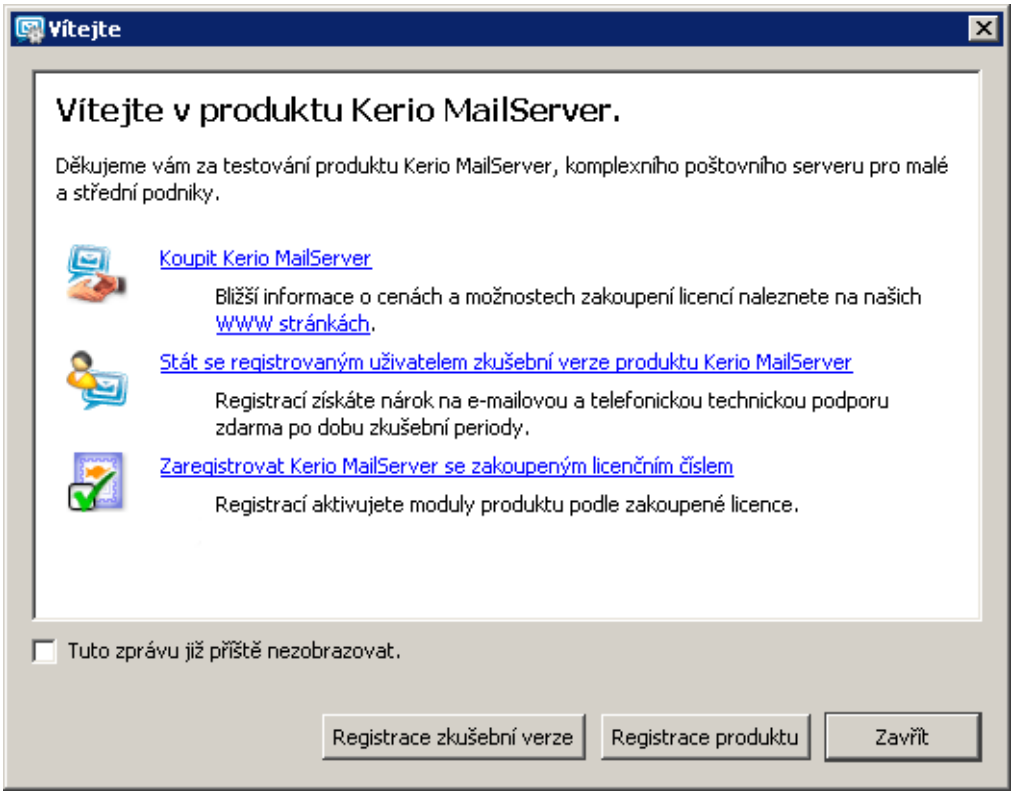
Upozornění: Je-li *Kerio MailServer* chráněn firewallem, potom je třeba povolit na tomto firewallu odchozí HTTPS komunikaci pro *Kerio MailServer* na standardním portu 443. Pokud nebude HTTPS komunikace povolena, *Kerio MailServer* se nebude moci přes zmíněný port připojit k registračnímu serveru firmy *Kerio Technologies*.

Bezprostředně po instalaci lze produkt zaregistrovat buď jako zkušební nebo jako plnou verzi:

Proč registrovat zkušební verzi produktu

Trial (zkušební) verze produktu slouží k seznámení se s konfigurací a funkčností produktu. Pokud se rozhodnete zkušební verzi zaregistrovat, budete mít nárok na plnou technickou podporu společnosti *Kerio Technologies* po celou dobu její platnosti (30 dní).

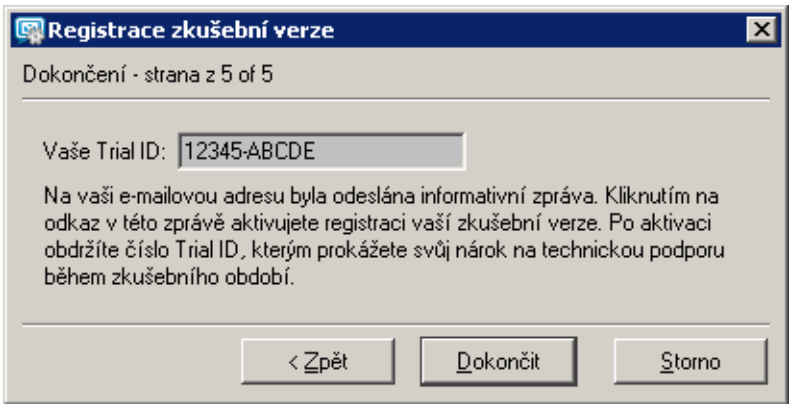
Bezprostředně po instalaci se otevře dialog informující správce o možnosti registrace zkušební verze (viz obrázek 3.1). Zkušební verzi produktu lze zaregistrovat na hlavní stránce produktu (více viz obrázek 3.7). Po otevření této stránky stačí kliknout na odkaz *Trial* a vyplnit registračního průvodce.



Obrázek 3.1 Registrace produktu

Doporučujeme věnovat pozornost pátému kroku, kde vám bude vygenerován speciální identifikační kód *Trial ID*, kterým bude třeba se identifikovat technické podpoře při zadávání dotazů. Trial ID se po úspěšné registraci zobrazí v *Kerio Administration Console* v okně s informacemi o licenci.

Poznámka: Chcete-li *Kerio MailServer* v zaregistrované zkušební verzi přeinstalovat nebo přenést na jiný počítač, doporučujeme nejprve zazálohovat soubor s konfigurací `mailserver.cfg`, který obsahuje mimo jiné i vaše Trial ID.



Obrázek 3.2 Trial ID

Proběhla-li registrace úspěšně, bude vám na váš e-mail vyplněný v registračním průvodci doručeno potvrzení o registraci.

Registrace plné verze produktu

Registrace plné verze produktu se spouští kliknutím na odkaz *Zaregistrovat produkt* na hlavní stránce (viz obrázek 3.7) administrační konzole:

- *Základní produkt* — V prvním kroku průvodce je třeba vyplnit licenční číslo získané při zakoupení produktu (*Licenční číslo*).

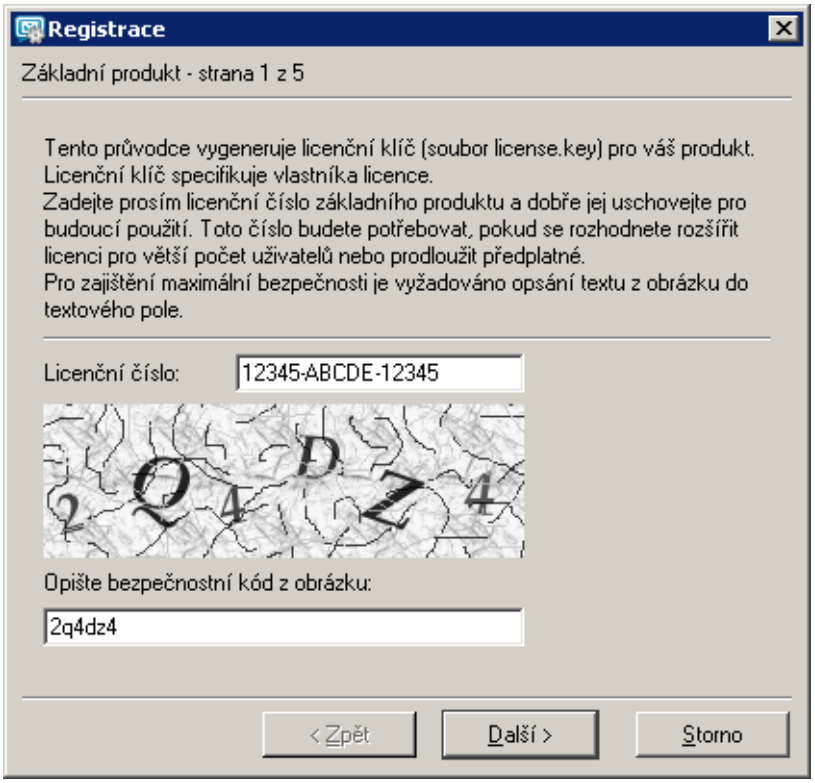
  Licenční číslo
  : Zadejte licenční číslo produktu.

  Bezpečnostní kód
  : Do pole opište kód z obrázku. Tento kód slouží jako ochrana proti automatickým generátorům licenčních čísel.
  Při zápisu se nerozlišují velká a malá písmena.

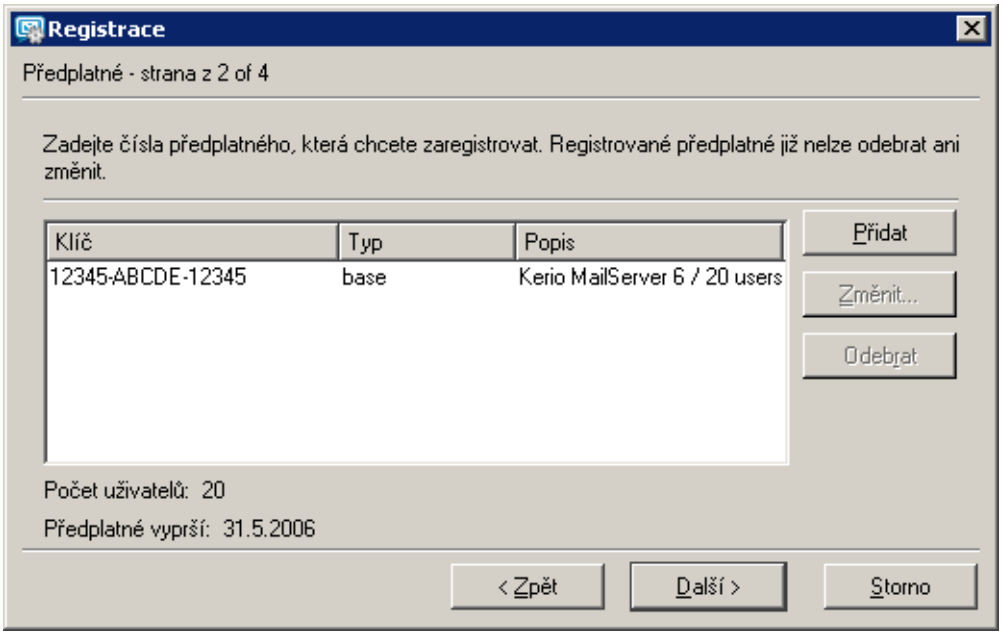
  Po stisknutí tlačítka *Další* naváže *Kerio MailServer* spojení s registračním serverem a zkontroluje platnost zadaného čísla. Je-li číslo neplatné, v registraci nelze pokračovat.

- *Předplatné* — Druhý krok průvodce umožňuje zadat čísla add-on licencí a předplatného. Pokud máte zakoupenu pouze základní licenci (typicky při první registraci produktu), pak tento krok přeskočte.

  Systém předplatného a add-on licencí je podrobně popsán na produktových stránkách společnosti *Kerio Technologies* `http://www.kerio.cz/subscr/`.



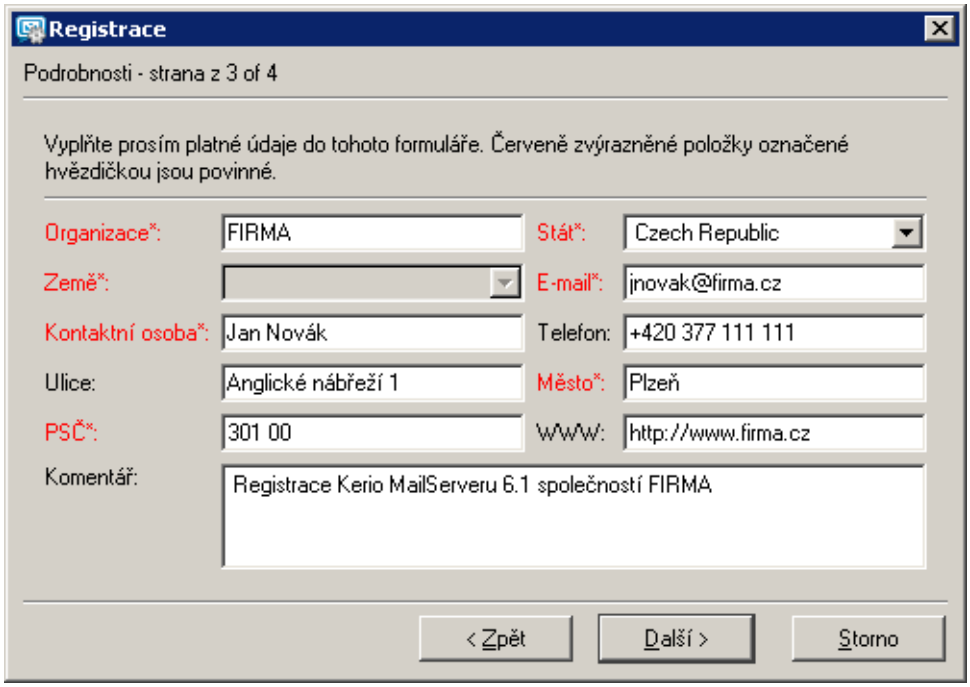
Obrázek 3.3 Licenční číslo



Obrázek 3.4 Čísla předplatného a add-on licencí

Do pole lze přidat jedno nebo více licenčních čísel získaných při koupi předplatného nebo add-on licence. Přidaná čísla lze dle potřeby opravit nebo odstranit. Všechna čísla budou zaregistrována najednou po stisknutí tlačítka *Další*.

- *Podrobnosti* — Ve třetím kroku jsou požadovány registrační informace o organizaci, na kterou je produkt registrován.



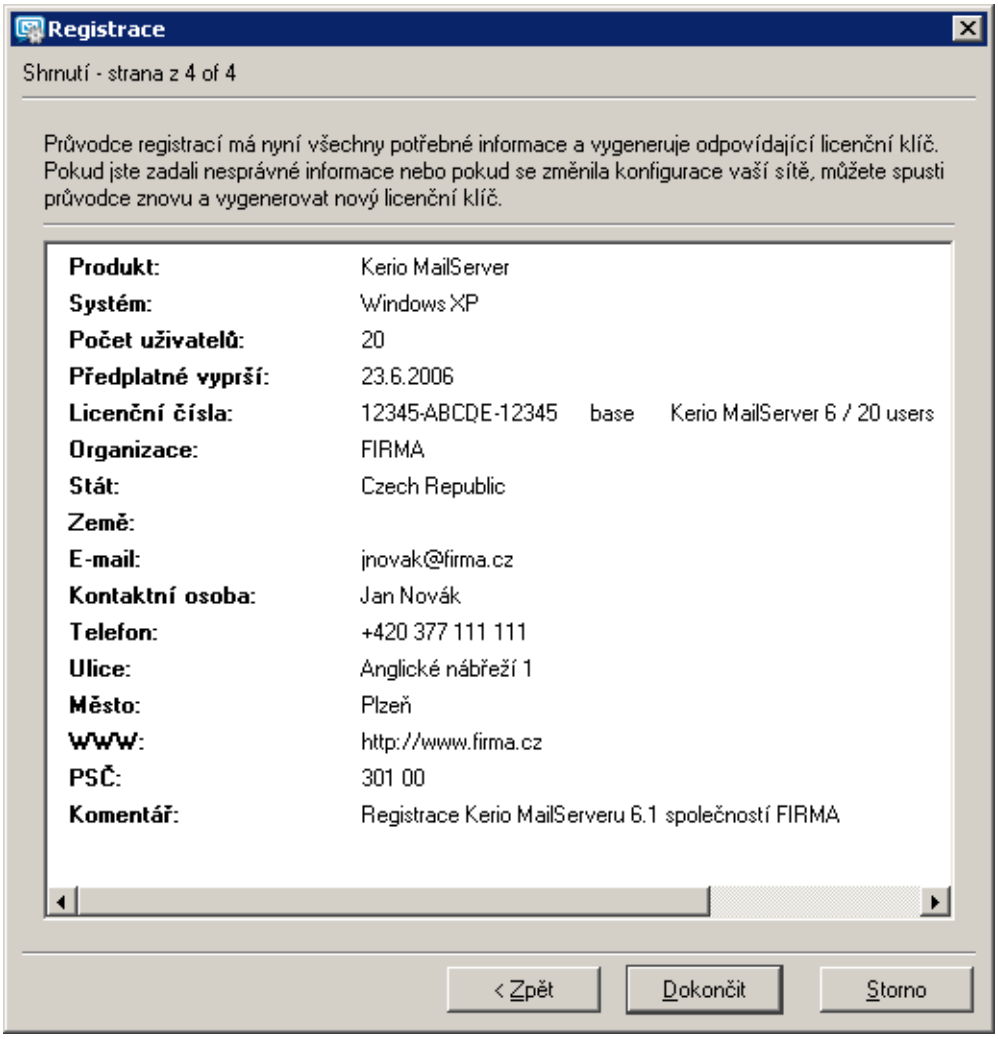
Obrázek 3.5 Registrační formulář

Červeně označené položky s hvězdičkou jsou povinné, tzn. musejí být vyplněny. Ostatní jsou volitelné.

- *Shrnutí* — Poslední krok průvodce registrací slouží ke kontrole údajů zadaných v předchozích krocích. Správce je informován o datu a čase vypršení předplatného (tj. nároku na bezplatné aktualizace produktu).

  Kerio MailServer naváže spojení s registračním serverem, ověří správnost zadaných údajů a automaticky stáhne licenční klíč (digitální certifikát).

  Stisknutím tlačítka *Dokončit* se průvodce uzavře.



Obrázek 3.6 Souhrn registračních údajů

3.3 Informace o licenci a import licenčního klíče

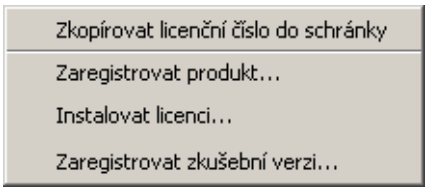
Informace o licenci se zobrazují na hlavní stránce *Kerio MailServeru*. Hlavní stránka *Kerio MailServeru* se zobrazí vždy bezprostředně po spuštění *Kerio Administration Console*. Kdykoli později je možno ji zobrazit kliknutím na *Kerio MailServer* v levém seznamu sekcí uspořádaném do stromové struktury (kapitola 5.2).

Plná verze *Kerio MailServeru* musí obsahovat tzv. licenční klíč. Licenční klíč je speciální soubor, který je třeba do produktu importovat. Licenční klíč lze získat třemi různými způsoby (záleží na typu registrace produktu a na tom, zda provedete registraci včas):

- Import licenčního klíče se provede automaticky během registrace produktu v administrační konzoli (kapitola 3.2).

Obrázek 3.7 Zobrazení informací o licenci

- *Import pomocí kontextového menu* — kliknutím pravého tlačítka myši na hlavní stránce (obrázek 3.7) se otevře kontextové menu, kde je třeba vybrat možnost *Instalovat licenci* (viz obrázek 3.8). Poté se zobrazí standardní dialog otevření souboru pro načtení licenčního klíče. Je-li import úspěšný, zobrazí se na hlavní stránce informace o nové licenci.



Obrázek 3.8 Kontextové menu hlavní stránky

  Pokud novou licencí rozšiřujete počet uživatelů, musí být po importu proveden restart *Kerio MailServer Engine*.

- *Ruční zkopírování souboru do adresáře license* — soubor `license.key` lze ručně zkopírovat do podadresáře `license` v adresáři, kde je *Kerio MailServer* nainstalován.

  Je-li potřeba importovat soubor ručně, pak je před importem vždy nutné nejprve zastavit *Kerio MailServer Engine*.

Produkt
Název produktu (*Kerio MailServer*).

Copyright
Copyright produktu.

Domovská stránka
Webová stránka společnosti *Kerio Technologies*.

Operační systém
Operační systém, pod kterým je aplikace spuštěna.

ID licence
Licenční číslo produktu.

Právo na aktualizaci končí
Datum skončení nároku na bezplatný upgrade.

Funkčnost produktu končí
Datum skončení funkčnosti produktu (pouze u demoverze nebo speciálních licencí).

Počet uživatelů povolený licencí
Počet uživatelů, který povoluje licence. V závorce je uveden počet všech e-mailových schránek využívajících *Kerio MailServer*. Patří sem jak uživatelské schránky založené lokálně, tak schránky mapované z adresářové služby.
Je-li počet aktivních schránek vyšší než počet povolených uživatelských licencí, řádek *Počet aktivních e-mailových schránek* se zabarví upozorňující červenou barvou.

Počet aktivních e-mailových schránek
Počet uživatelů, kteří se přihlásili v době od posledního restartu *Kerio MailServeru*. Jsou sem započítáni všichni lokální uživatelé, všechny e-mailové konference (1 konference = 1 licence) a všichni uživatelé mapovaní z adresářové služby.
V případě, že počet uživatelů překročí počet povolených licencí, se další uživatelé nebudou moci přihlásit ke své poště.

Společnost
Název společnosti (příp. osoby), na niž je produkt registrován.

Objeví-li se při spuštění konzole v informačním okně odkaz *K dispozici je nová verze programu...*, znamená to, že společnost *Kerio Technologies* uvolnila novou verzi produktu. Po kliknutí na tento odkaz se zobrazí webová stránka, kde lze vybrat a stáhnout novou verzi produktu. Nová verze je standardně ukládána do adresáře

```
Kerio/MailServer/store/tmp
```

3.4 Licenční politika

Počet uživatelů znamená počet e-mailových schránek/účtů a e-mailových konferencí vytvořených na *Kerio MailServeru* nebo importovaných z domény. Počet aliasů a domén není omezen.

Pokud jsou uživatelé mapování z LDAP databáze adresářové služby, počítají se jako licence všichni uživatelé založení v této databázi (všichni aktivní uživatelé).

V případě, že počet uživatelů překročí počet povolených licencí, se další uživatelé nebudou moci přihlásit ke své poště.

Předplatné

Systém předplatného a add-on licencí je podrobně popsán na produktových stránkách společnosti *Kerio Technologies* `http://www.kerio.cz/subscr/`.

Kapitola 4

Komponenty Kerio MailServeru

Kerio MailServer sestává z následujících součástí:

Kerio MailServer Engine
: Vlastní výkonný program, který realizuje všechny služby a funkce. Běží skrytě na pozadí (na Windows jako služba, v systémech typu Unix jako daemon).
Součástí *Kerio MailServer Engine* jsou také samostatně spuštěné procesy `avserver` a `spamserver`, které obsluhují antivirový plug-in a antispamový modul *SpamAssassin* (více viz sekci 4.2).

Kerio MailServer Monitor
: Slouží k monitorování a změně stavu *Engine* (zastaven/spuštěn), nastavení spouštěcích preferencí (tj. zda se má *Engine* a *Monitor* sám spouštět automaticky při startu systému) a snadnému spuštění administrační konzole. Podrobnosti najdete v kapitole 4.1.
Poznámka: Kerio MailServer Monitor je aplikace zcela nezávislá na *Kerio MailServer Engine* (který běží skrytě, příp. jako služba). *Engine* tedy může běžet, i když se na liště nezobrazuje ikona.

Kerio Administration Console
: Univerzální program pro lokální či vzdálenou správu produktů firmy Kerio Technologies. Pro připojení k určité aplikaci je třeba modul obsahující pro ni specifické rozhraní. Při instalaci *Kerio MailServeru* je *Administration Console* nainstalována s příslušným modulem (tzv. *plug-in*). Použití *Kerio Administration Console* pro správu *Kerio MailServeru* je podrobně popsáno v kapitole 5.

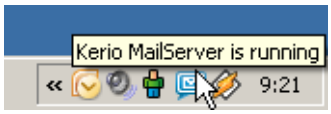
Performance Monitor
: Modul (plug-in) do systémové aplikace *Performance* pro sledování výkonu (resp. zatížení) jednotlivých komponent aplikace *Kerio MailServer*. Detaily naleznete v kapitole 22.9. Tento modul je možné použít pouze v operačním systému *MS Windows*.

4.1 Kerio MailServer Monitor

Kerio MailServer Monitor je utilita, která slouží k ovládání a monitorování stavu *MailServer Engine*. Tato komponenta je dostupná pouze v operačních systémech *Windows* a *Mac OS*.

Operační systém Windows

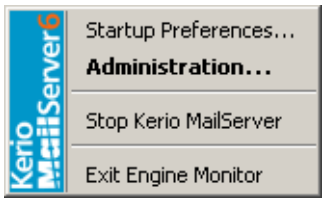
V operačním systému *Windows* se zobrazuje jako ikona v oznamovací oblasti na nástrojové liště.



Obrázek 4.1 Kerio MailServer Monitor

Je-li *Kerio MailServer Engine* zastaven, objeví se na ikonce zákaz. Spouštění či zastavování *Kerio MailServer Engine* může za různých okolností trvat až několik sekund. Po tuto dobu ikona zešedne a je neaktivní, tzn. nereaguje na kurzor.

Dvojitým kliknutím levým tlačítkem na tuto ikonu lze spustit program *Kerio Administration Console* (viz dále). Po kliknutí pravým tlačítkem se zobrazí menu, v němž je možno zvolit následující funkce:



Obrázek 4.2 Kerio MailServer Monitor — menu

Startup Preferences
: Volby pro automatické spouštění *Kerio MailServeru* a *Kerio MailServer Monitoru* při startu systému. Výchozí nastavení (po instalaci) je obě volby zapnuty.

Administration
: Tato volba spouští program *Kerio Administration Console* (totéž lze provést dvojitým kliknutím levým tlačítkem na ikonu *Kerio MailServer Monitoru*).

Start/Stop Kerio MailServer
: Spuštění nebo zastavení *MailServer Engine* (text se mění v závislosti na jeho stavu).

Exit Engine Monitor
: Ukončení programu *Kerio MailServer Monitor*. Tato volba nezastavuje *MailServer Engine*, na což je uživatel upozorněn varovným hlášením.

Operační systém Mac OS X

Kerio MailServer Monitor v operačním systému *Mac OS X* se zobrazuje ve speciálním okně (viz obrázek 4.3), které lze otevřít v *System Preferences* v sekci *Other*. Okno obsahuje následující možnosti:

Obrázek 4.3 Kerio MailServer Monitor — Kerio MailServer Status

- *About Kerio MailServer* — tlačítko otevře dialog *About*, který obsahuje základní informace o produktu a jeho verzi.
- *Stop/Start Server* — tlačítko umožňuje spustit nebo zastavit *Kerio MailServer Engine*.

  Pro zastavení nebo spuštění služby je nutné zadat uživatelské jméno (musí být součástí skupiny `Admins`) a heslo.
- *Configure Server* — tlačítko umožňuje spuštění *Kerio Administration Console*.

Kerio MailServer Monitor je možno ovládat také z terminálu nebo SSH klienta následujícími příkazy (s právy uživatele root):

Zastavení Kerio MailServer Engine

```
SystemStarter stop KerioMailServer
```

Spuštění Kerio MailServer Engine

```
SystemStarter start KerioMailServer
```

Restart Kerio MailServer Engine

```
SystemStarter restart KerioMailServer
```

Linux

Instalační balíčky pro linuxové distribuce neobsahují *Kerio MailServer Monitor*. *Kerio MailServer Engine* je možné spustit nebo zastavit následujícím příkazem:

```
/etc/rc.d/init.d/keriomailserver [start | stop]
```

4.2 Samostatné procesy serveru

`avserver` a `spamserver` jsou dva speciální procesy, které obsluhují aplikace vytvořené mimo společnost *Kerio Technologies*. Těmito aplikacemi jsou myšleny všechny antivirové plug-iny (ať už externí nebo McAfee antivirus) a antispamový filtr *SpamAssassin*. Jak napovídají jednotlivé názvy procesů, `avserver` obsluhuje antivirové plug-iny a `spamserver` obsluhuje *SpamAssassin*.

Oba dva procesy jsou umístěny v podobě spustitelných souborů v adresáři, kam byl *Kerio MailServer* nainstalován (`\Kerio\MailServer\plugins` v případě Windows, `/Kerio/mailserver/plugins` v případě platforem založených na unixové bázi).

Výše popsané procesy byly do *Kerio MailServeru* zavedeny ve verzi 6.2 a řeší problémy se stabilitou serveru, které se vyskytovaly v souvislosti se zmíněnými plug-iny.

V případě problému s některým z plug-inů (například při špatném ukončení spojení nebo takzvaném „vytuhnutí“spojení) proces provede automatický restart. To znamená, že pokud se v aplikaci projeví chyba, nespadne celý poštovní server, ani nebude na dlouhou dobu přerušena komunikace s příslušným plug-inem. Po restartu aplikace se také vytvoří a uloží záznam paměti, který by mohl s velkou pravděpodobností odhalit příčinu problému. Po přihlášení správce *Kerio MailServeru* se objeví dialog aplikace *Kerio Assist*, který se bude dotazovat, zda má být záznam paměti odeslán do společnosti *Kerio Technologies* k analýze.

Upozornění: Veškeré informace uložené ve výpisu budou použity pouze k odstranění problémů spojených s používáním produktů společnosti *Kerio Technologies*. Údaje ani elektronická adresa odesílatele nebudou žádným způsobem zneužity.

Kapitola 5

Správa Kerio MailServeru

Ke správě *Kerio MailServeru* slouží samostatný program *Kerio Administration Console* (univerzální aplikace pro správu serverových produktů firmy *Kerio Technologies*). *Kerio Administration Console* umožňuje lokální správu (tj. z téhož počítače, na kterém *Kerio MailServer Engine* běží) i vzdálenou správu (z libovolného jiného počítače). Komunikace mezi *Kerio Administration Console* a *Kerio MailServer Engine* je šifrována, což zabraňuje jejímu odposlechu a zneužití.

Administrace *Kerio MailServeru* je zcela nezávislá na platformě. Server spuštěný na operačním systému Linux je možno spravovat programem *Kerio Administration Console* spuštěným na systému Windows a naopak.

Program *Kerio Administration Console* se instaluje společně s aplikací *Kerio MailServer* (na platformách Windows a Linux lze *Kerio Administration Console* nainstalovat také zvlášť — například pro případ vzdálené správy *Kerio MailServeru*). Jeho použití je podrobně popsáno v samostatném manuálu *Kerio Administration Console — Nápověda*.

Poznámka: V případě eventuálního „zatuhnutí“ nebo pádu *Kerio Administration Console* se spustí speciální aplikace *Kerio Assist*, která po odsouhlasení správcem serveru odešle speciální soubor `mailadmin.dmp` k analýze do společnosti *Kerio Technologies*. Tento soubor obsahuje pouze data, která se týkají přímo *Kerio Administration Console*, nemohou být tedy žádným způsobem zneužita.

5.1 Lokalizace Kerio Administration Console

Kerio Administration Console lze spustit v několika jazykových mutacích (lokalizacích). Aktuální lokalizace *Kerio Administration Console* jsou následující:

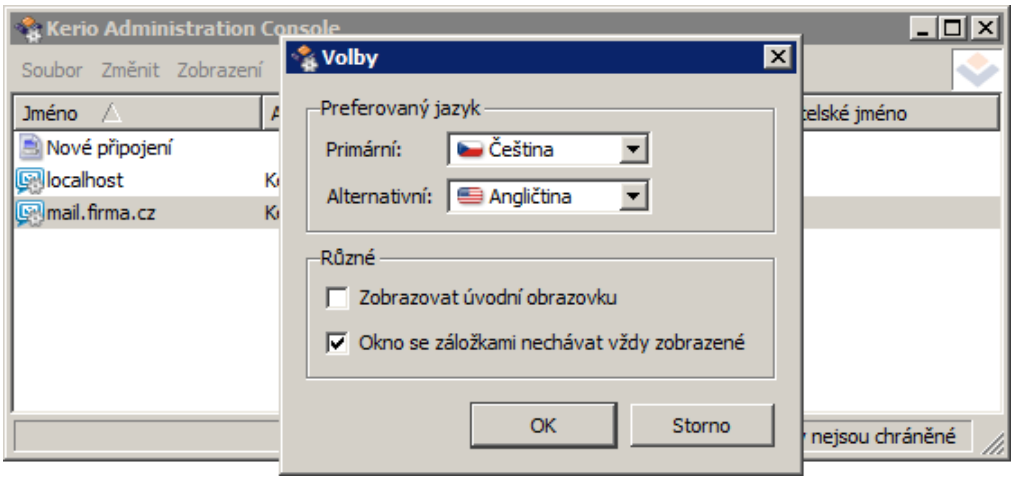
- Angličtina
- Čeština
- Čínština
- Italština
- Japonština
- Němčina
- Portugalština
- Ruština
- Slovenština

- Španělština
- Holandština
- Francouzština

Výchozí lokalizaci lze změnit takto:

1. Spustíme *Kerio Administration Console*.
2. Na panelu nástrojů *Kerio Administration Console* v menu *Nástroje* → *Možnosti* otevřeme dialog *Volby* (viz obrázek 5.1).

   V operačním systému Mac OS X najdeme stejný dialog v menu *Administration for Kerio MailServer* → *Preferences*.



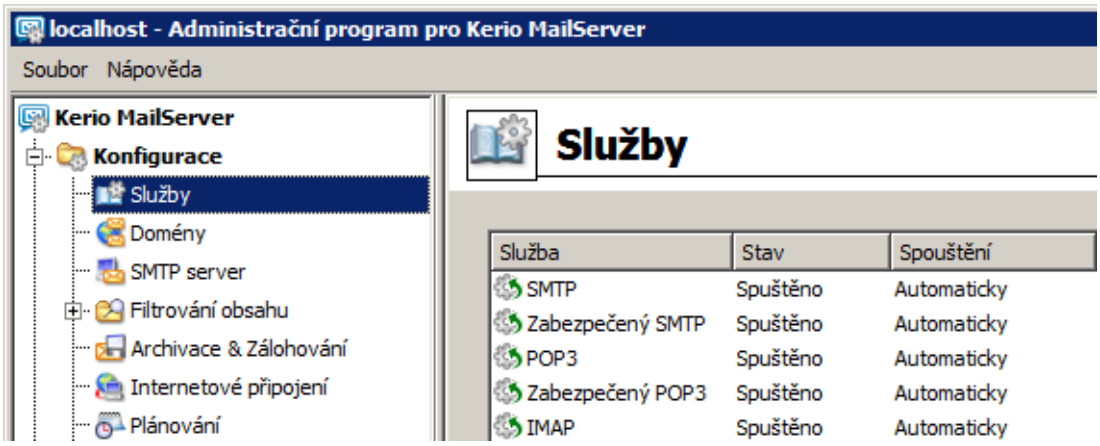
Obrázek 5.1 Kerio Administration Console — dialog Volby

3. V menu *Primární* nastavíme preferovaný jazyk.
4. Nastavení potvrdíme tlačítkem *OK*.

5.2 Administrační okno

Po úspěšném přihlášení programem *Kerio Administration Console* ke *Kerio MailServer Engine* se zobrazí hlavní okno modulu pro správu *Kerio MailServeru* (dále jen „administrační okno“). Toto okno je rozděleno na dvě části:

- Levý sloupec obsahuje seznam sekcí administračního okna uspořádaný do stromové struktury. Pro větší přehlednost lze jednotlivé části stromu skrývat a rozbalovat. *Kerio Administration Console* si při svém ukončení zapamatuje aktuální nastavení stromu a při dalším přihlášení jej zobrazí ve stejné podobě.
- Pravá část okna zobrazuje obsah sekce zvolené v levém sloupci (případně seznam sekcí ve zvolené skupině).



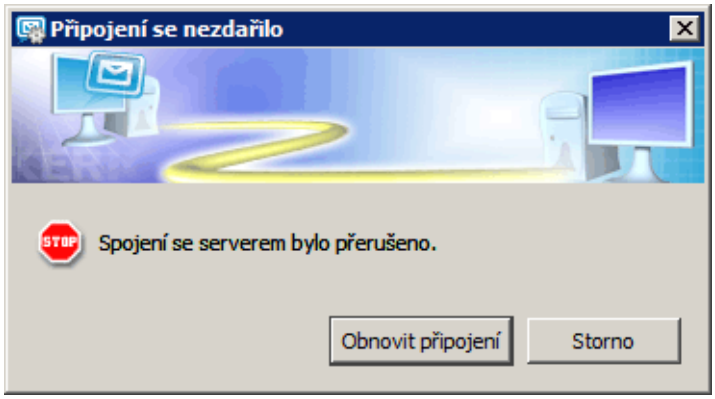
Obrázek 5.2 Kerio Administration Console

Hlavní menu administračního okna

Hlavní menu obsahuje tyto funkce:

Nabídka Soubor

- *Obnovit připojení* — připojení ke *Kerio MailServer Engine* po výpadku spojení (např. z důvodu restartu *Engine* či síťové chyby).



Obrázek 5.3 Obnovení připojení

- *Nové připojení* — tuto funkci lze využít, pokud chceme spravovat více serverových aplikací současně (např. *Kerio MailServer* na více serverech). Volba *Připojit k novému serveru* otevírá hlavní okno *Kerio Administration Console*, ze kterého se pak můžeme pomocí záložky nebo přihlašovacího dialogu připojit k požadovanému serveru (podrobnosti viz manuál *Kerio Administration Console — Nápověda*).
  Volba *Připojit k novému serveru* má stejný efekt jako spuštění *Kerio Administration Console* z nabídky *Start*.

- *Konec* — ukončení správy (odhlášení od serveru a uzavření administračního okna). Stejného efektu dosáhneme uzavřením okna kliknutím na závěr (křížek) v pravém horním rohu nebo kombinací kláves *Alt+F4*.

Nabídka Nápověda

- *Příručka administrátora* — otevření příručky administrátora (tohoto manuálu) ve formátu *HTML Help*. Podrobnosti o nápovědách naleznete v manuálu *Kerio Administration Console — Nápověda*.
- *O aplikaci* — informace o verzi aplikace (v tomto případě administračního modulu pro *Kerio MailServer*), odkaz na WWW stránku výrobce a další informace.

Stavový řádek

Na dolním okraji administračního okna je umístěn stavový řádek, který zobrazuje tyto informace (v pořadí zleva doprava):

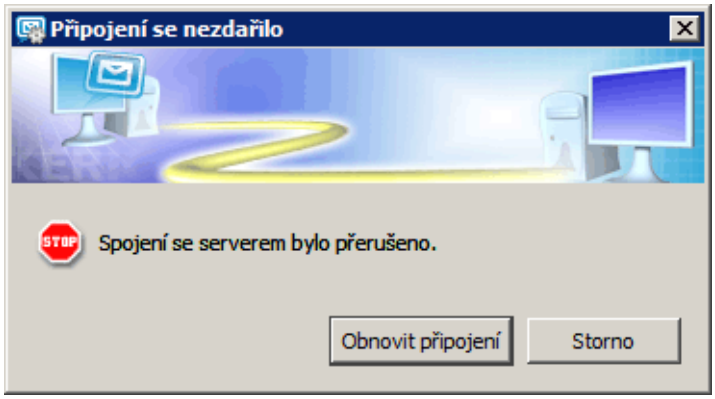
Obrázek 5.4 Stavový řádek

- Aktuální sekce administračního okna (vybraná v levém sloupci). Tato informace usnadňuje orientaci v administračním okně zejména v případech, kdy není vidět celý strom sekcí (např. při nižším rozlišení obrazovky).
- Jméno nebo IP adresa serveru a port serverové aplikace (*Kerio MailServer* používá port 44337).
- Jméno uživatele přihlášeného ke správě.
- Aktuální stav *Kerio Administration Console*: *Připraven* (čekání na akci uživatele), *Načítání* (přenos dat ze serveru) nebo *Ukládání* (zápis provedených změn na server).

Detekce výpadku připojení ke Kerio MailServer Engine

Administration Console dokáže automaticky detekovat, že došlo k výpadku připojení. Výpadek je zpravidla detekován při pokusu o čtení nebo uložení dat z/na server (tj. při stisknutí tlačítka *Použít* nebo přepnutí do jiné sekce *Administration Console*). V takovém případě se automaticky zobrazí dialog pro obnovení připojení s příslušným chybovým hlášením.

Po odstranění příčiny výpadku můžeme zkusit připojení obnovit. Pokud se připojení nepodaří obnovit, zobrazí se již pouze chybové hlášení. Pak můžeme zkusit připojení obnovit volbou *Soubor* → *Obnovit připojení* z hlavního menu, případně okno uzavřít a připojit se znovu standardním způsobem.

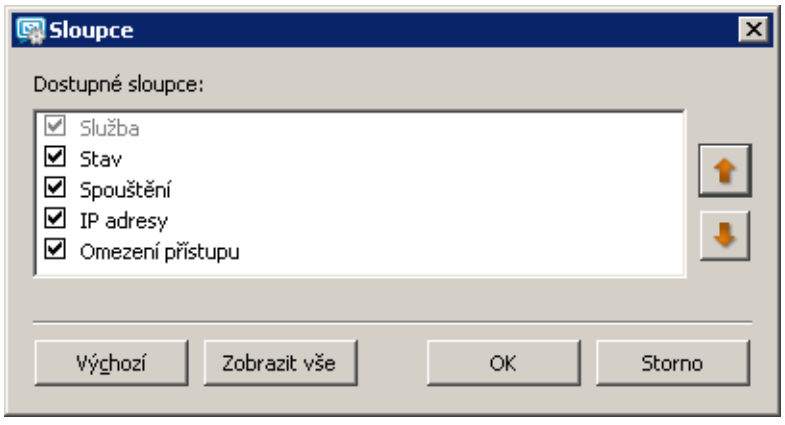


Obrázek 5.5 Detekce výpadku spojení s Kerio MailServer Engine

5.3 Nastavení pohledů

V mnoha sekcích *Kerio Administration Console* má zobrazení tvar tabulky, přičemž každý řádek obsahuje jeden záznam a sloupce obsahují jednotlivé položky tohoto záznamu.

Správce *Kerio MailServeru* má možnost upravit si způsob zobrazení informací v jednotlivých sekcích dle vlastní potřeby či vkusu. V každé z výše popsaných sekcí se po stisknutí pravého tlačítka myši zobrazí kontextová nabídka obsahující volbu *Nastavit sloupce*. Tato volba otevírá dialog, v němž je možné zaškrtnutím nastavit, které sloupce mají být zobrazeny, a které mají zůstat skryty.



Obrázek 5.6 Nastavení sloupců

Tlačítka *Posunout nahoru* a *Posunout dolů* slouží k posunu vybraného sloupce ve skupině nahoru nebo dolů. Tím můžete určit pořadí, v jakém mají být sloupce zobrazeny.

Pořadí sloupců lze také upravit v pohledu samotném: klikneme levým tlačítkem myši na název sloupce, podržíme jej a přesuneme na požadované místo.

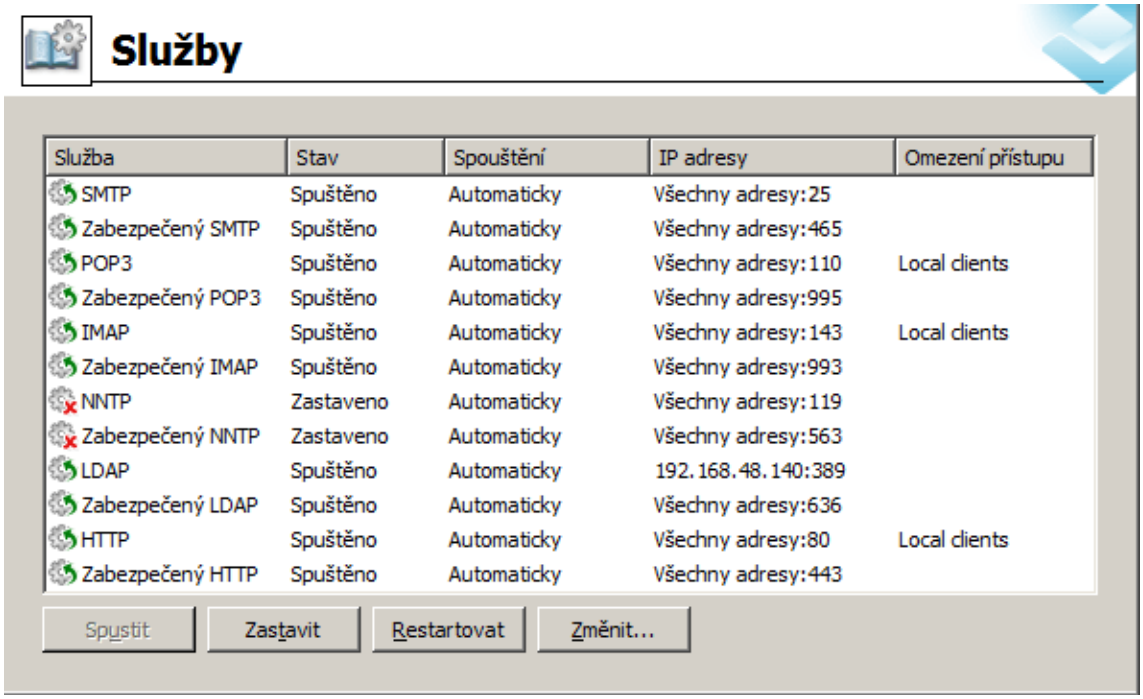
Šířku jednotlivých sloupců lze upravit posunutím dělicí čáry mezi záhlavími sloupců.

Další kapitoly tohoto manuálu již popisují jednotlivé sekce administračního okna *Kerio MailServeru*, které se zobrazí po úspěšném přihlášení ke *Kerio MailServer Engine*.

Kapitola 6

Služby

V sekci *Konfigurace* → *Služby* je možno nastavit parametry jednotlivých služeb *Kerio MailServeru*. Tlačítky *Spustit*, *Zastavit* nebo *Restartovat* umístěnými pod tabulkou lze službu spustit, zastavit nebo restartovat. Jedná se o následující služby:



Obrázek 6.1 Služby

SMTP

Server protokolu SMTP (Simple Mail Transfer Protocol) umožňující otevřené (nešifrované) i SSL zabezpečené spojení. SMTP server se používá pro odesílání odchozích zpráv (server odchozí pošty), pro zpracování příchozích zpráv (je-li primárním či záložním serverem pro danou doménu) a pro zprávy doručované e-mailovými konferencemi založenými v *Kerio MailServeru*.

Zabezpečený SMTP je SMTP server, jehož komunikace je šifrována SSL. Standardní port pro komunikaci je 465.

SMTP komunikace může být šifrována dvěma způsoby. Šifrování může probíhat buď přes SMTPS na portu 465 nebo přes SMTP na portu 25 (STARTTLS, pokud je

šifrování TLS[1] podporováno). Rozdíly mezi oběma způsoby zabezpečené komunikace jsou následující:

- SMTP na portu 25 se STARTTLS — komunikace na portu 25 začíná nešifrovaně. TLS je spuštěno přes STARTTLS, pokud obě strany TLS podporují. Pokud jej nepodporují, komunikace i nadále probíhá nešifrovaně.
- SMTP s SSL/TLS na portu 465 — komunikace je od počátku navázána jako šifrovaná.

Upozornění: Pokud komunikace mezi *Kerio MailServerem* a poštovním klientem probíhá na portu 25, může nastat problém s odesíláním pošty. Veřejné WiFi sítě často nepodporují komunikaci na nešifrovaných verzích protokolů, takže SMTP na portu 25 může být blokován. Uživatelé v takovém případě nemohou ze sítě odesílat svou poštu. SMTPS na portu 465 však obvykle bývá otevřeno. Z toho důvodu doporučujeme nevypínat SMTPS spojení, aby se uživatelé s notebooky nebo zařízeními *Apple iPhone* mohli přes tento port připojit k serveru. Zároveň je třeba uživatelům správně nastavit jejich poštovní klienty (šifrování pomocí SMTPS a port pro komunikaci).

POP3

Server protokolu POP3 (Post Office Protocol). Tento server umožňuje uživatelům — klientům vybírat (stahovat) zprávy ze svých schránek. Též bývá označován jako server příchozí pošty.

Zabezpečený POP3 je POP3 server, jehož komunikace je šifrována SSL. Šifrování komunikace znemožňuje její odposlech.

IMAP

Server protokolu IMAP (Internet Message Access Protocol). Rovněž zprostředkovává uživatelům přístup k jejich zprávám, ty však zůstávají uloženy ve složkách na serveru a může k nim tak být přistupováno z více míst současně.

Zabezpečený IMAP je IMAP server, jehož komunikace je šifrována SSL.

NNTP

Server protokolu NNTP (News Network Transfer Protocol) — přenosový protokol pro síťové diskusní skupiny v Internetu. Služba umožňuje uživatelům používat zprávy typu news a zobrazit pomocí tohoto protokolu veřejné složky.

Veřejnou složku lze přes protokol NNTP zobrazit pouze tehdy, pokud její název neobsahuje mezeru nebo znak . (tečka).

Zabezpečený NNTP je verze NNTP serveru, jehož komunikace je šifrována SSL.

LDAP

Jednoduchý LDAP server umožňující přístup k uživatelským a veřejným adresářům kontaktů. LDAP server umožňuje pouze čtení, neumožňuje zápis nových ani editaci existujících informací.

[1] TLS je následovník protokolu SSL, de facto SSL verze 3.1

Zabezpečený LDAP je LDAP server, jehož komunikace je šifrována SSL.
Pokud je *Kerio MailServer* nainstalován na serveru, který funguje jako doménový řadič (v *Active Directory*), potom je třeba služby LDAP i LDAPS spustit na nestandardním portu nebo je zakázat.

HTTP
Protokol HTTP se používá:

- pro přístup k uživatelským schránkám přes rozhraní *Kerio WebMail*,
- pro přístup ke správě uživatelů přes webové rozhraní *KMS Web Administration* (více viz kapitolu 31),
- pro přístup k poště klientem *Microsoft Entourage* (kapitola 38),
- pro přístup k *Free/Busy* serveru,
- při automatických upgradech nových verzí *Kerio Outlook Connectoru* a *Kerio Outlook Connectoru (Offline Edition)*.
- při synchronizaci přes *Kerio Synchronization Plug-in*.
- při synchronizaci přes protokol *ActiveSync*.
- při synchronizaci *BlackBerry* přes *NotifyLink*.
- při publikaci kalendářů ve formátu iCal.

Zabezpečený HTTP je šifrovaná verze tohoto protokolu (protokol HTTPS — SSL nebo TLS šifrování).

Bezprostředně po prvním spuštění *Kerio MailServeru* jsou všechny výše zmíněné služby spuštěny na standardních portech.

Poznámka: V případě, že určitě nebudete některé služby používat, doporučujeme je z důvodu vyšší bezpečnosti zastavit.

V případě, že na serveru již běží některá ze služeb, kterou poskytuje také *Kerio MailServer*, potom je třeba jedné ze služeb změnit port pro komunikaci. Pokud budete chtít změnit port služby v *Kerio MailServeru*, pak postupujte podle návodu v sekci 6.1.

6.1 Nastavení parametrů služeb

Seznam služeb (viz obrázek 6.1) obsahuje následující údaje:

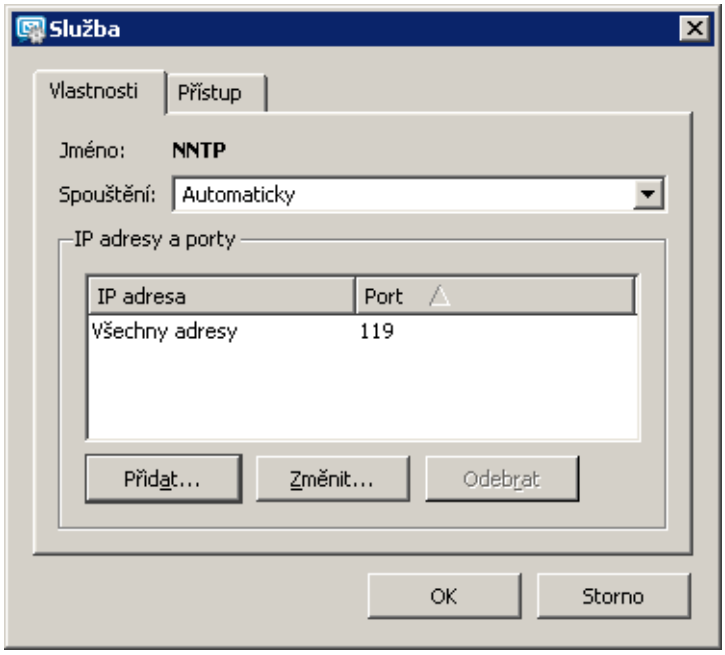
- Služba — zobrazuje název protokolu a ikonku, která zobrazuje, zda je služba spuštěna či zastavena.
- Stav (zastavena/spuštěna) — zobrazuje informaci o tom, zda je služba spuštěna nebo zastavena.
- Spouštění (ručně/automaticky) — zobrazuje informaci o tom, zda je službě nastaveno automatické nebo ruční spouštění po restartu *Kerio MailServeru*.
- IP adresy — zobrazuje všechny IP adresy a porty, na kterých daná služba *Kerio MailServeru* komunikuje.

- Omezení přístupu — *Kerio MailServer* umožňuje nastavení omezení přístupu na určitou skupinu IP adres, z nichž je možné danou službu využívat (typicky omezení nezabezpečených služeb pouze pro přístup z lokální sítě).

Vybrané službě lze změnit její parametry. K tomu slouží tlačítko *Změnit* umístěné pod seznamem služeb. Po jeho použití se otevře dialog *Služba* (viz obrázek 6.2). Dialog obsahuje dvě záložky:

Vlastnosti

V této záložce lze nastavit typ spouštění služby po restartu *Kerio MailServeru* a TCP port pro komunikaci.



Obrázek 6.2 Parametry služby

Jméno
Typ služby.

Spouštění
Kerio MailServer umožňuje dva typy spouštění:

- *Automaticky* — automatické spouštění znamená, že služba bude spuštěna ihned po startu *Kerio MailServeru*.
- *Ručně* — služba je po restartu serveru zastavena, musí být ručně spuštěna správcem.

IP adresy a porty

Kerio MailServer standardně poslouchá na všech IP adresách počítače na výchozích portech. Část dialogu nazvaná *IP adresy a porty* umožňuje přiřadit konkrétní IP adresu k portu, na kterém je služba spuštěna.

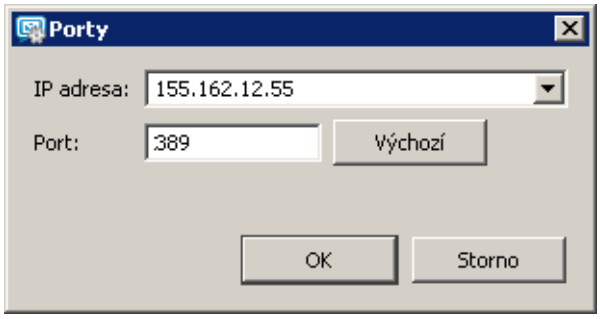
Přiřazení IP adresy ke standardnímu portu některé ze služeb spuštěných v *Kerio MailServeru* může pomoci v případě, že je na stejném počítači nainstalován *Kerio MailServer* a jiná aplikace poskytující stejné služby (například další LDAP server, webserver nebo poštovní server), potom je možné vyhradit *Kerio MailServeru* pouze jednu IP adresu pro každou službu, aby nedocházelo ke kolizím portů.

V praxi to znamená, že na dvou různých IP adresách můžou komunikovat dva různé WWW servery na standardním portu 80.

Poznámka: Samozřejmě je nutné stejné službě v jiné aplikaci také vyhradit IP adresu, kterou *Kerio MailServer* nepoužívá.

Upozornění: Přiřazování IP adres portům nedoporučujeme provádět v případě, že jsou adresy přidělovány dynamicky, například přes DHCP.

Tlačítkem *Přidat* můžete svázat adresu s portem.



Obrázek 6.3 Změna portu

Většina služeb využívá standardní porty, a nedoporučuje se je měnit, pokud to není nezbytné (např. v případě kolize s jinou aplikací téhož druhu). Výchozí nastavení lze obnovit tlačítkem *Výchozí*.

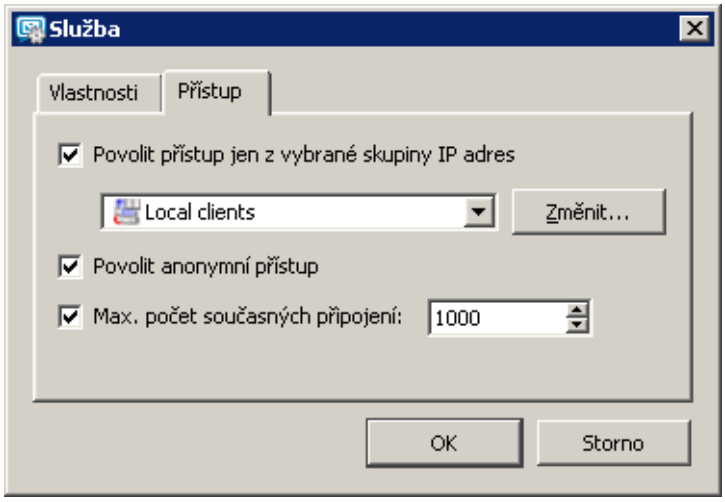
Přístup

Záložka *Přístup* umožňuje nastavení omezení přístupu k vybrané službě. V záložce lze nastavit následující:

Povolit přístup jen z vybrané skupiny IP adres

Omezení přístupu k této službě pouze z určitých IP adres (definovaných ve vybrané skupině). Skupinu IP adres lze definovat v sekci *Konfigurace* → *Definice* → *Skupiny IP adres* nebo přímo v tomto dialogu tlačítkem *Změnit*.

Omezení přístupu ke službě SMTP je možno podrobněji nastavit v sekci *Konfigurace* → *Antispamová ochrana*.



Obrázek 6.4 Omezení přístupu ke službě

Povolit anonymní přístup

Volba se vztahuje pouze na službu NNTP(S), proto dialogy příslušející ostatním službám tuto volbu neobsahují. Volba umožňuje neověřený přístup na NNTP server. V praxi to znamená, že ke konferenci, kam je povolen anonymní přístup, se může přihlásit kdokoli.

Max. počet současných připojení

Volba umožňuje omezit počet současných připojení na vybranou službu. Příliš mnoho současných připojení může přetížit server, což může vést až k jeho zastavení. Na tomto principu je založen DoS (Denial of Service) útok, kdy se útočník snaží přetížit server právě na základě vysokého počtu připojení ke službám. Omezení počtu připojení proto napomáhá k zamezení DoS (Denial of Service) útoku na váš server.

Upozornění: Při omezování počtu připojení vždy berte ohled na počet uživatelů využívajících server.

6.2 Důležité poznámky

Nezabezpečená a zabezpečená verze jedné služby se chovají duálně — tzn. de facto se jedná o dva různé způsoby přístupu k témuž serveru a uživatel (klient) má možnost volby, který z nich použít. Z hlediska bezpečnosti a ochrany soukromí jednoznačně doporučujeme používat zabezpečenou komunikaci, poštovní klient ji ovšem musí podporovat.

IMAP a HTTP přistupují identickým způsobem k téže IMAP schránce. Tyto dvě služby lze používat současně (střídavě) bez jakýchkoliv omezení a rizik. POP3 a IMAP (resp. HTTP) přistupují do téže fyzické schránky, ale protože protokol POP3 nepodporuje složky,

„vidí“ pouze zprávy ve složce *INBOX* (systémová složka pro příchozí zprávy), do níž jsou všechny příchozí zprávy ukládány. POP3 také stahuje zprávy ze serveru na klienta. Proto mohou nastat následující komplikace:

1. Jestliže se uživatel přihlásí do schránky nejprve protokolem POP3, zprávy ze složky *INBOX* budou staženy na jeho počítač. Po přihlášení protokolem IMAP tyto zprávy na serveru již nenalezne.

2. Přihlásí-li se uživatel nejprve protokolem IMAP (či HTTP) a přesune ručně zprávy do jiné složky, pak už je nebude možné protokolem POP3 stáhnout.

3. Má-li uživatel nastavena taková pravidla pro zprávy, aby se všechny zprávy přesouvaly do jiných složek, nebude možné protokolem POP3 stáhnout žádnou zprávu.

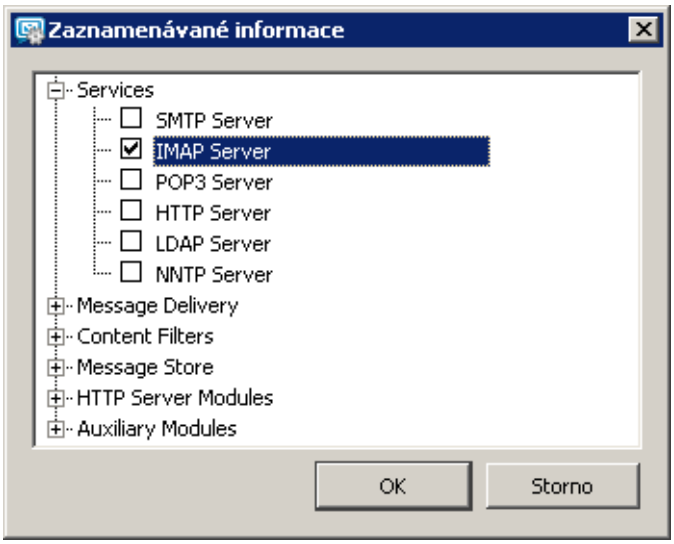
6.3 Řešení případných problémů

Při řešení případných problémů se službami může pomoci záznam komunikace mezi serverem a klienty. Zaznamenávání informací lze spustit zapnutím příslušné volby v sekci *Záznamy* → *Debug*, kterou obsahuje *Kerio Administration Console*:

1. Otevřeme v *Kerio Administration Console* sekci *Záznamy* a vybereme záznam *Debug*.

2. V okně záznamu pravým tlačítkem myši otevřeme kontextové menu a vybereme položku *Zprávy*.

3. Otevře se okno *Zaznamenávané informace*, kde vždy zapneme záznam pro příslušnou službu (viz obrázek 6.5).



Obrázek 6.5 Dialog pro nastavení záznamu Debug

4. Změnu potvrdíme tlačítkem OK.

K následujícím typům služeb patří tyto volby záznamu *Debug*:

SMTP
Pokud se v komunikaci mezi SMTP serverem a klientem objevují problémy, lze použít volby *SMTP Server* a *SMTP Client*.

POP3
Při řešení případných problémů na straně POP3 serveru může pomoci zaškrtnutí volby *POP3 Server*.

IMAP
Při řešení případných problémů na straně IMAP serveru může pomoci záznam *IMAP Server*.

NNTP
Při řešení případných problémů na straně NNTP serveru může pomoci záznam, který lze spustit volbou *NNTP Server*.

LDAP
Při řešení případných problémů na straně LDAP serveru může pomoci záznam, který lze spustit volbou *LDAP Server*.

HTTP

- *HTTP Server* — spustí záznam HTTP komunikace na straně serveru.
- *WebDAV Server Request* — spustí záznam dotazů ze strany WebDAV serveru. Lze využít v případě problémů s Exchange účty v *MS Entourage* nebo v *Apple Mail*.
- *SyncML Synchronization* — spustí záznam o synchronizaci kalendářů a kontaktů přes *SyncML Plug-in*. Lze využít při problémech se synchronizací přes *Kerio Synchronization Plug-in*.
- *PHP Engine Messages* — spustí záznam může napomoci při řešení problémů s webovým rozhraním *Kerio WebMail*.

Po vyřešení problému doporučujeme logování opět vypnout.

O záznamu *Debug* a jeho volbách se dozvíte více v kapitole 22.8.

Kapitola 7

Domény

Kerio MailServer umí obsluhovat několik nezávislých poštovních domén, pro které je možno definovat různé parametry.

V *Kerio MailServeru* je vždy jedna doména označena jako primární, a to ta, která je vytvořena jako první. Později, po vytvoření dalších domén lze jako primární nastavit libovolnou jinou doménu. Primární doména má tu vlastnost, že uživatelé v ní definovaní používají pro přihlášení pouze své uživatelské jméno, zatímco uživatelé v ostatních doménách musí zapsat uživatelské jméno i s celou poštovní doménou. Ukažme si to na příkladu:

Jako primární je definována doména `firma.cz`. V obou doménách je definován uživatel `uzivatel`. Uživatel v doméně `firma.cz` se bude ke své schránce přihlašovat jménem `uzivatel`, zatímco uživatel v doméně `jinafirma.cz` jménem `uzivatel@jinafirma.cz`.

Poznámka: Přihlášení celou e-mailovou adresou je možné i do primární domény.

Z výše uvedeného vyplývá, že pokud není žádný závažný důvod k nastavení jedné konkrétní domény jako primární, měla by být nastavena jako primární ta doména, která obsahuje největší počet uživatelů. Takto bude mít velký počet uživatelů zjednodušeno zadávání svého uživatelského jména při přihlašování k serveru.

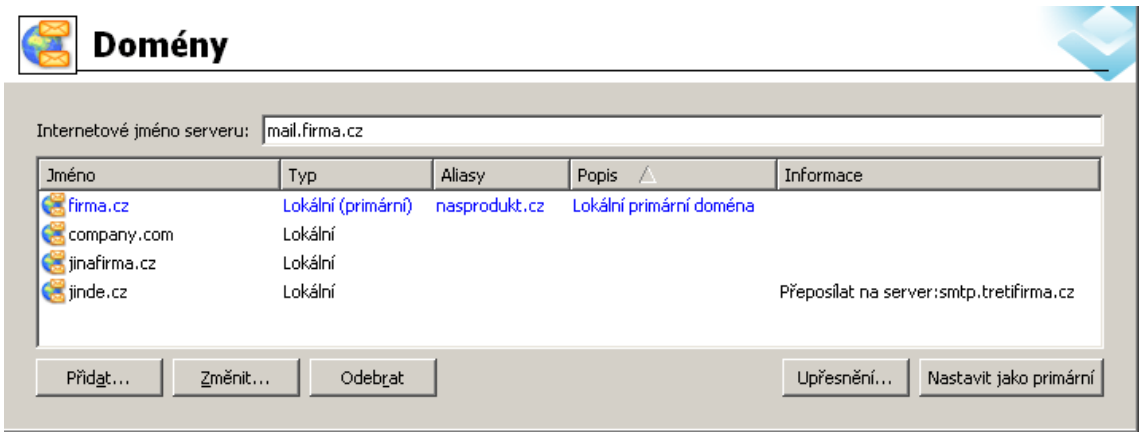
Uživatelské účty se definují v každé doméně zvlášť. Domény tedy musí být definovány dříve, než budou vytvářeny účty.

7.1 Definice domény

Definice domén se provádí v sekci *Konfigurace* → *Domény*.

V položce *Internetové jméno serveru* by mělo být uvedeno internetové DNS jméno počítače, na němž je *Kerio MailServer* spuštěn (typicky název počítače doplněný názvem primární domény — takto je jméno serveru automaticky vytvořeno instalačním průvodcem). Jméno serveru se používá pro identifikaci serveru při navazování SMTP komunikace.

Při navazování SMTP komunikace se používá příkaz EHLO pro zjištění reverzního DNS záznamu. Server, který komunikuje s *Kerio MailServerem* může reverzní DNS záznam kontrolovat.



Obrázek 7.1 Domény

Upozornění: Je-li *Kerio MailServer* umístěn za NAT, je nutné do položky *Internetové jméno serveru* doplnit jméno, které je možné zpětně převést na IP adresu odesílajícího serveru, tj. internetové jméno firewallu.

Tlačítko *Upřesnění* nastavuje umístění veřejných složek:

- *Vlastní pro každou doménu* — každá doména bude obsahovat vlastní veřejné složky. Toto nastavení neumožňuje, aby uživatel z jedné domény měl k dispozici jakoukoli veřejnou složku domény jiné.
  Zároveň to znamená, že pokud je založeno v *Kerio MailServeru* více domén, které obsahují uživatelské schránky, musí být v sekci *Uživatelské účty* (viz kapitolu 13) pro každou takovou doménu určen alespoň jeden uživatel, který bude veřejné složky spravovat.
- *Společné pro všechny domény* — uživatelé všech domén budou mít k dispozici tytéž veřejné složky.

Tlačítkem *Nastavit jako primární* je možné změnit typ domény (totéž lze provést v nabídce kontextového menu). Je-li doména přidávána jako první, může být pouze primární [*Lokální (primární)*]. Další přidávaná doména může být *Lokální (primární)* nebo *Lokální*.

Poznámka: Definujeme-li novou doménu a primární doména již existuje, pak je rovněž možno nastavit typ nové domény jako *Lokální (primární)*. V tom případě se nově vytvářená doména stane primární doménou a původní primární doména pouze lokální doménou.

Novou doménu je možno vytvořit tlačítkem *Přidat*.

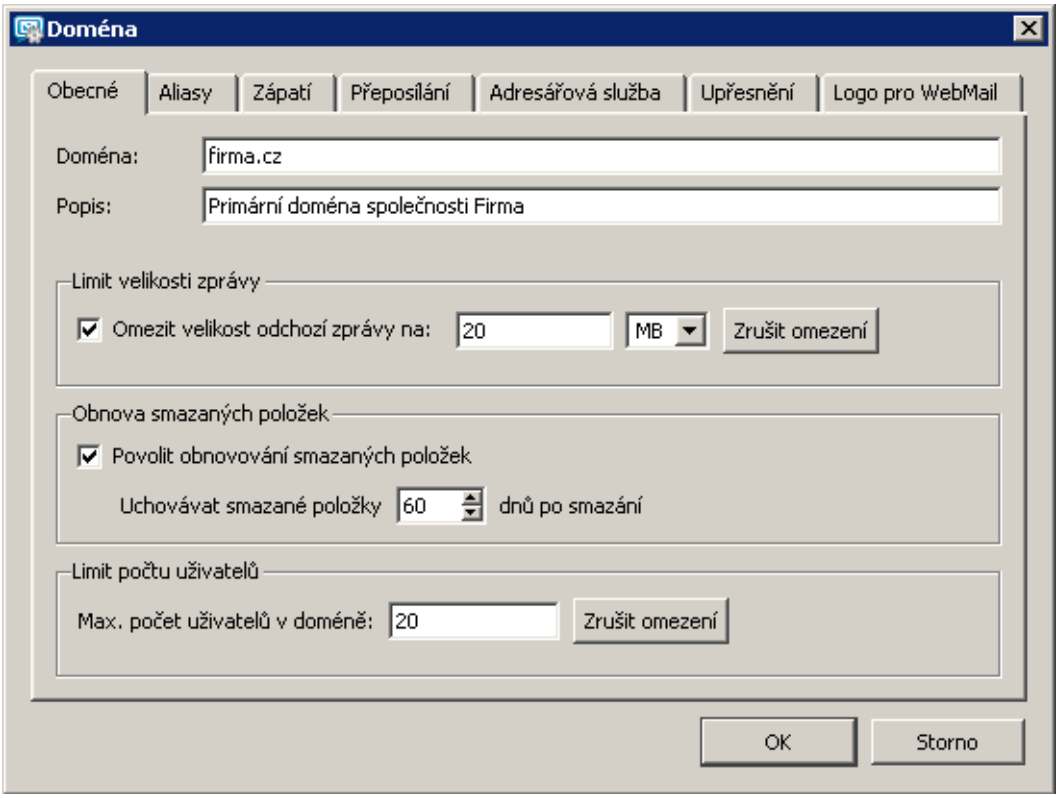
Zrušení domény

Tlačítkem *Odebrat* lze smazat vybranou doménu. Doménu není možné odstranit, jestliže:

- jsou v ní již definovány uživatelské účty nebo skupiny. Nejdříve musí být všechny účty smazány (podrobnosti viz kapitolu 13.5).
- jsou v ní definovány aliasy. Nejdříve musí být všechny aliasy smazány (podrobnosti viz kapitolu 15.3).
- se jedná o primární doménu. Je však možné vytvořit jinou doménu, tuto nastavit jako primární, a poté původní doménu odstranit.

7.2 Obecné

Základní parametry domény lze nastavit v záložce *Obecné*:



Obrázek 7.2 Nastavení domény — jméno a popis domény

Doména

Jméno nové domény.

Upozornění: Název domény nesmí obsahovat národní znaky a některé speciální znaky (viz tabulku *Povolené a zakázané znaky v názvu domény*).

Znaky	Způsob omezení
a–z	tyto znaky jsou povoleny bez omezení
0–9	tyto znaky jsou povoleny bez omezení
A–Z	tyto znaky jsou povoleny bez omezení
.	tento znak je povolen, nesmí však uvozovat nebo ukončovat řetězec a nesmí být použita dvakrát za sebou
-	tento znak je povolen bez omezení

Tabulka 7.1 Povolené znaky v názvu domény

Příklady správně vytvořených jmen:
`firma.cz`; `server.firma.cz`; `server-firma.cz`; `server---firma.cz`
Příklady špatně vytvořených jmen:
`firma..cz`; `firma...cz`; `.firma.cz`; `firma.cz.`; `server_firma.cz`

Popis

Libovolný textový komentář k vytvářené doméně (slouží pouze pro účely správce).

Limit velikosti zprávy

Nastavení limitu pro maximální velikost všech odchozích zpráv (přes SMTP, WebDAV, atd.). Limit platí pouze pro danou doménu.

Doporučujeme tuto volbu nastavit pro každou doménu, která obsahuje uživatelské schránky. Tímto způsobem lze jednoduše zabránit uživatelům, aby zahltili internetovou linku zprávami s obrovskými přílohami (fotografie, filmy, hudba a pod.).

Je-li limit nastaven na 0, chová se *Kerio MailServer* stejně, jako by limit nebyl nastaven.

Limit velikosti zprávy je možno nastavit také individuálně pro každého uživatele zvlášť (viz kapitolu 13.2). Limit nastavený konkrétnímu uživateli bude mít vyšší prioritu než limit nastavený doméně.

Obnova smazaných položek

Volba umožňuje obnovu smazaných položek (zpráv, událostí, kontaktů, poznámek a úkolů) zpět do složky *Odstraněná pošta*. Zároveň lze nastavit, jak dlouho se mají položky uchovávat, aby byla jejich obnova možná.

Vhodná doba nastavení souvisí s počtem uživatelských schránek v *Kerio MailServeru* a s volným místem na disku. Nesmí však přesáhnout dobu jednoho roku, tedy 365 dnů. Je-li nastaven vyšší počet dnů, nelze nastavení domény uložit.

Volbu doporučujeme zapnout u všech domén, které obsahují uživatelské schránky, protože je to nejsnazší cesta k dohledání omylem smazané položky (zprávy, události, kontaktu nebo úkolu) v konkrétní uživatelské schránce.
Obnovit položky zpět do složky *Odstraněná pošta* lze v sekci *Konfigurace* → *Nastavení domény* → *Uživatelské účty*. Jak obnovit položky konkrétním uživatelům popisuje kapitola 13.7.

Limit počtu uživatelů

Nastavení této položky je výhodné zejména v případě, že je využívána webová správa uživatelů (více viz kapitolu 31). Po nastavení limitu nemůže uživatel s právy pro správu uživatelských účtů ve své doméně tento limit překročit.

7.3 Aliasy

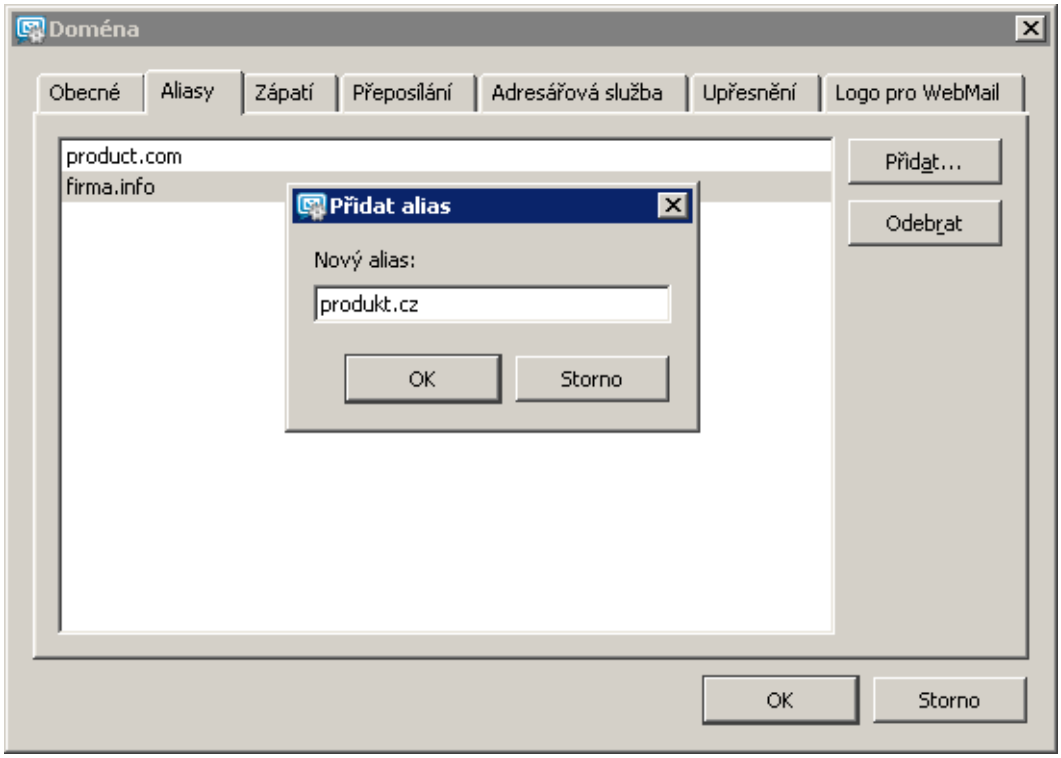
Každá poštovní doména může mít libovolný počet aliasů (tzv. virtuálních domén). Virtuální domény jsou alternativní jména (aliasy) pro jednu a tutéž doménu. Názvy virtuálních domén lze zadat do záložky *Aliasy*. E-mailové adresy ve virtuálních doménách jsou identické (doručují se do stejných schránek). Použití volby pouze umožňuje, aby jednotlivé uživatelské účty byly součástí více domén.

Využití doménových aliasů lze nejlépe vysvětlit na jednoduchém příkladu:

Firma využívá dvě domény s názvy `firma.cz` a `firma.com`. Jako poštovní doménu nastavil administrátor v *Kerio MailServeru* doménu `firma.cz`. E-mailová adresa pro uživatele bude tedy vypadat následovně: `uzivatel@firma.cz`. Vytvoříme-li pro doménu `firma.cz` doménový alias `firma.com`, může adresa téhož uživatele vypadat také `uzivatel@firma.com`. Odesílatel tedy může použít buď adresu `uzivatel@firma.cz` nebo `uzivatel@firma.com`. V obou případech bude pošta doručena stejnému uživateli.

Upozornění: Pokud se nejedná pouze o lokální alias (fiktivní doménu), musí být pro každou z těchto domén definovány příslušné MX záznamy v DNS. Prostá definice domény jako aliasu jiné domény nezajistí její existenci v Internetu.

Doménové aliasy je možno využít pouze pro příjem pošty. Uživatelé ji nemohou využívat pro přihlašování do *Kerio MailServeru* a nemohou ji využívat ani pro zobrazení *Free/Busy* serveru. Doménový alias nemá žádný význam pro správu.



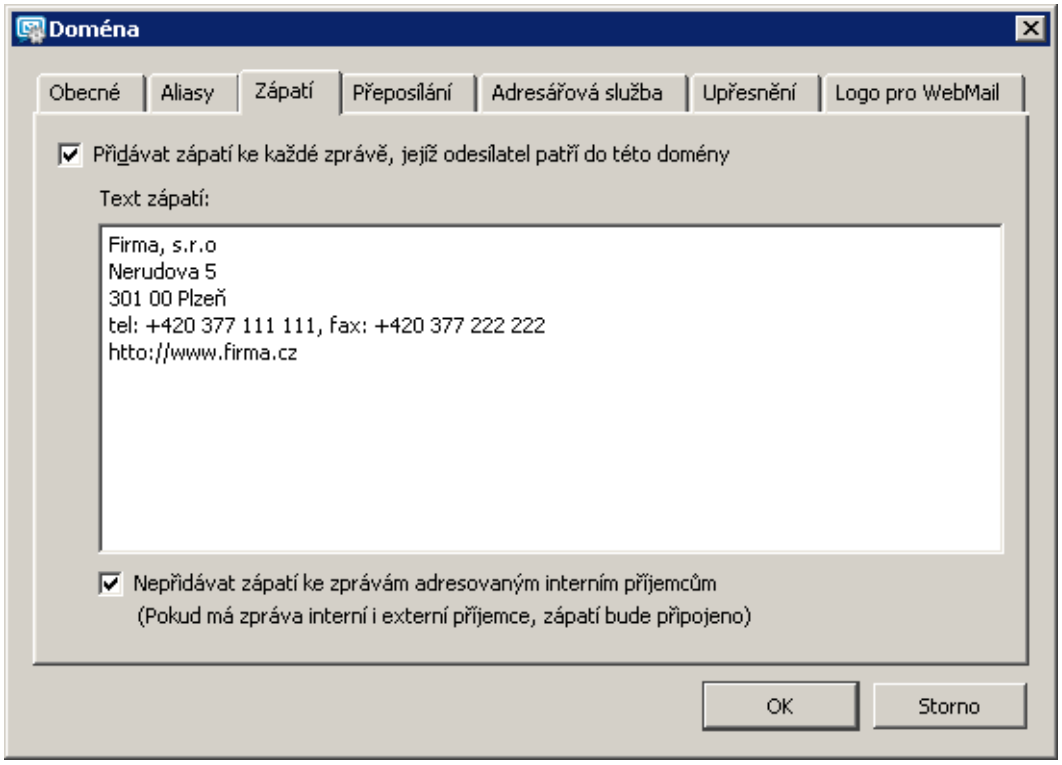
Obrázek 7.3 Nastavení domény — ekvivalentní domény

7.4 Zápatí

Tato záložka poskytuje možnost připojit k e-mailovým zprávám z této domény standardní zápatí (zápatí bude připojeno ke každé zprávě, kde adresa odesílatele obsahuje tuto doménu).

Poznámka: Pro text zápatí nelze využít HTML formát. Zápatí zobrazuje pouze prostý text.

Připojení zápatí ke zprávám, které jsou doručovány v rámci *Kerio MailServeru* bývá často zbytečné. Z toho důvodu je možné připojovat zápatí pouze ke zprávám, které nejsou doručovány lokálně. Toto nastavení lze provést zaškrtnutím volby *Nepřidávat zápatí ke zprávám adresovaným pouze interním příjemcům.*



Obrázek 7.4 Nastavení domény — zápatí

7.5 Přeposílání

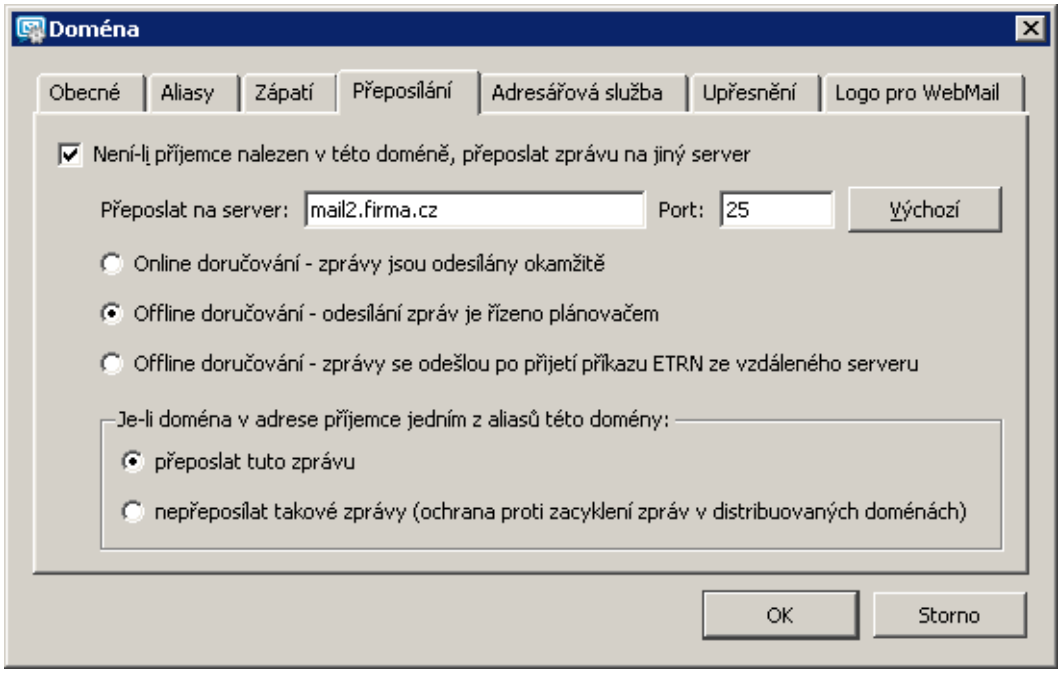
Záložka *Přeposílání* umožňuje přeposílání zpráv na jiný SMTP server. Přeposílání je možno využít zejména pro:

- rozložení domény na více serverů (více viz kapitolu 27.4),
- vytvoření záložního poštovního serveru (více viz kapitolu 27.5).

Není-li příjemce nalezen...
: Zaškrtnutím lze zapnout přeposílání zpráv na jiný SMTP server. Zprávy jsou přeposílány pouze v případě, že adresa příjemce není adresou žádného uživatele, žádné skupiny, ani aliasem v této doméně. Pokud nebude v této doméně definován žádný uživatel, skupina nebo alias, budou přeposlány všechny zprávy (ekvivalent domény typu *Forward* v *Kerio MailServeru 5.5* a starších).

Přeposlat na server
: DNS jméno nebo IP adresa SMTP serveru, na který budou zprávy přeposílány.

Port
: Port SMTP serveru. Tlačítko *Výchozí* dosazuje standardní port 25.



Obrázek 7.5 Nastavení domény — přeposílání zpráv

Online doručování — zprávy jsou odesílány okamžitě

Volbu lze využít, pokud je třeba nastavit rozložení domény na více serverů, a zároveň je k dispozici trvalé připojení do Internetu (více viz kapitolu 27.4).
Online doručování se řídí nastavením SMTP doručování (*Konfigurace* → *SMTP server* → *Volby pro frontu zpráv*). Bližší podrobnosti o této záložce najdete v kapitole 15.2.

Offline doručování — odesílání zpráv je řízeno plánovačem

Za normálních okolností *Kerio MailServer* odesílá zprávy pro domény přeposílající zprávy na definovaný SMTP server bezprostředně po jejich přijetí. Je-li připojen do Internetu vytáčenou linkou, může to mít za následek velmi časté vytáčení a zavěšování linky (a v důsledku toho vysoké náklady na připojení). Po zapnutí této volby budou zprávy pro doménu, která přeposílá zprávy, řazeny do fronty a odesílány pouze v časech daných plánovačem (více v kapitole 9).

Offline doručování — zprávy se odešlou po přijetí příkazu ETRN ...

Kerio MailServer odešle všechny zprávy pro tuto doménu na definovaný SMTP server až po přijetí příkazu ETRN s touto doménou jako parametrem (více viz kapitolu 15.1). Takto může být použit jako sekundární SMTP server pro doménu, jejíž primární server nemá trvalé připojení do Internetu.

Je-li doména v adrese...
V této části dialogu můžete vybrat, zda se mají zprávy, které mají v adrese příjemce obsažen jeden z doménových aliasů, přeposílat či nikoli. Volba *Nepřeposílat takové zprávy* zabrání vytvoření smyčky v případě, že není nalezen příjemce na žádném serveru obsluhujícím tuto doménu.
Poznámka: Pokud je doména rozložena na dvou serverech, volbu nastavte pouze na jednom z nich (přesný popis nastavení rozložení domény na dvou a více serverech najdete v kapitole 27.4).

7.6 Nastavení mapování adresářových služeb

Kerio MailServer může kromě vlastní (interní) databáze uživatelských účtů pracovat také s účty a skupinami, které jsou uloženy v LDAP databázi (v současné době jsou podporovány databáze *Microsoft Active Directory* a *Apple Open Directory*). Výhodou použití LDAP je, že jsou uživatelské účty udržovány na jednom místě, čímž se výrazně snižuje administrativní náročnost a pravděpodobnost vzniku chyb.

Příklad: Firma používá Windows 2000 doménu a *Kerio MailServer*. Do firmy byl přijat nový zaměstnanec. Dosavadní postup byl následující:

1. Vytvořit uživatelský účet v *Active Directory*.
2. Importovat uživatele do *Kerio MailServeru* (nebo zde založit účet stejného jména a nastavit ověřování pomocí systému Kerberos).

Při spolupráci s LDAP databází stačí provést pouze krok 1.

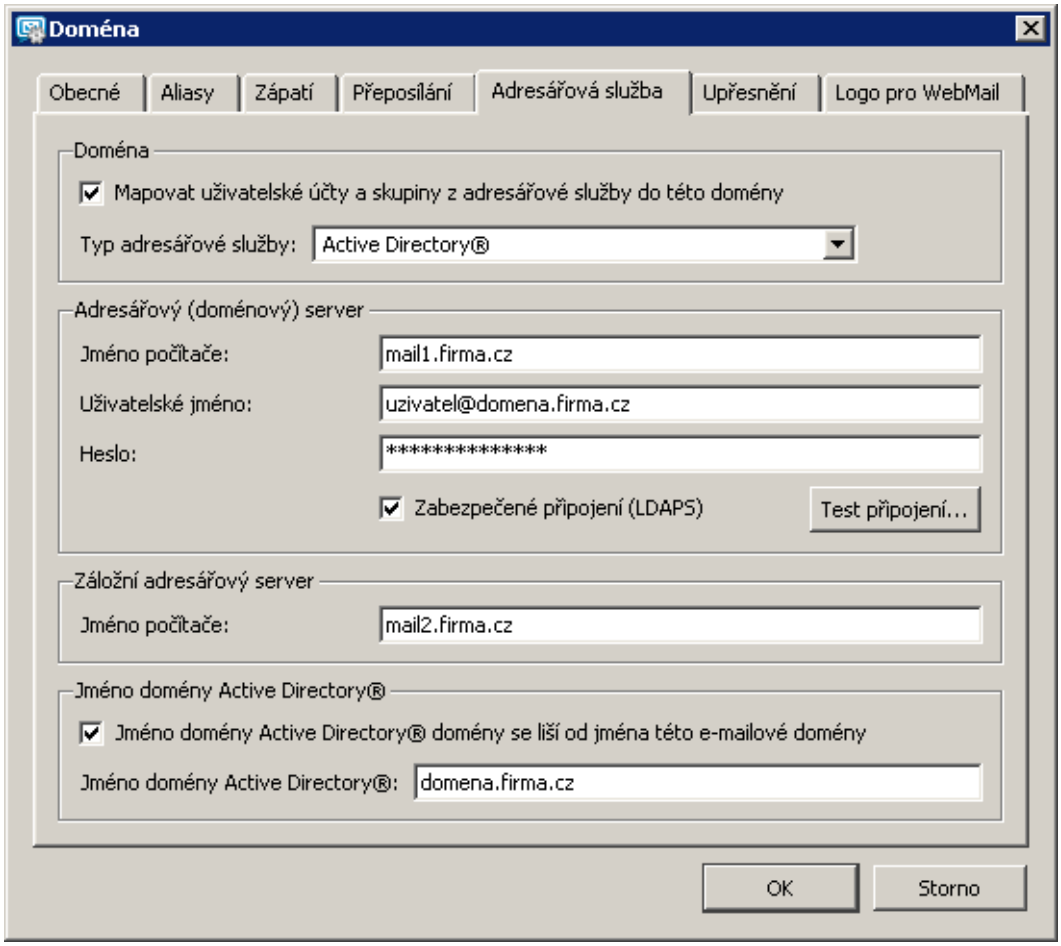
Poznámka: Kerio MailServer umožňuje používat v rámci jedné domény účty v LDAP databázi i účty definované lokálně. Toho lze využít např. pro vytvoření administrátorského účtu, který bude funkční i v případě nedostupnosti adresářového serveru.

K nastavení spolupráce s LDAP slouží záložka *Adresářová služba*:

Mapování účtů z Active Directory

Aby mohl *Kerio MailServer* plně spolupracovat s *Active Directory* (tzn. aby v této databázi mohly být uloženy všechny údaje o uživatelském účtu — viz kapitolu 13), je třeba na server s *Active Directory* nainstalovat *Kerio Active Directory Extensions*. Podrobnosti najdete v kapitole 29.

Mapovat uživatelské účty a skupiny...
Volba zapíná/vypíná spolupráci s LDAP databází (je-li tato volba vypnuta, v doméně bude možno vytvořit pouze lokální účty).



Obrázek 7.6 Nastavení domény — Active Directory

Typ adresářové služby

Typ LDAP databáze, kterou bude tato doména používat (*Active Directory*).

Jméno počítače

DNS jméno nebo IP adresa serveru, na němž LDAP databáze běží.

Služba LDAP standardně používá pro komunikaci port 389 (standardní port zabezpečené verze LDAPS je 636). Je-li třeba použít pro komunikaci mezi *Kerio MailServerem* a LDAP databází nestandardní port, je nutné jej doplnit k názvu nebo IP adrese serveru (např.: `mail1.firma.cz:12345` nebo `212.100.12.5:12345`).

Poznámka: Pokud pro připojení využíváte zabezpečenou verzi služby LDAP, musí být do položky doplněno vždy DNS jméno kvůli ověřovací proceduře SSL certifikátu.

Uživatelské jméno

Jméno uživatele (ve tvaru `xxxxx@firma.cz`), který má práva pro čtení LDAP databáze.

Heslo
: Heslo uživatele, který má práva pro čtení LDAP databáze.

Zabezpečené připojení (LDAPS)
: Při komunikaci mezi LDAP databází a *Kerio MailServerem* jsou posílána i data velmi citlivá na bezpečnost (například uživatelská hesla). Z toho důvodu doporučujeme komunikaci zabezpečit SSL. Pro spuštění služby LDAPS v *Active Directory* je třeba spustit na doménovém řadiči certifikační autoritu, která je pro *Kerio MailServer* důvěryhodná.
Upozornění: SSL šifrování má na server vyšší nároky ohledně výkonu (rychlost internetové linky, výkon procesoru). Zejména v případě navazování mnoha spojení při komunikaci mezi LDAP databází a *Kerio MailServerem* nebo velkého množství uživatelů v LDAP databázi může komunikaci výrazně zpomalovat. Zatěžuje-li SSL šifrování server neúměrně, doporučujeme využít pouze nezabezpečenou verzi služby LDAP.

Záložní adresářový server
: DNS jméno nebo IP adresa záložního serveru, na němž je spuštěna stejná LDAP databáze.
Poznámka: Pokud pro připojení využíváte zabezpečenou verzi služby LDAP, musí být do položky doplněno vždy DNS jméno kvůli ověřovací proceduře SSL certifikátu.

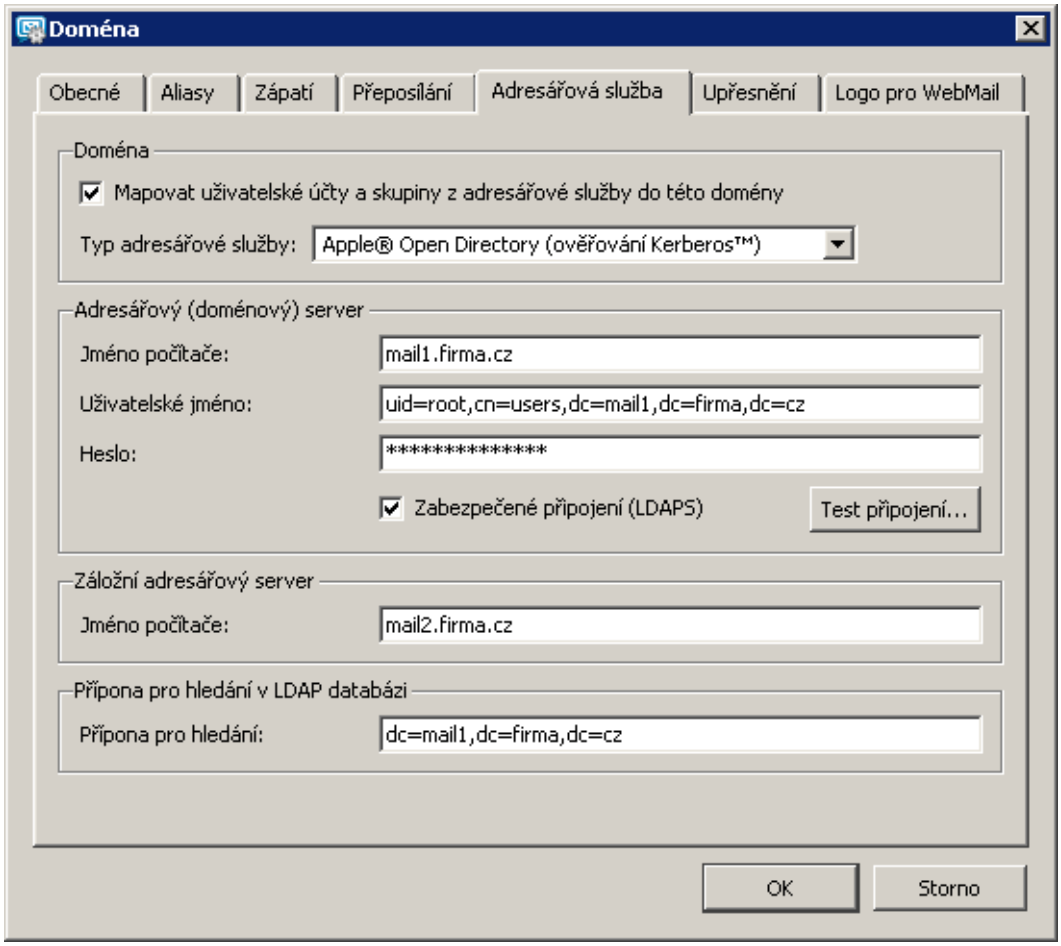
Jméno Active Directory domény...
: Pokud se název domény liší od názvu v *Active Directory*, zaškrtněte volbu a doplňte její jméno do pole *Jméno Active Directory domény*.

Tlačítkem *Test připojení* je možno vyzkoušet správnost nastavených parametrů. Testovány jsou položky jméno nebo adresa serveru (zda je možno se k němu připojit), uživatelské jméno a heslo (zda je možné ověření) a také zda jsou na serveru, kde je spuštěna *Active Directory*, nainstalovány *Kerio Active Directory Extensions* (viz kapitolu 29).

Poznámka: Výše popsaná spolupráce s LDAP databází nijak nesouvisí s vestavěným LDAP serverem — ten je určen pro přístup k adresáři kontaktů z poštovních klientů (podrobnosti viz kapitolu 19). Jestliže je *Kerio MailServer* nainstalován na stejném počítači jako *Active Directory*, je třeba z důvodu zabránění kolize změnit číslo portu služby LDAP (*Konfigurace* → *Služby*).

Mapování účtů z Apple Open Directory

Aby mohl *Kerio MailServer* plně spolupracovat s *Open Directory* (tzn. aby v této databázi mohly být uloženy všechny údaje o uživatelském účtu — viz kapitolu 13), je třeba nainstalovat na server s *Open Directory* aplikaci *Kerio Open Directory Extensions*. Podrobnosti najdete v kapitole 30.



Obrázek 7.7 Nastavení domény — Apple Open Directory

Mapovat uživatelské účty a skupiny...

Volba zapíná/vypíná spolupráci s LDAP databází (je-li tato volba vypnuta, v doméně bude možno vytvořit pouze lokální účty).

Typ adresářové služby

Typ LDAP databáze, kterou bude tato doména používat. Mapování účtů z *Apple Open Directory* má dvě varianty, které se liší typem ověřování. V *Apple Open Directory* je možné využít dva typy ověřování. Prvním je ověřování proti password serveru, druhým ověřování přes systém Kerberos.

Ověřování proti password serveru má jednu zásadní výhodu. Není třeba provádět žádná speciální nastavení na serveru, kde je nainstalován *Kerio MailServer*. Nevýhod tohoto ověřování je však více:

- Ověřování je zastaralé a méně bezpečné.
- Uživatelé si nemohou sami změnit své uživatelské heslo (v rozhraní *Kerio WebMail*).

- Firma *Apple* ukončuje podporu tohoto typu ověřování.
- Využít této metody ověřování lze pouze pokud je *Kerio MailServer* nainstalován na systému Mac OS X.

Ověřování proti Kerberos serveru je modernější a bezpečnější. Ověřování touto metodou však vyžaduje nastavení na serveru, kam je nainstalován *Kerio MailServer*. Tato nastavení jsou podrobně popsána v kapitole 24.

Kerio MailServer měl až do verze 6.1.3 nastaveno jako výchozí ověřování proti password serveru. Od verze *Kerio MailServer 6.1.4* je možné metodu ověřování zvolit.

Závěrem je třeba připomenout, že v administrační konzoli *Kerio MailServeru*, v sekci *Konfigurace* → *Domény*, v nastavení domény v záložce *Upřesnění* musí být vyplněn název Kerberos oblasti, proti které se bude mailserver ověřovat. Tento název musí souhlasit s názvem Kerberos oblasti uvedeným v souboru `/Library/Preferences/edu.mit.Kerberos`. V opačném případě nebude nastavení funkční. Podrobný popis nastavení ověřování proti Kerberos serveru na systémech Mac OS X najdete v kapitole 24.3).

Jméno počítače

DNS jméno nebo IP adresa serveru, na němž LDAP databáze běží.

Služba LDAP standardně používá pro komunikaci port 389 (standardní port zabezpečené verze LDAPS je 636). Je-li třeba použít pro komunikaci mezi *Kerio MailServerem* a LDAP databází nestandardní port, je nutné jej doplnit k názvu nebo IP adrese serveru (např.: `mail1.firma.cz:12345` nebo `212.100.12.5:12345`).

Poznámka: Pokud pro připojení využíváte zabezpečenou verzi služby LDAP, musí být do položky doplněno vždy DNS jméno kvůli ověřovací proceduře SSL certifikátu.

Uživatelské jméno

Jméno uživatele, který má práva pro čtení LDAP databáze. Může to být buď uživatel `root` nebo je možno použít administrátora *Open Directory* (`admin` pro *Mac OS X 10.3* či `diradmin` pro *Mac OS X 10.4*). V případě použití administrátora je nutné se ujistit, že se jedná o administrátora *Apple Open Directory* a ne o systémového administrátora na počítači, kde je *Apple Open Directory* spuštěna.

Pro připojení k databázi *Apple Open Directory* musí být vyplněno uživatelské jméno ve tvaru:

```
uid=xxx,cn=xxx,dc=xxx
```

- `uid` — jméno uživatele, pod kterým se připojujete do systému.
- `cn` — jméno kontejneru s uživateli (téměř vždy složka `users`).
- `dc` — jména domény i každé její subdomény (například *mail1.firma.cz* → `dc=mail1,dc=firma,dc=cz`)

Heslo
Heslo uživatele, který má práva pro čtení LDAP databáze.

Zabezpečené připojení (LDAPS)
Při komunikaci mezi LDAP databází a *Kerio MailServerem* jsou posílána i data velmi citlivá na bezpečnost (například uživatelská hesla). Z toho důvodu je možné tuto komunikaci zabezpečit SSL.
Upozornění: SSL šifrování má na server vyšší nároky ohledně výkonu (rychlost internetové linky, výkon procesoru). Zejména v případě navazování mnoha spojení při komunikaci mezi LDAP databází a *Kerio MailServerem*, nebo v případě velkého množství uživatelů v LDAP databázi může komunikaci výrazně zpomalovat. Zatěžuje-li SSL šifrování server neúměrně, doporučujeme využít pouze nezabezpečenou verzi služby LDAP.

Záložní doménový server
DNS jméno nebo IP adresa záložního serveru, na němž je spuštěna LDAP databáze.
Poznámka: Pokud pro připojení využíváte zabezpečenou verzi služby LDAP, musí být do položky doplněno vždy DNS jméno kvůli ověřovací proceduře SSL certifikátu.

Přípona pro hledání v LDAP databázi (search suffix)
Pokud je zvolen v položce *Typ adresářové služby Apple Open Directory*, doplňte do této položky příponu ve tvaru `dc=subdomena,dc=domena`.

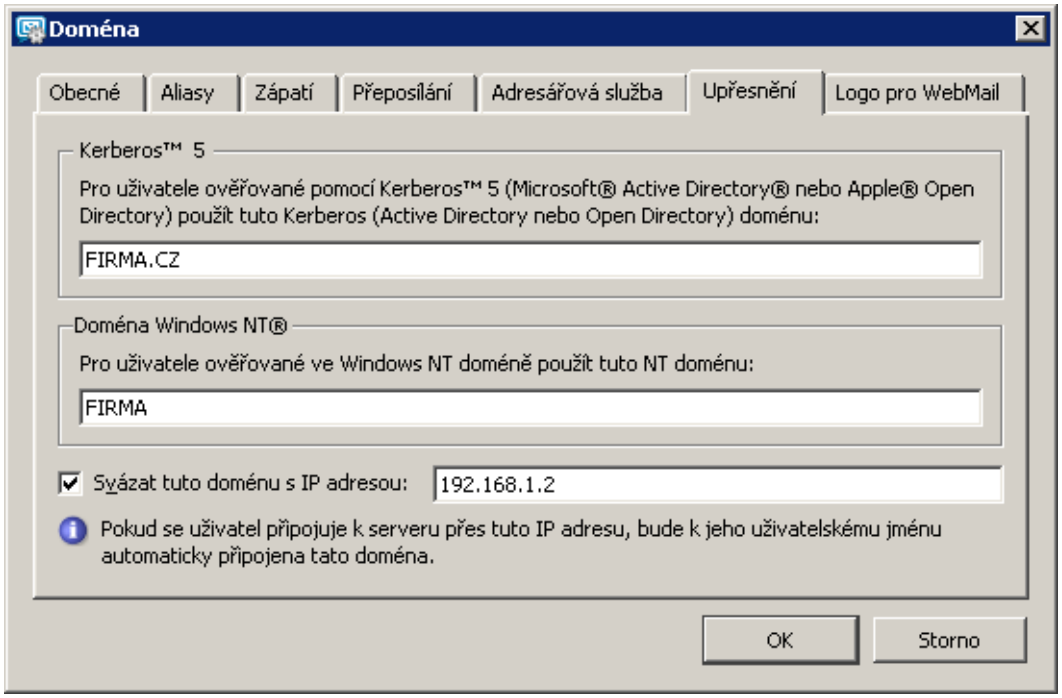
Tlačítkem *Test připojení* je možno vyzkoušet správnost nastavených parametrů. Testovány jsou položky jméno nebo adresa serveru (zda je možno se k němu připojit) a uživatelské jméno a heslo (zda je možné ověření).

Poznámka: Výše popsaná spolupráce s LDAP databází nijak nesouvisí s vestavěným LDAP serverem — ten je určen pro přístup k adresáři kontaktů z poštovních klientů (podrobnosti viz kapitolu 19). Jestliže je *Kerio MailServer* nainstalován na stejném počítači jako *Apple Open Directory*, je třeba z důvodu zabránění kolize změnit číslo portu služby LDAP (*Konfigurace* → *Služby*).

7.7 Nastavení ověřování uživatelů

V záložce *Upřesnění* je možno nastavit parametry ověřování uživatelů pro vytvářenou doménu:

Linux PAM
Tato volba je v *Kerio Administration Console* zobrazena pouze v instalaci pro operační systémy Linux.
PAM (Pluggable Authentication Modules) jsou autentizační moduly, které umí ověřit uživatele z domény (např. `firma.cz`) proti linuxovému serveru, na kterém je *Kerio MailServer* spuštěn. Do této položky se zadává jméno PAM služby (konfiguračního



Obrázek 7.8 Nastavení domény — parametry pro ověřování uživatelů

souboru), která bude pro ověřování uživatelů v této doméně použita. Součástí instalace *Kerio MailServeru* je konfigurační soubor pro PAM službu `keriomail` (najdete ho v adresáři `/etc/pam.d/keriomail`), který doporučujeme používat. Podrobnosti o konfiguraci PAM najdete v dokumentaci k vaší distribuci Linuxu.

Kerberos 5

Kerberos je protokol pro autorizaci a autentizaci (více najdete na stránkách: `http://web.mit.edu/Kerberos/`). *Kerio MailServer* využívá tento protokol pro autentizaci uživatelů proti Kerberos serveru (např. v *Active Directory*).

Do položky v dialogu se zadává název oblasti (domény) systému Kerberos (Kerberos realm), v níž mají být uživatele ověřováni. Od verze *Kerio MailServer 6.0.9* se jméno Kerberos oblasti automaticky zadává velkými písmeny.

Jsou-li uživatelské účty fyzicky uloženy v *Active Directory* nebo *Open Directory* (viz záložku *Adresářová služba*), je třeba do této položky zadat jméno *Active Directory* případně *Open Directory* domény. Při konfiguraci *Active Directory* nebo *Open Directory* v záložce *Adresářová služba* bude tato položka automaticky vyplněna.

Upozornění: Pokud používáte *Open Directory* nebo samostatný Kerberos server, důkladně zkontrolujte, zda Kerberos realm doplněný v záložce *Upřesnění* je shodný s názvem Kerberos oblasti, který je uveden v souboru `/Library/Preferences/edu.mit.Kerberos`. Konkrétně musí souhlasit s hodnotou `default_realm` v tomto souboru. Příslušný řádek tedy může vypadat

například takto `default_realm = FIRMA.CZ`
Nastavení ověřování na jednotlivých platformách je popsáno v kapitole 24.

Doména Windows NT
NT doména, v níž budou uživatelé ověřováni. Počítač, na němž *Kerio MailServer* běží, musí být přidán do této domény.
Příklad:
Pro doménu `firma.cz` je NT doménou `FIRMA`.

Poznámka: Při definici každého uživatele lze zvolit, jakým způsobem bude ověřován (viz kapitolu 13.2). V jedné e-mailové doméně tedy mohou být různí uživatelé ověřováni různými metodami.

Svázat s IP adresou
Každý uživatel se ke *Kerio MailServeru* může připojit přes libovolné rozhraní. Avšak každou doménu lze svázat s jednou IP adresou. Svázání IP adresy s doménou přinese ten efekt, že uživatelé z domény, kteří se připojí přes IP adresu svázanou s touto doménou, nemusejí při přihlašování uvádět uživatelské jméno včetně domény (například `jnovak@firma.cz`), ale stačí jej uvést samostatně (například `jnovak`), jako by se přihlašovali k primární doméně.
Upozornění: Správnou funkčnost svazování domén s IP adresou podmiňuje požadavek navázat nejvýše jednu doménu na každou IP adresu. V opačném případě server nepozná, do které domény uživatelské jméno bez domény patří.
Příklad: Počítač, na němž *Kerio MailServer* běží, má dvě rozhraní: `192.168.1.10` zapojené do sítě firmy *Firma* a `192.168.2.10` do sítě firmy *JinaFirma*. V lokální doméně `jinafirma.cz` (nejedná se o primární doménu) je vytvořen uživatelský účet `novak`.
Doména `jinafirma.cz` je svázána s IP adresou `192.168.2.10`. Uživatelé z domény `jinafirma.cz` se mohou z firmy přihlašovat ke službám *Kerio MailServeru* uživatelským jménem bez uvedení domény.
Poznámka: Budou-li se přes toto rozhraní připojovat uživatelé z primární domény, budou se muset přihlašovat celou e-mailovou adresou.

Řešení případných problémů externího ověřování

Pokud nastane s některou z ověřovacích metod problém, lze v *Kerio MailServeru* nastavit záznam externího ověřování uživatelů:

1. Otevřeme v *Kerio Administration Console* sekci *Záznamy* a vybereme záznam *Debug*.

2. V okně záznamu pravým tlačítkem myši otevřeme kontextové menu a vybereme položku *Zprávy*.

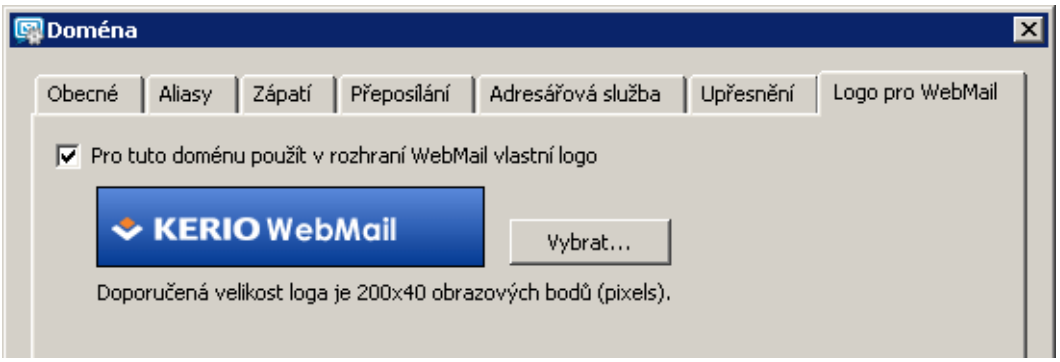
3. Otevře se okno *Zaznamenávané informace*, kde zaškrtneme volbu *User Authentication*.

4. Změnu potvrdíme tlačítkem OK.

Po vyřešení problému doporučujeme logování opět vypnout.

7.8 Logo pro WebMail

Každé doméně v *Kerio MailServeru* lze nastavit jiné logo pro rozhraní *Kerio WebMail* (nastavení loga podrobněji popisuje kapitola 11.2).



Obrázek 7.9 Nastavení domény — Logo pro rozhraní Kerio WebMail

Doporučené parametry loga jsou následující:

- Formát: GIF
- Rozměry: 200x40 pixelů

Tlačítko *Vybrat* umožňuje zadání cesty k souboru s logem.

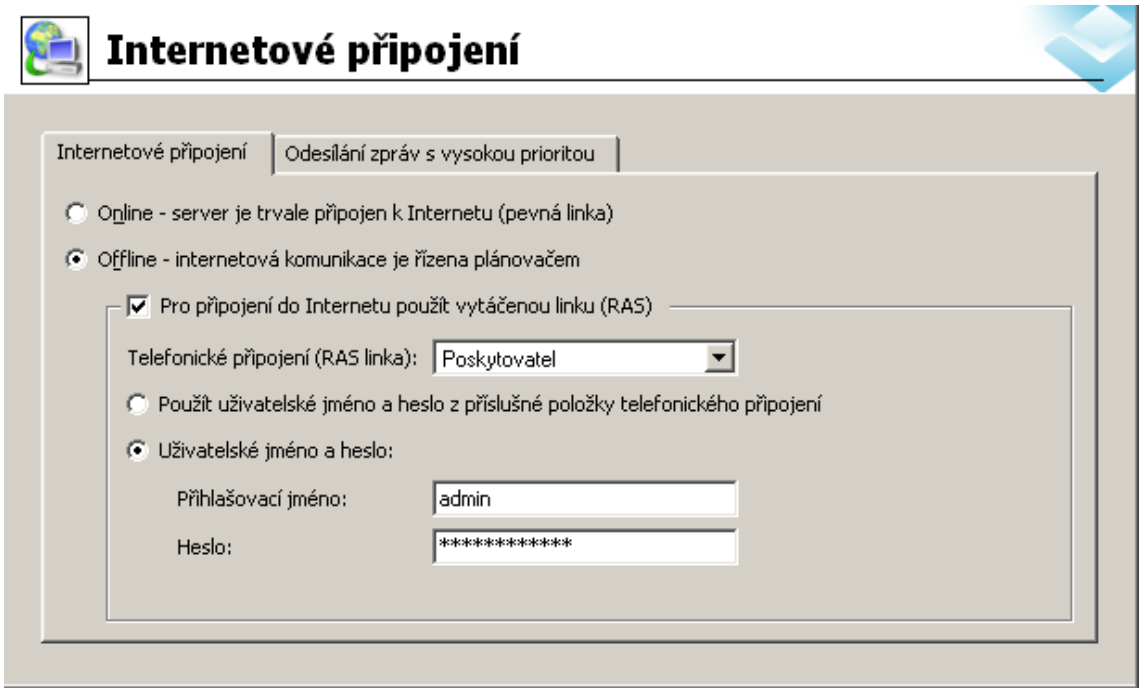
Kapitola 8

Internetové připojení

Nastavení typu internetového připojení se provádí v sekci *Konfigurace* → *Internetové připojení*.

8.1 Internetové připojení

Kerio MailServer může být nasazen na počítači, který má trvalé připojení do Internetu (pevná linka, bezdrátové připojení, kabelový modem, xDSL...), ale také s vytáčeným připojením (analogový modem nebo ISDN). Vestavěným plánovačem je možno řídit, kdy má poštovní server automaticky vytočit internetové připojení a provést odeslání a příjem pošty.



Obrázek 8.1 Připojení do Internetu

Online

Kerio MailServer má trvalé připojení do Internetu. Všechny odchozí zprávy budou okamžitě odesílány.

Offline

Server není trvale připojen do Internetu. Odchozí zprávy jsou řazeny do fronty a odesílány v časech určených plánovačem.

Upozornění: Offline připojení lze nastavit pouze na platformě *MS Windows*. *Linux* a *Mac OS* tuto možnost nepodporují. Proto se dialog na těchto platformách vůbec nezobrazuje.

Má-li se v těchto časech vytáčet internetová linka, zapněte volbu *Použít vytáčené připojení k Internetu*. V nabídce *Telefonické připojení (RAS linka)* se zobrazují položky telefonického připojení vytvořené ve Windows. *Kerio MailServer* může použít uživatelské jméno a heslo, které uživatel přidělil příslušnému telefonickému připojení (volba *Uživatelské jméno a heslo zadané v operačním systému*), nebo lze zadat uživatelské jméno a heslo přímo v tomto dialogu (volba *Uživatelské jméno a heslo*).

Upozornění: Telefonické připojení musí být vytvořeno pro všechny uživatele v systému (volba při definici připojení).

Poznámky:

1. Volba *Offline* má své opodstatnění i v případě, že není zapnuta volba *Použít vytáčené připojení k Internetu*. *Kerio MailServer* totiž může např. běžet na počítači v lokální síti připojené k Internetu vytáčenou linkou. V režimu *Online* by vznikaly velmi časté a nekontrolovatelné požadavky přístupu do Internetu a tedy vytočení linky na žádost. V režimu *Offline* se *Kerio MailServer* připojuje pouze v časech nastavených v plánovači, čímž lze optimalizovat náklady na připojení.

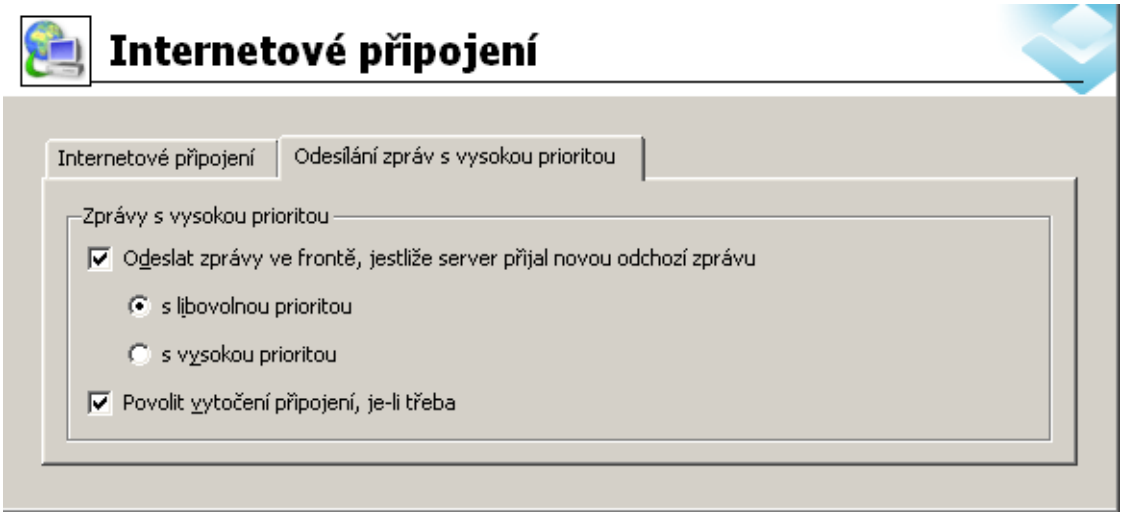
2. *Kerio MailServer* používá systémový telefonní seznam telefonického připojení (`rasphone.pbk`). Jiný telefonní seznam nelze použít.

3. Volba *Online* nevyřazuje plánovač z činnosti. Přestože odchozí zprávy jsou odesílány okamžitě, poštovní server může zároveň vybírat zprávy ze vzdálených POP3 schránek, což je vhodné provádět v pravidelných intervalech. Podrobnosti najdete v kapitole 15.4.

4. Podrobnosti o nastavení plánovače najdete v kapitole 9.

8.2 Zprávy s vysokou prioritou

Pokud server není trvale připojen do Internetu, tedy pracuje v režimu offline, lze nastavit v této záložce okamžité odesílání zpráv.



Obrázek 8.2 Nastavení odesílání zpráv s vysokou prioritou

Odeslat zprávy ve frontě, jestliže...
: Po zapnutí volby se budou odchozí zprávy ihned odesílat. Zároveň lze vybrat, zda se mají odesílat všechny zprávy (tedy zprávy s libovolnou prioritou) nebo jen zprávy, kterým byla nastavena vysoká priorita.

Povolit vytočení připojení, je-li třeba
: Zapnutí volby umožňuje automatické vytočení připojení, jestliže server přijal odchozí zprávu, která má být odeslána.

Kapitola 9

Plánování

Kerio MailServer obsahuje plánovač, který umožňuje řídit tři druhy akcí:

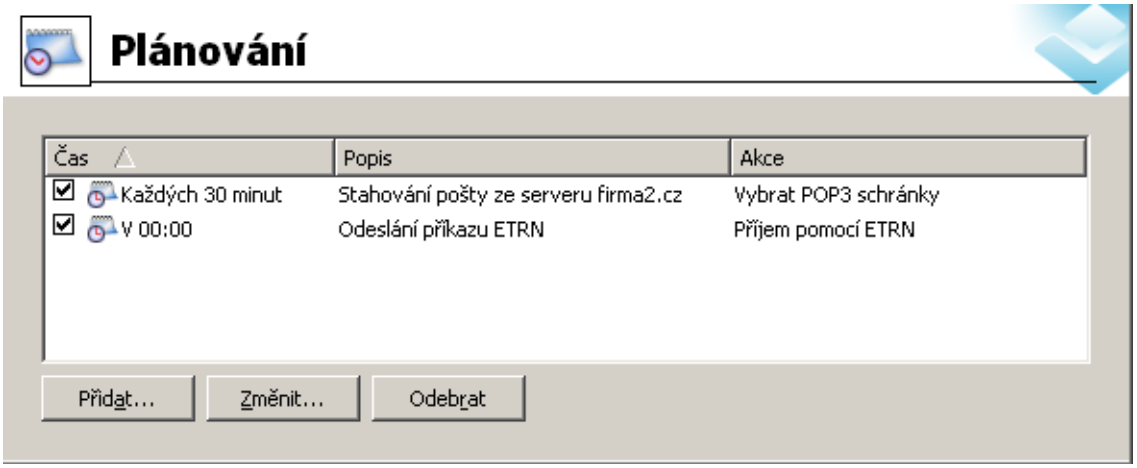
Vybírání vzdálených POP3 schránek
Vždy, je-li definována alespoň jedna schránka.

Vyslání příkazu ETRN na definované servery
Vždy, je-li definován alespoň jeden ETRN server.

Odesílání zpráv z odchozí fronty
Jestliže je nastaveno, že počítač, na němž *Kerio MailServer* běží, není trvale připojen do Internetu (viz kapitolu 8).

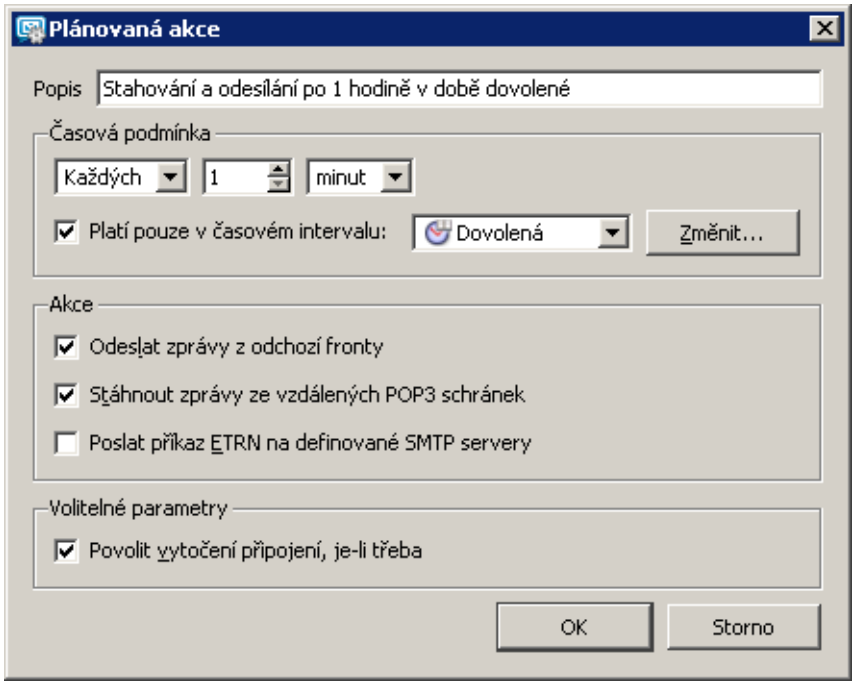
9.1 Nastavení plánovače

Nastavení se provádí v sekci *Konfigurace →Plánování*.



Obrázek 9.1 Plánování

Tlačítky *Přidat*, *Změnit* a *Odebrat* lze přidat, upravit nebo odstranit jednu položku v seznamu plánovaných akcí. Pro přidání nové položky nebo změnu stávající se zobrazí dialog, v němž lze nastavit následující parametry:



Obrázek 9.2 Editace plánování

Časová podmínka — kdy má být akce prováděna:

V intervalu (Každých) nebo v určitém čase (V)
: Např. „Každých 10 minut“ znamená, že se akce bude vyvolávat opakovaně po 10 minutách, zatímco „V 12:00“ znamená, že akce má být provedena každý den ve 12:00 hodin.

Platné pouze v čase
: Nastavené plánování platí pouze ve vybraném časovém intervalu. V nabídce se zobrazí všechny definované časové intervaly, tlačítkem *Změnit* je možno upravit vybraný interval nebo vytvořit nový. Podrobnosti najdete v kapitole 12.2.

Akce — jaká akce má být provedena:

Odeslat zprávy z odchozí fronty
: Odeslat všechny zprávy, které byly zařazeny do fronty (je-li v sekci *Konfigurace* → *Internetové připojení* nastaveno *Online*, zprávy odcházejí okamžitě — pak je tato volba de facto neúčinná).

Stáhnout zprávy ze vzdálených POP3 schránek
: Příjem pošty z POP3 schránek (je-li v sekci *Konfigurace* → *Stahování POP3 schránek* definována alespoň jedna vzdálená schránka). Plánování se uplatňuje na všechny POP3 schránky stejně.

Poslat příkaz ETRN na definované SMTP servery
: Příjem pošty pomocí příkazu ETRN (je-li v sekci *Konfigurace → Příjem pomocí ETRN* definován alespoň jeden SMTP server, na nějž má být příkaz ETRN posílán). Plánování se uplatňuje na všechny definované SMTP servery stejně.

Volitelné parametry akce:

Povolit vytočení připojení, je-li třeba
: Jestliže je v okamžiku vyvolání této akce linka zavěšena, vytočí se. Bude-li tato volba vypnuta, provede se akce pouze v případě, že bude v tomto okamžiku linka vytočena.

9.2 Optimální plánování

Optimální nastavení plánování závisí na způsobu, jakým je přijímána příchozí pošta, a na typu internetového připojení, které má *Kerio MailServer* k dispozici.

- Má-li *Kerio MailServer* trvalé připojení do Internetu (*Online*) a je-li veškerá příchozí pošta přijímána pouze protokolem SMTP (MX záznamy pro všechny lokální domény jsou nasměrovány na počítač, na němž *Kerio MailServer* běží, a není definována žádná vzdálená POP3 schránka ani ETRN server), není třeba nastavovat žádné plánování.
- Je-li k dispozici trvalé připojení do Internetu a je definovaná alespoň jedna POP3 schránka nebo příjem pošty pomocí příkazu ETRN, je nutno plánování nastavit také. V tomto případě mohou být intervaly mezi jednotlivými akcemi velmi krátké (např. 5 minut), protože počet připojení neovlivňuje náklady a není třeba uvažovat dobu potřebnou na vytočení linky.
- Pokud je *Kerio MailServer* připojen vytáčenou linkou, není z Internetu trvale dostupný a příjem pošty musí být prováděn pomocí ETRN nebo vybíráním ze vzdálených POP3 schránek. V tomto případě je nutno plánování nastavit, aby *Kerio MailServer* vytáčel linku, přijímal poštu a odesílal poštu z odchozí fronty.

Ve výše zmíněných případech, kdy je doporučeno plánování nastavit, mohou být vždy zapnuty všechny volby v poli Akce (*Odeslat zprávy z odchozí fronty*, *Stáhnout zprávy ze vzdálených POP3 schránek* a *Poslat příkaz ETRN na definované SMTP servery*). Je-li totiž např. odchozí fronta prázdná nebo není definována žádná vzdálená POP3 schránka, *Kerio MailServer* přejde k následující akci.

Kapitola 10

Certifikáty serveru

Princip bezpečných služeb *Kerio MailServeru* (služby šifrované SSL — např. HTTPS, IMAPS, POP3S, atd.) spočívá v tom, že se celé spojení mezi klientem a serverem šifruje, aby jej nebylo možné odposlechnout a zneužít přenášených informací. Šifrovací protokol SSL, který je k tomuto účelu běžně využíván, používá nejprve asymetrickou šifru pro výměnu symetrického šifrovacího klíče, kterým se pak šifrují vlastní přenášená data.

Asymetrická šifra používá dva klíče: veřejný pro šifrování a privátní pro dešifrování. Jak už jejich názvy napovídají, veřejný (šifrovací) klíč má k dispozici kdokoliv, kdo chce navázat se serverem spojení, zatímco privátní (dešifrovací) klíč má k dispozici pouze server a musí zůstat utajen. Klient ale také potřebuje mít možnost, jak si ověřit identitu serveru (zda je to skutečně on, zda se za něj pouze někdo nevydává). K tomu slouží tzv. certifikát. Certifikát v sobě obsahuje veřejný klíč serveru, jméno serveru, dobu platnosti a některé další údaje. Aby byla zaručena pravost certifikátu, musí být ověřen a podepsán třetí stranou, tzv. certifikační autoritou.

Komunikace mezi klientem a serverem pak vypadá následovně: Klient vygeneruje symetrický klíč a zašifruje ho veřejným klíčem serveru (ten získá z certifikátu serveru). Server jej svým privátním klíčem (který má jen on) dešifruje. Tento postup zaručuje, že symetrický klíč znají jen oni dva a nikdo jiný.

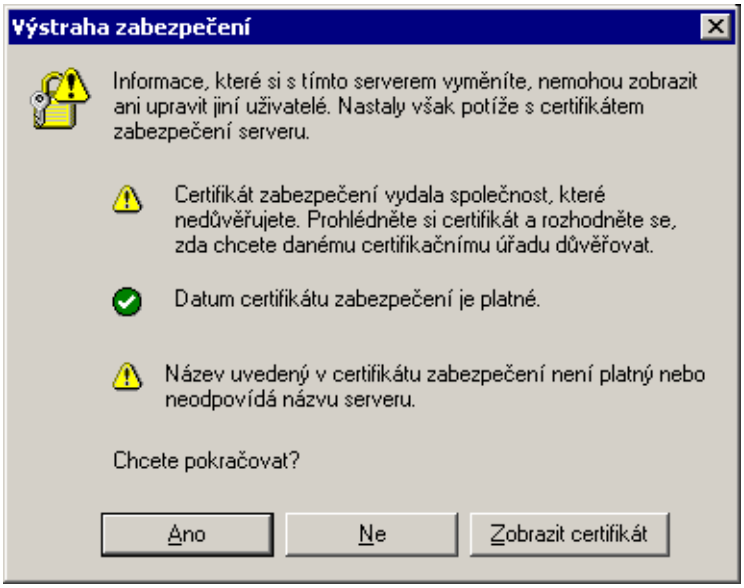
Poznámka: Chceme-li *Kerio MailServeru* zajistit vysokou bezpečnost, povolíme komunikaci pouze přes SSL spojení. Toto můžeme provést buď zastavením všech nešifrovaných služeb (viz kapitolu 6) nebo nastavením bezpečnostní politiky serveru (viz kapitolu 15.6). Po nastavení serveru je nutné instalovat certifikát (může být i self-signed) nebo certifikáty na klientské stanice všech uživatelů, kteří využívají služeb *Kerio MailServeru*.

10.1 Certifikát Kerio MailServeru

Jak fungují výše uvedené principy v praxi, si můžete nejsnáze ověřit při použití služby *Secure HTTP*. WWW prohlížeče totiž umějí zobrazovat informace o certifikátech, zatímco u ostatních služeb zůstane uživateli vše skryto.

Kerio MailServer od verze 6.0 vygeneruje automaticky při prvním spuštění po instalaci self-signed certifikát (certifikát podepsaný sám sebou) na jméno serveru. V adresáři, kde je *Kerio MailServer* instalován, je uložen v souboru `server.crt`. Druhý soubor `server.key` obsahuje privátní klíč serveru.

Pokusíte-li se bezprostředně po instalaci *Kerio MailServeru* přistoupit prohlížečem ke službě *Secure HTTP*, zobrazí se bezpečnostní varování obsahující zhruba následující informace (záleží na typu prohlížeče, zadaném jménu počítače atd.).



Obrázek 10.1 Výstraha zabezpečení

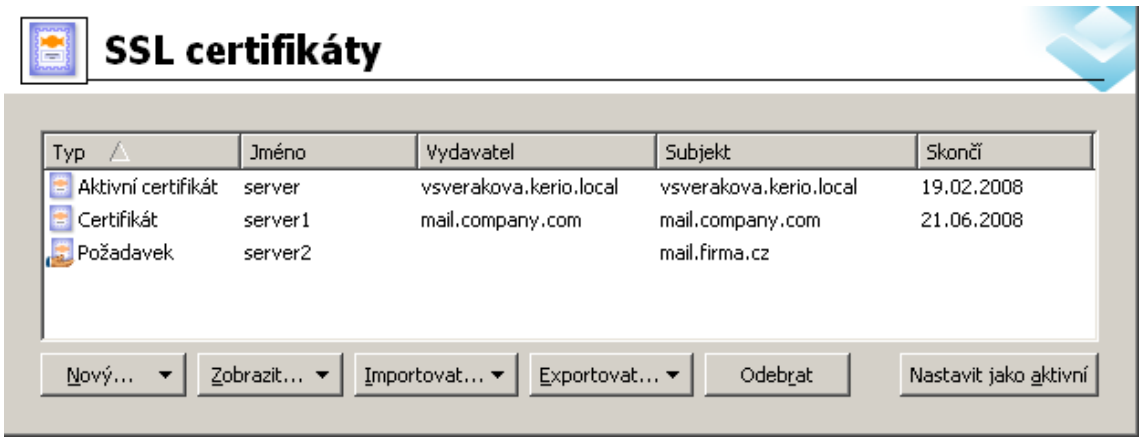
- Certifikát nebyl vydán organizací, kterou máte nastavenu jako důvěryhodnou. Certifikát je totiž podepsán sám sebou (tzv. self-signed certifikát). Toto varování se nebude zobrazovat, jestliže certifikát nainstalujete (což můžete provést, protože znáte jeho původ).
- Datum certifikátu je platné (certifikát je platný po omezenou dobu, typicky 1-2 roky).
- Jméno certifikátu neodpovídá jménu serveru. Certifikát se vydává na konkrétní jméno serveru (např. `mail.firma.cz`), které musíte také používat v klientovi (tento certifikát byl vystaven na fiktivní jméno `keriomail`).

Nyní máme k dispozici dvě možnosti. Nechat v *Kerio MailServeru* self-signed certifikát vygenerovaný během instalace *Kerio MailServeru*, nebo si obstarat certifikát ověřený důvěryhodnou certifikační autoritou. Nainstalovat na klientské stanice jdou obvykle oba typy certifikátů. V obou případech je také nutné certifikát spravovat v *Kerio MailServeru* v sekci *Konfigurace* → *SSL certifikáty* (viz obrázek 10.2).

V sekci *SSL certifikáty* lze certifikáty zakládat, generovat požadavky na certifikáty pro certifikační autority nebo certifikáty exportovat. Všechny možnosti si nyní postupně představíme:

Nový...

Stisknutím tlačítka *Nový* se zobrazí okno pro zadání údajů o vašem serveru a vaší



Obrázek 10.2 SSL certifikáty

organizaci. Po jejich vyplnění se vytvoří soubory `server.crt` a `server.key` v podadresáři `sslcert`.

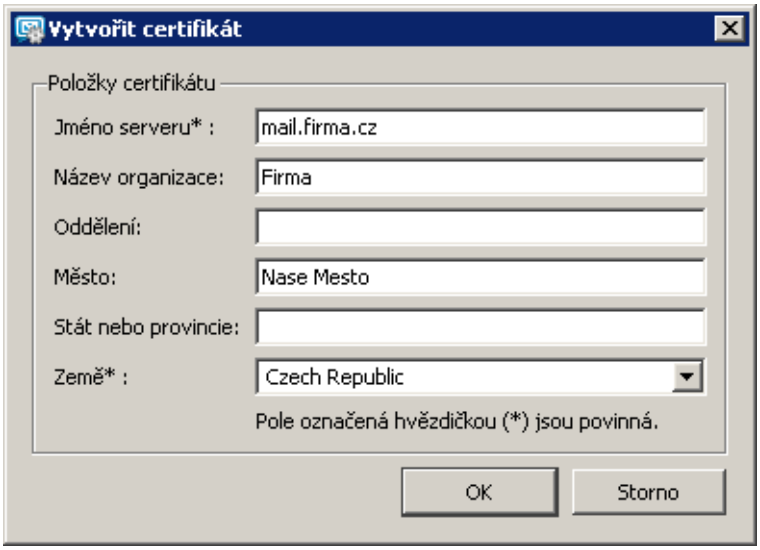
Vytvořený certifikát bude originální a bude vystaven vaší firmou vaší firmě na jméno vašeho serveru (self-signed certifikát — certifikujete sami sebe). Tento certifikát zajišťuje vašim klientům bezpečnost, protože příslušný privátní klíč znáte pouze vy a certifikát prokazuje identitu vašeho serveru. Klienti budou ve svých prohlížečích upozorněni na to, že se nejedná o důvěryhodnou certifikační autoritu. Protože však vědí, kdo tento certifikát vytvořil a proč, mohou si jej nainstalovat. Tím mají zajištěnu bezpečnou komunikaci a žádné varování se jim již zobrazovat nebude, protože váš certifikát nyní splňuje všechny potřebné náležitosti.

Chcete-li získat plnohodnotný certifikát, musíte kontaktovat veřejnou certifikační autoritu (např. *Verisign*, *Thawte*, *SecureSign*, *SecureNet*, *Microsoft Authenticode* apod.). Průběh certifikace je poměrně složitý a vyžaduje určité odborné znalosti. *Kerio MailServer* umožňuje vytvořit požadavek na certifikát, který lze exportovat a soubor odeslat certifikační organizaci.

Pozor: Nový certifikát bude používán až od příštího spuštění *Kerio MailServer Engine*. Chcete-li jej tedy využívat ihned, zastavte *Engine* a opět jej spusťte.

Tlačítko *Nový* lze použít jak pro vytvoření nového certifikátu (volba *Nový certifikát*), tak pro vytvoření požadavku na certifikát (volba *Nový požadavek na certifikát*). V obou případech vyplníte okno *Vytvořit certifikát*. Nutnými položkami pro vznik certifikátu jsou *Jméno serveru* a *Země*.

- *Jméno serveru* — doplníte jméno serveru, kde je spuštěna aplikace *Kerio MailServer*.
- *Název organizace* — doplníte jméno organizace.
- *Oddělení* — vyplňte pouze pokud má organizace více než jedno oddělení.
- *Město* — doplňte město, kde organizace sídlí.
- *Stát nebo provincie* — vyplňte kraj, ve kterém sídlí vaše organizace.

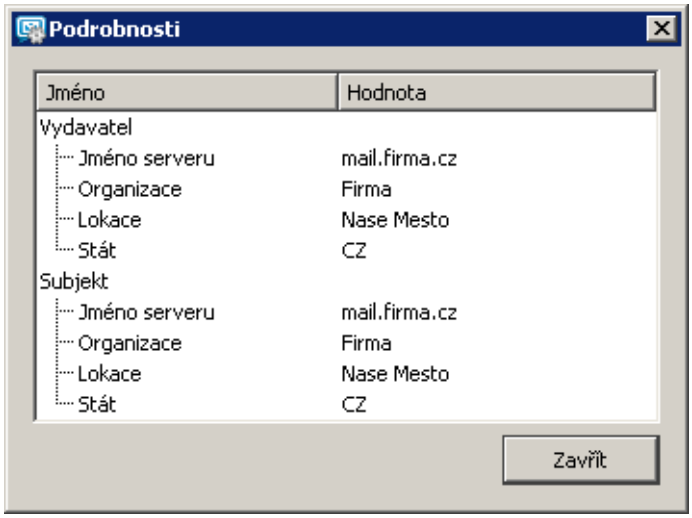


Obrázek 10.3 Vytvoření certifikátu

- *Země* — vybrání země je nutné pro vytvoření certifikátu.

Zobrazit

Označením certifikátu nebo požadavku na certifikát a použitím tlačítka *Zobrazit* se otevře okno s detaily certifikátu.



Obrázek 10.4 Podrobnosti certifikátu

Importovat...

Tlačítkem lze importovat certifikát (podepsaný sám sebou nebo vydaný certifikační autoritou).

Exportovat...
Tlačítko umožňuje export aktivního certifikátu, požadavku na certifikát nebo soukromého klíče. Exportovaný požadavek na certifikát můžete zaslat certifikační organizaci.

Odebrat
Tlačítkem lze vymazat označenou položku (certifikát nebo požadavek na certifikát).

Nastavit jako aktivní
Tlačítko umožňuje nastavit vybraný certifikát jako aktivní.

Intermediate certifikáty

Kerio MailServer umožňuje ověřování takzvaným „intermediate“ certifikátem. Aby bylo ověřování tímto typem certifikátu funkční, je třeba jej přidat do *Kerio MailServeru* jedním z následujících postupů:

Lokálně
Soubor s „intermediate“ certifikátem přidáme do adresáře `/sslca` a certifikát serveru spolu se soukromým klíčem umístíme do adresáře `/sslcert`. Oba zmiňované adresáře jsou umístěny v adresáři, kde je *Kerio MailServer* nainstalován.

Vzdáleně v Kerio Administration Console
Vzdáleně provedeme import certifikátů následovně:

1. V libovolném textovém editoru otevřeme certifikát serveru a „intermediate“ certifikát.
2. V „intermediate“ certifikátu označíme kurzorem řetězec certifikátu a zkopírujeme jej do souboru s certifikátem serveru za řetězec certifikátu serveru. Soubor s certifikátem pak bude vypadat následovně:

```
-----BEGIN CERTIFICATE-----
MIIDOjCCAqOgAwIBAgIDPmR/MA0GCSqGSIb3DQEBBAUAMFMxCzAJBgNVBAYTAl
MSUwIwYDVQQKExxUaGF3dGUgQ29uc3VsdGluZyAoUHR5KSBMdGQuMR0wGwYDVQ
     ..... this is a server SSL certificate ...
ukrkDt4cgQxE6JSEprDiP+nShuh9uk4aUCKMg/g3VgEMulkROzFl6zinDg5grz
QspOQTEYoqrc3H4Bwt8=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDMzCCApygAwIBAgIEMAAAATANBgkqhkiG9w0BAQUFADCBxDELMAkGA1UEBh
WkExFTATBgNVBAgTDFdlc3Rlcm4gQ2FwZTESMBAGA1UEBxMJQ2FwZSBUb3duMR
     ..... this is an intermediate SSL certificate which
           signed the server certificate...
5BjLqgQRk82bFi1uoG9bNm+E6o3tiUEDywrgrVX60CjbW1+y0CdMaq7dlpszRB
```

```
t14EmBxKYw==
-----END CERTIFICATE-----
```

3. Certifikát serveru uložíme.
4. Otevřeme *Kerio Administration Console* a přepneme se do sekce SSL certifikáty.
5. Certifikát serveru importujeme pomocí tlačítka *Importovat* → *Importovat nový certifikát*.

10.2 Instalace certifikátu na klientské stanice

Instalace certifikátu na klientskou stanici je potřeba pouze v následujících případech:

- Používáme-li na stanici *MS Outlook* s *Kerio Outlook Connectorem* a chceme mít šifrovanou HTTP komunikaci mezi serverem a klientem (týká se to hlavně pokud uživatelé využívají *Free/Busy* server). Pokud certifikát nenainstalujeme, potom komunikace nebude vůbec fungovat.
- Používáme-li na stanici *MS Outlook* s *Kerio Synchronization Plug-inem* a chceme složky synchronizovat protokolem zabezpečeným SSL šifrováním. Pokud certifikát nenainstalujeme, potom komunikace nebude vůbec fungovat.
- Používáme-li *MS Entourage* a chceme jeho služby zabezpečit SSL šifrováním. Pokud certifikát nenainstalujeme, potom komunikace nebude vůbec fungovat.
- Při připojení ke *Kerio WebMailu* přes HTTPS. Pokud certifikát nenainstalujeme, bude se při každém přihlášení otevírat varovné okno (viz obrázek 10.1) upozorňující na absenci certifikátu.

Nejjednodušším způsobem, jak certifikát nainstalovat, je využít k tomuto účelu webový prohlížeč.

Instalace pomocí prohlížeče Internet Explorer

Internet Explorer využijeme v případech, kdy je potřeba nainstalovat certifikát do úložiště aplikace *MS Outlook* (*Internet Explorer* a *MS Outlook* mají společné úložiště certifikátů) nebo pokud se chceme připojovat ke *Kerio WebMailu* přes HTTPS.

Postup instalace certifikátu je následující:

1. Spustíme prohlížeč *Internet Explorer* a zadáme do něj URL adresu pro přihlášení k rozhraní *Kerio WebMail*. K serveru je třeba se připojit protokolem zabezpečeným SSL šifrováním. Adresa tedy musí začínat na `https://` (příklad: `https://mail.firma.cz/`).

2. Otevře se okno *Výstraha zabezpečení* (viz obrázek 10.1). V tomto okně klikneme na tlačítko *Zobrazit certifikát*.

3. Otevře se okno s podrobnostmi certifikátu, kde klikneme na tlačítko *Nainstalovat certifikát*.

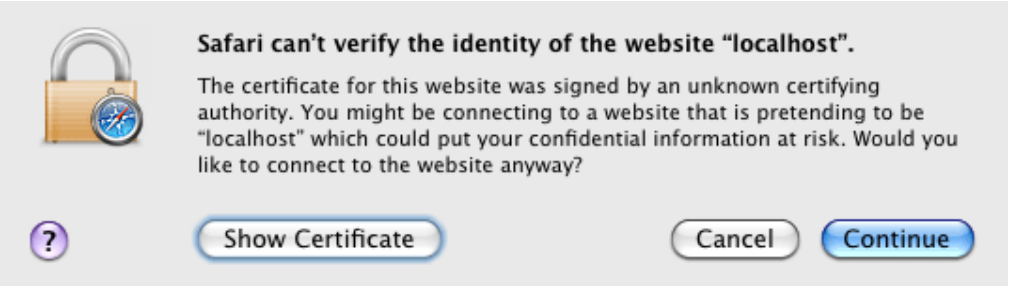
4. Otevře se průvodce instalací certifikátu. V průvodci není třeba nic nastavovat. Všechny kroky postupně odsouhlasíme, a po jeho ukončení bude certifikát nainstalován.

Instalace pomocí prohlížeče Safari

SSL certifikát je třeba nainstalovat vždy, když aplikace mají komunikovat s *Kerio MailServerem* službami zabezpečenými SSL. Certifikát *Kerio MailServeru* instalujeme pomocí prohlížeče Safari (stačí se přihlásit k rozhraní *Kerio WebMail* přes `https://`):

1. Otevřeme okno prohlížeče *Safari* a zadejte do něj URL adresu pro přihlášení k rozhraní *Kerio WebMail*. K serveru je třeba se připojit protokolem zabezpečeným SSL šifrováním. Adresa tedy musí začínat na `https://` (příklad: `https://mail.firma.cz/`).

2. Než se načte přihlašovací stránka *Kerio WebMailu*, otevře se varovné okno, že server, ke kterému se připojujeme systém nemůže ověřit, protože certifikát je ověřen neznámou autoritou (viz obrázek 10.5).

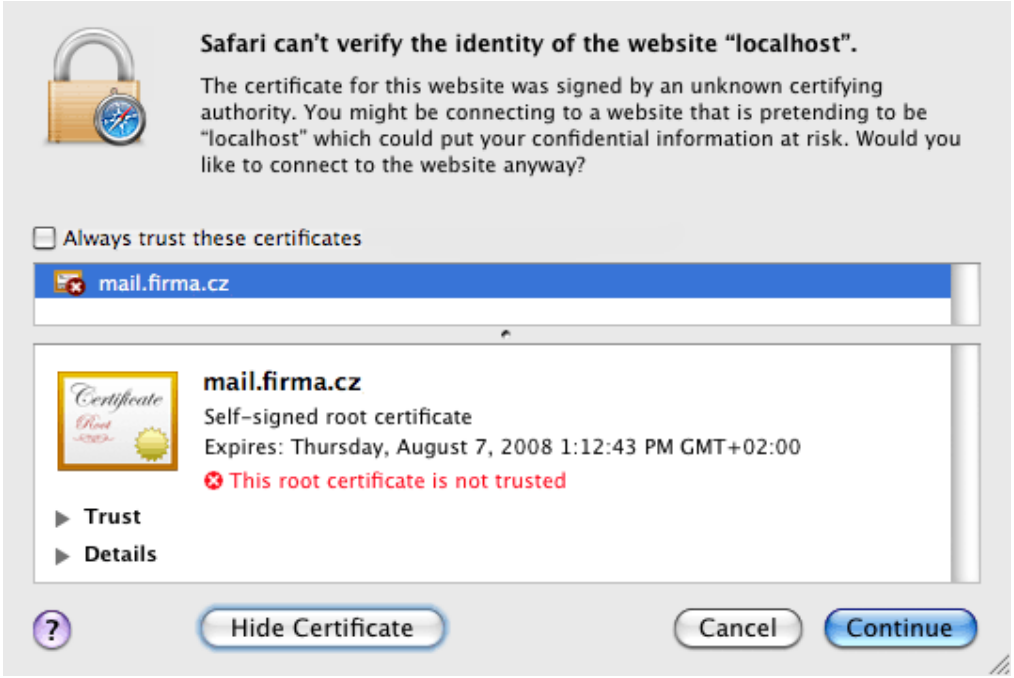


Obrázek 10.5 Informace o tom, že certifikát není důvěryhodný

3. Varovné okno obsahuje tlačítko *Show certificate*. Klikneme na toto tlačítko a certifikát se zobrazí (viz obrázek 10.6).

4. Kurzorem myši přesuneme ikonu certifikátu na plochu, jak to zobrazuje obrázek 10.7.

Nyní záleží na verzi systému Mac OS. Pro Mac OS X 10.3 Panther a Mac OS X 10.4 Tiger je postup následující:



Obrázek 10.6 Podrobnosti certifikátu

Obrázek 10.7 Přesun certifikátu na plochu

1. Klikneme na certifikát na ploše. Otevře se okno *Add Certificates* (viz obrázek 10.8), kde je třeba v menu *Keychain* zvolit jako typ úložiště *X509Anchors*. Do úložiště

X509Anchors jsou ukládány certifikáty, které mohou podepisovat další (kterým lze důvěřovat) a také všechny důvěryhodné certifikáty.[2]

Obrázek 10.8 Dialog Add Certificates

2. Pokud nejste přihlášení jako root nebo uživatel s administrátorskými právy, bude po vás nyní vyžadováno administrátorské heslo ověření.

3. Zároveň s dialogem *Add Certificates* se otevře úložiště klíčů *Keychain Access*. Pokud se neotevře, najdete ho v *Applications* → *Utilities* → *Keychain Access*.

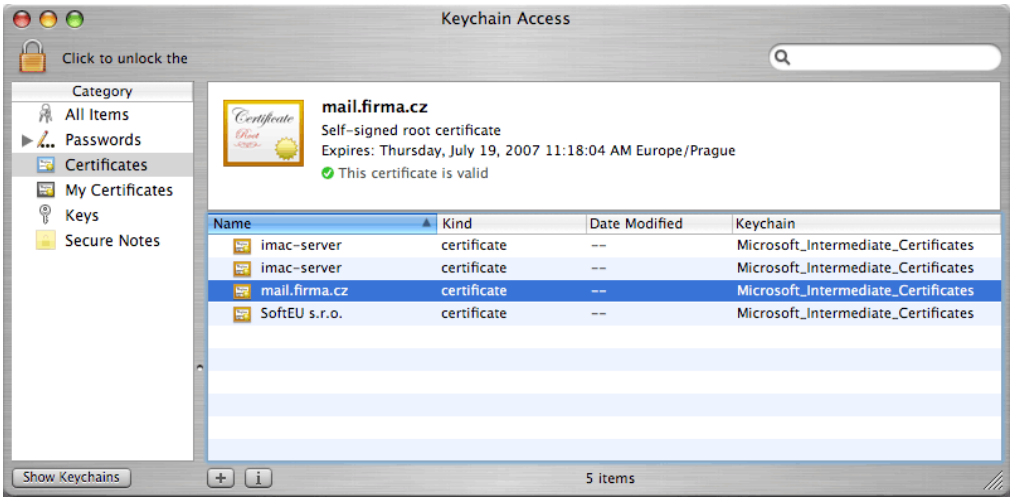
4. V aplikaci *Keychain Access* se přepněte do záložky *Certificates*.

5. Najděte na ploše certifikát a přesuňte ho do okna aplikace *Keychain Access*. Zkontrolujte, že se po přesunu certifikát objevil v seznamu certifikátů (viz obrázek 10.9).

Pro Mac OS X 10.5 Leopard je postup následující:

1. Klikneme na certifikát na ploše. Otevře se okno *Add Certificates* (viz obrázek 10.10), kde je třeba v menu *Keychain* zvolit možnost *System* (certifikát budou moci využívat všichni uživatelé systému) nebo *Login* (certifikát bude moci využívat pouze právě přihlášený uživatel). Volbu odsouhlasíme tlačítkem OK.

[2] Jakýkoliv certifikát bude funkční pouze v případě, že bude ve formátu X509, kódovaný Base64. Pokud váš certifikát tyto podmínky nesplňuje, lze jej převést a uložit do správného formátu pomocí speciální aplikace *Microsoft Cert Manager*. Tuto aplikaci najdete v *Applications* → *Microsoft Office* → *Office* → *Microsoft Cert Manager*. Nicméně v našem případě tato aplikace nebude potřeba. *Kerio MailServer* vytváří certifikáty ve formátu X509, kódované Base64.



Obrázek 10.9 Keychain Access — záložka Certificates

Obrázek 10.10 Dialog Add Certificates

2. Otevře se aplikace *Keychain Access* a zeptá se, zda opravdu chceme certifikát nainstalovat. Odsouhlasení je třeba potvrdit zadáním uživatelského jména a hesla s administračními právy.

Instalace certifikátu na mobilní zařízení

Do mobilních zařízení lze SSL certifikát nainstalovat pomocí *Internet Exploreru*. Import a instalace certifikátu se liší podle typu zařízení. Návody na instalaci SSL certifikátu pro všechna podporovaná zařízení najdeme v kapitole 36.4.

Kapitola 11

Parametry pro Kerio WebMail

Podrobné informace k uživatelskému rozhraní *Kerio WebMail* najdete v manuálu *Kerio MailServer, Příručka uživatele* na produktových stránkách společnosti *Kerio Technologies* `http://www.kerio.cz/kms-manual`.

11.1 Skiny

Rozhraní *Kerio WebMail* obsahuje několik standardních skinů (skin = vzhled *Kerio WebMailu*). Skiny jsou uloženy v adresáři

```
Kerio\MailServer\webmail\default\skins
```

Skiny jsou tvořeny kaskádovými styly (CSS) a obrázky. Kaskádový styl (CSS) je nástroj, kterým je možno přizpůsobit vzhled WWW stránek (barvy, typ písma, odsazení objektů atd.). Pokud je uživatel schopen pracovat s kaskádovými styly a obrázky, může si do velké míry *Kerio WebMail* přizpůsobit. Lze vycházet z některého z výchozích skinů nebo je možné vytvořit skin úplně nový. Nový skin musí být uložen v adresáři

```
\Kerio\MailServer\webmail\default\skins\xyz
```

kde `xyz` je název nového schématu.

11.2 Logo

V záhlaví každé stránky se zobrazuje logo společnosti *Kerio Technologies*. Toto logo můžete nahradit vlastním logem, případně libovolným jiným obrázkem.

Logo lze změnit buď globálně, pak bude platit pro všechny domény v *Kerio MailServeru*, nebo pro každou doménu zvlášť. Globálně se logo nastavuje v záložce *Logo* v sekci *Další volby* (bližší popis viz kapitolu 15.6). Loga pro jednotlivé domény se nastavují v sekci *Domény* (viz kapitolu 7.8). Pokud jsou v *Kerio Administration Console* nastavena jak globální, tak doménová loga, vyšší prioritu budou mít vždy loga nastavená pro jednotlivé domény.

Takto lze loga nastavit pouze v případě, že rozhraní *Kerio WebMail* používá výchozí skin. Je-li pro *Kerio WebMail* použit jiný než výchozí skin, musí být nové logo zkopírováno

přímo do adresáře se skinem a soubor musí být nazván jedním ze dvou níže uvedených způsobů (kde `xyz` je název příslušného skinu):

`Kerio\MailServer\webmail\default\skins\xyz\logo_my.domain.gif` (pokud mají být použita různá loga pro různé domény)

`Kerio\MailServer\webmail\default\skins\xyz\logo.gif` (pokud má být použito jedno globální logo)

Pokud v používaném skinu bude umístěn alespoň jeden z těchto dvou souborů (`logo_my.domain.gif`,`logo.gif`), nebude použito ani jedno z globálních log. Pokud bude používaný skin obsahovat jak doménová, tak globální loga, budou použita automaticky doménová.

11.3 Jazyk

V současné době *Kerio WebMail* obsahuje následující lokalizace:

- Angličtina
- Čeština
- Čínština
- Francouzština
- Holandština
- Chorvatština
- Italština
- Japonština
- Mad'arština
- Němčina
- Polština
- Portugalština
- Ruština
- Slovenština
- Španělština
- Švédština

Vytvoření vlastní lokalizace

Pokud *Kerio WebMail* neobsahuje lokalizaci do jazyka, která je požadována, lze vytvořit lokalizaci vlastní.

Veškeré texty pro jeden jazyk, které se v *Kerio WebMailu* zobrazují, jsou uloženy v samostatném lokalizačním souboru. Lokalizační soubory jsou uloženy ve formátu XML a jsou uloženy v podadresáři `/translations` (v adresáři, kde je *Kerio MailServer* nainstalován). Kódování souborů je vždy UTF-8.

Název každého souboru je tvořen zkratkou jazyka (např. `cs` pro češtinu, `en` pro angličtinu atd.) a příponou `.def`. Z toho vyplývá, že přidat další jazyk lze jednoduše přidáním odpovídajícího definičního souboru. Správce *Kerio MailServeru* tedy může vytvořit vlastní jazykovou mutaci tím, že zkopíruje některý z definičních souborů do souboru s novým názvem a přeloží (či nechá přeložit) texty v něm.

Formát XML začíná i končí tagem `<translation>`. Jednotlivé řádky je třeba zaznamenat ve tvaru:

```
<text id="head-user">Uživatel</text>
```

Postup vytvoření vlastního lokalizačního souboru pro nový jazyk je následující:

1. zkopírujeme lokalizační soubor ve zdrojovém jazyce (z něhož budeme překládat) do souboru nazvaného podle nového jazyka,

2. přeložíme všechny texty na jednotlivých řádcích souboru.

Načtení nového lokalizačního souboru vyžaduje restart *Kerio MailServeru*.

Kontrola pravopisu a slovníky

Kontrola pravopisu v rozhraní *Kerio WebMail* funguje na základě porovnání slov se slovníkem a je tedy možná pouze v jazycích, pro něž jsou v *Kerio MailServeru* nakopírované slovníky. Tyto slovníky lze nalézt ve složce `myspell`, kde je *Kerio MailServer* nainstalován. Výchozími verzemi slovníků pro pravopis jsou angličtina a čeština. Další verze je v případě potřeby nutné do složky `myspell` nakopírovat. Pro správnou funkci slovníků je nutné, aby vyhovovaly standardu produktů `myspell`. Tyto slovníky jsou volně dostupné na Internetu (například na adrese `http://wiki.services.openoffice.org/wiki/Dictionaries`). Každý ze slovníků obsahuje dva soubory, jeden ve tvaru `nazev_jazyka.aff` (například `fr_FR.aff`) a druhý ve tvaru `nazev_jazyka.dic` (například `fr_FR.dic`). Oba tyto soubory nakopírujeme do zmíněné složky `myspell`.

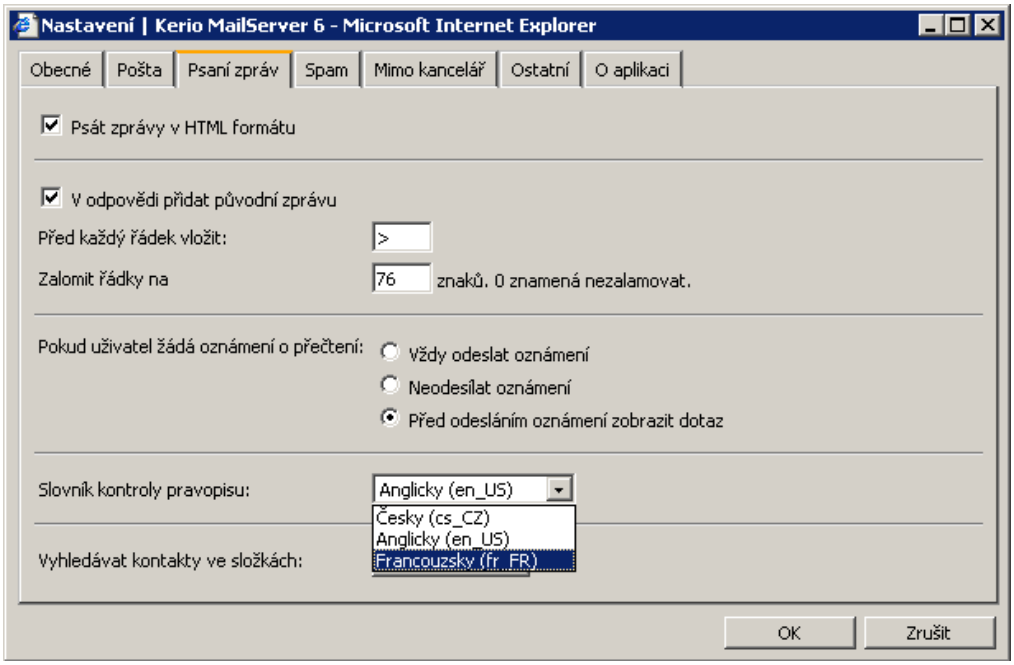
Aby se nový slovník začal požívat ke kontrole pravopisu, musí si jej každý uživatel nastavit jako preferovaný v uživatelském nastavení *Kerio WebMailu*:

1. Otevřeme plnou verzi rozhraní *Kerio Webmail*.

2. Klikneme na tlačítko *Nastavení* umístěné na panelu nástrojů.

3. Otevře se okno s několika záložkami. Přepneme se do záložky *Psaní zpráv*.

4. V položce *Slovník kontroly pravopisu* vybereme nový slovník (viz obrázek 11.1).



Obrázek 11.1 Výběr slovníku v nastavení Kerio WebMail

Kapitola 12

Nástroje

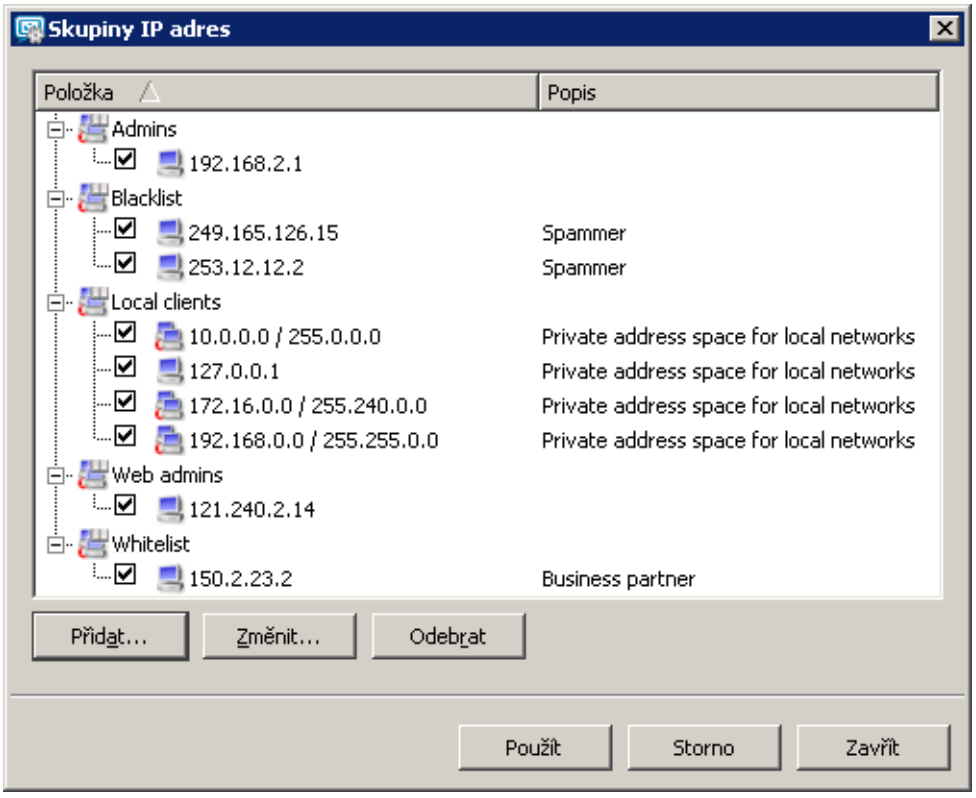
12.1 Skupiny IP adres

Skupiny IP adres slouží k jednoduché definici přístupu k určitým službám (např. vzdálená administrace, antispam atd.). Při nastavování přístupu se použije jméno skupiny, a ta pak může obsahovat libovolné kombinace jednotlivých počítačů (IP adres), rozsahů IP adres, subsítí či jiných skupin.

Vytvoření či úprava skupiny IP adres

Definice skupin IP adres se provádí v sekci *Konfigurace* → *Definice* → *Skupiny IP adres*.

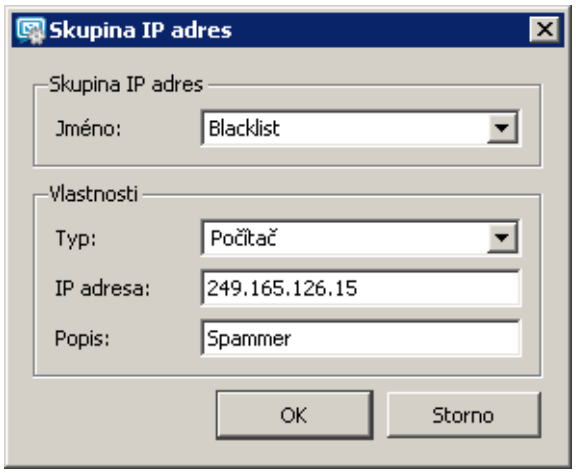
Standardně je doplněna skupina IP adres lokálních rozsahů. Tuto skupinu je možné v případě potřeby upravovat nebo ji smazat stejně jako ostatní, ručně vytvořené skupiny IP adres.



Obrázek 12.1 Skupiny IP adres

Tlačítkem *Přidat* lze přidat novou skupinu (nebo položku do existující skupiny), tlačítkem *Změnit* upravit a tlačítkem *Odebrat* smazat vybranou skupinu či položku.

Po stisknutí tlačítka *Přidat* se zobrazí dialog pro vytvoření nové skupiny IP adres.



Obrázek 12.2 Vytvoření skupiny IP adres

Jméno
: Název skupiny. Buď je možno zadat nový (vytvoření nové skupiny), nebo vybrat již existující — tím se přidá nová položka do stávající skupiny.

Typ
: Druh přidávané položky. Možnosti: jedna IP adresa (*Počítač*), rozsah IP adres (*Subsíť / rozsah*), subsíť s příslušnou maskou (*Subsíť / maska*) nebo jiná skupina IP adres (*Skupina adres*). Z toho vyplývá, že skupiny adres lze také vnořovat do sebe.

IP adresa, Maska...
: Parametry přidávané položky (v závislosti na zvoleném typu).

Popis
: Textový popis (komentář) ke skupině IP adres. Slouží pouze pro potřeby správce.

12.2 Časové intervaly

Časové intervaly v *Kerio MailServeru* slouží k omezení plánovaných akcí na určité časové období. Nejedná se o interval v pravém slova smyslu, ale o skupinu, která může obsahovat libovolný počet jednorázových nebo opakujících se časových úseků. Časové intervaly je možno definovat v sekci *Konfigurace* → *Definice* → *Časové intervaly*.

Obrázek 12.3 Časové intervaly

Platnost časového intervalu

Při definici časového intervalu lze použít tři druhy časových úseků (subintervalů):

Absolutní
: Interval je přesně ohraničen počátečním a koncovým datem, neopakuje se.

Týdenní
: Opakuje se každý týden (ve stanovených dnech).

Denní
: Opakuje se každý den (ve stanovených hodinách).

Je-li určitý časový interval složen z více úseků různého typu, platí v čase, který je dán průnikem absolutních úseků se sjednocením denních a týdenních úseků. Vyjádřeno symbolicky:

```
(d1 | d2 | w1 | w2) & (a1 | a2)
```

kde:

`d1`, `d2` — denní úseky

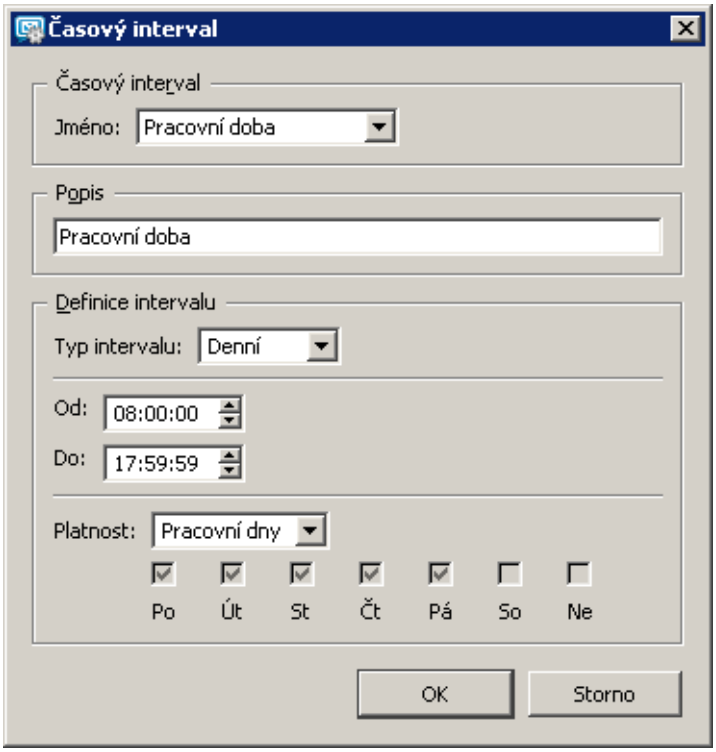
`w1`, `w2` — týdenní úseky

`a1`, `a2` — absolutní úseky

Definice časových intervalů

Vytvoření, úpravu nebo smazání časového intervalu lze provést v sekci *Konfigurace* → *Definice* → *Časové intervaly*.

Po stisknutí tlačítka *Přidat* se zobrazí dialog pro definici časového intervalu:



Obrázek 12.4 Nastavení časového intervalu

Jméno
: Jednoznačný název (identifikace) časového intervalu. Zde je možno buď zadat nový název (vytvořit nový interval) nebo vybrat již existující a přidat do něj další položku.

Popis
: Textový popis intervalu (slouží pouze pro účely správce).

Typ intervalu
: Typ časového intervalu: *Denní*, *Týdenní* nebo *Absolutní* (jednorázový) — tedy začínající a končící konkrétním datem.

Od, Do
: Začátek a konec časového úseku. Zde je možno zadat počáteční a koncový čas, případně také den v týdnu nebo datum (v závislosti na zvoleném typu intervalu).

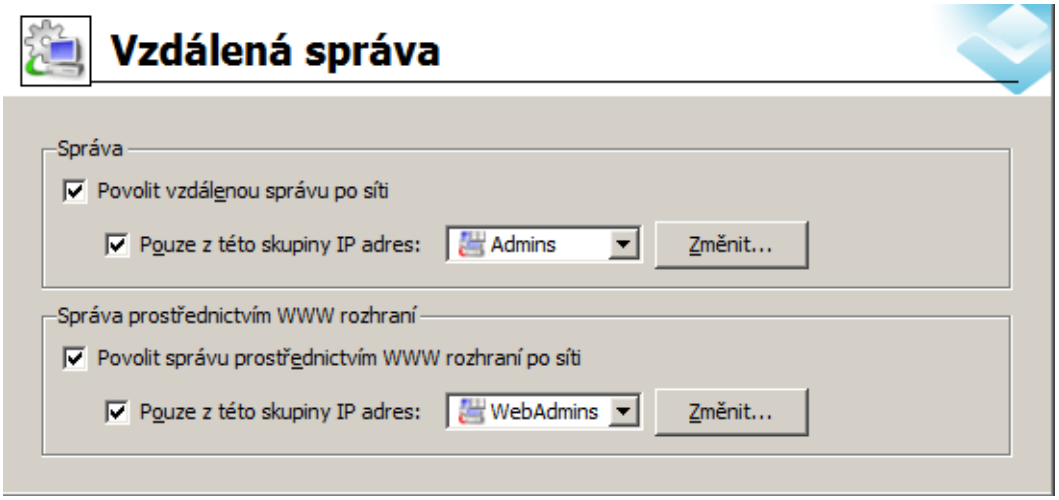
Platnost
: Dny v týdnu, v nichž má být interval platný. Buď je možno označit konkrétní dny (*Vybrané dny*), nebo použít některou přednastavenou volbu (*Všechny dny*, *Pracovní dny* — pondělí až pátek, *Víkend* — sobota a neděle).

Vytvořené časové intervaly nelze do sebe vnořovat.

12.3 Nastavení vzdálené správy

Chcete-li *Kerio MailServer* spravovat z jiného počítače, než na kterém běží, je třeba povolit vzdálenou administraci. Její nastavení se provádí v sekci *Konfigurace* → *Vzdálená správa*.

Vzdálenou správu je možno povolit jednak pro *Kerio Administration Console* a jednak pro *KMS Web Administration*:



Obrázek 12.5 Vzdálená správa

Vzdálená správa Kerio MailServeru

Port, na kterém probíhá komunikace mezi *Kerio Administration Console* a *Kerio MailServer Engine*, je 44337 (používány jsou protokoly TCP i UDP).

Povolit vzdálenou správu po síti
: Povolení vzdálené administrace (je-li tato volba vypnuta, bude možno *Kerio MailServer* spravovat pouze z počítače, na němž běží).

Pouze z této skupiny IP adres
: Komunikace mezi *Kerio MailServerem* a *Kerio Administration Console* je chráněna silným šifrováním (SSL protokol), takže vzdálená správa je bezpečná a přenášená data nemohou být odposlechnuta a zneužita. Přístup ke správě by měl vždy být chráněn heslem (tj. nedoporučuje se ponechávat uživateli s administračními právy heslo prázdné), přesto lze ochranu ještě zesílit povolením vzdálené správy pouze z určitých IP adres.

V menu je možno vybrat skupinu IP adres, z nichž bude vzdálená správa povolena. Tlačítkem *Změnit* lze skupinu upravit nebo vytvořit novou (dialog je shodný jako v sekci *Konfigurace* → *Definice* → *Skupiny IP adres* — viz kapitolu 12.1).

Správa uživatelů, skupin a aliasů přes web

Povolit správu prostřednictvím WWW rozhraní ...

Povolení správy prostřednictvím WWW rozhraní. Je-li tato volba vypnuta, nebude možno k rozhraní přistupovat. Správu prostřednictvím WWW rozhraní podrobně popisuje kapitola 31.

Pouze z této skupiny IP adres

Ochranu přístupu lze zesílit povolením vzdálené správy pouze z některých IP adres. V menu je možno vybrat skupinu IP adres, z nichž bude správa prostřednictvím WWW rozhraní po síti povolena. Tlačítkem *Změnit* lze skupinu upravit nebo vytvořit novou (dialog je shodný jako v sekci *Konfigurace* → *Definice* → *Skupiny IP adres* — viz kapitolu 12.1).

Kapitola 13

Uživatelské účty

Uživatelské účty v *Kerio MailServeru* reprezentují fyzické e-mailové schránky. Uživatelské jméno a heslo tedy slouží jako ověření přístupu k této schránce. Protože *Kerio MailServer* může obsluhovat více nezávislých domén, nemají uživatelské účty globální platnost, ale patří vždy do konkrétní domény. Z toho vyplývá, že domény musí být definovány dříve, než budou vytvářeny uživatelské účty (podrobnosti viz kapitolu 7).

Uživatelské účty mohou být umístěny:

1. lokálně — uživatelské schránky jsou umístěny přímo v *Kerio MailServeru* a i veškerá správa účtů se provádí v *Kerio MailServeru* (kapitola 13.2),

2. v LDAP databázi — účty jsou do *Kerio MailServeru* pouze mapovány. Mapování účtů je možné z *Active Directory* a *Apple Open Directory* (kapitola 7.6).

Uživatelské účty je možné do *Kerio MailServeru* jednoduše importovat z jiné databáze uživatelů:

- import z Novell eDirectory (kapitola 13.10),
- import z NT domény (kapitola 13.10),
- import z Active Directory domény (kapitola 13.10),
- importovány z textového souboru.

13.1 Administrátorský účet

Kromě přístupu ke své e-mailové schránce může být uživatelský účet použit také pro přístup ke správě *Kerio MailServeru*, má-li k tomu příslušná práva. Základní administrátorský účet se vytváří přímo při instalaci. Tento účet se ničím neliší od ostatních uživatelských účtů a může být i odstraněn, pokud jsou alespoň jednomu dalšímu uživateli udělena plná práva pro přístup ke správě.

Základní administrátorský účet má povoleno vytvářet a spravovat veřejné složky.

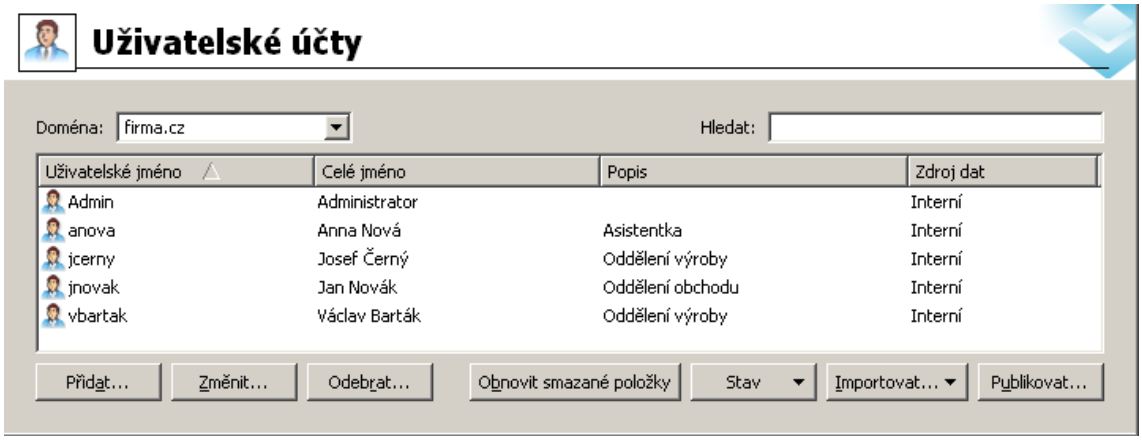
Základní administrátorský účet standardně spravuje také archivní složky (pokud je povolena archivace — viz kapitolu 18.2). V archivní složce je možné dohledat jakoukoli zprávu, která prošla *Kerio MailServerem*.

Administrátor může archivní složku nasdílet jiným uživatelům. Je třeba si uvědomit, že do těchto složek se zálohují zprávy všech uživatelů, a proto by k nim měl mít přístup pouze důvěryhodný správce (nanejvýš malá skupina osob).

Upozornění: Hesla k uživatelským účtům, která mají plný přístup ke správě, by měla být důsledně uchovávána v tajnosti, aby nemohlo dojít k jejich zneužití neoprávněnou osobou.

13.2 Založení uživatelského účtu

Definice uživatelských účtů se provádí v sekci *Nastavení domény* → *Uživatelské účty*.



Obrázek 13.1 Uživatelské účty

Nejprve je nutno v poli *Doména* vybrat lokální doménu, v níž mají být účty definovány. V každé doméně mohou existovat jak lokální účty, tak i účty uložené v adresářové službě (např. *Microsoft Active Directory*). V seznamu uživatelů dané domény se zobrazují účty obou typů. Přidávat lze však pouze lokální účty (účty v příslušné adresářové službě musejí být vytvářeny nástrojem pro její správu — např. *Active Directory Users and Computers*). Účtům v adresářové službě je možno měnit některé jejich vlastnosti.

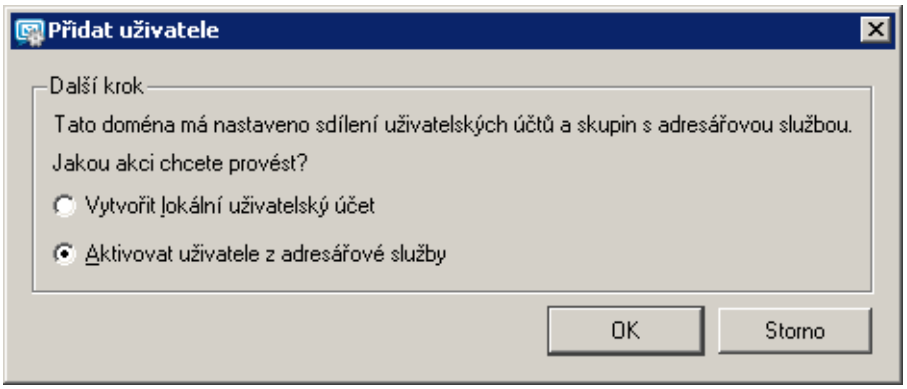
Upozornění: Je-li smazán v administrační konzoli účet namapovaný z adresářové služby, účet v *Kerio MailServeru* se deaktivuje.

Poznámka: Význam jednotlivých sloupců tohoto okna bude zřejmý z následujícího popisu jednotlivých položek v definici uživatelského účtu. Jedinou výjimkou je sloupec *Zdroj dat*, který zobrazuje, o jaký typ účtu se jedná:

- *Interní* — účet je uložen v interní databázi uživatelů.
- *LDAP* — účet je uložen v adresářové službě (*Active Directory*, *Apple Open Directory*).

Stisknutím tlačítka *Přidat* se zobrazí průvodce vytvořením nového uživatelského účtu. Je-li doména konfigurována pro spolupráci s adresářovou službou (viz kapitolu 7.6), zobrazí se okno s výběrem, zda chcete aktivovat uživatele z adresářové služby nebo vytvořit lokální účet.

Aktivovat uživatele znamená, že uživatelský účet je uložen v adresářové službě, a od okamžiku aktivace s ním *Kerio MailServer* může pracovat. Všechny údaje se budou ukládat do adresářové služby.



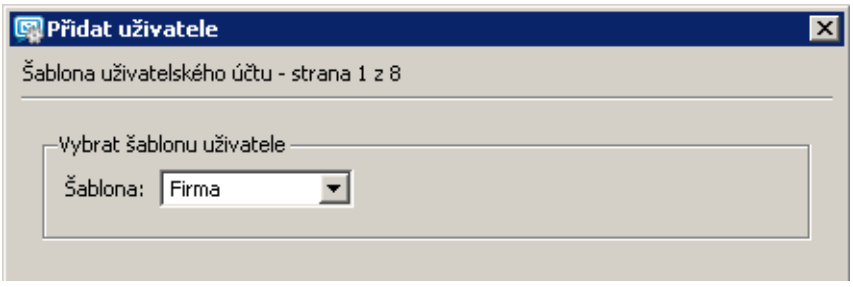
Obrázek 13.2 Aktivace uživatele z adresářové služby

Pokud zvolíte aktivaci uživatele, otevře se okno s nabídkou uživatelů adresářové služby, na kterou je doména napojena. Dále jen vyberete příslušné uživatele a potvrdíte. Tlačítka v levém dolním rohu okna slouží k usnadnění výběru uživatelů. *Vybrat vše* — označí všechny uživatele a *Zrušit výběr* — zruší označení všech uživatelů.

Vytvoření lokálního uživatelského účtu se provádí následujícím průvodcem:

Krok 1 — šablona

První krok průvodce se zobrazuje pouze v případě, že je vytvořena alespoň jedna šablona pro vytváření nových účtů. Šablonu pro založení nových uživatelských schránek lze vytvořit v sekci *Definice* → *Šablony uživatelů*. Šablonu je dobré použít zejména v případě, že zakládáme najednou více uživatelských účtů, které mají některé parametry shodné (například nastavení typu ověřování, kvóty, atd.). Založením šablony a vyplněním těchto shodných parametrů přímo do ní se vyhneme zbytečné práci navíc.



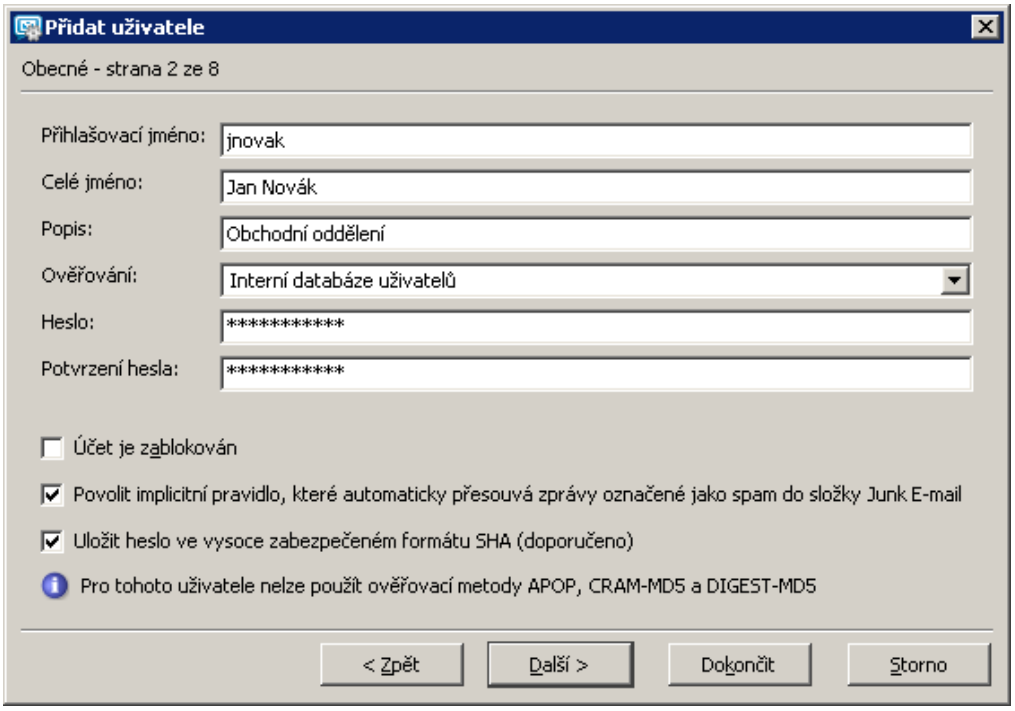
Obrázek 13.3 Založení uživatele — šablona

Založení nové šablony je popsáno v samostatné kapitole 13.12.

Krok 2 — základní údaje

Přihlašovací jméno

Přihlašovací jméno (pozor: nejedná-li se o lokální primární doménu, pak se uživatel musí přihlašovat celou svou e-mailovou adresou, tedy např. `uzivatel@jinafirma.cz`, nikoliv pouze `uzivatel`).
Ve jménu uživatele se nerozlišují malá a velká písmena.



Obrázek 13.4 Založení uživatele — základní údaje

Upozornění: Přihlašovací jméno nesmí obsahovat národní a některé speciální znaky (viz tabulku 13.1).
Příklady správně vytvořených jmen:
`novak`, `jan.novak`, `ing.jan.novak`, `jan_novak`, `jan-novak`, `jan---novak`, `jan_jakub-novak`, `jan_-_novak-_`
Příklady špatně vytvořených jmen:
`jan..novak`, `jan...novak`, `jan.novak.`, `.novak`, `novak.`

Celé jméno

Plné jméno (typicky jméno a příjmení daného uživatele). Položku je nutné vyplnit v případě, že uživatelské údaje z tohoto účtu budou exportovány do veřejné složky s kontakty.

Znaky	Povolení použití
a–z	znaky jsou povoleny bez omezení
0–9	znaky jsou povoleny bez omezení
A–Z	znaky jsou povoleny bez omezení
.	znak je povolen, nesmí však uvozovat nebo ukončovat řetězec a nesmí být použit dvakrát za sebou
-	znak je povolen bez omezení
_	znak je povolen bez omezení

Tabulka 13.1 Povolené znaky v přihlašovacím jménu uživatele

Popis

Textový popis uživatele (např. funkce). Položka *Popis* má pouze informativní charakter. Může obsahovat libovolné informace nebo nemusí být vyplněna vůbec.

Ověřování

Způsob ověřování uživatele lze zvolit v menu:

- *Interní databáze uživatelů*
  Uživatel je ověřován pouze v rámci *Kerio MailServeru*. V tomto případě je potřeba zadat heslo do položek *Heslo* a *Potvrzení hesla* (své heslo pak může uživatel sám změnit pomocí rozhraní *Kerio WebMail*).
  Upozornění: Heslo může obsahovat pouze tisknutelné znaky (písmena, číslice, interpunkční znaménka). V hesle se rozlišují malá a velká písmena.
- *Doména Windows NT*
  Uživatel bude ověřován v doméně Windows NT. Název NT domény je třeba zadat ve vlastnostech e-mailové domény (záložka *Upřesnění*, položka *Doména Windows NT*). Tento způsob ověřování lze použít, pouze běží-li *Kerio MailServer* na operačním systému Windows 2000/XP a 2003. Podrobnosti viz kapitolu 7.7.
- *Kerberos 5*
  Ověření se provede pomocí ověřovacího systému Kerberos verze 5.
- *PAM služba*
  Ověřování službou PAM (Pluggable Authentication Modules — možno pouze na operačním systému Linux).
- *Apple Open Directory*
  Ověřování v databázi *Apple Open Directory* (pouze pro *Mac OS X*). Volbu lze nastavit pouze v případě, že je uživatel namapován z *Apple Open Directory*.

Heslo a Potvrzení hesla

Heslo uživatele lze zadat nebo změnit pouze lokálním uživatelům. Každý uživatel by měl bezprostředně po založení účtu heslo změnit.

Bude-li heslo obsahovat speciální (národní) znaky, uživatelé se nebudou moci z některých poštovních klientů připojit ke *Kerio MailServeru*. Pro zadávání hesel uživatelů proto doporučujeme používat pouze ASCII znaky.

Povolit implicitní pravidlo, ...

Zaškrtnutím volby se při zakládání uživatelského účtu vytvoří pravidlo pro nevyžádanou poštu. Všechny příchozí zprávy, které byly antispamovou kontrolou označeny jako nevyžádané, budou automaticky přesunuty do složky *Nevyžádaná pošta*. Pravidlo je možno v nastavení účtu vytvořit pouze při jeho zakládání. Filtr a pravidla pro příchozí poštu blíže popisuje manuál *Kerio MailServer, Příručka uživatele*.

Upozornění: Nedoporučujeme vytvoření tohoto pravidla, pokud uživatel ke své poště přistupuje přes protokol POP3. V takovém případě se na lokální klientskou stanici stáhne pouze složka *Doručená pošta* a uživatel nemá možnost provést kontrolu, zda je pošta zařazená do složky *Nevyžádaná pošta* opravdu nevyžádaná.

Uložit heslo ve vysoce zabezpečeném formátu SHA

Heslo uživatele je standardně šifrováno symetrickým klíčem (DES). Volba *Uložit heslo v bezpečnějším formátu* umožňuje použití bezpečnější, nesymetrické šifry (SHA řetězec). Nevýhodou SHA šifrování je, že není možné využít některé metody ověřování pro přístup na *Kerio MailServer*, konkrétně jsou to metody APOP, CRAM-MD5 a Digest-MD5. Pro ověřování přístupu lze tedy využít pouze metody LOGIN a PLAIN (důrazně doporučujeme používat pro přihlašování pouze SSL spojení).

Po zaškrtnutí volby je nutné změnit heslo uživatele. To může udělat buď administrátor nebo uživatel (např. přes rozhraní *Kerio WebMail*).

Upozornění: Hesla uložená ve formátu SHA jsou podporována od verze *Kerio MailServer 6.0.5*. Bude-li konfigurace s SHA hesly přenesena na starší verzi *Kerio MailServeru*, nebude ověřování fungovat.

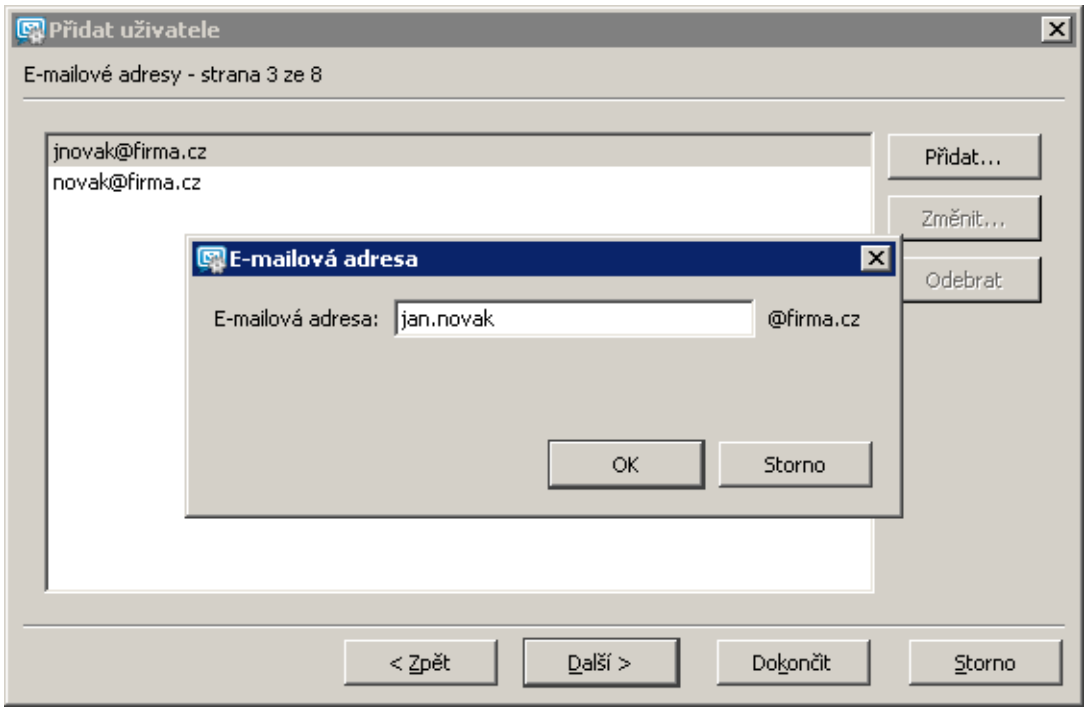
Účet je zablokován

Dočasné zrušení „vypnutí“ účtu bez nutnosti jej odstraňovat.

Upozornění: tato položka nijak nesouvisí s blokováním účtů, které se nastavuje v sekci *Konfigurace* → *Další volby*, v záložce *Bezpečnostní politika* (viz sekci 15.6). Pokud uživatel při přihlášení zadá omylem několikrát za sebou neplatné heslo a překročí tak limit nastavený v záložce *Bezpečnostní politika*, pak se účet automaticky zablokuje. Tuto blokaci je třeba zrušit taktéž v záložce *Bezpečnostní politika* tlačítkem *Odblokovat všechny účty*.

Krok 3 — e-mailové adresy

V tomto kroku průvodce je možno zadat všechny požadované e-mailové adresy daného uživatele. Primární adresa uživatele (kterou nelze zrušit) je tvořena jeho uživatelským jménem a doménou, v níž se účet nachází. Ostatní adresy jsou tzv. aliasy. Aliasy lze zadávat přímo v definici uživatele, nebo v sekci *Nastavení domény* → *Aliasy*. Doporučujeme však zadávat aliasy přímo v definici uživatele — je to jednodušší a navíc jsou aliasy přístupné v *Active Directory* doméně.

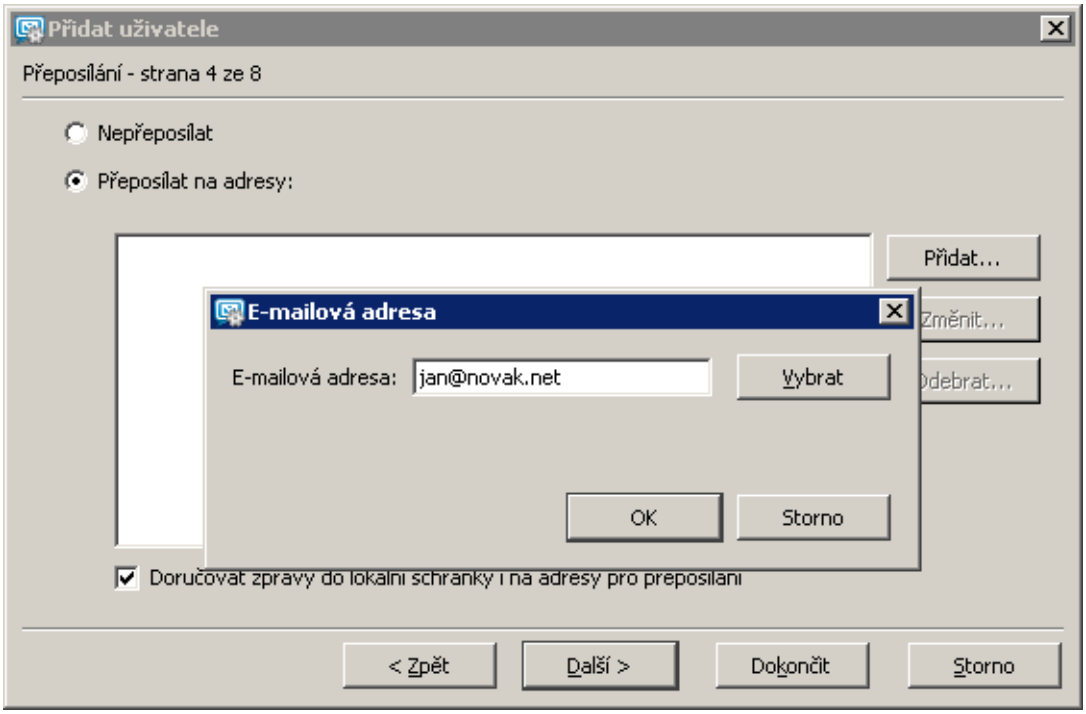


Obrázek 13.5 Založení uživatele — přidělení e-mailových adres

Poznámka: Jsou-li uživatelské účty udržovány v *Active Directory* (viz kapitolu 7.6), pak je možné zadávat jejich aliasy přímo v panelu *Active Directory Users and Computers*. Globální aliasy (tj. v sekci *Nastavení domény* → *Aliasy*) takto zadávat nelze.

Krok 4 — přeposílání zpráv na jiné adresy

Zprávy pro uživatele mohou být volitelně přeposílány na další e-mailové adresy. Volba *Doručovat zprávy...* zajistí, že zpráva bude uložena do lokální schránky a zároveň přeposlána na uvedené adresy (jinak bude pouze přeposlána a do lokální schránky se neuloží).

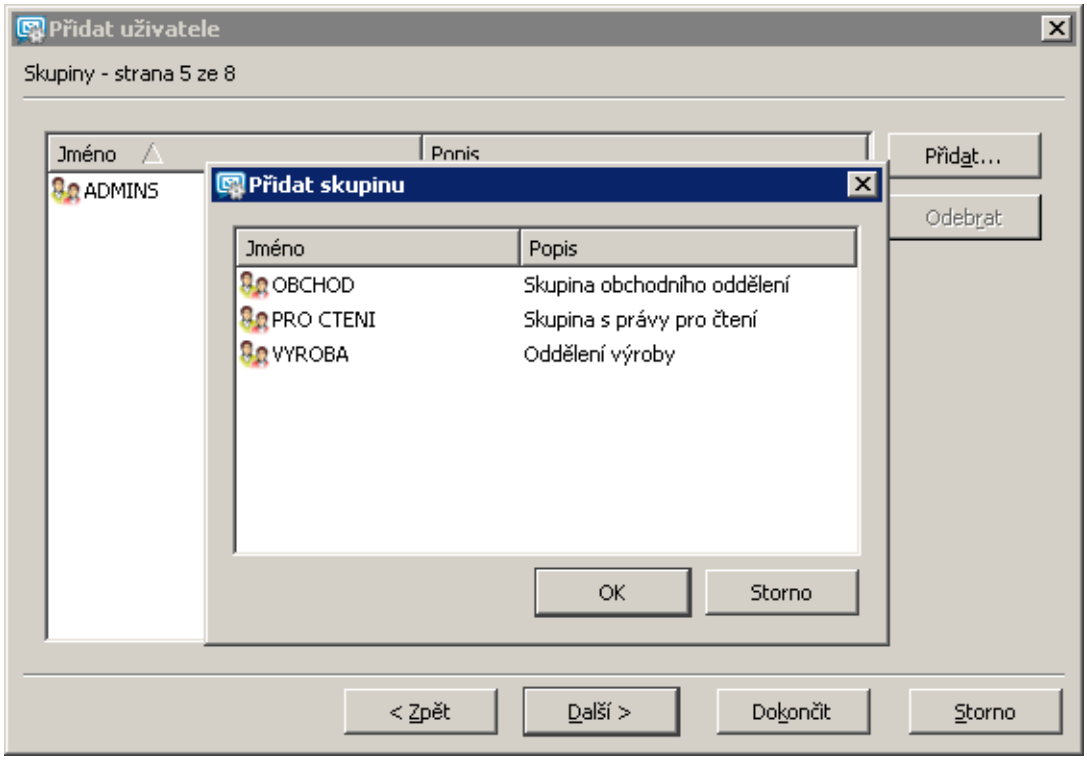


Obrázek 13.6 Založení uživatele — přeposílání zpráv

Poznámka: Toto lze rovněž řešit pomocí aliasů, nastavení v definici uživatele je však jednodušší a přehlednější.

Krok 5 — skupiny

V tomto dialogu je možno (tlačítky *Přidat* a *Odebrat*) přidat nebo odebrat skupinu, do níž má být uživatel zařazen. Skupiny je nutno nejprve vytvořit v sekci *Nastavení domény* → *Skupiny*. Při definici skupin je ale možno stejným způsobem do skupin přidávat uživatele, a proto nezáleží na tom, zda budou nejprve vytvořeny skupiny nebo uživatelé.



Obrázek 13.7 Založení uživatele — přidělení uživatele do skupiny

Krok 6 — nastavení přístupových práv

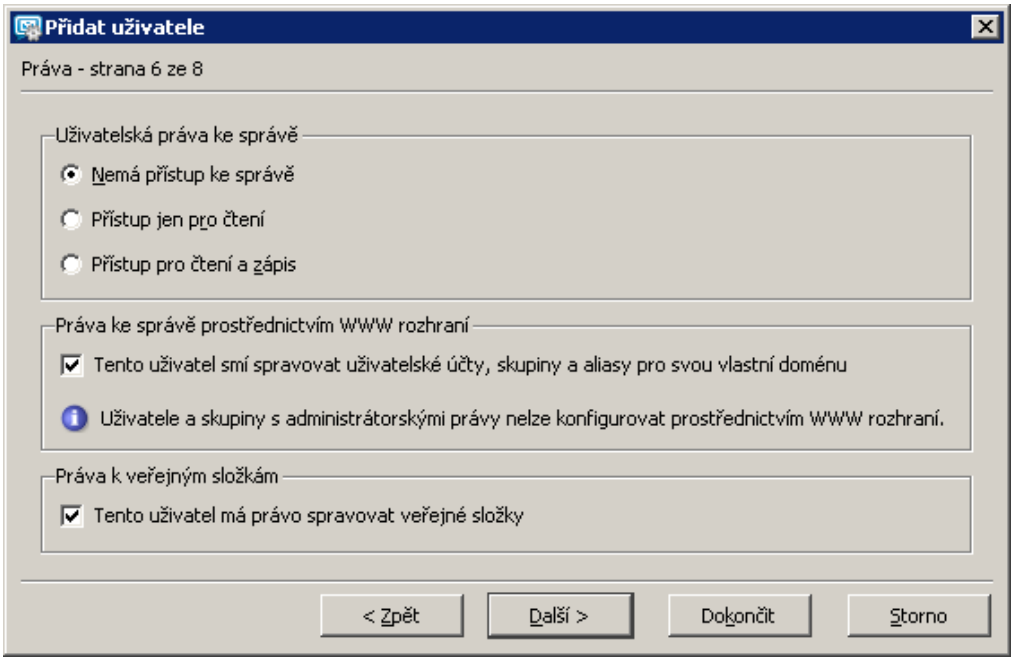
Každý uživatel musí mít nastavenu jednu ze tří úrovní přístupových práv.

Bez přístupu ke správě
: Uživatel nemá práva pro přihlášení ke správě *Kerio MailServeru*. Toto nastavení je typické pro většinu uživatelů — budou mít přístup pouze ke své poštovní schránce.

Přístup jen pro čtení
: Uživatel se může přihlásit ke správě *Kerio MailServeru*, může však pouze prohlížet záznamy a nastavení, nemá právo provádět žádné změny.

Přístup pro čtení a zápis
: Uživatel má plná práva ke správě, je ekvivalentní uživateli `Admin`. Existuje-li alespoň jeden uživatel s těmito právy, může být účet Admin odstraněn.

Tento uživatel smí spravovat aliasy a uživatelské účty/skupiny ...
: Speciální právo pro přístup do *KMS Web Administration* (více viz kapitolu 31). Toto oprávnění je nezávislé na nastavení přístupových práv do *Kerio Administration Console*.



Obrázek 13.8 Založení uživatele — nastavení uživatelských práv

Tento uživatel má právo spravovat ...

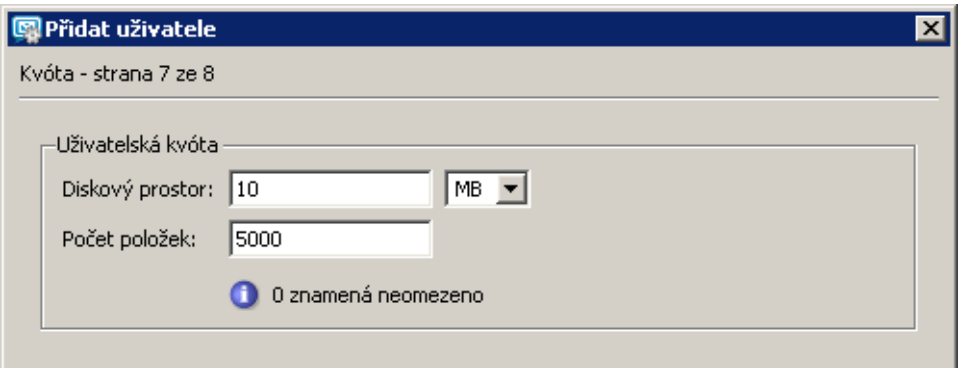
Správu veřejných složek má standardně povolenu pouze *Admin* primární domény. Pokud *Kerio MailServer* obsahuje více lokálních domén, na kterých jsou založeny uživatelské účty, musí být tato volba zaškrtnuta vždy alespoň jednomu uživateli v každé doméně. *Kerio MailServer* je nastaven tak, že každá doména má vlastní veřejné složky a uživatelé jiné lokální domény k ní nemají přístup (toto nastavení lze změnit tak, aby veřejné složky byly přístupny všem doménám a tedy i všem uživatelům společně — bližší popis tohoto nastavení je uveden v kapitole 7.1).

Standardně mají všichni uživatelé z jedné domény nastavené k veřejným složkám právo pro čtení. Práva k veřejným složkám může přidělovat každý uživatel, který má sám právo tyto složky spravovat. Práva lze uživatelům přidělit také přes rozhraní *Kerio WebMail* a *MS Outlook* doplněný o *Kerio Outlook Connector*.

Všechny typy veřejných složek (pošta, kalendáře, kontakty, úkoly, poznámky) v *Kerio MailServeru* jsou zobrazovány pouze v aplikaci *MS Outlook* doplněné o *Kerio Outlook Connector* a v *Kerio WebMailu*. V jiných poštovních klientech se obvykle zobrazují pouze veřejné složky typu pošta (přesnější informace o všech podporovaných poštovních klientech najdete v manuálu *Kerio MailServer, Příručka uživatele*).

Krok 7 — nastavení uživatelské kvóty

Uživateli lze nastavit určitá omezení na jeho poštovní schránku.



Obrázek 13.9 Založení uživatele — nastavení kvóty

Diskový prostor
: Nastavení maximálního prostoru ve schránce. Pro pohodlné zadání číselného údaje je možno přepínat jednotky: kilobyty (*KB*), megabyty (*MB*) a gigabyty (*GB*).

Počet zpráv
: Maximální počet zpráv ve schránce.

Každou z těchto položek lze nastavit na hodnotu *0* (nula), což znamená, že se na schránku žádné omezení nevztahuje.

Uživatelská kvóta slouží především k ochraně serveru proti zaplnění diskového prostoru. Bude-li splněna alespoň jedna z těchto podmínek, budou další zprávy adresované tomuto uživateli serverem odmítány.

Po naplnění kvóty bude uživateli zaslána varovná zpráva s doporučením na snížení počtu zpráv ve schránce. Zároveň nezáleží na tom, zda byl překročen počet zpráv či vyhrazená velikost diskového prostoru. Kvóta je naplněna ve chvíli, kdy byla uložena do složky zpráva (událost, kontakt nebo úkol), která překročila jeden nebo druhý nastavený limit.

Prahem pro odeslání upozornění je 90% nastavené hodnoty v kvótě (90% nastaveného počtu položek nebo 90% nastavené velikosti diskového prostoru). Tuto hodnotu lze ručně změnit v konfiguračním souboru *Kerio MailServeru*:

1. Zastavíme *Kerio MailServer Engine*.

2. V adresáři, kam je nainstalován *Kerio MailServer* najdeme soubor `mailserver.cfg`

   Pokud soubor editujeme na platformách *Mac OS X* nebo *Linux*, potom se nejprve do systému přihlásíme jako root (speciální uživatel s plnými přístupovými právy do systému).

3. Otevřeme soubor `mailserver.cfg` a najdeme proměnnou `QuotaWarningThreshold`. Celý řádek bude vypadat takto:

   ```
   <variable name="QuotaWarningThreshold">90</variable>
   ```

4. Změníme hodnotu proměnné na vyhovující a soubor uložíme.

5. Spustíme *Kerio MailServer*.

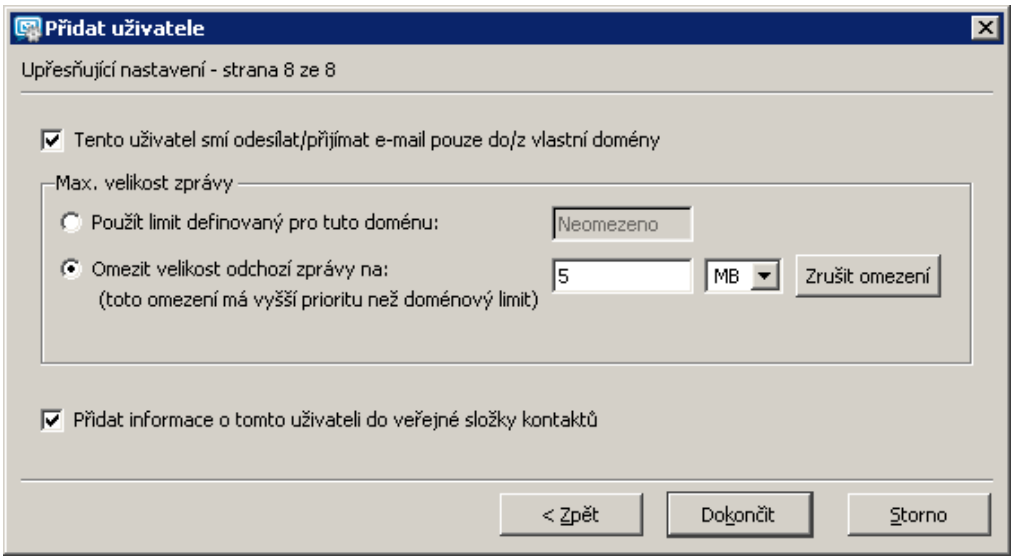
Varovná zpráva je serverem odesílána vždy jednou za 24 hodin, ne častěji. I v případě, že uživatel vymaže některé zprávy a dostane se pod hranici nastavené kvóty, a poté ji ještě ten den znovu překročí, další zpráva bude doručena 24 hodin od prvního upozornění.

Poznámka: Pokud se v souvislosti s nastavením kvóty objevily nějaké potíže, mohou vám při jejich řešení pomoci informace zaznamenané v *Debug* logu. Záznam *Debug* je umístěn v administrační konzoli v sekci *Záznamy* → *Debug*. Aby se do záznamu vypisovaly informace o chování kvóty, je třeba zapnout volbu *Quota and Login Statistics* (více viz kapitolu 22.8).

Krok 8 — upřesňující nastavení

Tento uživatel smí odesílat/přijímat ...

Volba umožňuje správci *Kerio MailServeru* omezit komunikaci uživatele pouze na lokální úroveň. To může být v mnoha společnostech užitečné například při řešení interní komunikace. Zaškrtnutím této volby docílíme, že daný uživatel nebude moci odesílat ani přijímat zprávy z externích domén.



Obrázek 13.10 Založení uživatele — přidání kontaktu uživatele do veřejné složky

Max. velikost zprávy

Nastavení limitu pro maximální velikost odchozích zpráv. Každý uživatel může mít buď nastaven rozdílný limit, nebo je možné nastavit limit shodný pro celou doménu (kapitola 7.1). Doporučujeme tuto volbu nastavit, zejména pokud není žádný limit nastaven pro celou doménu.

Zadáním tohoto limitu lze jednoduše zabránit uživatelům, aby zahltili internetovou linku odesíláním zpráv s příliš velkými přílohami.

Jsou-li oba limity nastaveny na 0, chová se *Kerio MailServer* stejně, jako by žádný limit nastaven nebyl.

Limit nastavený uživateli má vyšší prioritu než limit nastavený celé doméně.

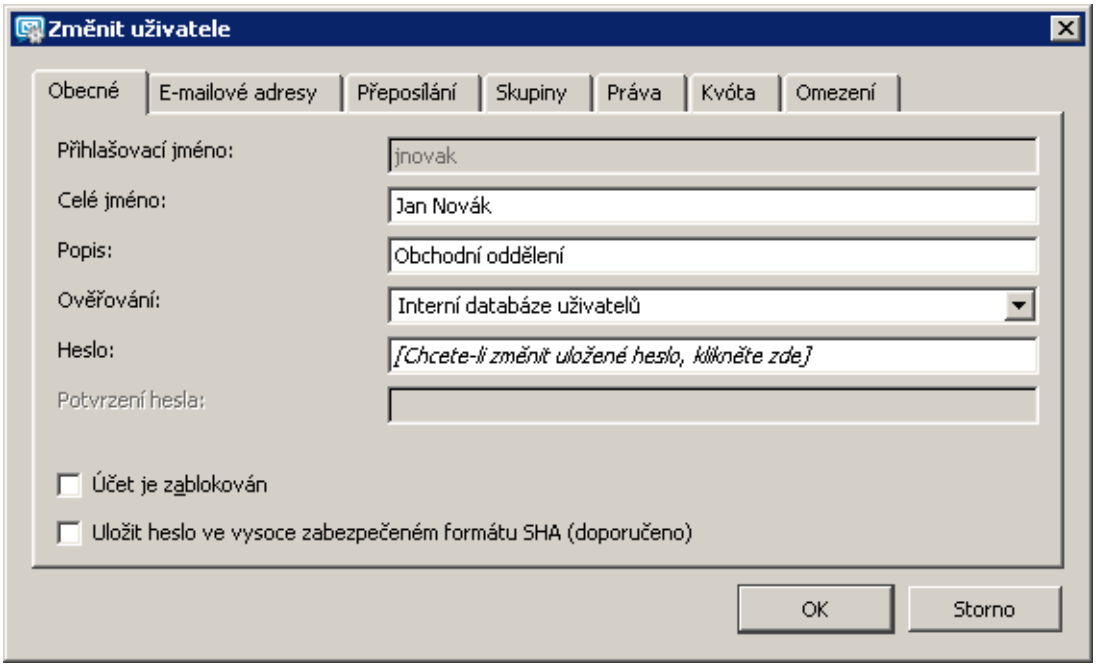
Přidat informace o tomto uživateli ...

Po zaškrtnutí volby bude do složky s veřejnými kontakty přidán kontakt uživatele. Kontakt bude do veřejné složky přidán pouze v případě, že byla v prvním (při použití šablony v druhém) kroku průvodce vyplněna položka *Celé jméno*.

Poznámka: Při importu uživatelů z *Kerio MailServeru 5* budou do veřejné složky s kontakty přidaní pouze uživatelé primární domény.

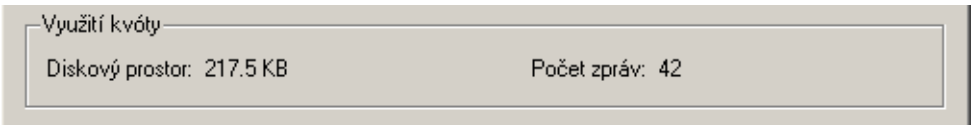
13.3 Úprava uživatelského účtu

Tlačítko *Změnit* otevírá dialog pro změnu parametrů uživatelského účtu.

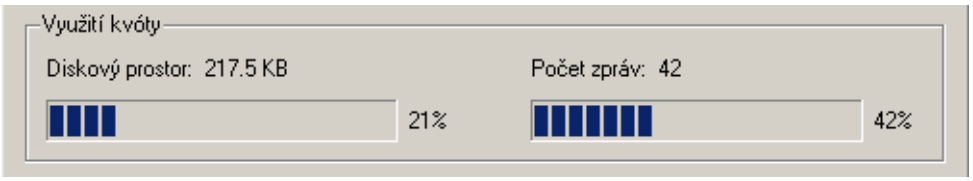


Obrázek 13.11 Úprava uživatelského účtu

Tento dialog obsahuje výše popsané části průvodce vytvořením účtu, uspořádané do záložek v jednom okně. V záložce *Kvóta* se také zobrazuje aktuální využití této kvóty. Pokud kvóta není nastavena, resp. není omezena, nezobrazuje se procentuální zaplnění kvóty.



Obrázek 13.12 Kvóta není nastavena

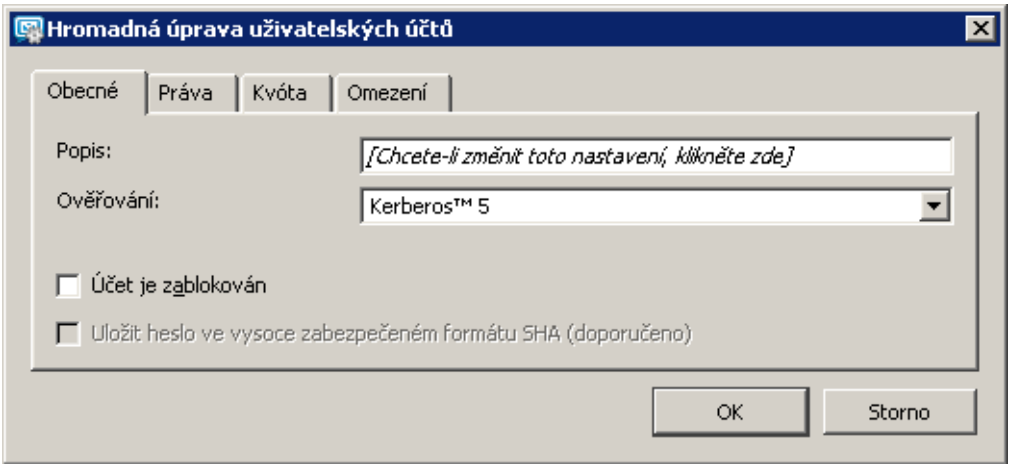


Obrázek 13.13 Kvóta je nastavena

13.4 Hromadná změna uživatelských účtů

Kerio MailServer umožňuje provádět hromadnou změnu uživatelských účtů. Stačí potřebné účty označit kurzorem a použít tlačítko *Změnit*.

Dialogové okno pro hromadnou úpravu účtů obsahuje čtyři záložky, kterými je možno změnit u vybraných účtů parametry týkající se kvóty, práv uživatelů, obecného nastavení (popis účtu, nastavení typu ověřování, nastavení bezpečnějšího formátu hesla, zablokování účtů) a omezení uživatelských účtů.



Obrázek 13.14 Hromadná změna účtů

Při práci s tímto dialogovým oknem platí, že se mění pouze položka nebo položky, které mají být hromadně přenastaveny ve všech vybraných účtech. Volby *Uložit heslo ve vysoce zabezpečeném formátu SHA* a *Účet je zablokován* v záložce *Obecné* mají tři stavy, které se mění kliknutím na zaškrtávací okénko:

- *neaktivní, šedá* — v každém z vybraných účtů bude zachováno původní nastavení,
- *zaškrtnuto* — položka se ve všech vybraných účtech zaškrtne,
- *nezaškrtnuto* —položka se ve všech vybraných účtech odškrtne.

Volby jsou třístavové pouze za předpokladu, že jsou v účtech nastaveny různě. Pokud mají všechny účty nastavení stejné, mají volby dva stavy, a to *zaškrtnuto* nebo *nezaškrtnuto*.

Záložky *Práva*, *Kvóta* a *Omezení* se nastavují stejným způsobem jako při editaci jednoho účtu.

Příklad:

Typickým příkladem použití hromadného nastavení účtů je omezení maximální velikosti zpráv uživatelů. Správce *Kerio MailServeru* nastavil omezení velikosti odchozích zpráv pro doménu *firma.cz* na 20 MB. Několik uživatelů z této domény ovšem potřebuje odesílat zprávy s přílohami většími, než je nastavený limit.

Kerio MailServer umožňuje označit pomocí kurzoru a klávesy `Ctrl` účty všech uživatelů z domény *firma.cz*, kteří mají s nastaveným limitem potíže a v dialogu pro hromadnou úpravu uživatelských účtů v záložce *Omezení* limit buď zvýšit nebo jej úplně zrušit.

13.5 Odstranění účtu

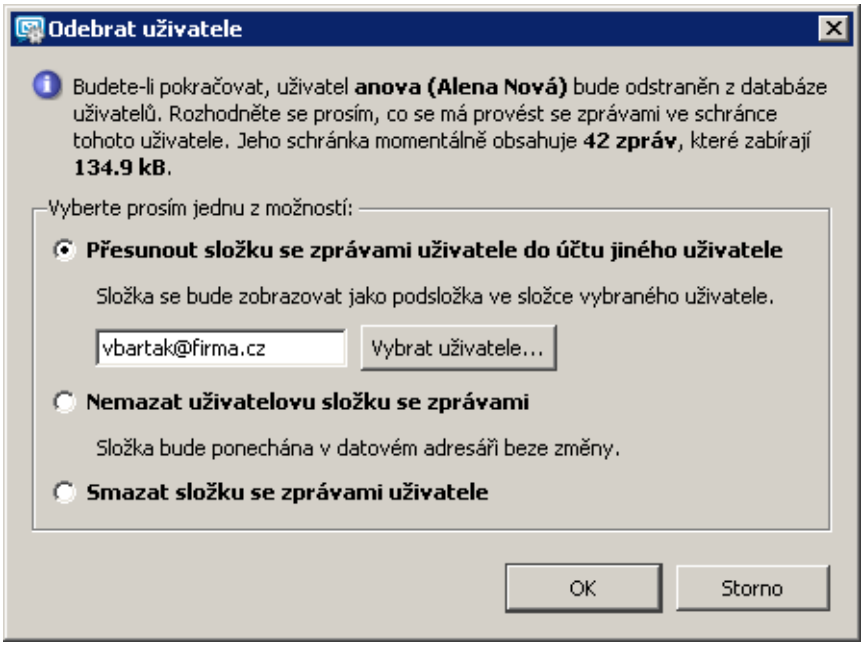
Odstranit uživatelský účet lze pomocí tlačítka *Odebrat*. *Kerio MailServer* umožňuje provádět různé akce s původní schránkou uživatele. K tomuto účelu slouží dialog, který se otevře bezprostředně po stisknutí tlačítka *Odebrat*. Dialog umožňuje nastavit, zda má být schránka vymazána nebo přesunuta jinému uživateli, nebo zda má prostě zůstat v adresáři `store`.

Přesunout složku se zprávami uživatele do účtu...

Celá uživatelská složka bude přesunuta jako podsložka kořenové složky vybraného uživatelského účtu. Název složky bude ve tvaru *Deleted mailbox — uzivatelske_jmeno@domena*. Tato složka bude obsahovat všechny původní složky smazané schránky.

Tato volba je užitečná zejména v případě, že jiný uživatel potřebuje se zprávami, událostmi a úkoly z této složky dále pracovat.

Poznámka: Nastane-li při přesunu uživatelské schránky problém, potom se podrobnosti o něm zaznamenají do *Warning* logu (více viz kapitolu 22.5).



Obrázek 13.15 Dialog pro odebrání uživatele

Nemazat uživatelovu složku se zprávami
Uživatelská složka zůstane v úložišti, aby byla v případě potřeby k dispozici.

Smazat složku se zprávami uživatele
Volbu lze využít hlavně v případě, že uživatelská složka neobsahuje žádné, nebo žádné důležité položky.

13.6 Vyhledávání

Pole *Hledat* napomáhá při hledání konkrétních položek v seznamu uživatelů. Do pole *Hledat* je možno zadat řetězec a v tabulce se automaticky objeví pouze položky, které daný řetězec obsahují.

13.7 Obnova smazaných položek

Tlačítko se zobrazuje pouze v případě, že je povolena příslušná volba v první záložce nastavení domény (viz kapitolu 7.2) a nastaven počet dní, po který má být obnova možná. Pro každou doménu musí být tato volba povolena zvlášť.

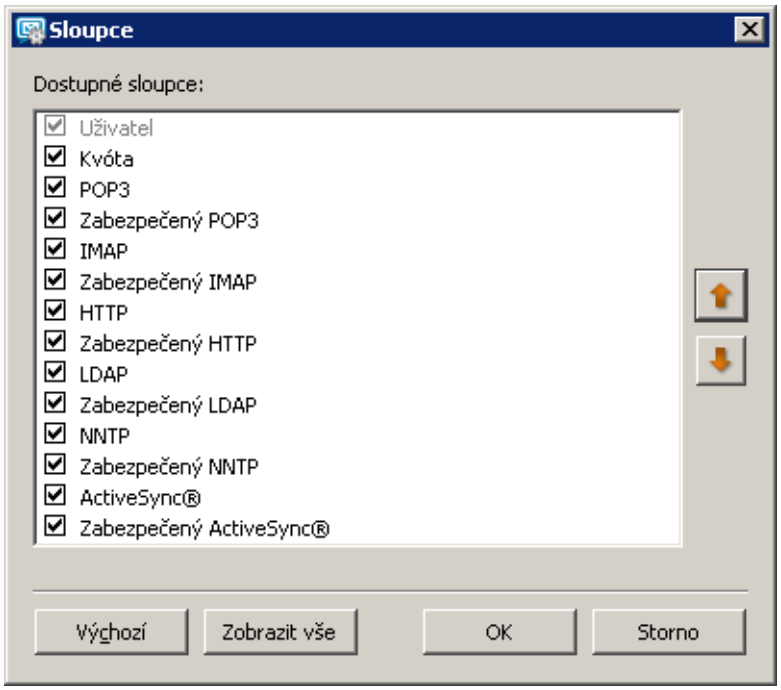
Je-li v nastavení domény vše správně povoleno, zobrazí se v sekci *Uživatelské účty* tlačítko *Obnovit smazané položky*. Poté stačí označit uživatele, který si například omylem smazal důležitou zprávu a všechny položky (zprávy, události, úkoly a kontakty) nastaveného časového úseku se mu obnoví do složky *Odstraněná pošta*.

Je-li potřeba obnovit položku starší, než je časový úsek nastavený pro danou doménu, je nutno použít archiv (kapitola 18.2).

13.8 Statistiky

Uživatelské statistiky jsou měřeny od začátku provozu (tj. od instalace) *Kerio MailServeru*. Aby byly zachovány i při vypnutí serveru, jsou údaje pro každého uživatele ukládány do souboru `stats.usr` v jeho domovském adresáři.

Použitím tlačítka *Stav* → *Uživatelské statistiky* ve složce *Nastavení domény* → *Uživatelské účty* se otevře statistická tabulka obsahující vybrané uživatelské účty, *služby*, pro něž jsou statistiky měřeny, *poslední přihlášení* (datum a čas posledního přihlášení uživatele ke službě) a *počet přihlášení* (celkový počet přihlášení uživatele ke službě).



Obrázek 13.16 Výběr sloupců ve statistikách

Správce *Kerio MailServeru* má možnost upravit si způsob zobrazení informací v jednotlivých sekcích dle vlastní potřeby. V okně *Statistiky* se po stisknutí pravého tlačítka myši zobrazí kontextová nabídka obsahující volbu *Nastavit sloupce*. Tato volba otevírá dialog, v němž je možné nastavit, které sloupce mají být zobrazeny, a které mají zůstat skryty.

Pro další zpracování uživatelských statistik je lze exportovat do dvou formátů: XML a CSV (jednotlivé položky jsou odděleny čárkami). Tlačítko pro export je umístěno pod statistikou.

Poznámka: Pokud pro zobrazení a další zpracovávání statistik používáte *MS Excel*, mohou nastat problémy s oddělovačem textu. CSV formát používá jako oddělovač standardně čárku. Aplikace *MS Outlook* však vyžaduje v některých lokalizacích středník (např. česká lokalizace *MS Office*). Abychom předešli problémům se správným zobrazením statistiky v tabulce, provedeme následující:

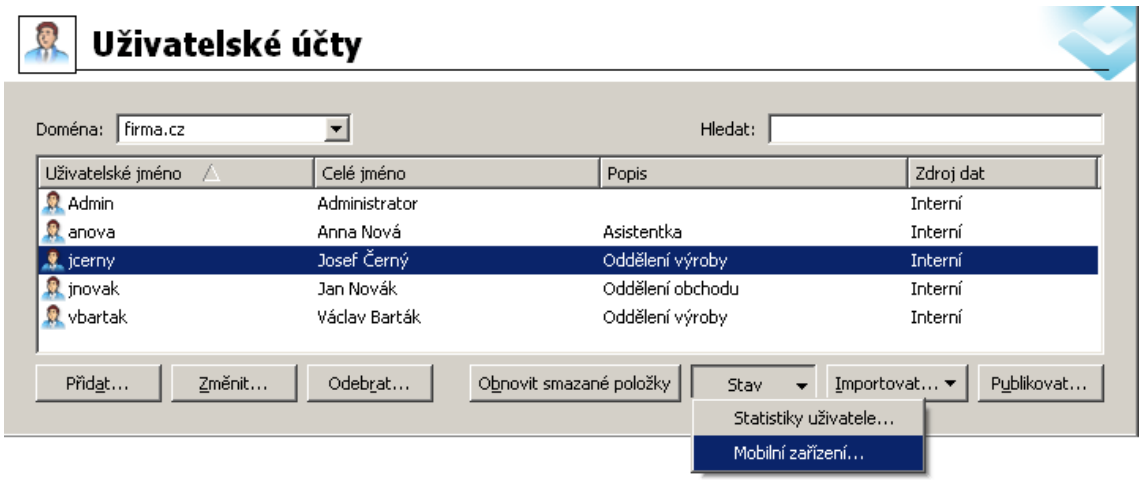
1. Vybereme data pro statistiku a stiskneme tlačítko *Exportovat* → *Exportovat do CSV*.
2. Ve standardním okně pro uložení souboru pojmenujeme soubor a uložíme do vybraného adresáře.
3. Otevřeme *MS Excel*.
4. V menu *Data* klikneme na položku *Importovat externí data* → *Importovat data*.
5. Otevře se okno *Vybrat zdroj dat*, pomocí kterého najdeme a otevřeme soubor se statistikou.
6. Otevře se *Průvodce importem textu*, kde přepneme nastavení textu na *Oddělovač* (pokud to neuděláme, nebudou jednotlivé položky statistiky odděleny do sloupců).
7. Klikneme na tlačítko *Další*.
8. V následujícím dialogu vybereme jako typ oddělovače čárku.
9. Klikneme na tlačítko *Dokončit*.

13.9 Správa mobilních zařízení

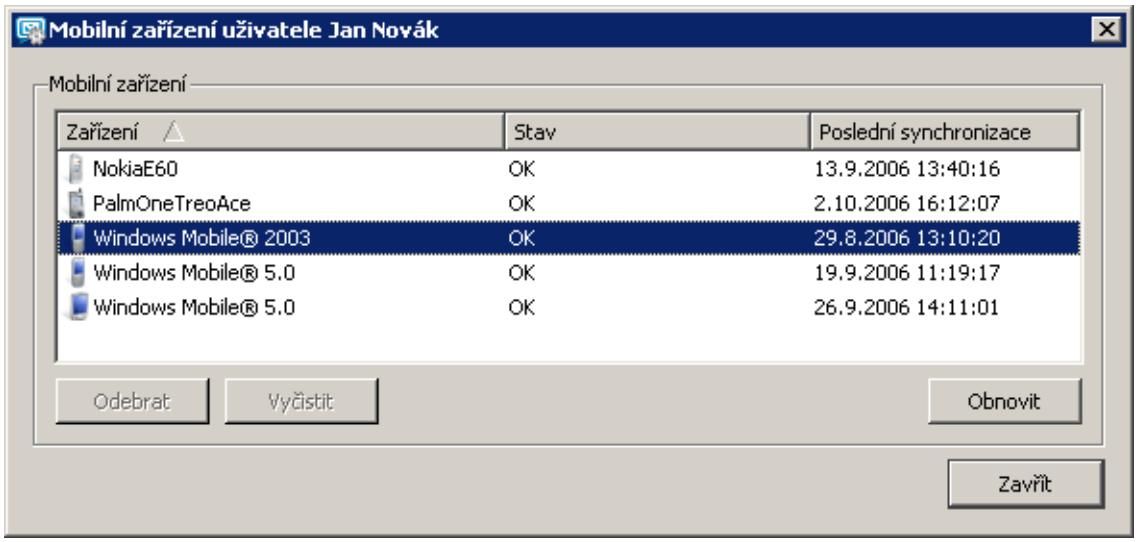
Uživatelé se ke *Kerio MailServeru* mohou připojovat pomocí různých mobilních zařízení (PDA nebo takzvaných „chytrých“ telefonů). Spojení mobilního zařízení a *Kerio MailServeru* umožňuje podpora protokolu *ActiveSync* (tento protokol a jeho využití blíže popisuje samostatná kapitola 36).

Administrační konzole obsahuje nástroj pro správu mobilních zařízení, aby měl správce *Kerio MailServeru* přehled o aktuálně používaných zařízeních jednotlivými uživateli.

Správce mobilních zařízení obsahuje sekce *Nastavení domény* → *Uživatelské účty*. V této sekci stačí vybrat uživatele, který používá mobilní zařízení a připojuje se s ním k serveru. Klikneme na tlačítko *Stav* a v jeho menu vybereme položku *Mobilní zařízení* (viz obrázek 13.17). Otevře se okno *Mobilní zařízení*, které zobrazuje všechna zařízení, kterými se uživatel připojuje k serveru (viz obrázek 13.18). Pod seznamem zařízení je k dispozici několik tlačítek:

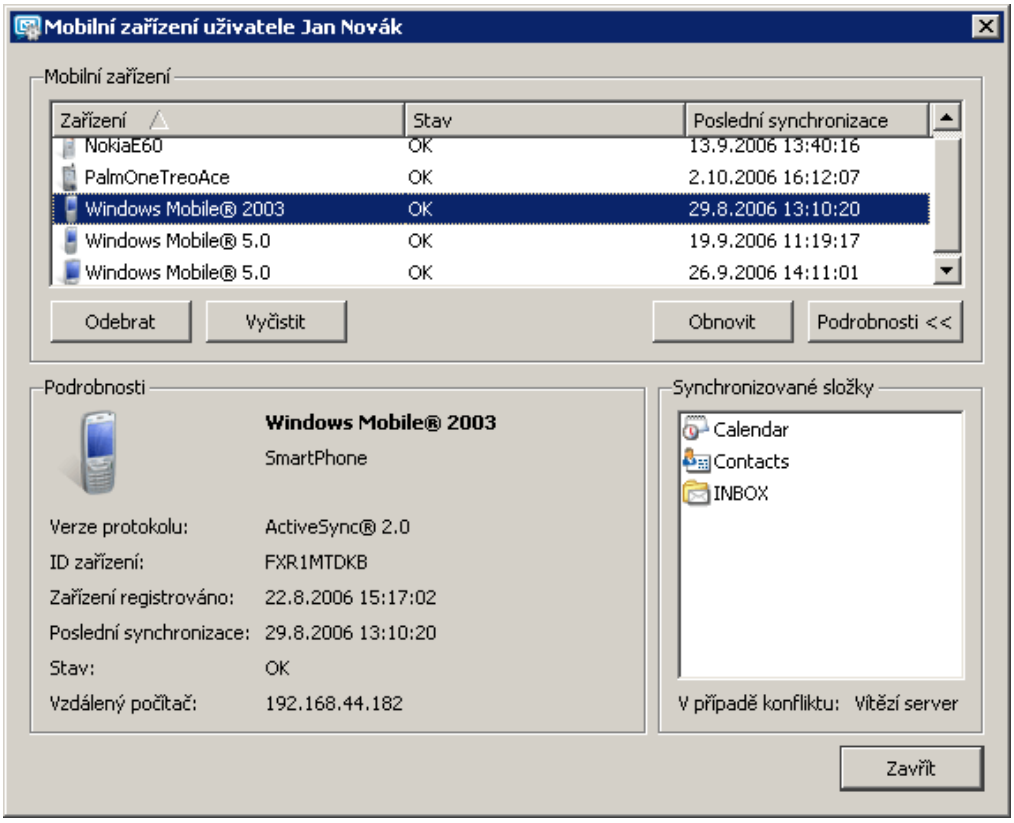


Obrázek 13.17 Kontextové menu uživatele — Mobilní zařízení



Obrázek 13.18 Mobilní zařízení

- *Odebrat* — vymaže zařízení ze seznamu. Používá se hlavně v případě, že uživatel již zařízení nepoužívá (tuto funkci podrobně popisuje kapitola 36.6).
- *Vyčistit* — toto tlačítko umožňuje vzdálené vymazání uživatelských dat ze zařízení (tuto funkci podrobně popisuje kapitola 36.5).
- *Obnovit* — tlačítko umožňuje aktualizovat stav připojených zařízení.
- *Podrobnosti* — tlačítko slouží k zobrazení dalších údajů o vybraném zařízení. Po stisknutí tohoto tlačítka se pod seznamem objeví druhá část okna, která obsahuje podrobnosti jednak o připojeném zařízení a jednak o synchronizaci. Podrobnosti se dělí na dvě části (viz obrázek 13.19). První část se nazývá přímo *Podrobnosti* a obsahuje údaje o připojeném zařízení a synchronizaci:



Obrázek 13.19 Mobilní zařízení — podrobnosti

Operační systém zařízení a jeho typ
: V prvním řádku se zobrazuje ikona zařízení (ikona reflektuje skutečnou podobu mobilního zařízení). Vedle ikony je tučně zobrazen typ systému, který zařízení obsahuje a také zda se jedná o PDA či Smartphone.

Verze protokolu
: Verze protokolu *ActiveSync*.

ID zařízení
: Sériové číslo zařízení.

Zařízení registrováno
: Datum, kdy uživatel zadal údaje o serveru do aplikace *ActiveSync* a poprvé se připojil.

Poslední synchronizace
: Datum a čas poslední synchronizace.

Stav
: Stav průběhu synchronizace. V této položce lze zjistit, zda při synchronizaci nenastal problém, a zda byla dokončena úspěšně.

Vzdálený počítač
IP adresa, která byla přidělena síťovému adaptéru zařízení.

Druhá část se jmenuje *Synchronizované složky* a zobrazuje seznam všech složek, které jsou synchronizovány. Starší typy zařízení obvykle podporují pouze synchronizaci pošty, kalendáře a kontaktů, novější typy zařízení navíc podporují úkoly.

Pod oknem, kde jsou zobrazeny složky je obsažena informace o nastavení řešení kolizí synchronizace. Kolize nastaven vždy, když se v době od poslední synchronizace změní stejná data jak na serveru, tak v zařízení.

- *Vítězí server* — v případě kolize data uložená na serveru přepíší data v zařízení.
- *Vítězí klient* — v případě kolize data uložená v zařízení přepíší data na serveru.

13.10 Import uživatelů

Uživatelské účty mohou být nejen ručně definovány, ale mohou být také načteny (importovány) z jiných zdrojů:

- ze souborů v CSV formátu
- NT domény
- Active Directory
- Novell eDirectory

Upozornění:

- Používáte-li doménu Windows 2000 nebo 2003 (*Active Directory*), pak je jednodušší a výhodnější nastavit *Kerio MailServer* tak, aby přímo spolupracoval s databází *Active Directory* (viz kapitolu 7.6). Importováním uživatelů totiž dojde k vytvoření lokálních účtů v *Kerio MailServeru*. Při změnách v *Active Directory* (přidání nebo smazání uživatele) je pak nutné provést změny i v konfiguraci *Kerio MailServeru* (nový import nebo smazání účtu).
- Před započetím importu doporučujeme v záznamu *Debug* zapnout volbu *Directory Service Lookup* (kde a jak volbu zapnout se dozvíte v kapitole 22.8). Informace ze záznamu průběhu importu vám mohou pomoci k úspěšnému řešení případných problémů.

Tlačítko *Importovat* pod seznamem uživatelů se chová zároveň jako menu. Nabízí import z adresářové služby (NT doména, Active Directory, Novell eDirectory) nebo import ze souboru ve formátu CSV. Po výběru příslušné volby se otevře dialog pro import uživatelů:

Import ze souboru

Uživatelské účty je možné importovat ze souborů ve formátu CSV. Data v souboru musí být uložena v určitém tvaru. Nadpisy jednotlivých sloupců musí korespondovat s položkami v *Kerio MailServeru*. Podporovány jsou následující:

- Name — uživatelské jméno (např. `jnovak`). Povinná položka.
- Password — heslo uživatele. Volitelná položka.
- FullName — plné jméno uživatele (např. `Jan Novák`). Volitelná položka.
- MailAddress — e-mailová adresa uživatele. Do sloupce se vyplňuje pouze část před zavináčem. Adres může být libovolný počet (např. `jnovak`, `novak`, `honza`, `jan.novak`). Volitelná položka.
- Groups — skupiny, do kterých je uživatel přihlášen. Opět jich v jednom poli může být zadáno více. Volitelná položka.
- Description — popis uživatele. Volitelná položka.

Sloupce lze do tabulky poskládat podle potřeby, na jejich pořadí nezáleží. Také je možné využít pouze některé z nich (kromě sloupce Name, ten je povinný).

Při vytváření souboru vhodného pro import je velmi důležité, zda jsou data oddělována čárkou (`,`) nebo středníkem (`;`). Pokud jsou data oddělována středníkem, pak je další postup jednodušší. Stačí vytvořit tabulku, v jejímž záhlaví jsou uvedeny standardní názvy položek (viz výše) a doplnit data. V případě položek `MailAddress` a `Groups` je možné zadat i více e-mailových adres nebo skupin. Jednotlivé adresy či skupiny je třeba oddělit čárkou (viz tabulku 13.2).

Name	Password	FullName	Description	MailAddress	Groups
jnovak	VbD66op1	Jan Novák	Vývoj	jnovak	cteni,vsichni
jcerny	Ahdpppu4	Josef Černý	Obchod	jcerny,cerny	obchod,vsichni
anova	SpoiuS158	Alena Nová	Asistentka ředitele	anova,alena.nova	vsichni
dlunt	pfgzInI1	David Lunt	Ředitel	dlunt,lunt	vsichni,obchod

Tabulka 13.2 Importovaná data — oddělovačem je středník

Pokud jako oddělovač použijeme čárku, potom je třeba použít oddělovače pro položky `MailAddress` a `Groups`, protože jednotlivé položky v nich jsou odděleny čárkami. Jako oddělovač lze použít buď uvozovky `"..."` nebo apostrofy `'...'`. Tabulka 13.3 zobrazuje verzi s uvozovkami.

Po vytvoření CSV souboru je postup následující:

1. Spustíme *Kerio Administration Console*.

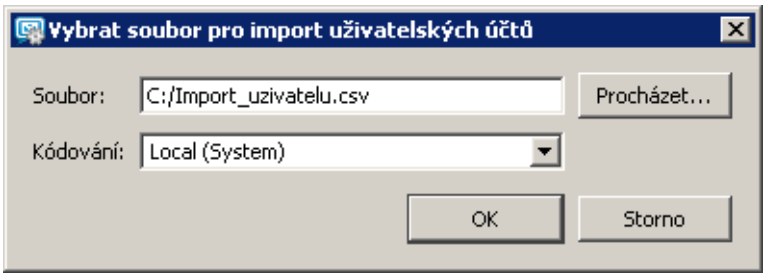
2. V sekci *Nastavení domény* → *Uživatelské účty* klikneme na tlačítko *Importovat* a

Name	Password	FullName	Description	MailAddress	Groups
jnovak	VbD66op1	Jan Novák	Vývoj	jnovak	"cteni, vsichni"
jcerny	Ahdpppu4	Josef Černý	Obchod	"jcerny,cerny"	"obchod, vsichni"
anova	SpoiuS158	Alena Nová	Asistentka ředitele	"anova,alena.nova"	"vsichni"
dlunt	pfgzInI1	David Lunt	Ředitel	"dlunt,lunt"	"vsichni,obchod"

Tabulka 13.3 Importovaná data — oddělovačem je čárka

vybereme volbu *Importovat ze souboru ve formátu CSV*.

3. Otevře se dialog (viz obrázek 13.20), kam zadáme cestu k souboru a nastavíme typ kódování, ve kterém jsou data uložena (ve většině případů stačí nechat v položce standardní *Local (System)*).



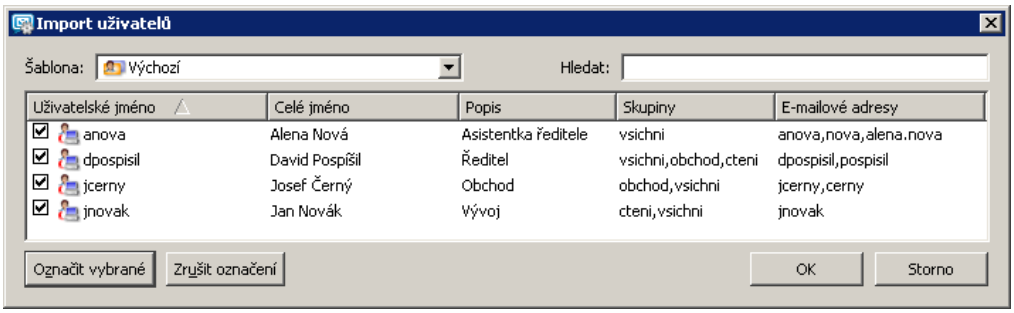
Obrázek 13.20 Import ze souboru — výběr souboru

4. Klikneme na tlačítko *OK* a počkáme, až se soubor načte. Otevře se dialog *Import uživatelů*, kde se zobrazí seznam všech uživatelů, kteří byli uloženi v CSV souboru (viz obrázek 13.21).

   Pokud se nepodaří data načíst, důvody mohou být následující:

   - Soubor není uložen ve formátu CSV.
   - Sloupce v souboru nejsou správně označeny nebo nejsou označeny vůbec. CSV soubor musí obsahovat úvodní řádek s názvy sloupců, jinak *Kerio MailServer* data nepřečte.
     Správně:
     ```
     Name;Password;FullName;MailAddress
     jnovak;VbD66op1;Jan Novák;jnovak
     jcerny;Ahdpppu4;Josef Černý;jcerny,cerny
     ```
     Špatně:
     ```
     jnovak;VbD66op1;Jan Novák;jnovak
     jcerny;Ahdpppu4;Josef Černý;jcerny,cerny
     ```

- Oddělovače pro data jsou použity nesprávným způsobem. Správný postup pro oddělení dat je popsán výše.



Obrázek 13.21 Import ze souboru — importovaní uživatelé

5. Zaškrtneme všechny uživatele, kteří mají být importováni. Pokud je třeba označit velké množství uživatelů, mohou nám při práci pomoci tlačítka *Označit vybrané* a *Zrušit označení*, která jsou umístěna vlevo dole pod seznamem uživatelů.
   - *Označit vybrané* — po použití tlačítka budou označeni všichni uživatelé, kteří byli vybráni kurzorem myši (pomocí kláves `Shift` a `Ctrl`).
   - *Zrušit označení* — všem uživatelům, kteří již byli označeni, se označení zruší.
6. Pokud máme nastavenou šablonu pro vytváření poštovních schránek, vybereme ji v menu *Šablona*. Pokud připravenou šablonu nemáme, ponecháme výchozí nastavení.

   Pokud nevíte co je šablona a k čemu se používá, popis najdete v sekci 13.12.
7. Po výběru uživatelů pro import stačí nastavení potvrdit tlačítkem *OK*.

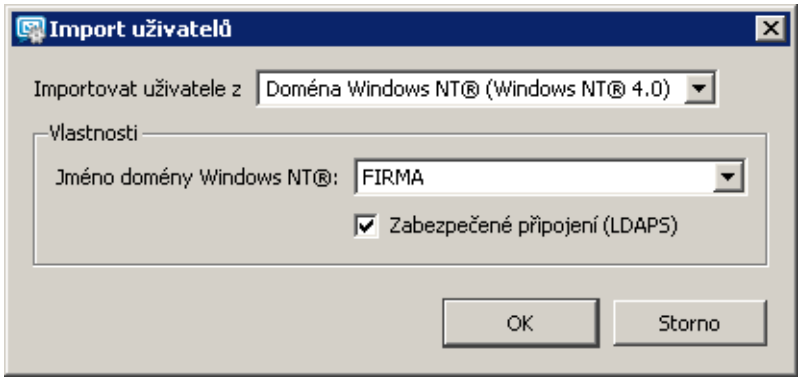
NT doména (Windows NT 4.0)

Volba *Importovat uživatele z* umožňuje vybrat zdroj, z něhož budou uživatelé importováni. V našem případě to bude možnost *Doména Windows NT (Windows NT 4.0)*.

V tomto případě stačí uvést jediný parametr — *Jméno NT domény*. Počítač, na němž *Kerio MailServer* běží, musí být přidán do této domény.

Nepoužívejte tento způsob importu uživatelů, jestliže doménový server běží pod operačním systémem Windows 2000! V tomto případě proveďte vždy import z *Active Directory* — viz dále.

Upozornění: Import uživatelů z NT domény funguje pouze je-li *Kerio MailServer* nainstalován na platformě *MS Windows*.



Obrázek 13.22 Import uživatelů z NT domény

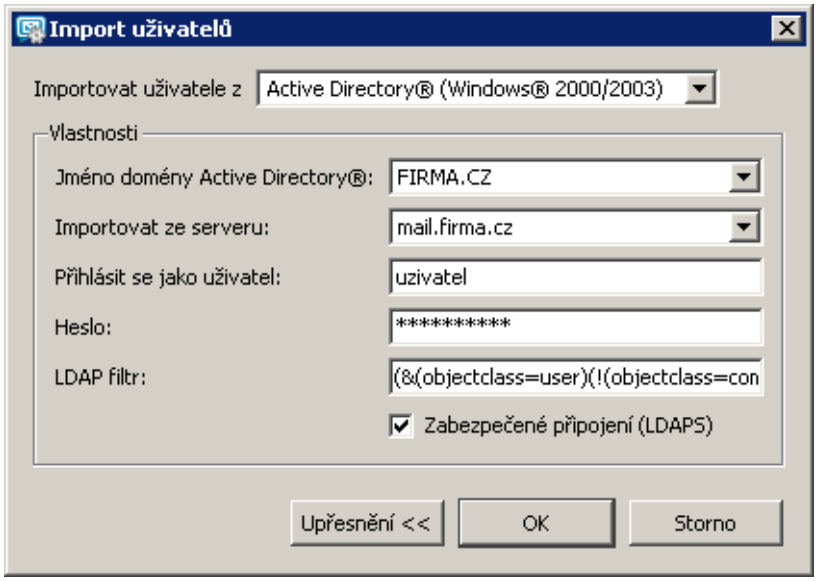
Při importu uživatelských účtů z LDAP databáze do *Kerio MailServeru* jsou posílána i data velmi citlivá na bezpečnost (například uživatelská hesla). Z toho důvodu je možné komunikaci zabezpečit SSL šifrováním.

Active Directory

Volba *Importovat uživatele z* umožňuje vybrat zdroj, z něhož budou uživatelé importováni. V našem případě to bude možnost *Active Directory (Windows 2000/2003)*.

Pro import uživatelů z *Microsoft Active Directory* je třeba specifikovat následující údaje:

- *Jméno Active Directory domény* — název domény, z níž mají být uživatelé importováni (zadává se jako DNS doména — tedy např. `domena.cz`)
- *Importovat ze serveru* — název serveru, na němž služba *Active Directory* pro danou doménu běží.
  Má-li služba LDAP(S) nastaven nestandardní port, je možno název serveru doplnit i s příslušným portem (např.: `mail1.firma.cz:12345`).
- *Přihlásit se jako uživatel*, *Heslo* — jméno a heslo uživatele, který má v této doméně vytvořen účet. Pro ukládání a změny nastavení je třeba právo zápisu.
- *LDAP filtr* — položka se objeví pouze po kliknutí na tlačítko *Upřesnění*. Umožňuje úpravu dotazu na LDAP server, ze kterého budou uživatelé importováni. Využití této možnosti doporučujeme pouze zkušeným administrátorům. Bližší podrobnosti k syntaxi dotazu lze nalézt v manuálu ke konkrétnímu LDAP serveru.
- Při importu uživatelských účtů z LDAP databáze do *Kerio MailServeru* jsou posílána i data velmi citlivá na bezpečnost (například uživatelská hesla). Z toho důvodu je možné komunikaci zabezpečit SSL šifrováním.



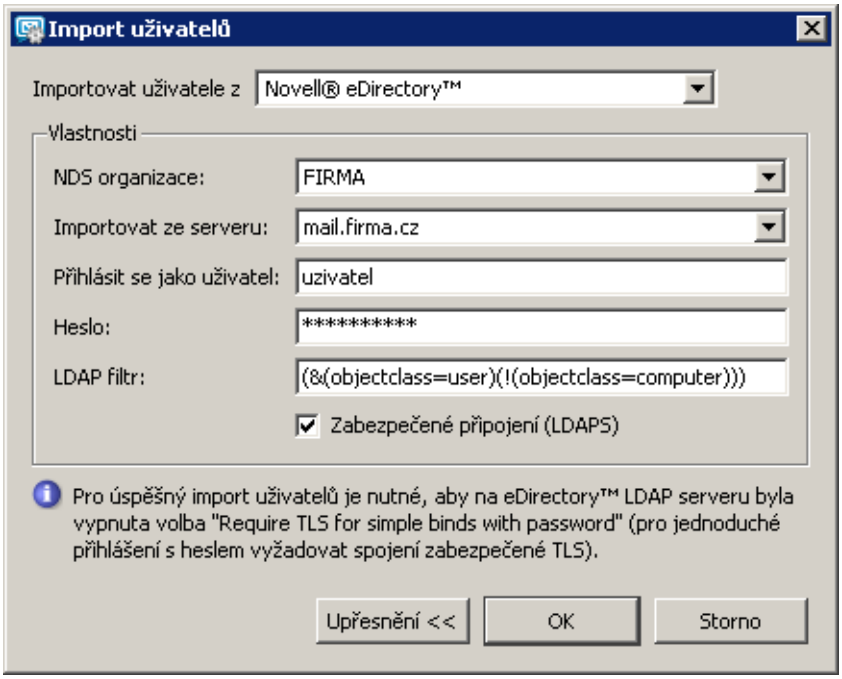
Obrázek 13.23 Import uživatelů z Active Directory

Novell eDirectory

Volba *Importovat uživatele z* umožňuje vybrat zdroj, z něhož budou uživatelé importováni. V našem případě to bude možnost *Novell eDirectory*.

Pro import uživatelů z *Novell eDirectory* je nutné zadat tyto údaje:

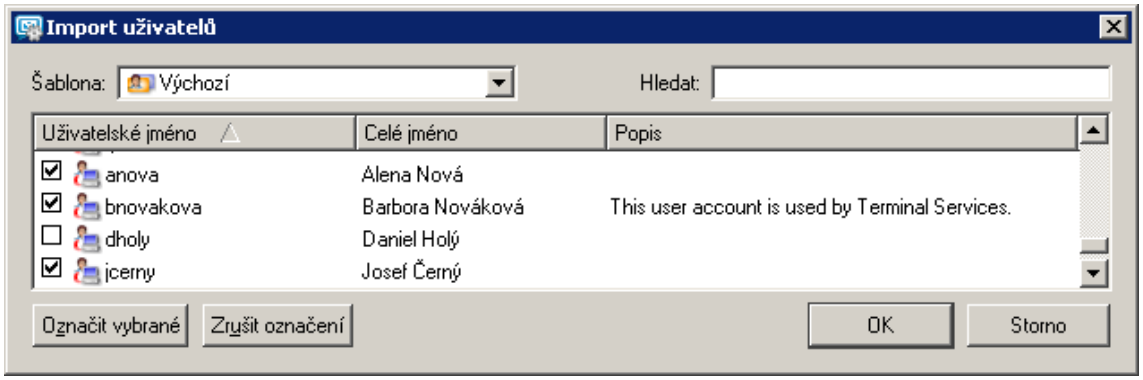
- *NDS organizace* — název NDS organizace, z níž mají být uživatelé importováni.
- *Importovat ze serveru* — název nebo IP adresa serveru, na němž služba pro danou doménu běží.
  Má-li služba LDAP(S) nastaven nestandardní port, je možno název serveru doplnit i s příslušným portem (např.: `mail1.firma.cz:12345`). Pouze *Kerio Administration Console* pro *Mac OS X* obsahuje pro tyto účely volbu *Zabezpečené připojení (LDAPS)*.
- *Přihlásit se jako uživatel*, *Heslo* — jméno a heslo uživatele, který má v této doméně vytvořen účet. Pro ukládání a změny nastavení je třeba právo zápisu.
- *LDAP filtr* — položka se objeví pouze po kliknutí na tlačítko *Upřesnění*. Umožňuje úpravu dotazu na LDAP server, ze kterého budou uživatelé importováni. Využití této možnosti doporučujeme pouze zkušeným administrátorům. Bližší podrobnosti k syntaxi dotazu lze nalézt v manuálu ke konkrétnímu LDAP serveru.
- Při importu uživatelských účtů z LDAP databáze do *Kerio MailServeru* jsou posílána i data velmi citlivá na bezpečnost (například uživatelská hesla). Z toho důvodu je možné komunikaci zabezpečit SSL šifrováním.



Obrázek 13.24 Import uživatelů z Novell eDirectory

Výběr uživatelů

Jsou-li splněny všechny předpoklady (byly zadány správné údaje, příslušný server je dostupný atd.), pak se po stisknutí tlačítka *OK* zobrazí seznam uživatelů (viz obrázek 13.25):



Obrázek 13.25 Výběr uživatelů pro import

1. Zaškrtneme uživatele, které chceme do *Kerio MailServeru* importovat.

2. Pokud máme nastavenou šablonu pro vytváření poštovních schránek, vybereme ji v menu *Šablona*. Pokud připravenou šablonu nemáme, ponecháme výchozí nastavení.

   Pokud nevíte co je šablona a k čemu se používá, popis najdete v sekci 13.12.

3. Stiskneme tlačítko *OK*.

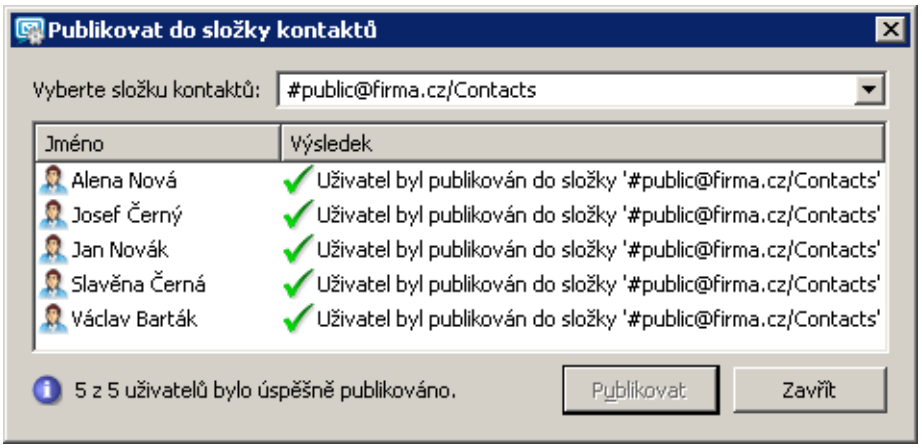
Poznámky:

- Při importu uživatelů z *Active Directory* nezáleží na platformě, na které je *Kerio MailServer* nainstalován.
- Importovaným uživatelům bude nastaven typ ověřování podle toho, odkud byli importováni: *Doména Windows NT* uživatelům z NT domény a *Kerberos 5* uživatelům z *Active Directory*.

13.11 Publikace uživatelů do adresáře

Informace o vybraných uživatelích (nezáleží na tom, zda se jedná o lokální účty či účty v adresářové službě) je možno publikovat do veřejného adresáře, tj. do některé z veřejných složek typu *Kontakty*. K tomuto účelu slouží tlačítko *Publikovat* (vpravo dole pod seznamem uživatelských účtů). Tlačítko je standardně neaktivní, nejprve je třeba kurzorem označit uživatele, kteří mají být publikováni.

Po použití tlačítka *Publikovat* se zobrazí dialog pro výběr složky, do níž budou údaje o uživatelích publikovány. Zároveň dialog formou seznamu zobrazuje všechny uživatele, kteří byli k exportu vybráni (viz obrázek 13.26).



Obrázek 13.26 Export uživatelů

Pokud žádná veřejná složka kontaktů dosud neexistuje, nabídne se složka `#public@domena/Contacts`, která bude při první publikaci automaticky vytvořena.

Publikovanými údaji jsou pouze celé jméno a e-mailová adresa uživatele (ostatní parametry uživatelského účtu nemají v adresáři smysl). Ostatní údaje může doplnit uživatel s příslušnými právy např. pomocí rozhraní *Kerio WebMail*.

Poznámka: Publikaci uživatelů do adresáře může provést kterýkoliv uživatel s administračními právy ke *Kerio MailServeru* (viz kapitolu 13.2). Na právech k veřejným složkám v tomto případě nezáleží.

Po provedení publikace uživatelů je v dialogu zobrazen výsledek (viz obrázek 13.26).

13.12 Šablony uživatelských účtů

Šablony slouží pro usnadnění vytváření většího počtu uživatelských účtů (typicky uživatelé v jedné doméně). V šabloně je možno definovat všechny parametry účtu kromě uživatelského jména a hesla (pokud se používá interní ověřování). Uživatelské účty lze pak definovat s použitím vytvořené šablony, přičemž stačí vyplnit pouze položky *Jméno*, *Celé jméno* a *Popis* (příp. *Heslo* a *Potvrzení hesla*). Položky *Celé jméno* a *Popis* jsou nepovinné. V nejjednodušším případě tedy stačí vyplnit jedinou položku — *Jméno*.

Definice šablony

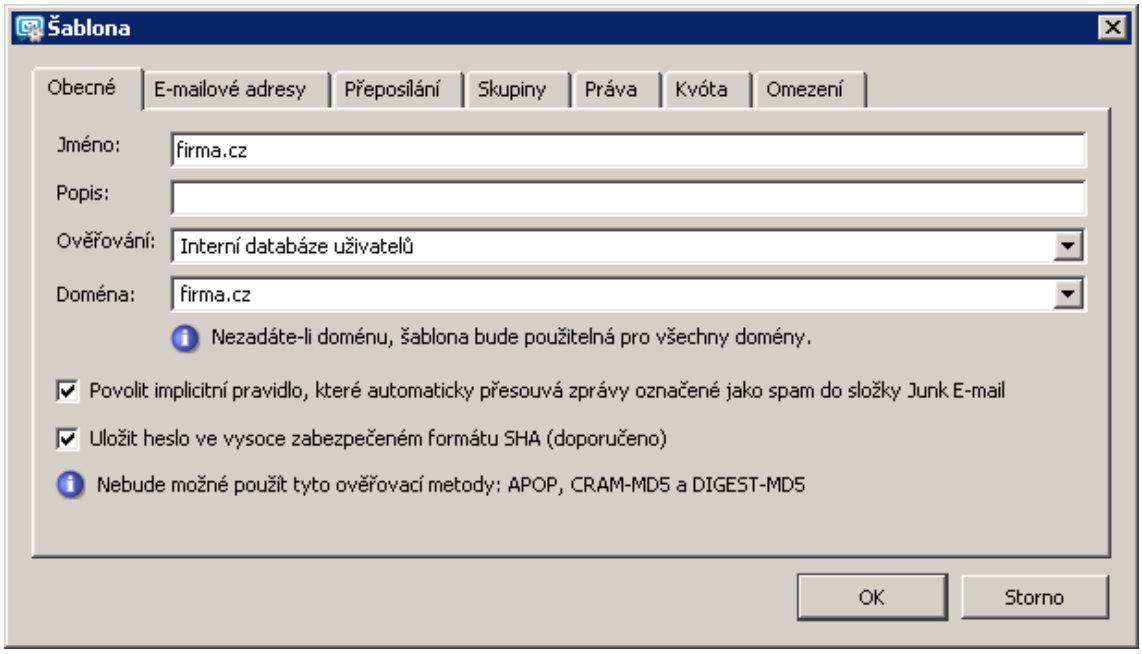
Definice šablony se provádí v sekci *Konfigurace* → *Definice* → *Šablony uživatelů*. Dialog pro přidání či změnu šablony je téměř shodný s dialogem pro vytvoření uživatelského účtu.

Jméno
: Název šablony (jednoznačné jméno, kterým bude šablona identifikována).

Popis
: Tato položka má dvojí význam. Jednak představuje popis šablony, který se zobrazuje vedle jejího názvu v seznamu šablon, a jednak se kopíruje do položky *Popis* uživatelského účtu, který je podle této šablony vytvořen.

Ověřování
: Způsob ověřování uživatele (více viz kapitolu 13.2).

Doména
: Výběr domény, pro kterou bude tato šablona použita. Zde je možno vybrat některou z lokálních domén, které jsou v *Kerio MailServeru* definovány, nebo doménu nespecifikovat. Není-li doména specifikována, může být šablona použita pro vytvoření uživatelského účtu v libovolné doméně (tzv. obecná šablona).



Obrázek 13.27 Založení šablony

Povolit implicitní pravidlo ...

Zapnutím volby se bude veškerý rozpoznaný spam automaticky přesouvat do složky určené pro nevyžádanou poštu.

Uložit heslo ve vysoce zabezpečeném ...

Heslo uživatele je standardně šifrováno symetrickým klíčem (DES). Volba *Uložit heslo v bezpečnějším formátu* umožňuje použití bezpečnější, nesymetrické šifry (SHA řetězec), a tudíž nelze žádným způsobem heslo znovu přečíst. Nevýhodou SHA šifrování je, že není možné využít některé metody ověřování pro přístup na *Kerio MailServer*, konkrétně jsou to metody APOP, CRAM-MD5 a Digest-MD5. Pro ověřování přístupu lze tedy využít pouze metody PLAIN a LOGIN, které ovšem žádným způsobem nešifrují heslo, z toho důvodu důrazně doporučujeme používat pro přihlašování uživatelů k serveru pouze SSL spojení.

Po zaškrtnutí volby je nutné změnit heslo uživatele. To může udělat buď administrátor nebo uživatel (např. přes rozhraní *Kerio WebMail* nebo jakéhokoliv e-mailového klienta).

Všechny ostatní položky v tomto dialogu jsou shodné s položkami v dialogu pro vytvoření, resp. změnu uživatelského účtu. Hodnoty, které zde budou zadány, budou automaticky doplněny do odpovídajících položek ve vytvářeném účtu. Podrobnosti najdete v kapitole 13.2.

Použití šablony

Vytvořenou šablonu je možno použít přímo při definici uživatelského účtu v sekci *Nastavení domény* → *Uživatelské účty*. Je-li definována alespoň jedna šablona, zobrazí se po stisknutí tlačítka *Přidat* v prvním kroku průvodce možnost výběru šablony.

V dialogu průvodce se zobrazí pouze ty šablony, které byly vytvořeny pro danou doménu, nebo šablony, v nichž není doména specifikována (obecné šablony). Volba *Žádná šablona* znamená, že se pro definici účtu nepoužije žádná šablona (většina položek bude prázdná nebo bude mít nastaveny výchozí hodnoty).

Po výběru šablony se otevře průvodce vytvořením uživatelského účtu, v němž budou do jednotlivých položek dosazeny příslušné hodnoty z použité šablony. Podrobnosti najdete v kapitole 13.2.

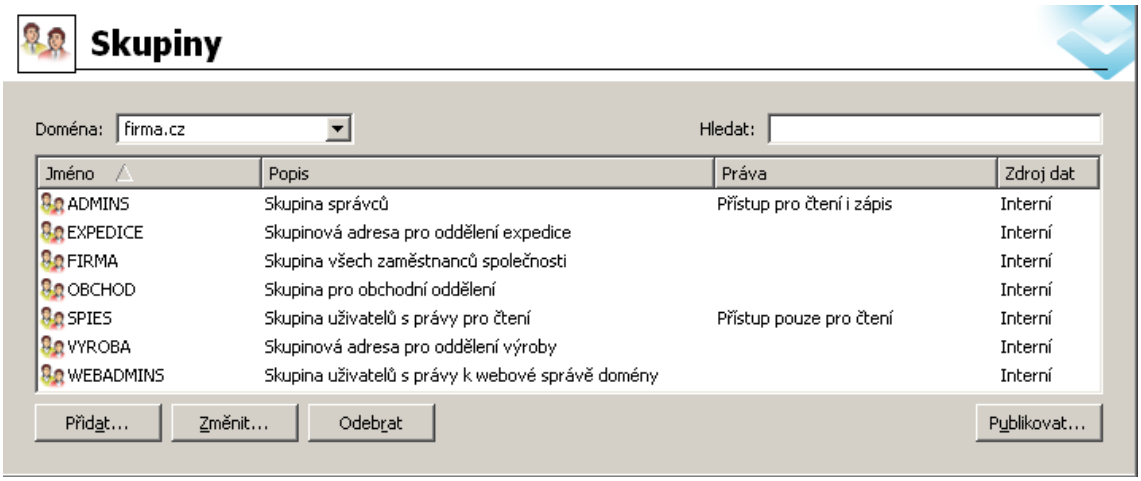
Kapitola 14

Skupiny uživatelů

Uživatelské účty v rámci každé domény je možno řadit do skupin. Hlavní důvody vytváření skupin uživatelů jsou následující:

- Pro skupiny uživatelů mohou být pomocí aliasů vytvořeny tzv. skupinové adresy — e-mail poslaný na tuto adresu bude doručen všem členům skupiny.
- Skupině uživatelů mohou být nastavena specifická přístupová práva. Tato práva doplňují práva jednotlivých uživatelů.

Definice skupin uživatelů se provádí v sekci *Nastavení domény* → *Skupiny*.



Obrázek 14.1 Skupiny

Pole *Hledat* a tlačítko *Publikovat* splňují stejnou funkci jako v sekci *Uživatelé* a jejich bližší popis najdete v kapitolách 13.6 a 13.11.

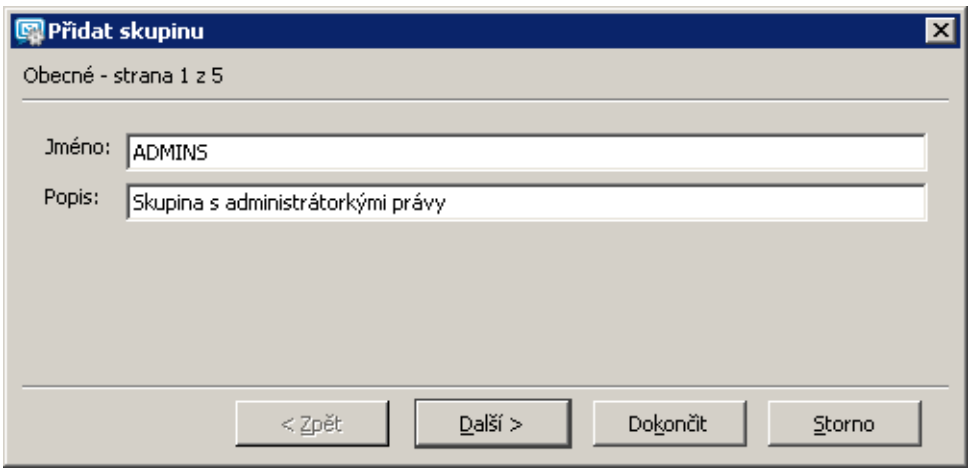
14.1 Vytvoření skupiny uživatelů

Novou skupinu uživatelů lze vytvořit tlačítkem *Přidat*. Po jeho stisknutí se zobrazí průvodce vytvořením skupiny uživatelů.

Krok 1 — název a popis skupiny

Jméno

Název skupiny (jednoznačně identifikuje skupinu).



Obrázek 14.2 Založení skupiny — obecné údaje

Popis

Textový popis skupiny (má pouze informativní charakter, může obsahovat libovolné informace nebo zůstat prázdný).

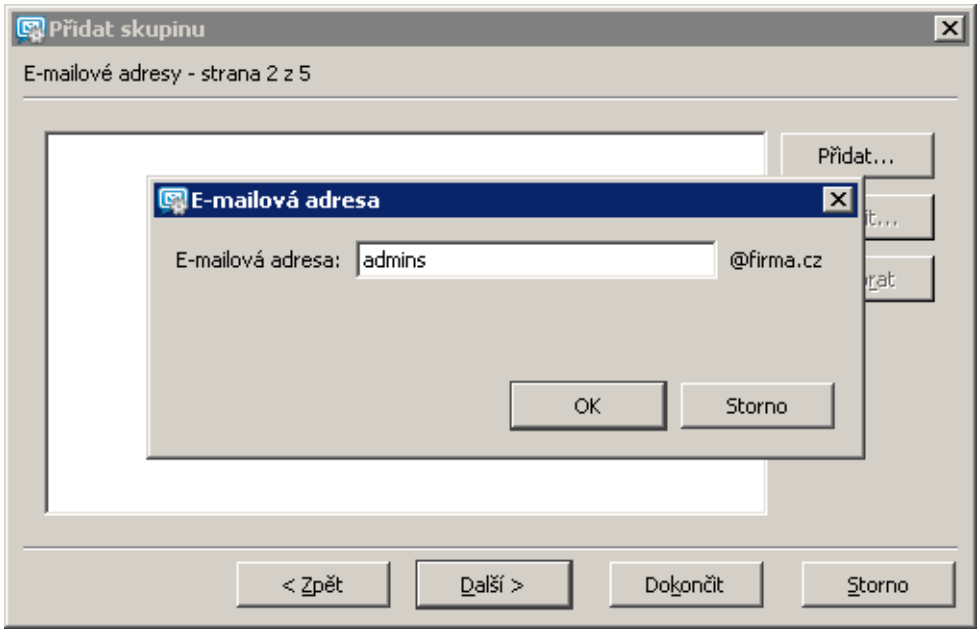
Poznámka: Tlačítkem *Dokončit* lze průvodce vytvořením skupiny v kterékoliv fázi ukončit. Skupina se vytvoří, přičemž do položek, které byly „přeskočeny“, budou dosazeny výchozí hodnoty.

Krok 2 — e-mailové adresy

V tomto kroku průvodce je možno zadat všechny požadované e-mailové adresy (aliasy) dané skupiny. Skupina nemusí mít přiřazenu žádnou adresu (na rozdíl od uživatelského účtu není automaticky vytvářena adresa ze jména skupiny a domény, v níž je skupina definována).

Adresy skupiny lze zadávat přímo v definici skupiny, nebo v sekci *Nastavení domény* → *Aliasy*. Doporučujeme však zadávat aliasy přímo v definici skupiny — je to jednodušší a přehlednější.

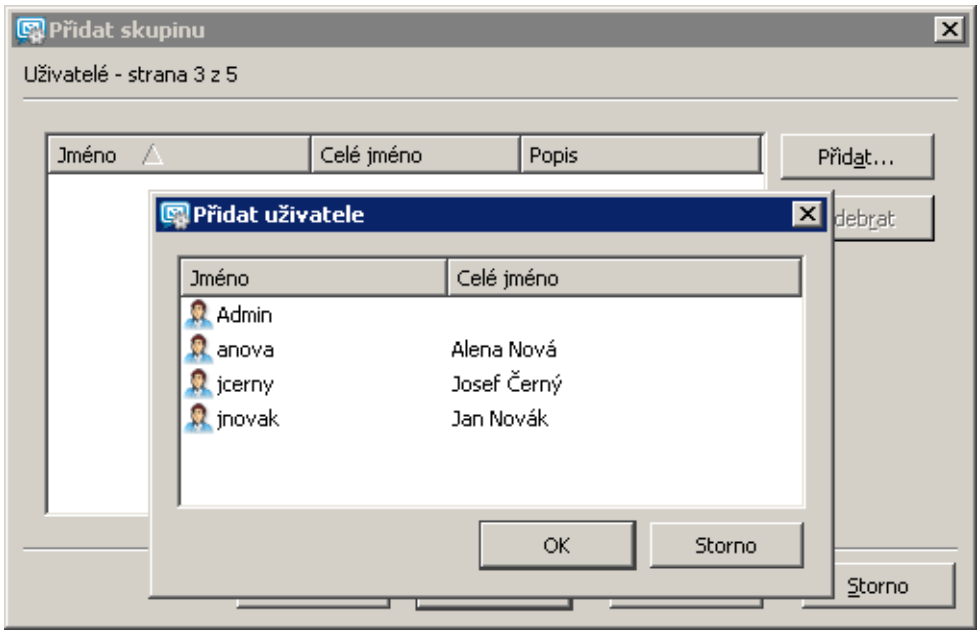
Poznámka: Jsou-li uživatelské účty a skupiny udržovány v *Active Directory* (viz kapitola 7.6), pak je možné zadávat jejich aliasy přímo v panelu *Active Directory Users and Computers*. Globální aliasy (tj. v sekci *Nastavení domény* → *Aliasy*) takto zadávat nelze.



Obrázek 14.3 Založení skupiny — přidělení e-mailových adres

Krok 3 — členové skupiny

Tlačítky *Přidat* a *Odebrat* lze přidat či odebrat uživatele do/z této skupiny. Nejsou-li uživatelské účty dosud vytvořeny, může skupina zůstat prázdná a uživatelé do ní mohou být zařazeni při definici účtů (viz kapitolu 13.2).

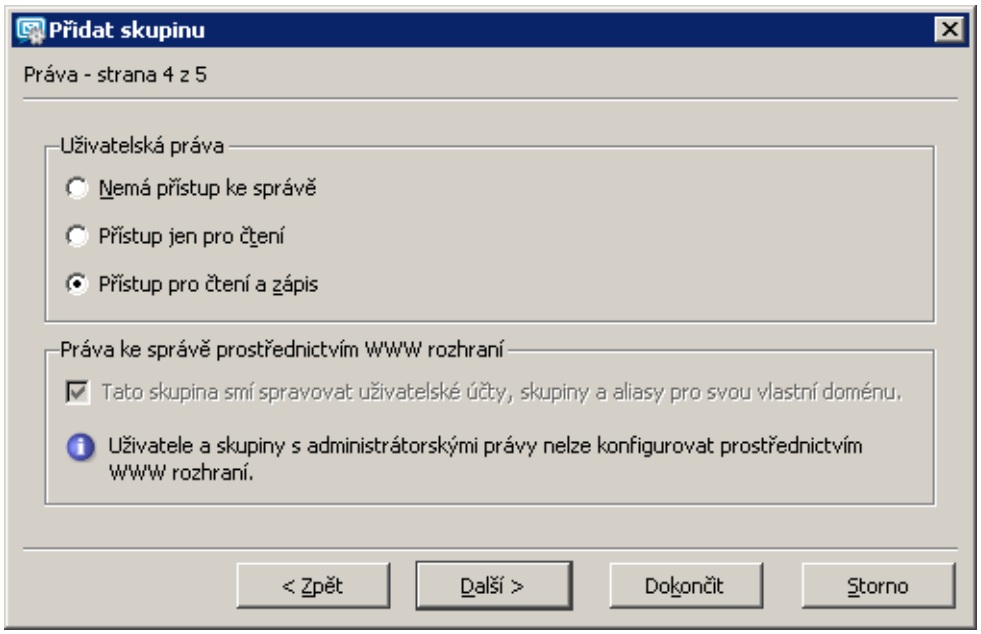


Obrázek 14.4 Založení skupiny — přidání uživatelů

Krok 4 — nastavení přístupových práv

Skupina má vždy nastavenu jednu ze tří úrovní přístupových práv:

Bez přístupu ke správě
Uživatelé v této skupině nemají práva pro přihlášení ke správě *Kerio MailServeru*.



Obrázek 14.5 Založení skupiny — nastavení uživatelských práv

Přístup jen pro čtení
Uživatelé v této skupině se mohou přihlásit ke správě *Kerio MailServeru*, mohou však pouze prohlížet záznamy a nastavení, nemají právo provádět žádné změny.

Přístup pro čtení a zápis
Uživatelé v této skupině mají plná práva ke správě.

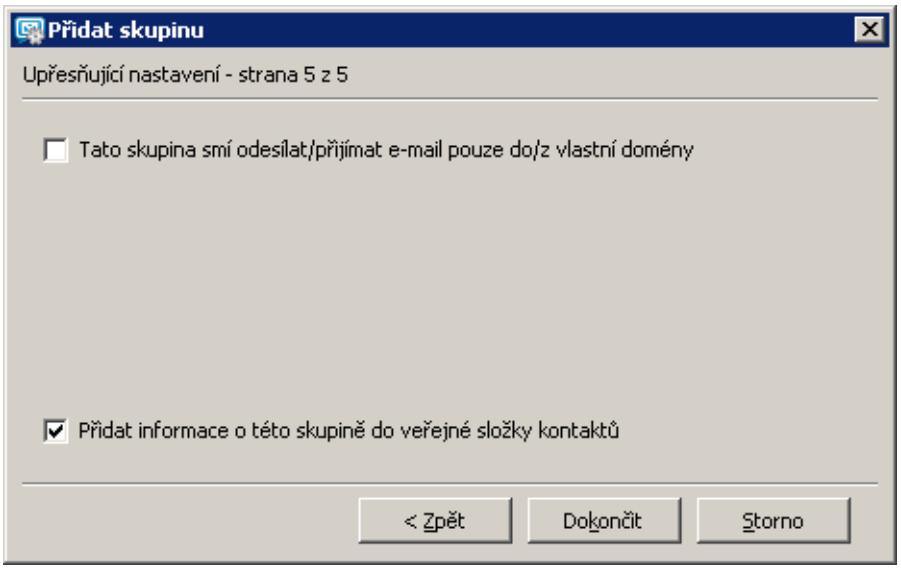
Tato skupina smí spravovat uživatelské účty, ...
Speciální právo pro přístup do *Kerio Web Administration* (více viz kapitolu 31). Toto oprávnění je nezávislé na nastavení přístupových práv do *Kerio Administration Console*.

Přístupová práva skupiny se kombinují s vlastními právy uživatele — výsledná práva uživatele tedy odpovídají buď jeho vlastním právům, nebo právům skupiny, podle toho, která práva jsou vyšší.

Krok 5 — upřesňující nastavení

Tato skupina smí přijímat/odesílat zprávy ...

Volba umožňuje správci *Kerio MailServeru* omezit komunikaci pro všechny členy skupiny pouze na úroveň lokální domény. To může být v mnoha společnostech užitečné například při řešení vnitro firemní komunikace. Zaškrtnutím této volby docílíme, že žádný z uživatelů dané skupiny nebude moci odeslat ani přijmout zprávu z žádné externí domény.



Obrázek 14.6 Založení skupiny — přidání kontaktů uživatelů do veřejné složky

Přidat informace o této skupině ...

Volba přidá/nepřidá skupinu a její případnou elektronickou adresu do složky s veřejnými kontakty.

Kapitola 15

Odesílání a příjem pošty

15.1 Doručování pošty v síti Internet

Pro pochopení problematiky správného nastavení vašeho poštovního serveru je nutno znát základní principy doručování elektronické pošty v Internetu. Tato kapitola obsahuje ve stručné podobě nejdůležitější informace o této problematice. Zkušení síťoví administrátoři mohou tuto kapitolu přeskočit. J

MX záznamy

Pro každou internetovou doménu (např. `firma.cz`) musí být zaneseny příslušné záznamy do DNS (DNS je celosvětová distribuovaná databáze doménových jmen). Jedním z těchto údajů je takzvaný záznam MX (Mail eXchanger neboli poštovní server). Záznamy pro doménu `firma.cz` by mohly vypadat např. takto:

```
firma.cz                MX      10      mail.firma.cz
                        MX      20      smtp.poskytovatel.cz
mail.firma.cz           A               215.75.128.33
smtp.poskytovatel.cz    A               215.75.128.1
```

První dva záznamy říkají, že poštovním serverem s preferencí 10 je počítač `mail.firma.cz` a serverem s preferencí 20 počítač `smtp.poskytovatel.cz`. Preference má význam ceny serveru. Čím nižší preference, tím vyšší bude priorita tohoto serveru — z toho vyplývá, že server `mail.firma.cz` je poštovním serverem domény `firma.cz` s nejvyšší prioritou a server `smtp.poskytovatel.cz` serverem s druhou nejvyšší prioritou pro tuto doménu. MX záznamů pro danou doménu může být definován libovolný počet. Mají-li dva nebo více záznamů stejnou prioritu, pak se náhodně vybírá jeden z těchto serverů (rozdělení zátěže — load balancing).

Druhé dva záznamy již nejsou typu MX, ale typu A (Address). Ty říkají, jakou IP adresu má počítač daného jména (MX záznam totiž nemůže být nastaven na IP adresu, ale pouze na jméno serveru).

Doručení e-mailu

Co se tedy děje s e-mailem na cestě od odesílatele k příjemci?

Poštovní klient odesílatele odešle e-mail na svůj SMTP server. Server zkontroluje adresu příjemce, a pokud je doména na tomto serveru lokální, uloží jej přímo do příslušné schránky. Není-li doména příjemce lokální, SMTP server zjistí z DNS (vyšle DNS dotaz) jméno primárního poštovního (SMTP) serveru cílové domény a pošle e-mail na tento server. Ten jej uloží do schránky, odkud si jej příjemce svým poštovním klientem stáhne a přečte.

Jestliže odesílající SMTP server zjistí, že je primární server cílové domény nedostupný, pokusí se kontaktovat sekundární server (resp. server s nejbližší vyšší preferencí) a odeslat e-mail na něj. Není-li dostupný žádný ze serverů uvedených v MX záznamech pro cílovou doménu, bude odeslání v předdefinovaných intervalech opakovat, a pokud nebude v určitém čase úspěšný, vrátí e-mail odesílateli jako nedoručitelný.

Je-li např. primární server domény nedostupný, a sekundární dostupný, odešle se e-mail na sekundární server. Principiálně tedy může jako sekundární (terciární atd.) server fungovat libovolný SMTP server v Internetu (proč jen principiálně, bude objasněno dále).

Odesílání pošty přes jiný SMTP server (Relaying)

Cesta e-mailu od odesílatele k příjemci může mít ještě druhou podobu. Klient odešle e-mail na svůj SMTP server, který jej předá jinému SMTP serveru a ten jej pak doručí do cílové domény výše popsaným způsobem. Toto předávání veškeré odchozí pošty se nazývá relaying (předávání na nadřazený server).

Výhodou je, že odeslání odchozího e-mailu je jednorázová akce (e-maily navíc mohou být řazeny do fronty a odesílány v určitých intervalech po dávkách). Odesílající SMTP server se nemusí zabývat dotazováním DNS na servery cílových domén, opakováním odeslání v případě nedosažitelnosti cílových serverů atd. Toto je velmi užitečné zejména v případě pomalých a vytáčených linek do Internetu — u vytáčené linky se tím ušetří nemalá částka za připojení.

Většina SMTP serverů v Internetu je ale proti relayingu ochráněna, a to z toho důvodu, aby nemohly být zneužity k rozesílání nevyžádaných e-mailů (spamů). Chcete-li tedy odesílat veškerou poštu přes jiný SMTP server, musíte se dohodnout s jeho správcem, aby relaying povolil (typicky na základě kontroly IP adresy vašeho serveru nebo ověření jménem a heslem).

Příkaz ETRN

ETRN je příkaz SMTP protokolu, který slouží k vyžádání pošty uložené na jiném SMTP serveru. Typicky se používá v následujících případech:

1. Zákazník má vlastní doménu (např. `firma.cz`) a jeho server je do Internetu připojen vytáčenou linkou. Vytáčená linka musí mít přidělenu pevnou IP adresu. Primární MX záznam pro doménu `firma.cz` je nasměrován na SMTP server poskytovatele Internetu (např. `smtp.poskytovatel.cz`). V okamžiku připojení do Internetu vyšle SMTP server zákazníka na primární server příkaz ETRN, který v podstatě říká: „Teď jsem online, pošli mi poštu.“ Má-li primární server nějaké zprávy pro danou doménu, pak mu je pošle. Pokud ne, může vyslat zápornou odpověď, nebo neodpoví vůbec. Server zákazníka musí mít proto nastavenu určitou dobu (timeout), po níž čekání na odpověď primárního serveru ukončí.

   Poznámka: Po přijetí příkazu ETRN naváže primární server nové spojení na server zákazníka a tímto spojením poštu posílá. Je-li tedy server zákazníka chráněn firewallem, je třeba, aby byl do Internetu zpřístupněn (otevřen) port 25.

2. Předpokládejme, že doména `firma.cz` má primární server `smtp.firma.cz` a sekundární server `smtp2.firma.cz`. Oba tyto servery mají trvalé připojení do Internetu. Za normálních okolností jsou všechny zprávy pro tuto doménu posílány na primární server `smtp.firma.cz`. Jestliže dojde k výpadku tohoto serveru (přetížení, přerušená linka apod.), jsou tyto zprávy posílány na sekundární server `smtp2.firma.cz`. Primární server pak může v pravidelných intervalech vysílat na sekundární server příkaz ETRN, čímž si vyžádá uloženou poštu. Průběh komunikace je shodný jako v předchozím případě (podrobný popis nastavení sekundárního SMTP serveru je popsán v samostatné kapitole 27.5).

   Tento způsob vyžádání pošty je rychlejší a spolehlivější než čekání, až sekundární server sám poštu pošle (viz sekci *Doručení e-mailu*). Navíc je příkaz ETRN použitelný i pro vytáčené linky.

Doménový koš

Primární server domény nemusí být vždy server, na němž jsou umístěny schránky lokálních uživatelů. Je-li např. firma, které daná doména patří, připojena do Internetu vytáčenou linkou, může mít u poskytovatele Internetu zřízen tzv. doménový koš, což je jedna schránka, do níž se ukládá pošta pro celou doménu. Koncový poštovní server pak může tuto schránku vybírat (v časech či intervalech dle potřeby) a poštu třídit do jednotlivých lokálních schránek. V MX záznamech pro tuto doménu je pak jako primární server uveden SMTP server poskytovatele, u něhož je doménový koš umístěn.

Doménový koš přijímá zprávy z Internetu přes SMTP protokol. Každá zpráva tedy obsahuje jak tělo, tak i SMTP obálku. Doménový koš přijímá pouze tělo zprávy. Informace z obálky se zkopírují do některé z hlaviček zprávy (záleží na nastavení doménového koše).

Kerio MailServer se přihlásí a ověří do doménového koše. Poté zprávy protokolem POP3 stáhne a začne je třídit podle třídicích pravidel nastavených v *Kerio MailServeru*. Aby se zpráva správně zatřídila, musí obsahovat informaci o příjemci (buď v některé ze speciálních hlaviček nebo v položkách *To* či *Cc*). Pokud zpráva žádnou informaci o příjemci neobsahuje, bude systémem vrácena odesílateli. Pouze v případě, že je v *Kerio MailServeru* nastaveno speciální třídicí pravidlo (kapitola 15.4), budou se zprávy bez příjemce ukládat v nastavené schránce.

Poznámka: Pro třídění pošty doporučujeme nastavit speciální hlavičku `X-Envelope-To:`, protože tato hlavička obsahuje přesné informace o příjemcích. Nemůže se potom stát, že zpráva pro více příjemců přijde každému tolikrát, kolik příjemců zpráva obsahuje.

Přístup poštovních klientů k uživatelským schránkám

Ke svým poštovním schránkám mohou uživatelé přistupovat různými způsoby:

POP3

POP3 (Post Office Protocol version 3) je internetový protokol navržený pro stahování pošty ze serveru na jiný server (viz sekci *Doménový Koš*) nebo na poštovního klienta. POP3 protokol je definován v RFC 1939.

POP3 protokol pracuje na bázi klient-server. Komunikaci vždy navazuje klient, dále se dotazy klienta a odpovědi serveru pravidelně střídají, dokud nedojde k ukončení komunikace. Jakmile klient inicializuje komunikaci a provede autentizaci (ověření jménem a heslem), je možné s poštou začít pracovat (stahovat ji na klienta, mazat ji, a podobně).

Kerio MailServer běžně funguje jako server, ale v případě, že stahuje poštu ze vzdálených POP3 schránek, může fungovat také jako klient.

POP3 protokol je dnes již poněkud jednoduchý a zastaralý. Umí v podstatě pouze stáhnout poštu do klientské aplikace, umí pracovat pouze s jednou složkou (INBOX). To znamená, že pokud uživatel přesune v klientovi zprávu do jiné složky, bude tato zpráva ze serveru přesunuta (de facto smazána). Obdobně se mailbox chová i v opačném případě. Pokud uživatel má na serveru přístup k více složkám a zprávu z Inboxu přesune do jiné složky, tak se zpráva do klientské aplikace nemůže stáhnout. Obecně lze říci, že je doporučováno využívat pro práci s poštou modernější protokol IMAP. Výhody protokolu IMAP jsou zjevné zejména ze srovnávací tabulky 15.1.

Jedinou výhodou použití tohoto protokolu může být ušetření místa na disku serveru. Uživatelé si svou poštu stáhnou lokálně na disk a zde si ji mohou roztřídit do složek, mazat ji, atd. Z toho důvodu jsou POP3 účty využívány zejména v případě freemailových služeb, kde mohou uživatelé využívat schránku o několika MB a poštu si více méně pravidelně stahují lokálně na svůj disk. Další výhodou může být snadná možnost práce offline, kterou lze využít v případě časově omezeného připojení do Internetu. Dnes však již téměř všichni poštovní klienti umí pracovat v režimu offline jak s účty typu POP3, tak s IMAP účty.

IMAP

IMAP (Internet Mail Access Protocol) je internetový protokol používaný, stejně jako protokol POP3, pro připojení k poštovnímu serveru a čtení nebo jiné manipulaci s poštou. IMAP protokol je definován v RFC 3501.

Protokol IMAP umožňuje uživatelům nejen stahování pošty na svůj počítač (do svého e-mailového klienta), ale také správu účtu přímo na serveru. Díky tomu je možné k účtu přistupovat z různých klientských stanic. Na rozdíl od protokolu POP3 nechává protokol IMAP poštu na serveru a přímo tam lze zprávy s pomocí poštovního klienta číst, rušit a ukládat do nově vytvořených složek, tak jako by byla schránka uložena přímo na disku klienta. Zároveň je možné mít poštu uloženou v poštovním klientovi. Toto řešení je žádoucí především tehdy, pokud uživatel používá časově omezené připojení do Internetu, nebo je z jiných důvodů připojen k serveru jen někdy a je nutné mít k dispozici svou poštu offline. Po opětovném připojení k síti se složky na serveru a klientovi synchronizují.

Dalším ne nepodstatným rozdílem mezi protokoly POP3 a IMAP je možnost manipulace se zprávami již během stahování pošty do lokálního úložiště. V případě protokolu IMAP se totiž nejprve stáhnou hlavičky e-mailů a uživatel si tak může vybrat, který si chce přečíst jako první. Po označení vybrané zprávy dostane tato zpráva prioritu ve stahování na klienta a je možné ji přečíst nebo přesunout do jiné složky nebo cokoliv jiného, zatímco jsou stahovány ostatní zprávy.

Přístup přes rozhraní MAPI (MS Outlook)

Kerio MailServer umožňuje přístup k poště přes rozhraní MAPI. MAPI (Messaging Application Programming Interface) je univerzální rozhraní pro přenos zpráv, které vyvinula společnost Microsoft. Je to softwarové rozhraní, které umožňuje libovolnému MAPI klientskému programu komunikovat s libovolným poštovním serverem (v našem případě *MS Outlook — Kerio MailServer*).

Aby byla komunikace přes rozhraní MAPI umožněna, společnost *Kerio Technologies* vyvinula speciální aplikaci *Kerio Outlook Connector*, která se instaluje na klienta a funguje jako rozšíření aplikace *MS Outlook*. *MS Outlook* s *Kerio Outlook Connectorem* pracuje s poštou stejným způsobem jako protokol IMAP, ale obsahuje řadu možností navíc.

Díky této úpravě je *MS Outlook* schopen ve spolupráci s *Kerio MailServerem* pra-

POP3	IMAP
nešifrovaný i šifrovaný (POP3S)	nešifrovaný i šifrovaný (IMAPS)
umožňuje autorizaci	umožňuje autorizaci
pracuje pouze s jednou složkou	umožňuje manipulaci se složkami (například přesouvání zpráv z jedné složky do druhé) a všechny složky jsou vytvářeny a uchovávány přímo na serveru
stahuje celou zprávu (zprávy se zobrazují postupně jak jsou stahovány ze serveru)	stahuje nejprve hlavičky zprávy, a teprve poté i těla zpráv
synchronní (v době stahování pošty s ní není možné nijak manipulovat, je třeba počkat, až bude k dispozici lokálně na disku)	asynchronní (při stahování pošty není zablokována práce s jednotlivými zprávami)
k účtu může přistupovat pouze jeden klient	k účtu může přistupovat více klientů zároveň

Tabulka 15.1 Srovnání protokolů POP3 a IMAP

covat s groupwarovými daty (kontakty, kalendáři, úkoly a poznámkami) uloženými v úložišti *Kerio MailServeru*. Hlavní výhodou společného úložiště dat je jejich dostupnost odkudkoli, kde je k dispozici Internet. Pro přístup k datům stačí Internet a internetový prohlížeč (rozhraní *Kerio WebMail*) nebo *MS Outlook* s *Kerio Outlook Connectorem*.

MS Outlook s *Kerio Outlook Connectorem* také umožňuje lepší plánování schůzek a úkolů (*Free/Busy* kalendář) a sdílení různých typů dat mezi uživateli (sdílené a veřejné složky).

O *Kerio Outlook Connectoru* se dozvíte více v kapitole 32.2.

Přístup přes rozhraní WebDAV (MS Entourage)

Kerio MailServer podporuje rozhraní WebDAV (Web Distribution Authoring and Versioning), přes které lze také přistupovat k poštovním účtům. WebDAV je rozhraní rozšiřující protokol HTTP o možnost skupinově editovat a spravovat soubory umístěné na serverech.

Podpora rozhraní WebDAV v *Kerio MailServeru* umožňuje připojení poštovního klienta *MS Entourage*. *MS Entourage* je poštovní klient ze sady *MS Office 2004 for Mac*, který dovede pro připojení k poštovnímu serveru využívat protokoly POP3, IMAP a rozhraní WebDAV.

Uživatel, který se chce připojit klientem *MS Entourage* ke *Kerio MailServeru*, může využít speciální rozhraní původně určené pro komunikaci s *MS Exchange*. Toto spe-

ciální rozhraní označované v *MS Entourage* jako účet typu *Exchange* je založeno na WebDAV komunikaci.
Rozhraní WebDAV v *MS Entourage* poskytuje podobné možnosti jako *Kerio Outlook Connector*. To znamená, že kromě práce s elektronickou poštou umožňuje také pracovat s groupwarovými daty (pošta, kalendář, kontakty a veřejné složky), umí využívat *Free/Busy* server, atd.
Ve starších verzích se pro přístup k poště využíval protokol IMAP a pro ostatní typy složek rozhraní WebDAV. *MS Entourage 2004* však již používá WebDAV i pro přístup k poštovním složkám.
Podpora pro spolupráci *Kerio MailServeru* a *MS Entourage* je přímá. To znamená, že se na klientské stanice nemusí instalovat žádná rozšiřující aplikace, pouze je nutné správně nastavit základní parametry účtu pro *Exchange*.
O *MS Entourage* a jeho správném nastavení se dozvíte více v kapitole 38.

15.2 SMTP server

Nastavení SMTP serveru chrání proti zneužití server na němž *Kerio MailServer* běží.

Ochrana SMTP serveru určuje, kdo a jakým způsobem smí tento server používat a zabraňuje tak jeho zneužití. Je-li SMTP server zpřístupněn do Internetu (což musí být vždy, pokud je na něj nasměrován alespoň jeden MX záznam a je zpřístupněn port 25), může se na něj připojit libovolný klient a poslat přes něj e-mail. Tímto způsobem lze server zneužít k rozesílání nevyžádaných zpráv (tzv. spamů). Příjemce takové zprávy pak v jeho zdrojovém textu vidí jako odesílající server váš SMTP server, a může si zablokovat příjem zpráv z tohoto serveru. Vaše firma tak může být považována za rozesílatele spamů, a v krajním případě může být váš server zaznamenán do databáze spam serverů.

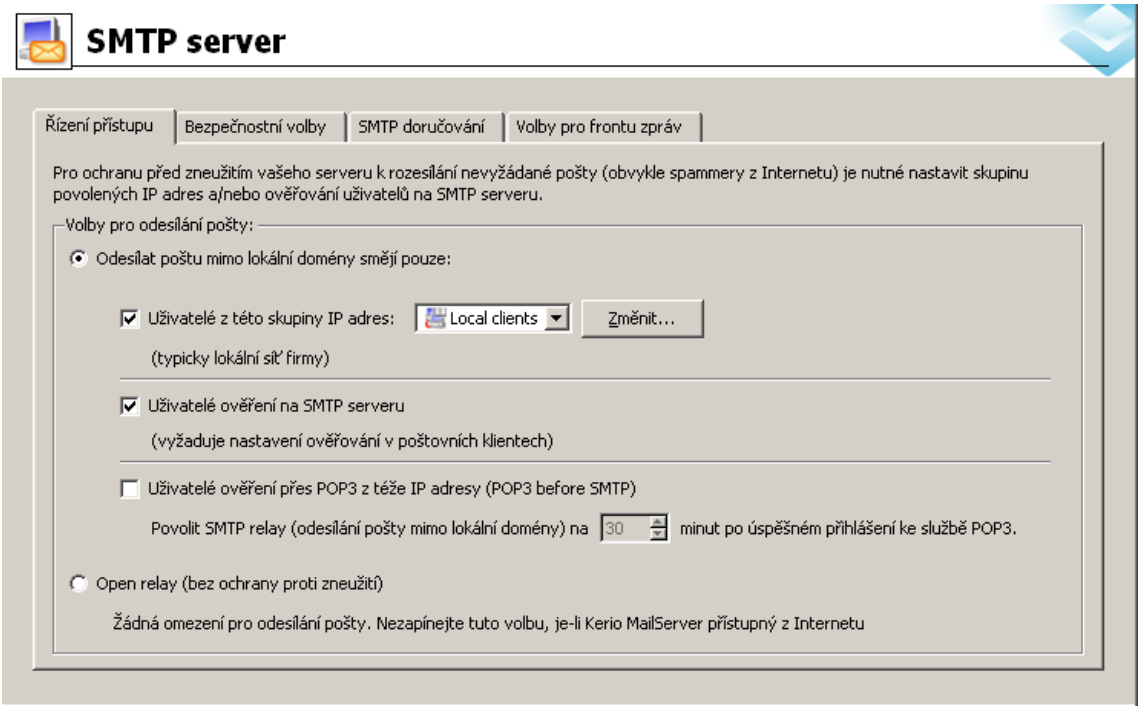
Kerio MailServer obsahuje ochranu, která umožňuje definovat, kdo smí přes tento server odesílat zprávy a kam. V principu se může na SMTP server připojit kdokoliv, aby poslal zprávu do některé z lokálních domén. Odesílat zprávy do jiných domén naopak smějí pouze oprávnění (typicky lokální) uživatelé.

V této sekci lze také nastavit parametry pro doručování:

Záložka Řízení přístupu

V záložce *Řízení přístupu* je možno nastavit skupinu povolených IP adres a/nebo ověřování uživatelů na SMTP serveru.

Odesílat poštu mimo lokální domény smějí pouze
Tato volba zapíná režim ověřování odesílatelů dle IP adresy nebo jména a hesla (viz dále). Obecně platí, že ověření odesílatelé smějí přes tento server odeslat zprávu do libovolné domény, zatímco neověření uživatelé pouze do lokálních domén.



Obrázek 15.1 Řízení přístupu

Do této skupiny IP adres zařaďte také všechny důvěryhodné servery. Tyto servery nebudou kontrolovány *SPF* a *Caller ID* kontrolou (více viz kapitolu 16.5). Důvěryhodné servery nebudou standardně kontrolovány ani systémem *SpamAssassin*. Speciální volbou v sekci *Filtr spamu* v záložce *Hodnocení spamu* však tuto kontrolu lze explicitně povolit (více viz kapitolu 16.1).

Uživatelé z této skupiny IP adres

Zde je možno nastavit skupinu IP adres, z nichž bude možno odeslat zprávu do libovolné domény. V poli *Skupina IP adres* se zobrazují skupiny definované v sekci *Konfigurace* → *Definice* → *Skupiny IP adres*. Tlačítkem *Změnit* je možno upravit vybranou skupinu nebo vytvořit novou (viz kapitolu 12.1).

Uživatelé ověření na SMTP serveru

Právo odeslat zprávu do libovolné domény budou mít uživatelé, kteří budou na SMTP serveru ověřeni uživatelským jménem a heslem. Tuto možnost mají tedy všichni uživatelé, kteří mají v *Kerio MailServeru* vytvořen svůj uživatelský účet.

Uživatelé ověření přes POP3 z téže IP adresy

Volba umožňuje uživatelům ověřeným POP3 (uživatelské jméno a heslo), aby se při odesílání pošty nemuseli ověřovat po dobu zadanou v poli *Povolit SMTP relay na ... minut po úspěšném přihlášení ke službě POP3* na SMTP server.

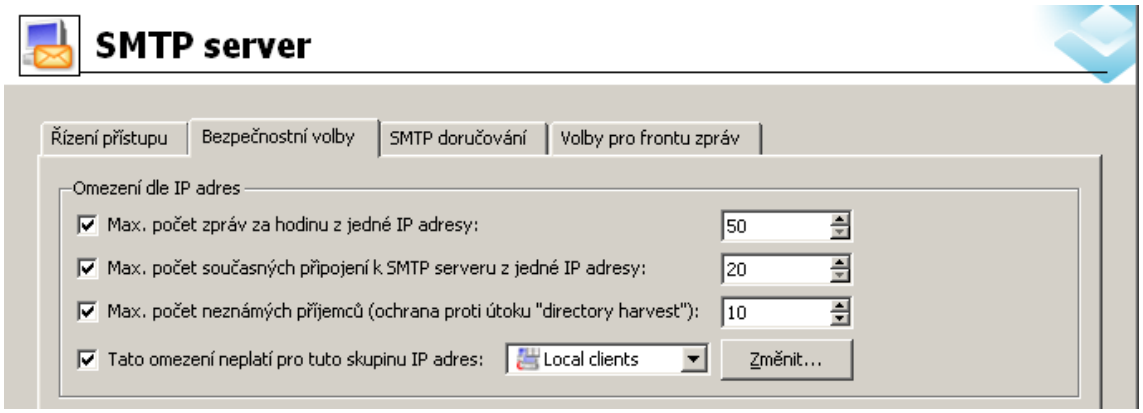
Ověřování podle IP adres a podle uživatelských jmen funguje nezávisle — uživatel tedy musí splnit alespoň jednu z těchto podmínek. Pokud jsou zapnuty volby *Uživatelé z IP adres z této skupiny* a *Uživatelé ověření na SMTP serveru* zároveň, pak v případě neúspěšného ověření na SMTP serveru *Kerio MailServer* nekontroluje, zda uživatel patří nebo nepatří do povolené skupiny IP adres.

Open relay

Je-li zvolen tento režim, pak SMTP server nekontroluje uživatele, kteří přes něj odesílají zprávy. Libovolný uživatel tedy může odeslat zprávu do libovolné domény. *Upozornění:* Nedoporučujeme používat tento režim, jestliže je *Kerio MailServer* dostupný z Internetu (tzn. má veřejnou IP adresu a port 25 není blokován firewallem). V takovém případě je totiž téměř jisté, že bude dříve nebo později zneužit k rozesílání nevyžádaných reklamních zpráv (tzv. spamů), čímž zahltí vaší internetovou linku. Může se také dostat do veřejných databází nežádoucích SMTP serverů (viz dále).

Záložka Bezpečnostní volby

Kromě úplného blokování určitých odesílatelů umožňuje *Kerio MailServer* nastavit také obecná omezení, která nebrání v odesílání pošty, ale zamezují např. zahlcení serveru dávkovým odesíláním velkého počtu zpráv či navázáním velkého počtu spojení (tzv. DoS útok). Tato nastavení se provádějí v záložce *Bezpečnostní volby*.



Obrázek 15.2 Bezpečnostní volby — Omezení dle IP adres

Max. počet zpráv za hodinu ...

Maximální počet zpráv, který smí být odeslán z jedné IP adresy během jedné hodiny. Takto se server brání zaplnění diskového prostoru velkým počtem zpráv (zpravidla identických a nežádoucích).

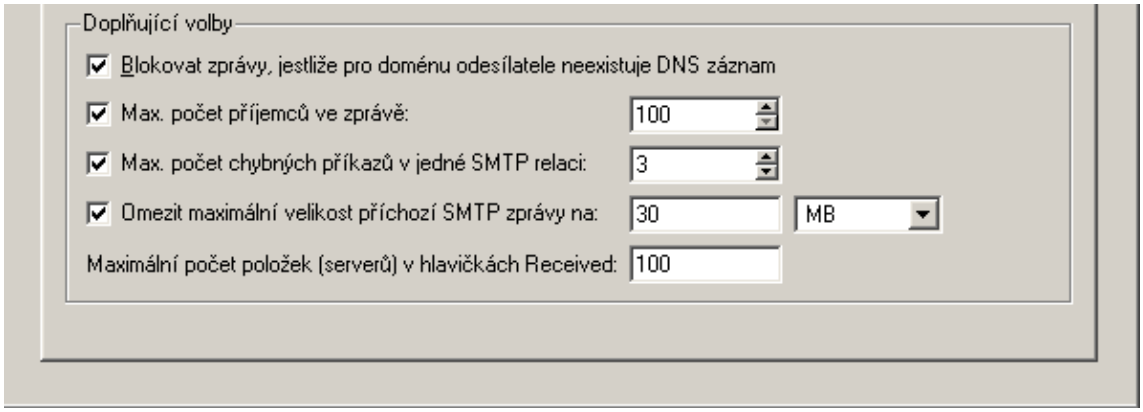
Poznámka: Maximální počet zpráv za hodinu z jedné IP adresy se kontroluje vždy za poslední hodinu, tedy zpětně. Pokud nastavíte toto omezení, zahodí se okamžitě

každá nová zpráva, která byla odeslána z IP adresy, ze které byl za poslední hodinu překročen limit.

Max. počet současných připojení k SMTP ...
Maximální počet současných TCP spojení na port SMTP serveru z jedné IP adresy. Toto je ochrana proti tzv. DoS útoku (Denial of Service — velké množství současně navázaných spojení vyčerpá systémové prostředky a ostatní klienti již nemohou spojení se serverem navázat).

Max. počet neznámých příjemců
Directory harvest je typ spamového útoku, kdy se na váš SMTP server napojí aplikace generující pomocí slovníků pravděpodobná uživatelská jména a zjišťuje tak platné adresy uživatelů serveru. Nastavením tohoto typu ochrany lze zajistit, aby server, který posílá zprávy na neznámého příjemce byl na jednu hodinu zablokován.

Tato omezení neplatí pro tuto skupinu IP adres
Skupina IP adres, na niž se výše uvedená omezení nevztahují. Zpravidla to bývá skupina lokálních uživatelů (viz záložka *Kontrola přístupu*). Tito uživatelé odesílají přes *Kerio MailServer* veškerou svou odchozí poštu — počet zpráv odeslaných na tento server je proto výrazně vyšší než v případě vnějších uživatelů (serverů), kteří jej používají pouze pro odeslání pošty do některé z lokálních domén.
Dále doporučujeme do skupiny povolených IP adres zařadit sekundární SMTP server, protože v určitých případech může vykazovat známky chování útočícího serveru.



Obrázek 15.3 Bezpečnostní volby — Doplňující volby

Blokovat, jestliže pro doménu odesílatele...
Při přijetí zprávy *Kerio MailServer* zkontroluje, zda pro doménu odesílatele existuje záznam v DNS, a pokud ne, zprávu odmítne. Toto je ochrana proti smyšleným adresám odesílatelů.
Poznámka: Zapnutí této volby může zpomalovat činnost *Kerio MailServeru* (doby odezvy DNS serverů mohou být i několik sekund).

Max. počet příjemců ve zprávě
Maximální akceptovatelný počet adresátů v e-mailové zprávě (tj. počet příkazů RCPT v SMTP obálce).

Max. počet chybných příkazů ...
Spamy jsou často rozesílány speciální aplikací, která se připojí na SMTP server a nebere ohled na chybová hlášení serveru. Po nastavení této volby *Kerio MailServer* automaticky ukončí SMTP spojení, jestliže klient již vyslal daný počet chybných příkazů.

Omezit maximální velikost příchozí SMTP zprávy na
Maximální velikost zprávy, kterou SMTP server akceptuje. Toto slouží jako ochrana před zahlcením serveru objemnými zprávami, které jednak zabírají místo na disku, a jednak zatěžují internetovou linku. Proto doporučujeme tuto položku nastavit. Hodnota *0* (nula) znamená, že není nastaveno žádné omezení. Pro pohodlné zadání číselného údaje je možno přepínat jednotky: kilobyty (*KB*) nebo megabyty (*MB*).

Maximální počet položek (serverů) v hlavičce Received
Nastavení tohoto parametru slouží především k zablokování zprávy, která se „zacyklila“ mezi několika SMTP servery.

SMTP doručování

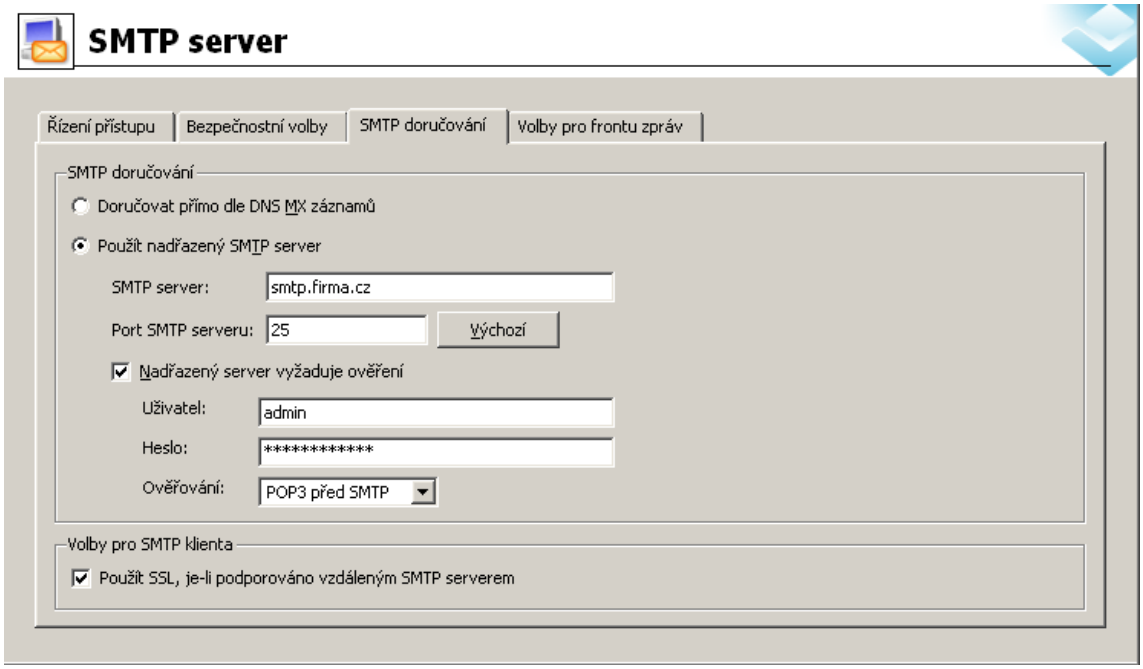
V této sekci lze také nastavit parametry pro doručování:

Doručovat přímo dle DNS MX záznamů
Pošta bude doručována přímo do cílových domén na základě MX záznamů.

Použít nadřazený SMTP server
Veškerá odchozí pošta bude odesílána přes jiný (nadřazený) SMTP server.

SMTP server
DNS jméno nebo IP adresa nadřazeného SMTP serveru.

Port SMTP serveru
Port, na němž nadřazený SMTP server běží. V naprosté většině případů běží SMTP server na standardním portu 25 (tuto hodnotu rovněž dosazuje tlačítko *Výchozí*).



Obrázek 15.4 SMTP doručování

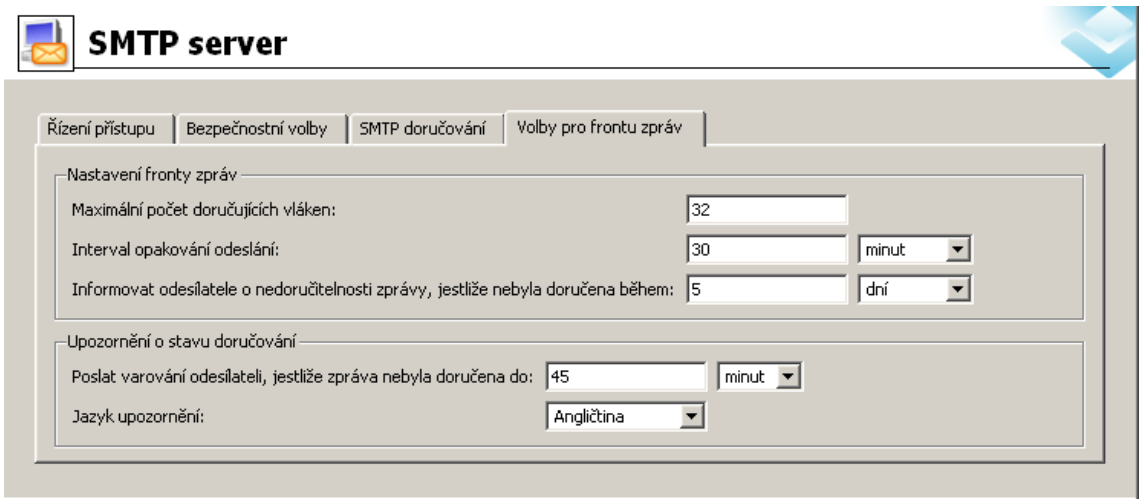
Nadřazený server vyžaduje ověření
: Nastavte tuto volbu, jestliže nadřazený server vyžaduje ověření odesílatele (tj. *Kerio MailServeru*) uživatelským jménem a heslem. Do položek *Uživatel* a *Heslo* zadejte příslušné jméno a heslo.

Ověřování
: Způsob ověření na nadřazeném serveru: *Příkaz SMTP AUTH* nebo *POP3 před SMTP*. Uživatel se nejprve přihlásí k POP3 schránce na tomto serveru, tím je ověřen a může poslat poštu přes SMTP server. Pro přihlášení ke schránce se použije zde uvedené jméno a heslo a ze schránky se nevybírají žádné zprávy. K tomuto účelu tedy není třeba definovat schránku v sekci *Konfigurace → Stahování POP3 schránek*.

Použít SSL, je-li podporováno...
: SMTP server se při odesílání každé zprávy pokusí navázat nejprve šifrované spojení (SSL), a teprve pokud zjistí, že jej vzdálený server nepodporuje, naváže nešifrované spojení. Tak je zajištěna maximální možná bezpečnost odesílaných zpráv.

Volby pro frontu zpráv

Záložka umožňuje nastavení fronty zpráv, která se zobrazuje v sekci *Stav → Fronta zpráv*.



Obrázek 15.5 Volby pro frontu zpráv

Maximální počet doručujících vláken
: Maximální počet současně vytvořených procesů, které budou odesílat zprávy z odchozí fronty (jinými slovy maximální počet současně odesílaných zpráv). Nastavená hodnota by měla zohledňovat výkon procesoru, ale zejména rychlost internetové linky.

Interval opakování odeslání
: Doba, po které se server pokusí zopakovat odeslání e-mailu, jestliže byl při předchozím pokusu neúspěšný (tj. žádný ze serverů cílové domény nebyl dostupný).

Informovat odesílatele o nedoručitelnosti zprávy, ...
: Jestliže se nepodaří zprávu doručit po této době, bude zpráva zahozena a její hlavička spolu s DSN (*Delivery Status Notification* — zprávy generované serverem) bude doručena odesílateli. Zároveň bude zpráva vyřazena z fronty a v pokusech o její odeslání již server nebude pokračovat.

Pro pohodlné zadání časového údaje je možno přepínat jednotky: minuty, hodiny a dny.

Tři výše uvedené časy nemají smysl, jestliže se odchozí zprávy odesílají na nadřazený SMTP server.

Poslat varování odesílateli...
: Jestliže se nepodařilo zprávu doručit po této době, pošle se varovná zpráva odesílateli (a bude se nadále pokračovat v pokusech o odeslání).

Jazyk upozornění
: Jazyk, v němž budou zasílána chybová, varovná a informativní hlášení serveru (např. informace o nedoručitelnosti zprávy, o nalezeném viru, přihlášení a odhlášení z e-mailové konference atd.).

Poznámka: Hlášení serveru jsou uložena v podadresáři `reports` adresáře, kde je *Kerio MailServer* nainstalován (soubory používají kódování znaků UTF-8). Zkušený správce tak může jednotlivá hlášení modifikovat, případně vytvořit vlastní jazykovou variantu.

15.3 Aliasy

Aliasy slouží k vytváření tzv. virtuálních e-mailových adres. Princip virtuálních adres nejlépe objasní několik jednoduchých příkladů:

1. Všechny zprávy poslané na adresu `info@firma.cz` mají být ukládány do veřejné složky *Info*. Definujeme alias:

   `info` → `#public/Info`

2. Zprávy poslané na neplatné adresy (tj. adresy, kde část před znakem `@` neodpovídá žádnému uživatelskému účtu ani aliasu) mohou být doručovány vybranému uživateli (typicky správci). Toto zajistí alias:

   `*` → `Admin`

   Nebude-li tento (nebo následující) alias definován, pak bude *Kerio MailServer* takové zprávy vracet odesílatelům jako nedoručitelné.

3. Pro doplnění libovolného počtu znaků v aliasu lze použít znak `*` (např.: `*sms*`, `a*00*` apod.). Alias pak bude fungovat pro všechny e-mailové adresy, které vyhoví této masce.

4. Pro doplnění právě jednoho znaku v aliasu lze použít znak `?` (např.: `vo?ka` pokryje adresy `vozka` i `voska`).

5. Pošta bude doručována na obě adresy současně:

   `jnovak` → `info`

   `jnovak` → `jnovak`

   Takový alias doporučujeme nastavit přímo v nastavení konkrétního uživatelského účtu (kapitola 13.2), je to přehlednější.

Každé schránce nebo skupině je možné vytvořit libovolné množství aliasů. Stejně tak na existující alias lze vytvořit další alias. Aby nebylo možné vytvořit z aliasů smyčku, tak se k uživatelskému jménu, na které byla zpráva adresována, označí příznakem. Jakmile zpráva dorazí k uživatelskému jménu označenému příznakem, zůstane ve schránce, pro kterou byl vytvořen poslední neoznačený alias:

`jnovak` → `novak`

`novak` → `jan.novak`

`jan.novak` → `novak`

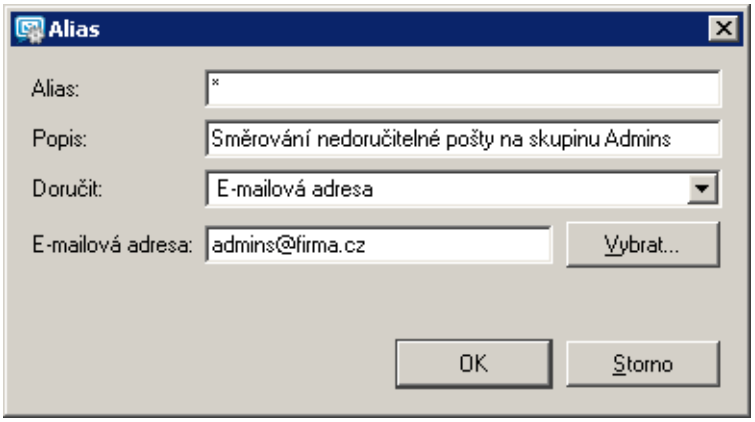
Poznámka: Aliasy lze rovněž použít pro přiřazení další adresy uživateli nebo skupině, případně přeposílání pošty pro uživatele či skupinu na jiné adresy. Toto však doporučujeme provádět přímo v definici uživatele (viz kapitolu 13.2), resp. skupiny (viz kapitolu 14.1).

Definice aliasů

Definice aliasů se provádí v sekci *Nastavení domény* → *Aliasy*.

Nejprve je třeba zvolit doménu, v níž budou aliasy definovány. Aliasy se totiž vždy vztahují k některé z lokálních domén, a proto stačí do záhlaví aliasu zapsat pouze lokální část adresy (tj. část před znakem `@`).

Přidání aliasu se provede tlačítkem *Přidat*, po jehož stisknutí se zobrazí dialog s těmito položkami:



Obrázek 15.6 Vytvoření aliasu

Alias
: Virtuální adresa (např. `obchod` nebo `jan.novak`).

Popis
: Textový popis aliasu. Slouží pouze pro potřebu správce, může obsahovat libovolné informace nebo zůstat nevyplněn.

Doručit
: Kam mají být zprávy poslané na tuto adresu doručovány. V položce lze vybrat, kam má být zpráva uložena:

- *E-mailová adresa* — libovolná e-mailová adresa. Tlačítkem *Vybrat* lze vybrat uživatele nebo skupinu ze seznamu.
- *Veřejná složka* — název veřejné složky ve tvaru `#public/Slozka`. Položka je k dispozici pouze v případě, že je založena alespoň jedna veřejná složka typu pošta.

Typ znaku	Popis
a–z	všechna malá písmena abecedy kromě národních znaků
A–Z	všechna velká písmena abecedy kromě národních znaků
0–9	všechny číslice
.	tečka
-	pomlčka
_	podtržítko
?	otazník
*	hvězdička

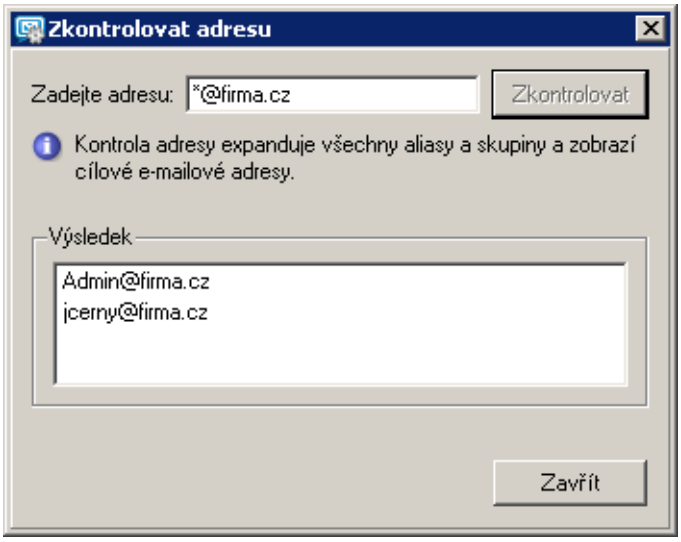
Tabulka 15.2 Povolené znaky v názvu aliasu

Stejný dialog bude zobrazen také po stisknutí tlačítka *Změnit* (úprava aliasu). Tlačítkem *Odebrat* lze alias odstranit.

Kontrola aliasů

Vytváříme-li složitější aliasy (víceúrovňové, vícenásobné atd.), může snadno dojít k chybě (např. pouhým překlepnutím při zapisování). *Kerio MailServer* obsahuje funkci pro kontrolu aliasů, která pro zadanou e-mailovou adresu zobrazí seznam lokálních účtů a externích adres, na něž bude e-mail doručen.

Ke kontrole aliasů slouží tlačítko *Zkontrolovat adresu*. Po jeho stisknutí je třeba zadat adresu, která má být zkontrolována (byl-li předtím nějaký alias v seznamu označen, nabídne se automaticky). Po provedení kontroly se zobrazí výsledek ve spodní části dialogu (tzn. seznam adres, na které bude tento alias doručován).



Obrázek 15.7 Kontrola aliasu

15.4 Vzdálené POP3 schránky

Kerio MailServer umí vybírat zprávy z POP3 schránek na jiných poštovních serverech a doručovat je buď do lokálních schránek, nebo je odesílat na jiné e-mailové adresy.

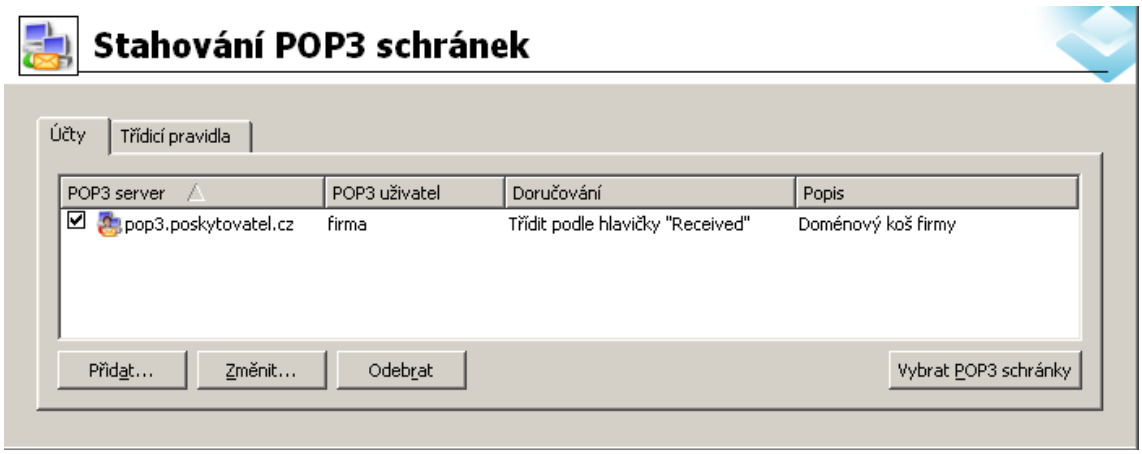
Stahování POP3 schránek je řízeno pouze plánovačem (viz kapitolu 9). Je důležité si uvědomit, že podnětem k vybrání vzdálených schránek není připojení klienta na svou schránku v *Kerio MailServeru* nebo odeslání e-mailu.

Stahování POP3 schránek znemožňuje použití antispamových funkcí, které jsou závislé na přijetí zpráv protokolem SMTP, typicky DNS blacklisty a kontrola odesílajících serverů Caller ID a SPF. Konfiguraci a vlastnosti antispamových filtrů popisuje kapitola 16.

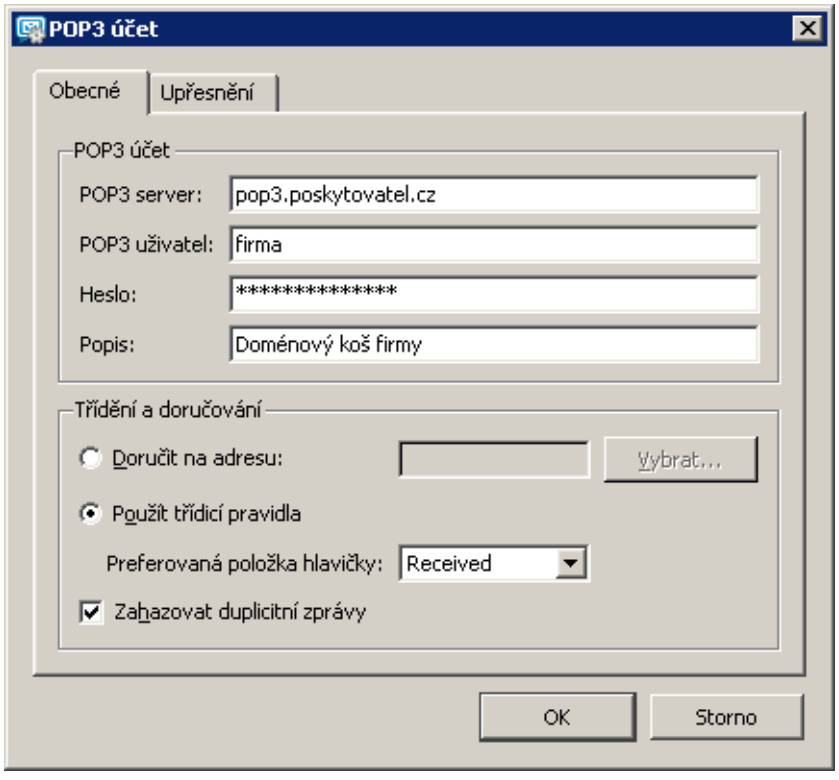
Definice vzdálených POP3 schránek

Vzdálené schránky, které mají být vybírány, je možno definovat v sekci *Konfigurace* → *Stahování POP3 schránek*, záložka *Účty*.

Tlačítko *Přidat* zobrazí dialog pro přidání nového účtu (vzdálené schránky). Záložka *Obecné* slouží k nastavení základních parametrů přístupu ke schránce a způsobu doručování stažených zpráv.



Obrázek 15.8 Stahování POP3 schránek



Obrázek 15.9 Nastavení parametrů pro přístup ke schránce

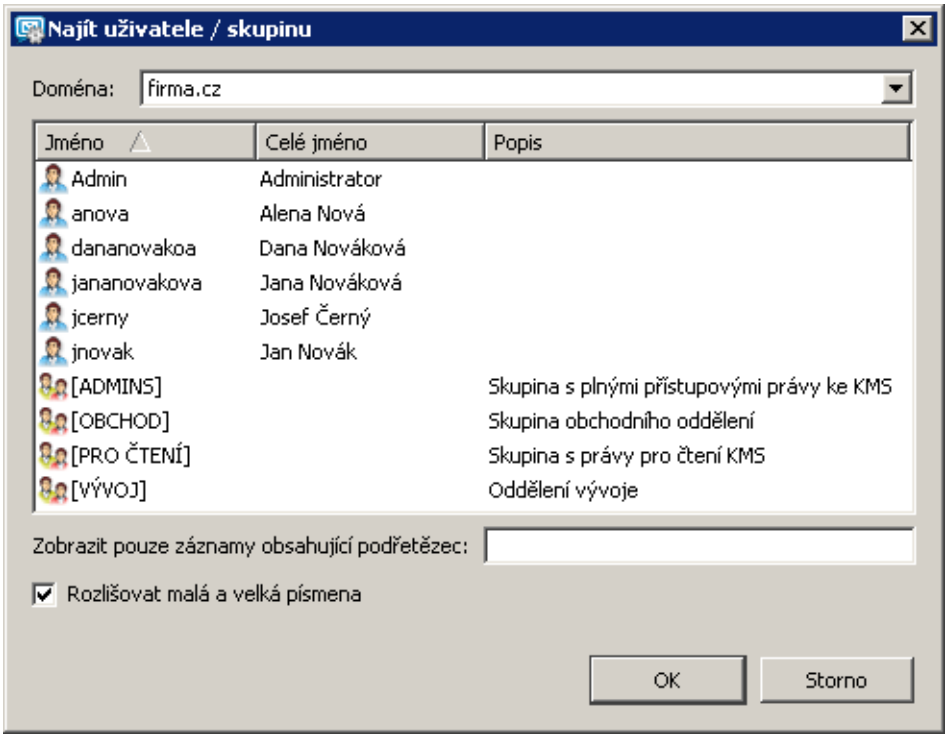
POP3 server

DNS jméno nebo IP adresa POP3 serveru, na němž se schránka nachází.

Uživatelské jméno, Heslo
Uživatelské jméno a heslo k této schránce.

Popis
Libovolný textový popis POP3 účtu (pro lepší orientaci správce).

Doručit na adresu
Všechny zprávy z této schránky mají být doručeny na jednu adresu. Zde je možno zadat: lokálního uživatele, lokální skupinu, alias nebo externí e-mailovou adresu. Lokálního uživatele nebo skupinu lze vybrat ze seznamu stisknutím tlačítka *Vybrat*.



Obrázek 15.10 Dialog pro výběr uživatele nebo skupiny

Dialog pro výběr uživatele nebo skupiny (viz obrázek 15.10) umožňuje vyhledávání podle řetězce a nastavení rozlišování velkých a malých písmen. Tyto možnosti nastavení výrazně zrychlují vyhledávání zejména v případě velkého množství uživatelů a skupin v doméně.

Použít třídicí pravidla
Zprávy z této schránky budou tříděny podle třídicích pravidel (viz dále).

Preferovaná položka hlavičky
Položka hlavičky, která bude primárně použita k třídění. Je možno zadat libovolnou hlavičku (název bez dvojtečky) nebo vybrat z předdefinovaných (`X-Envelope-To`, `Received` nebo `Delivered-To`). Nebude-li v hlavičce e-mailu tato položka nalezena, nebo v této položce není žádná adresa, která by vyhovovala alespoň jednomu třídi-

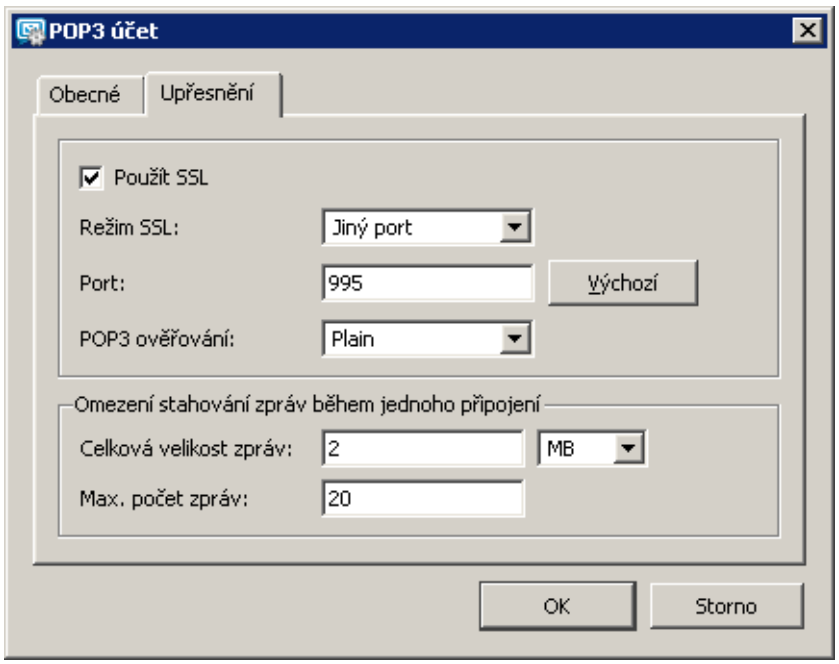
címu pravidlu, program pokračuje prohledáváním položek `Resent-To` a `Resent-Cc` a v případě neúspěchu ještě položek `To` a `Cc`. Není-li adresa nalezena ani v těchto položkách, zpráva bude doručena podle implicitního pravidla (viz dále) nebo bude zahozena.

Zahazovat duplicitní zprávy

Bude-li po zapnutí této volby ve vzdálené schránce nalezena tatáž zpráva ve více identických kopiích, bude tato zpráva zpracována pouze jednou a ostatní kopie budou zahozeny.

K duplikaci zpráv dochází, jestliže je do doménové schránky doručena zpráva, jejíž hlavička obsahuje více příjemců z této domény. Pak je zpráva do schránky doručena tolikrát, kolik bylo původních příjemců. Tyto zprávy se liší pouze svou SMTP obálkou, která je však při uložení do schránky oříznuta. Jednotlivé kopie zprávy ve schránce jsou pak již zcela identické. Při klasickém POP3 třídění pak každý příjemce dostane každou z těchto zpráv, protože ve všech je obsažena jeho adresa (tzn. každý příjemce obdrží tuto zprávu tolikrát, kolik je příjemců). Zahazování duplicitních zpráv zajistí, že každý příjemce obdrží tuto zprávu pouze jednou.

V záložce *Upřesnění* je možno definovat další upřesňující parametry:



Obrázek 15.11 Upřesňující nastavení stahování POP3 schránek

Použít SSL
Spojení s POP3 serverem bude zabezpečeno (šifrováno) SSL.

Režim SSL
Způsob zabezpečení celé komunikace s POP3 serverem. Možnosti jsou: *Speciální port* (spojení šifrované SSL bude navázáno na speciálním portu) nebo *Příkaz STLS* (nejprve se naváže nešifrované spojení, poté se příkazem STLS přepne do šifrovaného režimu). Informaci o zabezpečení komunikace s POP3 serverem vám poskytne jeho správce.

POP3 ověřování
Způsob ověřování na POP3 serveru: *Plain* (heslo se posílá v přímém tvaru) nebo *APOP* (heslo se posílá zašifrovaně, aby nemohlo být odposlechnuto a zneužito). Informaci o tom, který typ ověřování má být použit, získáte od správce POP3 serveru.

Omezení stahování zpráv během jednoho připojení

- *Celková velikost zpráv* — Do pole je možno nastavit maximální limit celkové velikosti stahovaných zpráv během jednoho POP3 spojení. Hodnota *0* (nula) znamená, že není nastaven žádný limit.
- *Max. počet zpráv* — Maximální počet zpráv, který má být stažen během jednoho připojení. Hodnota *0* (nula) znamená, že není nastaven žádný limit.

Nastavení omezení celkové velikosti zpráv a maximálního počtu zpráv slouží k zabránění potřeby opětovného stahování zpráv v případě přerušení POP3 spojení.
Důvodem je způsob fungování POP3 protokolu. Zprávy, které mají být smazány, se fyzicky na serveru smažou až po úspěšném ukončení celého spojení příkazem QUIT. Pokud se stane, že je POP3 spojení přerušeno, zprávy se nesmažou a server je bude stahovat znovu v následujícím POP3 spojení. Nastavení limitu tedy napomáhá řízení objemu dat přenášených v opakovaných spojeních.

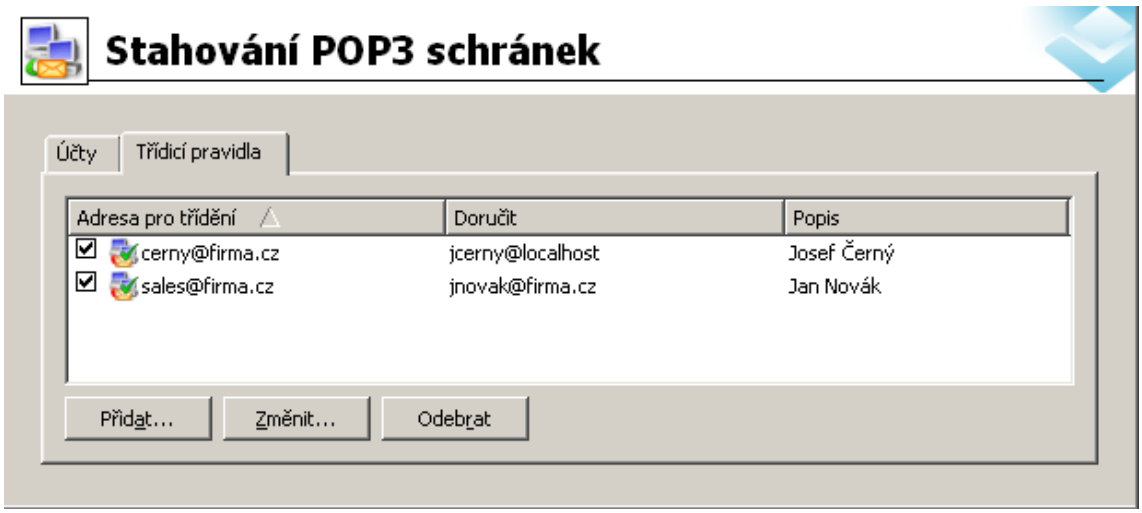
Pomocí zaškrtávacího pole vlevo vedle definice pravidla lze vybrané pravidlo dočasně „vyřadit“.

Třídicí pravidla

Třídicí pravidla určují, jakým způsobem mají být zprávy vybrané ze vzdálené POP3 schránky rozděleny lokálním uživatelům, případně přeposlány na externí e-mailové adresy. K definici třídicích pravidel slouží záložka *Třídicí pravidla*.

Tlačítkem *Přidat* lze přidat nové třídicí pravidlo:

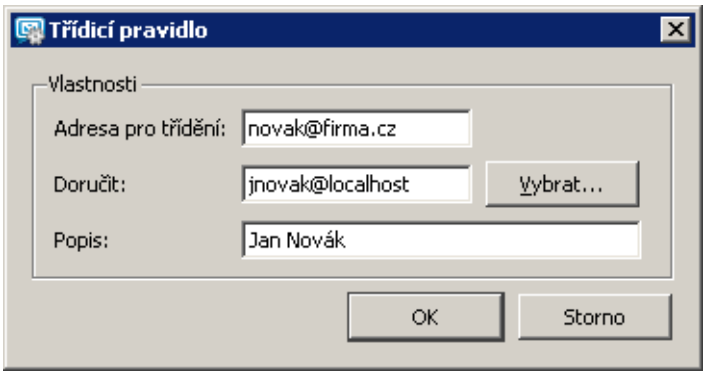
Adresa pro třídění
E-mailová adresa, která bude hledána ve vybrané položce hlavičky zprávy. Musí být uvedena kompletní, podřetězec je nepřípustný.



Obrázek 15.12 Třídicí pravidla

Doručit

Pole určuje, komu má být zpráva vyhovující tomuto pravidlu doručena. Je možno zadat:



Obrázek 15.13 Vytvoření třídicího pravidla

- lokálního uživatele nebo skupinu — lokálního uživatele nebo skupinu lze vybrat ze seznamu stisknutím tlačítka *Vybrat*,
- alias — zapíšeme do pole vybraný alias,
- externí e-mailovou adresu — do pole zapíšeme jakoukoliv jinou adresu.

Poznámka: Pokud má být zpráva doručena skupině, musí být skupině přiřazena adresa, zprávy se pak doručují na tuto adresu (případně lze na ni vytvořit alias). Podrobnosti najdete v kapitole 14.1.

Popis

Libovolný textový popis třídicího pravidla (např. pro vysvětlení jeho účelu).

Pomocí zaškrtávacího pole vlevo vedle definice pravidla lze vybrané pravidlo dočasně „vyřadit“.

Speciální třídicí pravidla

V třídicích pravidlech mohou být také definována pravidla v tomto tvaru:

- `*` → `adresa` (tzv. implicitní pravidlo) — na tuto adresu budou doručovány všechny e-maily, které nevyhoví žádnému jinému třídicímu pravidlu. Nebude-li toto pravidlo definováno, budou takové e-maily zahazovány.
- `*@domena.cz` → `*@jinadomena.cz` — všechny zprávy, jejichž adresy obsahují zadanou doménu, budou přeposílány do specifikované domény.

Žádné jiné použití znaku hvězdička (např. pro doplnění části adresy) není povoleno.

Příklad využití hvězdičkových pravidel

Pro příklad si uvedeme, jakým způsobem je možné hvězdičková pravidla využít pro nejjednodušší variantu konfigurace třídicích pravidel. Konfigurace je kombinací dvou následujících pravidel:

- První pravidlo třídí zprávy podle nastavení aliasu a podle adres uživatelských účtů.

  `*@firma.cz` → `*@firma.cz`

- Druhé pravidlo zatřídí zprávy, které z nějakého důvodu nelze zatřídit do konkrétního uživatelského účtu.

  `*` → `admin@firma.cz`

Poznámka: Pokud před tato pravidla umístíme jakékoliv jiné pravidlo, bude bráno v úvahu dříve. Pravidla jsou vždy vykonávána v následujícím pořadí:

1. `adresa@domena`
2. `*@domena`
3. `*`

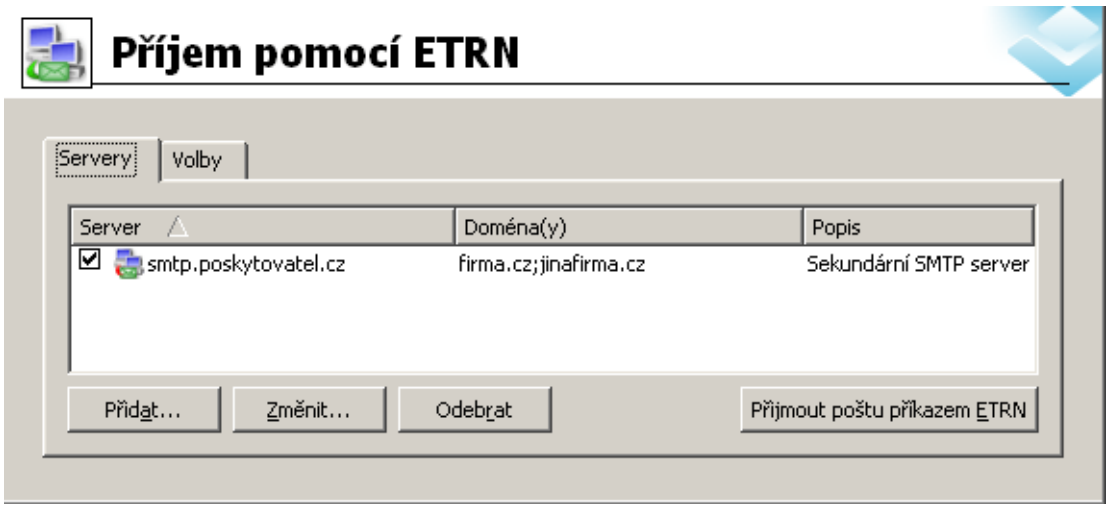
15.5 Příjem pošty pomocí příkazu ETRN

V sekci *Konfigurace* → *Příjem pomocí ETRN* je možno definovat SMTP servery, z nichž má být pošta přijímána pomocí příkazu ETRN (typicky se jedná o sekundární, příp. terciální servery pro danou doménu či domény).

Tlačítkem *Přidat* lze přidat další server, z něhož má být pošta tímto způsobem přijímána:

Server

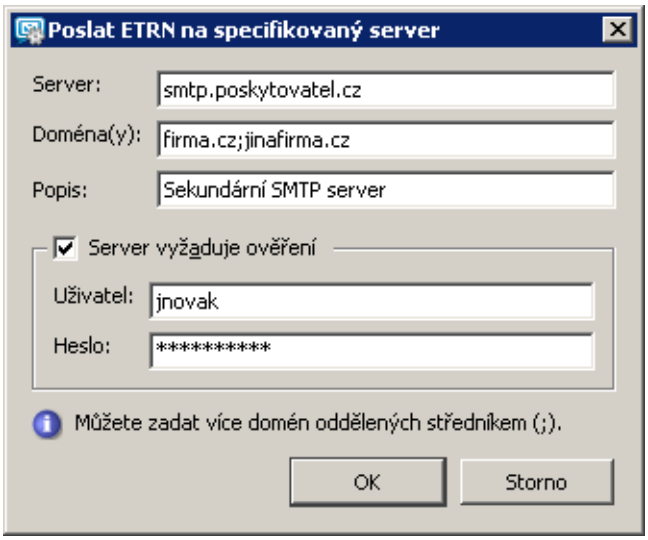
DNS jméno nebo IP adresa serveru.



Obrázek 15.14 Příjem pomocí ETRN

Doména(y)

Výčet domén, pro něž tento server uchovává poštu. Názvy jednotlivých domén se oddělují středníkem (;).



Obrázek 15.15 Nastavení parametrů pro přístup k serveru

Popis

Textový popis definice ETRN serveru. Slouží pouze pro potřebu správce, může obsahovat libovolné informace nebo zůstat nevyplněn.

Server vyžaduje ověření

Zapněte tuto volbu, jestliže tento server vyžaduje ověření uživatelským jménem a heslem.

Uživatel, Heslo
Příslušné uživatelské jméno a heslo.

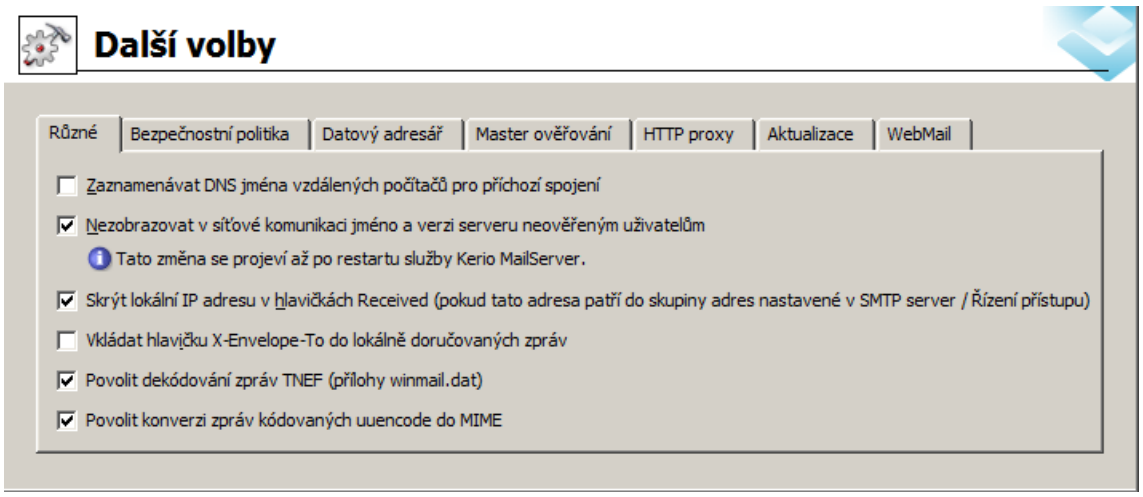
Tlačítkem *Změnit* lze upravit nastavení vybraného serveru a tlačítkem *Odebrat* tento server odstranit. Pomocí zaškrtávacího pole vlevo vedle definice serveru můžete tento server dočasně „vyřadit“.

Záložka *Volby* poskytuje možnost nastavit maximální dobu čekání na odezvu na vytáčené lince.

15.6 Upřesňující nastavení

V sekci *Konfigurace* → *Další volby* lze nastavit některé upřesňující parametry poštovního serveru.

Různé



Obrázek 15.16 Různé

Zaznamenávat DNS jména vzdálených ...
Převádět IP adresy vzdálených klientů a serverů, které se na *Kerio MailServer* připojují, na DNS jména. Tím dojde k zpřehlednění záznamů, ale činnost *Kerio MailServeru* se tím může zpomalit.

Nezobrazovat v síťové komunikaci jméno a verzi serveru...
Zapněte tuto volbu, pokud má být utajena verze a jméno programu poštovního serveru, který doménu obsluhuje.
Upozornění: Aktivace nebo deaktivace této volby vyžaduje restart *Kerio MailServeru*.

Skrýt lokální IP adresu ...

Kerio MailServer bude skrývat lokální IP adresu (ze skupiny IP adres nastavené v sekci *Konfigurace → SMTP server* v záložce *Řízení přístupu*) v položce `Received` v hlavičce zprávy.

Do této položky zaznamenává každý SMTP server, přes nějž zpráva projde, od koho a kým byla přijata. První záznam v položce `Received` tedy obsahuje e-mailovou adresu a IP adresu odesílatele. Je-li SMTP server umístěn v privátní síti chráněné firewallem, pak se do této položky zaznamená privátní adresa klienta. To znamená, že v odchozích e-mailových zprávách se de facto rozesílají informace o privátní síti, která je jinak vůči Internetu skryta. Tyto informace by mohly případnému hackerovi usnadnit napadení této sítě. Zapněte tedy tuto volbu, jestliže je *Kerio MailServer* provozován v privátní síti za firewallem (i v případě, že běží na tomtéž počítači jako firewall).

Vazba na řízení přístupu je zde z toho důvodu, aby SMTP server rozpoznal lokální IP adresu. V řízení přístupu se zpravidla používá skupina lokálních IP adres, z nichž je možno odesílat poštu do libovolných domén (viz kapitolu 15.2), což je výhodné i pro tento účel.

Poznámka: Nebude-li tedy zapnuto řízení přístupu nebo v něm nebude definována žádná skupina lokálních IP adres, bude tato volba neúčinná.

Vkládat hlavičku X-Envelope-To...

Volba umožňuje dosadit do hlavičky lokálně doručované zprávy položku `X-Envelope-To:` (tj. adresu skutečného příjemce ze SMTP obálky). Položku je vhodné využít zejména v případě, že je v *Kerio MailServeru* zřízen doménový koš.

Povolit dekódování zpráv TNEF

TNEF (Transport Neutral Encapsulation Format) je proprietární formát firmy *Microsoft*, který primárně slouží k zasílání zpráv s rozšířeným formátováním z aplikace *MS Outlook*. Součástí každé zprávy, která je odeslána v tomto formátu, je příloha `winmail.dat`. Tato příloha obsahuje kopii celé zprávy ve formátu RTF a všechny případné přílohy zprávy. Pokud tedy uživatel nepoužívá pro přístup k poště *MS Outlook* a bude mu doručena zpráva s přílohou v tomto formátu, potom se k příloze ve zprávě nedostane.

Dekodér TNEF zabudovaný do *Kerio MailServeru* dekóduje TNEF zprávy na straně serveru do standardního MIME formátu a odstraní tak uživatelům problémy se zprávami s `winmail.dat` přílohou.

Tuto volbu je výhodné využít zejména pokud uživatelé nepoužívají pro přístup k poště výhradně aplikaci *MS Outlook*.

Poznámka: Při problémech s dekódováním zpráv vám může pomoci záznam *Debug*, kde je třeba zapnout volbu *Message decoding*. Více najdete v kapitole 22.8

Povolit konverzi zpráv kódovaných uuencode do MIME

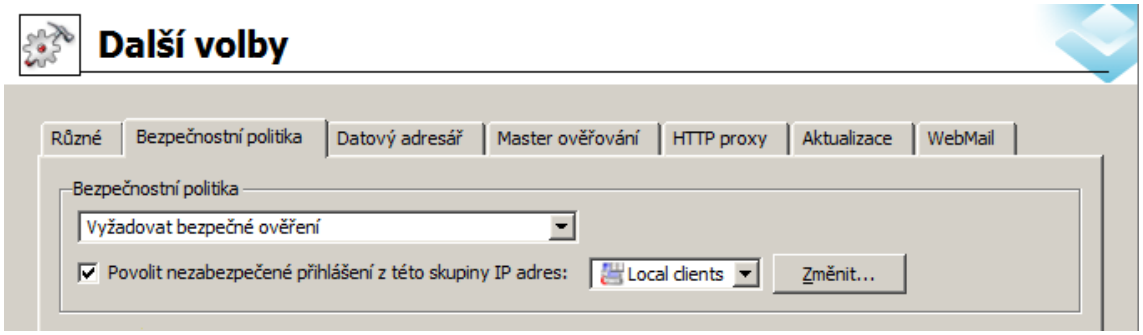
Uuencode (Unix-to-Unix Encoding) je typ kódování využívaný pro odesílání souborů pomocí elektronické pošty. Kóduje binární data do textového formátu tak, že mohou být vložena přímo do těla zprávy. Problémem je, že ne každý poštovní klient obsahuje speciální dekodér, který umí zakódované soubory dekódovat do původního tvaru. Z toho důvodu obsahuje *Kerio MailServer* zabudovaný Dekodér Uudecode (Unix-to-Unix decoding). Zprávy jsou dekódovány již na straně serveru do standardního MIME formátu a odstraní tak uživatelům případné problémy s dekódováním takovýchto zpráv.

Doporučujeme volbu *Povolit konverzi zpráv kódovaných uuencode do MIME* povolit zvláště tehdy, pokud uživatelé využívají pro přístup ke svým schránkám *Kerio WebMail* a *MS Outlook* s *Kerio Outlook Connectorem*.

Poznámka: Při problémech s dekódováním zpráv vám může pomoci záznam *Debug*, kde je třeba zapnout volbu *Message decoding*. Více najdete v kapitole 22.8

Bezpečnostní politika

Kerio MailServer umožňuje nastavení bezpečnostní politiky, tzn. minimální požadované úrovně bezpečnosti. Tato nastavení se provádějí v sekci *Konfigurace* → *Další volby* v záložce *Bezpečnostní politika* (viz obrázek 15.17).



Obrázek 15.17 Bezpečnostní politika

Menu v záhlaví stránky umožňuje výběr jedné ze tří politik:

Žádná omezení

K serveru se bude možno připojit bez jakéhokoliv omezení.

Vyžadovat bezpečné ověřování

Kerio MailServer bude vždy vyžadovat bezpečné ověření uživatele. To znamená, že ověření musí být provedeno některou z následujících metod — CRAM-MD5, DIGEST-MD5, NTLM nebo musí uživatel použít SSL tunel — povolit SSL komunikaci ve svých poštovních klientech.

V případě, že uživatelé používají pro přístup ke své poště rozhraní *Kerio WebMail*, kde se nelze ověřit některou z ověřovacích metod, použije se automaticky protokol HTTP zabezpečený SSL.

Po nastavení bezpečného ověřování se zobrazí možnost povolení nezabezpečeného přihlášení ze zadané skupiny IP adres. Skupinu je možno vybrat buď z existujících nebo vytvořit novou. O možnostech nastavení skupin IP adres pojednává samostatná kapitola 12.1.

Upozornění: Neaplikujte tuto možnost, pokud mají uživatelé nastaveno ukládání hesel na serveru v SHA formátu.

Vyžadovat šifrované spojení

Po zapnutí této volby se klientské aplikace budou moci připojit ke kterékoliv službě pouze šifrovaným spojením (komunikaci tedy nebude možno v žádném případě odposlouchávat).

Na všech klientských stanicích je nutno povolit všem protokolům komunikaci přes SSL. Při přihlášení k rozhraní *Kerio WebMail* se šifrované spojení nastaví automaticky.

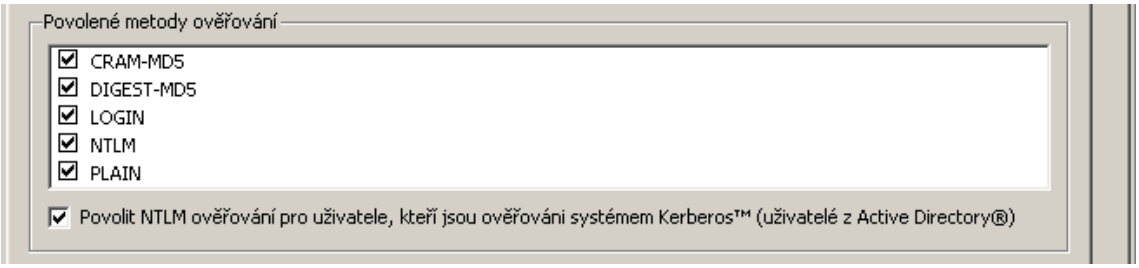
Jediný protokol, na který se toto omezení nevztahuje, je SMTP. Vzhledem k množství SMTP serverů, které nepodporují SMTPS nebo STARTTLS, není možné tento protokol omezit pouze na zabezpečenou verzi. Aby se i přes to podařilo zajistit bezpečnost, vyžaduje server pro protokol SMTP po nastavení volby *Vyžadovat šifrované spojení* bezpečné ověřování hesla. Jméno a heslo se tedy odesílá pomocí některé z podporovaných bezpečných metod ověřování.

Po nastavení této bezpečnostní politiky lze z omezení vyjmout skupinu IP adres, z nichž nebude šifrované spojení vyžadováno. Skupinu je možno buď vybrat z existujících nebo vytvořit novou. O možnostech nastavení skupin IP adres pojednává kapitola 12.1.

Pokud využijete tuto možnost ochrany komunikace, je důležité, aby všichni uživatelé měli na svých klientských stanicích nainstalovaný platný ověřovací certifikát (více viz kapitolu 10).

Podporované metody ověřování

Kerio MailServer podporuje několik metod ověřování uživatelských hesel:



Obrázek 15.18 Metody ověřování

- CRAM-MD5 — metoda ověřování hesel (autentizace pomocí MD5 digestů). Tento způsob šifrování je obecně rozšířený, podporuje ho většina poštovních klientů.
- DIGEST-MD5 — metoda ověřování hesel (autentizace pomocí MD5 digestů).
- LOGIN — uživatelská hesla nejsou při přenosu po síti žádným způsobem chráněna. Budete-li využívat tento způsob přenosu hesla, důrazně doporučujeme zapnutí komunikace přes SSL tunel.
- NTLM — tuto ověřovací metodu je možno využít pouze v případě, že se uživatelé ověřují proti *Active Directory* doméně. To znamená, že lze takto ověřovat pouze účty, které jsou buď mapovány nebo importovány z *Active Directory*. Nastavení NTLM ověřování popisuje samostatná kapitola 25.
- PLAIN — uživatelská hesla nejsou při přenosu po síti žádným způsobem chráněna. Budete-li využívat tento způsob přenosu hesla, důrazně doporučujeme zapnutí komunikace přes SSL tunel.
- APOP — ověřovací metoda se v seznamu nezobrazuje, *Kerio MailServer* ji automaticky používá ke stahování POP3 účtů.

Server standardně nabízí všechny metody ověřování. Nabízí je klientovi postupně tak, jak jsou seřazeny v seznamu (začíná metodou CRAM-MD5). Pokud klient danou metodu podporuje, další v pořadí již nebudou použity. Toto chování může způsobit problém, pokud je heslo na serveru uloženo v bezpečném formátu (SHA1). S SHA šifrou nelze využívat jiné metody přenášení hesla než LOGIN a PLAIN. Poštovní klient, pokud budou povoleny bezpečné metody CRAM-MD5 a DIGEST-MD5, vybere samozřejmě některou z bezpečných metod pro ověření hesla a nebude se moci do *Kerio MailServeru* přihlásit. Nelze-li tedy přímo v poštovních klientech nastavit použitou metodu, je nutno v případě ukládání hesel ve formátu SHA vypnout všechny metody kromě LOGIN a PLAIN.

Doporučení:

- Selže-li ověřovací metoda pro klienta, je nejlépe ji v *Kerio MailServeru* vypnout (odškrtnout v seznamu *Povolené metody ověřování*).
- Nezávisle na použití typu ověřovací metody doporučujeme nastavit na poštovních klientech přihlašování k serveru přes SSL.

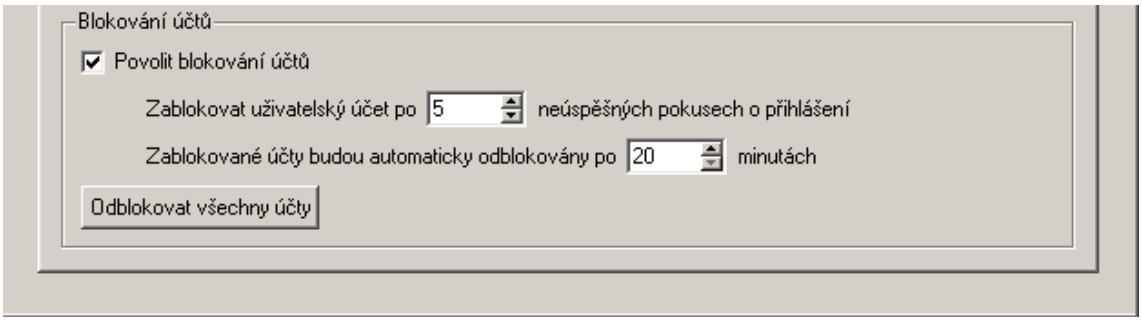
Zaškrtnutí volby *Povolit NTLM ověřování pro uživatele, kteří jsou ověřováni systémem Kerberos* umožňuje uživatelům z *Active Directory* domény ověřovat se při přihlášení ke *Kerio MailServeru*. Aby bylo NTLM ověřování funkční, je nutné, aby počítač i uživatelský účet byly součástí domény, proti které se uživatel ověřuje. Další nutnou podmínkou pro správnou funkci tohoto typu ověřování je povolení NTLM (SPA) ověřování v poštovních klientech uživatelů.

Co vše je potřeba v *Kerio MailServeru* nastavit, aby bylo NTLM ověřování uživatelů funkční, najdete v samostatné kapitole 25.

Oddíl *Blokování účtů* umožňuje nastavit tyto parametry (viz obrázek 15.19):

Operační systém	Ověřování proti Active Directory	Uživatelské schránky jsou uloženy lokálně a hesla jsou zabezpečena DES šifrováním	Uživatelské schránky jsou uloženy lokálně a hesla jsou zabezpečena SHA šifrováním
MS Windows	NTLM LOGIN PLAIN	CRAM-MD5 DIGEST-MD5 LOGIN PLAIN	LOGIN PLAIN
LINUX	LOGIN PLAIN	CRAM-MD5 DIGEST-MD5 LOGIN PLAIN	LOGIN PLAIN
Mac OS X	LOGIN PLAIN	CRAM-MD5 DIGEST-MD5 LOGIN PLAIN	LOGIN PLAIN

Tabulka 15.3 Použití metod ověřování



Obrázek 15.19 Blokování účtů

Povolit blokování účtů
Po zaškrtnutí této volby se budou uživatelské účty blokovat podle níže nastavitelných pravidel. Tato nastavení slouží k větší bezpečnosti uživatelských účtů, chrání je před průlomem hesel a následným zneužitím účtu.

Zablokovat uživatelský účet...
Počet neúspěšných pokusů uživatele o přihlášení k uživatelskému účtu z jedné IP adresy.

Zablokované účty se budou automaticky...
Doba (v minutách), po které se uživatelský účet automaticky odblokuje.

Použitím tlačítka *Odblokovat všechny účty* odblokujete všechny účty, které byly dosud blokovány.

Upozornění: Blokování účtů závisející na neúspěšných pokusech o přihlášení nijak nesouvisí s blokací v nastavení uživatelských účtů (viz sekci 13.2).

Datový adresář

V záložce *Datový adresář* je možno nastavit adresáře pro ukládání zpráv (uživatelské a veřejné složky) a pro zálohování. Do *datového adresáře* se ukládají zprávy v uživatelských a veřejných složkách, záznamy, zprávy k odeslání a soubory, které se právě kontrolují antivirovým programem.

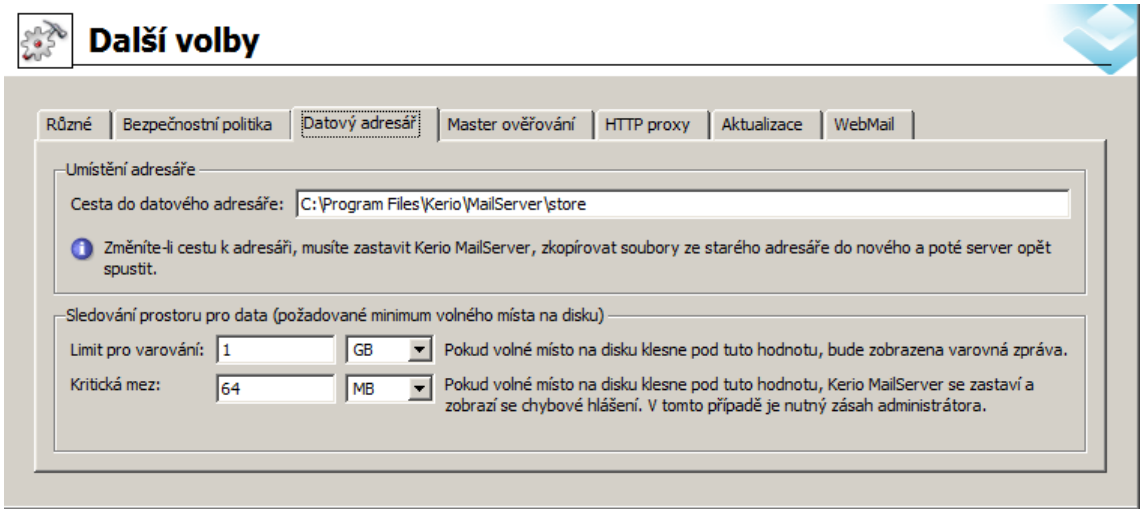
Cesta do datového adresáře
Úplná cesta k datovému adresáři (dle konvence operačního systému, na kterém *Kerio MailServer* běží). Z technických důvodů je třeba datový adresář umístit lokálně (na serveru kde je *Kerio MailServer* spuštěn).
Pokud je třeba cestu do datového adresáře změnit, potom proveďte následující:

1. Založíme nový adresář pro úložiště.
2. V *Kerio Administration Console* (*Konfigurace* → *Další volby* → *Datový adresář*) změníme cestu k datovému adresáři.
3. Zastavíme *Kerio MailServer*.
4. Přesuneme všechny soubory datového adresáře do nového úložiště.
5. Spustíme *Kerio MailServer*.

Upozornění: Do pole *Cesta do datového adresáře* nelze zadat UNC cestu.

Limit pro varování
Po dosažení nastavené hodnoty zobrazí *Kerio MailServer* varovné hlášení při každém přihlášení do administrační konzole. Po dosažení limitu se provede zápis do záznamu *Error* (bližší informace viz kapitolu 22.6).

Kritická mez
Limit, po jehož zaplnění se *Kerio MailServer Engine* a *Kerio MailServer Monitor* zastaví. *Kerio Administration Console* lze spustit. Bezprostředně po přihlášení se zobrazí varovné hlášení o dosažení kritické meze. Zápis o přeplnění diskového prostoru se ukládá do záznamu *Error* (bližší informace viz kapitolu 22.6).



Obrázek 15.20 Datový adresář

Upozornění: Pokud nastavíte limit nebo kritickou mez na hodnotu 0, zobrazí se varovná zpráva, resp. chybové hlášení s každým přijatým e-mailem.

Změny těchto nastavení se projeví až po restartu *MailServer Engine*. Neprovádíte-li tyto změny bezprostředně po instalaci *Kerio MailServeru*, bude třeba po zastavení *Engine* přesunout všechny soubory ze starého umístění do nového a teprve pak službu opět spustit.

Master ověřování

Heslo pro master ověřování je speciální typ univerzálního hesla. Heslo je určeno aplikacím, které potřebují hromadný přístup k poštovním schránkám v *Kerio MailServeru* bez nutnosti znát hesla k jednotlivým uživatelským účtům.

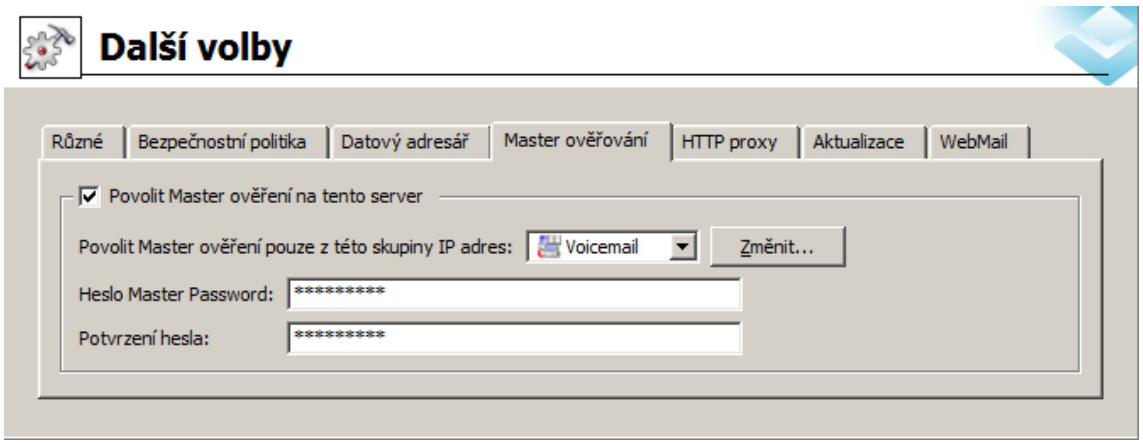
Klasickým příkladem aplikace využívající master ověřování je *Kerio Exchange Migration Tool*. Tento nástroj potřebuje k migraci účtů přístup do jednotlivých schránek. Nastavení master ověřování umožňuje migračnímu nástroji, aby mohl přistupovat do všech účtů bez nutnosti zadávat heslo pro každý z nich zvlášť.

Upozornění:

1. Heslo *Master Password* nelze použít pro přístup k uživatelským účtům z poštovních klientů nebo přes rozhraní *Kerio WebMail*. Není to univerzální administrátorské heslo (nelze se jím přihlásit do *Administration Console*).

2. Heslo *Master Password* je od verze *Kerio MailServer 6.0.5* ukládáno v novém formátu (SHA). Z tohoto důvodu nebude při přenosu konfigurace serveru na starší verzi původní heslo funkční a je nutné jej změnit.

Nastavení master ověřování se provádí ve stejnojmenné záložce sekce *Další volby*.



Obrázek 15.21 Master ověřování

Povolit Master ověřování na tento server

Tato volba zapíná/vypíná Master ověřování v *Kerio MailServeru*. Doporučujeme zapínat Master ověřování pouze v případě, že bude skutečně účelně využita (např. aplikací *Kerio Exchange Migration Tool*).

Povolit Master ověřování pouze z této skupiny IP adres

V tomto poli je třeba vybrat skupinu IP adres, z níž má být Master ověřování povoleno. Tato skupina musí být předem definována v sekci *Konfigurace* → *Definice* → *Skupiny IP adres* (viz kapitolu 12.1) z bezpečnostních důvodů není možné povolit Master ověřování z libovolné IP adresy. Tlačítko *Změnit* umožňuje pomocí jednoduchého dialogu přidat do výběru další skupinu IP adres.

Heslo Master Password

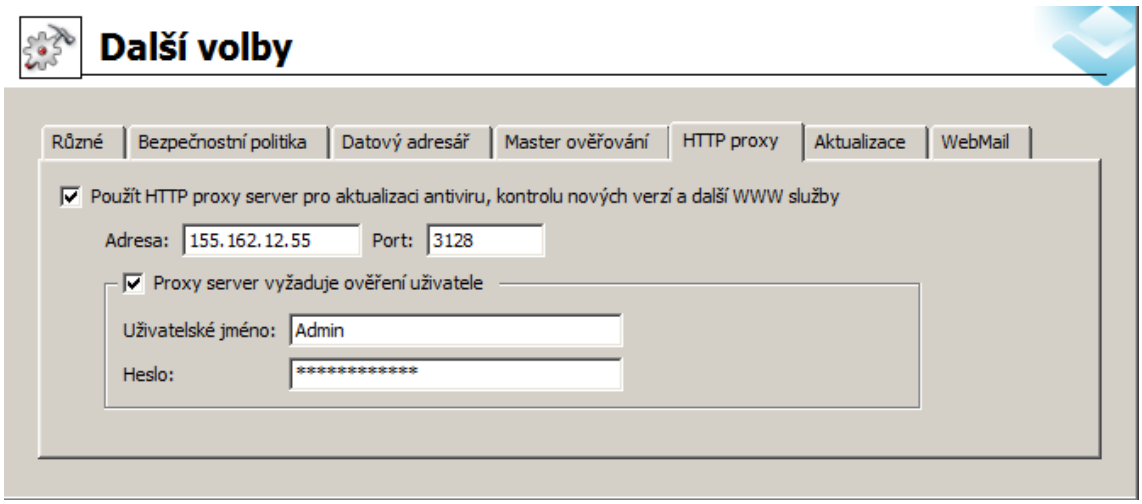
Do tohoto pole zadejte heslo, které bude použito pro přístup ke všem schránkám. Toto heslo by měl znát naprosto minimální počet osob. Získá-li heslo *Master Password* neoprávněná osoba, může dojít k narušení soukromí všech uživatelů, kteří mají na daném serveru schránky!

Potvrzení hesla

Heslo musí být potvrzeno z důvodu eliminace překlepů při zadávání.

HTTP Proxy

Pokud je *Kerio MailServer* nainstalován na počítač umístěný za firewallem, může se pomocí proxy serveru připojit do Internetu. Této vlastnosti lze využít například pro aktualizaci a zjišťování nových verzí *Kerio MailServeru* nebo antiviru.



Obrázek 15.22 HTTP proxy

Použít HTTP proxy server pro ...
Pro správnou funkci musí být vyplněna adresa proxy serveru a port, na němž služba běží.

Proxy server vyžaduje ověření uživatele
Pokud proxy server vyžaduje ověření, musí být vyplněno uživatelské jméno a heslo.

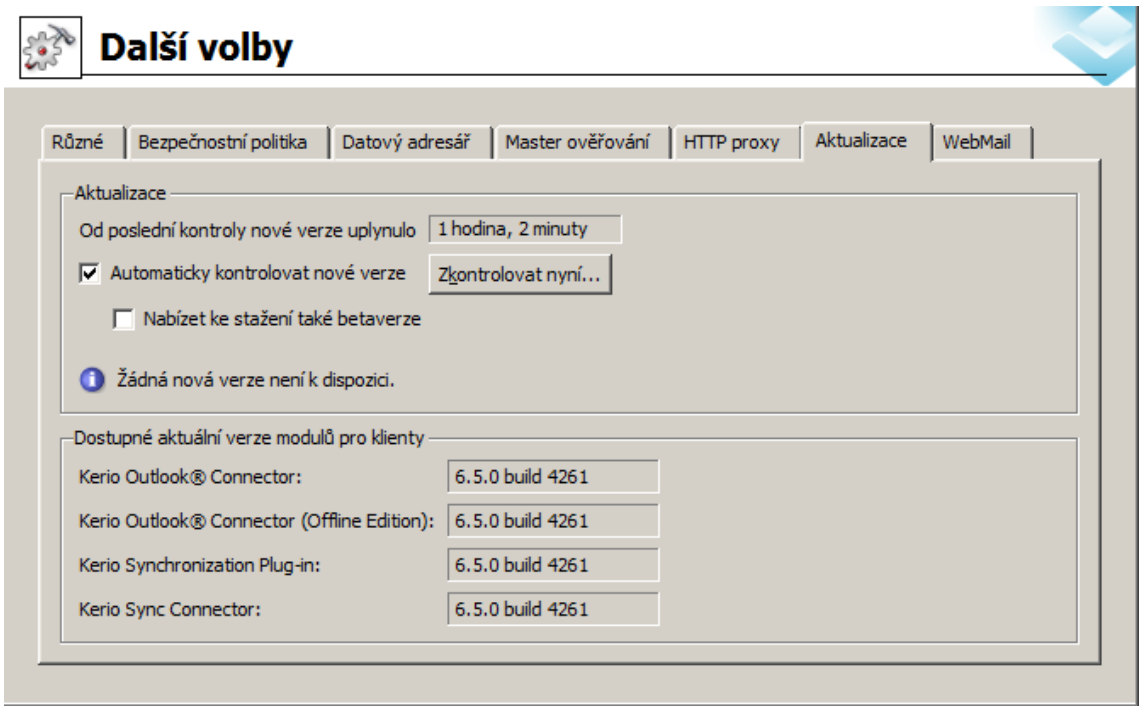
Uživatelské jméno
Do položky je třeba zadat uživatelské jméno pro přihlášení k příslušnému proxy serveru.

Heslo
Do položky je třeba zadat heslo pro přihlášení k proxy serveru.

Aktualizace

Záložka spravuje aktualizaci nových verzí *Kerio MailServeru* a automatickou aktualizaci *Kerio Outlook Connectoru* a *Kerio Synchronization Plug-inu*:

Od poslední kontroly nové verze ...
Čas uplynulý od poslední kontroly. Nové verze produktu se kontrolují každých 24 hodin.
Tlačítko *Zkontrolovat nyní* spustí kontrolu nové verze. V případě nalezení nové verze je tato nabídnuta ke stažení a instalaci, jinak je uživatel informován, že k dispozici nová verze není.



Obrázek 15.23 Aktualizace

Automaticky kontrolovat nové verze...
Povoluje automatickou kontrolu, zda je na serveru společnosti *Kerio Technologies* k dispozici nová verze *Kerio MailServeru*.
Byla-li společností *Kerio Technologies* uvolněna nová verze aplikace, zobrazí se v záložce *Aktualizace* odkaz na WWW stránku, odkud je možno novou verzi produktu stáhnout.

Nabízet ke stažení také betaverze
Volba umožňuje zapnout také upozorňování na betaverze *Kerio MailServeru*.
Upozornění: Pokud se chcete podílet na testování betaverzí, zaškrtněte volbu *Nabízet ke stažení také betaverze*. V případě, že je *Kerio MailServer* nasazen v ostrém provozu, nedoporučujeme betaverze instalovat — volbu nezapínejte.

Součástí instalačního balíku jsou také automatické instalace *Kerio Outlook Connectoru*, *Kerio Outlook Connectoru (Offline Edition)*, *Kerio Synchronization Plug-inu* a *Kerio Sync Connectoru for Mac*.

Pole *Dostupné aktuální verze modulů pro klienty* informuje o aktuálně používaných verzích modulů (včetně čísla buildu).

- *Kerio Outlook Connector* — balík je všem uživatelům aktualizován automaticky ihned po aktualizaci serveru.
- *Kerio Outlook Connector (Offline Edition)* — balík je všem uživatelům aktualizován

automaticky ihned po aktualizaci serveru.
- *Kerio Synchronization Plug-in* — balík je všem uživatelům aktualizován automaticky ihned po aktualizaci serveru.
- *Kerio Sync Connector for Mac* — uživatelům na klientských stanicích se zobrazí informace o možnosti aktualizace *Kerio Sync Connectoru*. Po odsouhlasení dialogu program aktualizuje.

Kerio MailServer provádí automatickou kontrolu verzí *Kerio Outlook Connectoru*, *Kerio Outlook Connectoru (Offline Edition)* a *Kerio Synchronization Plug-inu*. Tato kontrola zamezuje problémům způsobeným špatnou komunikací staršího serveru a novější verze plug-inu, nebo naopak novějšího serveru a starší verze plug-inu. V praxi kontrola verzí znamená, že v případě zjištěné nekonzistence se uživateli zobrazí upozornění, že by měl být proveden upgrade/downgrade plug-inu. Po odsouhlasení upozornění se nainstaluje správná verze. V případě, že uživatel nechce nainstalovat novou verzi, záleží, zda se verze serveru liší pouze v čísle buildu nebo v čísle verze:

1. Liší se číslem buildu — plug-in se normálně spustí spolu s aplikací *MS Outlook*. Před každým novým spuštěním aplikace *MS Outlook* se ovšem znovu objeví upozornění, že je třeba plug-in aktualizovat.

2. Liší se číslem verze — plug-in se k serveru odmítne připojit, dokud nebude aktualizován.

Nové verze *Kerio Outlook Connectoru*, *Kerio Outlook Connectoru (Offline Edition)*, *Kerio Synchronization Plug-inu* a *Kerio Sync Connectoru*jsou ukládány do adresáře

```
Kerio\MailServer\webmail\download
```

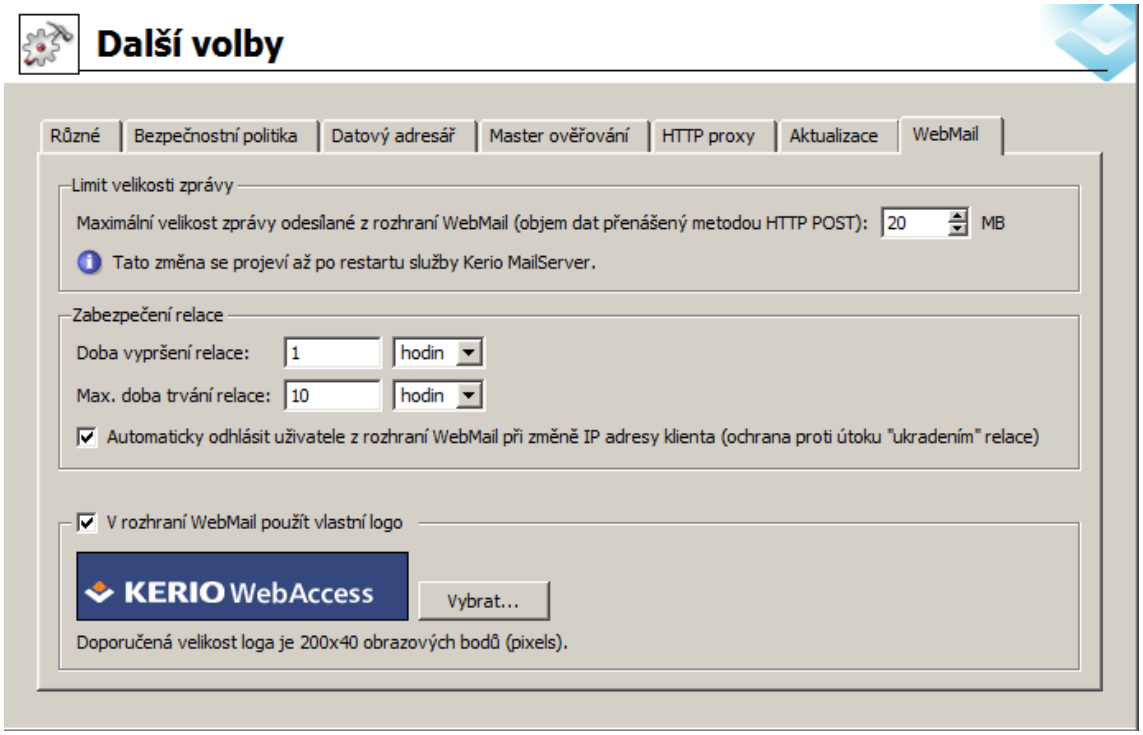
Upozornění: Pro aktualizaci všech plug-inů musí být spuštěna služba HTTP nebo její zabezpečená verze HTTPS. Pouze pro *Kerio Synchronization Plug-in* — je-li v *Kerio MailServeru* povolena pouze komunikace přes HTTPS (například z důvodu bezpečnostní politiky serveru), musí být v *Internet Exploreru* všech klientů nainstalován důvěryhodný certifikát *Kerio MailServeru* (může to být i self-signed certifikát). V opačném případě nebudou nové verze automaticky aktualizovány.

Certifikát serveru lze vytvořit přímo v administrační konzoli *Kerio MailServeru*. Přesný návod obsahuje kapitola 10.

Poznámka: Pokud se v souvislosti s aktualizací vyskytnou nějaké problémy, zapněte v záznamu *Debug* volbu *Update Checker Activity* (kde a jak tuto volbu zapnout najdete v kapitole 22.8). Informace ze záznamu vám mohou pomoci k úspěšnému řešení problému.

WebMail

V *Kerio Administration Console* lze nastavit některé parametry pro rozhraní *Kerio WebMail* (viz obrázek 15.24):



Obrázek 15.24 WebMail

Limit velikosti zprávy

Nastavení limitu velikosti zprávy slouží ke dvěma účelům:

- omezení velikosti příloh odesílaných požadavkem `HTTP POST` do *Kerio WebMailu*,
- nastavení maximální velikosti alokace paměti v *Kerio MailServeru* pro každý `HTTP POST` požadavek.

Upozornění: Maximální hodnota limitu je omezena 128 MB. Vyšší hodnotu nelze do *Kerio Administration Console* zadat.

Pro lepší pochopení smyslu tohoto limitu je třeba vysvětlit, jakým způsobem je zpráva napsaná v *Kerio WebMailu* odesílána do *Kerio MailServeru*. Každá nová zpráva napsaná přes webové rozhraní je de facto odeslána prohlížečem přes protokol HTTP pomocí `HTTP POST` požadavku do rozhraní *Kerio WebMail*. Rozhraní zprávu přijme a zpracuje ji do takového formátu, aby ji *Kerio MailServer* mohl dále odeslat přes protokol SMTP k příjemci.

Jeden `HTTP POST` požadavek obsahuje vždy jednu celou zprávu včetně všech hlaviček a příloh. Limit, který nastavuje tato položka, omezuje velikost každého `HTTP`

POST požadavku, který je směrován k rozhraní *Kerio WebMail*. Omezení velikosti požadavku tedy musí zákonitě omezit také velikost e-mailové zprávy.

Limit velikosti HTTP POST požadavku platí pro všechny soubory odeslané z rozhraní *Kerio WebMail* do *Kerio MailServeru* a platí globálně pro všechny uživatele *Kerio MailServeru*. Výchozí hodnotou pro maximální velikost zprávy odeslané z rozhraní *Kerio WebMail* je 20 MB. Tento limit by měl plně postačovat převážné většině uživatelů.

Minimální hodnotou limitu jsou 2 MB. Pokud bude do položky *Max. velikost odchozí zprávy* nastaven jakýkoliv nižší limit, *Kerio MailServer* nastaví automaticky 2 MB.

Obsahuje-li zpráva přílohy, jsou vždy zakódovány metodou Base64. Tento typ kódování může přenášená data zvětšit až o jednu třetinu (v případě binárních dat), takže minimální dvoumegabajtový limit může vystačit na 1 — 1,5 MB přílohu.

Pro požadavky typu HTTP POST musí být v *Kerio MailServeru* nastavena hodnota pro alokaci paměti. Čím objemnější požadavek je, tím je třeba alokovat více paměti. Po změně limitu se tedy změní velikost paměti alokované procesem *Kerio MailServeru*.

Upozornění: Z důvodu přepisu alokace paměti v *Kerio MailServeru* je třeba po každé změně limitu provést restart *Kerio MailServeru*.

Zabezpečení relace

Zabezpečení relace se váže k připojení uživatelů využívajících *Kerio WebMail*. Uživatelé si často příliš nelámou hlavu s odhlašováním z *Kerio WebMailu* a po ukončení práce prostě zavřou prohlížeč. V takových případech ovšem relace není přerušena a zvyšuje se tak riziko jejího zneužití (toto riziko se zvyšuje s dobou, po kterou je relace navázána). Z toho důvodu je možné nastavit dobu, po kterou má relace trvat. Pokud uživatel během této doby relaci nevyužívá, potom se po jejím uplynutí spojení se serverem automaticky přeruší. Doba vypršení relace je standardně nastavena na jednu hodinu.

Kromě nastavení doby vypršení relace lze nastavit také maximální dobu trvání relace. Tedy celkovou dobu od přihlášení uživatele. Pokud uživatelé používají rozhraní *Kerio WebMail* jako hlavní přístup ke své schránce, nastavte dobu na 8 až 10 hodin. Nastavení příliš krátkého intervalu může způsobit nevhodné ukončení relace například uprostřed rozepsané zprávy. To je pro uživatele nežádoucí.

Poznámka: Pokud má uživatel v době vypršení relace rozepsanou zprávu, bude muset po přerušení spojení zadat znovu své uživatelské jméno a heslo. Rozepsanou zprávu poté bude možno dopsat a odeslat.

Volba *Automaticky odhlásit uživatele z rozhraní WebMail při změně IP adresy klienta* chrání relaci jiným způsobem. Může se stát, že se na relaci jednoho z uživatelů napojí útočník (zejména pokud uživatel nepoužívá ke komunikaci HTTP zabezpečené SSL) a získá tak přístup k serveru. Napojením útočníka na relaci se samozřejmě změní IP adresa klienta. Je-li volba *Automaticky odhlásit uživatele z rozhraní Web-*

Mail při změně IP adresy klienta zaškrtnuta, změnu IP adresy zaznamená *Kerio MailServer* a relaci okamžitě ukončí.
Upozornění:

- Ochranu proti útoku „ukradením“ relace je třeba vypnout v případě, že uživatelé *Kerio MailServeru* využívají společné účty. Volba neumožní připojit se k jednomu účtu z více počítačů (IP adres) najednou.
- Ochranu proti útoku „ukradením“ relace nelze použít ani v případě, že váš poskytovatel Internetu v průběhu spojení mění IP adresy (například při připojení přes GPRS nebo WiFi).

V rozhraní WebMail použít vlastní logo

V záhlaví každé stránky *Kerio WebMailu* se zobrazuje logo společnosti *Kerio Technologies*. Toto logo můžete nahradit vlastním logem, případně libovolným jiným obrázkem (více o nastavení loga najdete v kapitole 11.2). Parametry obrázku jsou následující:

- Formát: GIF
- Rozměry: 200x40 pixelů

Tlačítko *Vybrat* umožňuje zadání cesty k souboru s logem.

Kapitola 16

Antispamová kontrola SMTP serveru

Antispamová kontrola SMTP serveru slouží k ochraně uživatelů proti nevyžádané poště (tzv. spamu). Spam je nevyžádaný, zpravidla reklamní e-mail. Spamy bývají rozesílány hromadně, přičemž adresy příjemců získávají rozesílatelé nelegálními cestami (např. odposloucháváním síťové komunikace).

Kerio MailServer obsahuje celou řadu možností, jak se zbavit nevyžádané pošty. Tyto možnosti představují různé filtry, testy a kontrolní mechanizmy, díky kterým lze poměrně přesně zjistit, která zpráva je vyžádaná, a která nikoliv.

Kerio MailServer používá k rozpoznání a eliminaci spamu následující metody a testy:

- SpamAssassin (funkce a nastavení jsou podrobně popsány v sekci 16.4).
- Black/White listy (funkce a nastavení jsou podrobně popsány v sekci 16.2).
- Vlastní filtrovací pravidla (funkce a nastavení jsou podrobně popsány v sekci 16.3).
- Caller ID (funkce a nastavení jsou podrobně popsána v sekci 16.5).
- SPF (funkce a nastavení jsou podrobně popsány v sekci 16.5).
- Zpoždění odpovědi na SMTP pozdrav (funkce a nastavení jsou podrobně popsány v sekci 16.6).

Každý test pro určování spamu lze používat samostatně, nebo je možné testy různě kombinovat. Doporučujeme druhé řešení, tedy kombinaci pokud možno všech dostupných antispamových testů. Čím více testů je pro určení spamu použito najednou, tím hustší je antispamové síto, a tím méně spamu bude uživatele obtěžovat. Zároveň bude identifikace spamu přesnější, takže i počet korektních zpráv, které byly omylem označeny jako spam (tzv. „false positives“), se sníží na minimum.

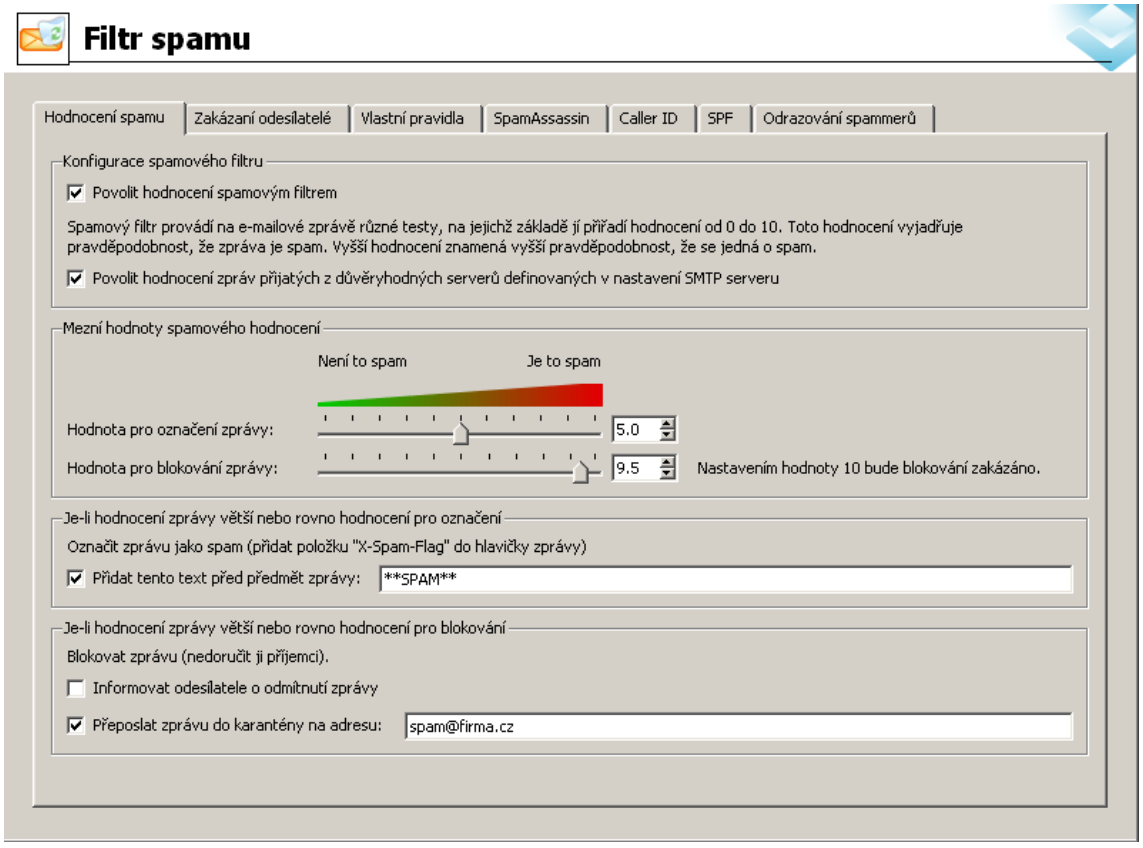
Každý typ testu používá pro určování spamu jiné metody. Jedno má však většina testů společné. Pro téměř každou metodu (kromě zpoždění odpovědi na SMTP pozdrav) je možno nastavit dva různé způsoby, co dělat při nalezení spamu. Prvním řešením je odmítnutí přijetí takové zprávy. V druhém případě lze zprávě zvýšit tzv. spamové skóre (více viz sekci 16.1). Pokud zpráva dostane vyšší skóre od více testů zároveň, bude zahozena (jednotlivá skóre se sčítají). První řešení nastavení testů může mírně snížit zatížení serveru, druhé řešení má tu výhodu, že je méně náchylné na „false positives“.

Upozornění: Při offline připojení *Kerio MailServeru* účinnost spamové kontroly zásadně klesá.

Nastavit spamový filtr *Kerio MailServeru* lze v sekci *Konfigurace* → *Filtrování obsahu* → *Filtr spamu*.

16.1 Hodnocení spamu

Záložka *Hodnocení spamu* povoluje/zakazuje hodnocení spamovým filtrem a upravuje, za jakých podmínek má být spam blokován, pokud je použito navyšování spamového skóre u různých testů spamového filtru:



Obrázek 16.1 Hodnocení spamu

Povolit hodnocení spamovým filtrem

Jednotlivé spamové testy mohou číselně ohodnotit každou příchozí zprávu, přičemž čím vyšší je číslo, tím vyšší je pravděpodobnost, že zpráva obsahuje spam. Číselnému hodnocení, které zpráva po provedení antispamového testu obdrží, říkejme spamové skóre. Pokud zpráva projde více testy, spamová skóre z jednotlivých testů se sčítají a výsledek se ve zprávě uloží do speciální hlavičky `X-Spam-Status`.

Po vypnutí této položky budou zprávy hodnoceny spamovým skóre i nadále, avšak výsledky testů nebudou spamovým filtrem brány v úvahu. Na kontrolované zprávy se budou vztahovat pouze takové testy, kde je nastaveno blokování zpráv.

Povolit hodnocení zpráv přijatých z ...

Zapíná/vypíná kontrolu zpráv odeslaných lokálními (důvěryhodnými) uživateli. Skupinu důvěryhodných IP adres je možno nastavit v sekci *Konfigurace → SMTP server → Řízení přístupu* (více viz kapitolu 15.2).

Tato volba se nevztahuje na kontrolu „email policy“ záznamů (sekce 16.5) a na „black/white listy“ (sekce 16.2).

Mezní hodnoty spamového hodnocení

Poté, co zpráva projde všemi povolenými druhy testů a filtrů a je jí přiděleno výsledné spamové skóre, určí *Kerio MailServer* zda je zpráva legitimní nebo zda je nevyžádaná. Stupnice *Mezní hodnoty spamového hodnocení* umožňuje ruční úpravu hranice, kdy je zpráva považována za spam, a kdy má tak vysoké spamové skóre, že není žádných pochyb, že je nevyžádaná a může být blokována:

- *Hodnota pro označení zprávy*
  Je-li hodnocení zprávy vyšší nebo rovno nastavené hodnotě, bude zpráva označena jako spam. *Kerio MailServer* pak přidá do zprávy hlavičku `X-Spam-Flag`, podle které může poštovní klient rozeznat, že se jedná o spam.
  Do pole nebo na stupnici lze doplnit desetinné číslo upřesněné na 1 desetinné místo v rozsahu od `0.0` do `10.0` (čím nižší číslo zadáte, tím méně nevyžádané pošty přes filtr projde).
  Doporučená hodnota pro práh hodnocení je `5.0` — podle statistik přes filtr neprojde, respektive bude označeno jako spam 91.12% nevyžádaných zpráv. Zároveň ovšem filtr označí jako spam i 0.62% korektních zpráv. Zvýšením hodnocení (např. na `8.0`) lze snížit pravděpodobnost, že budou odfiltrovány korektní zprávy (0.04%), zároveň se však sníží účinnost filtrace spamu (74.36%).
  Upozornění:
  1. Pokud bude zadána příliš nízká hodnota, bude každá nebo téměř každá zpráva považována za spam.
  2. Začne-li se snižovat účinnost spamového filtru, nesnižujte hranici pro označení nebo blokování spamu. Lepším způsobem je zapojení více různých testů do spamového filtru.
- *Hodnota pro blokování zprávy*
  Je-li hodnocení zprávy vyšší nebo rovno nastavené hodnotě, zpráva bude zahozena.
  Pokud nastavíte tuto hodnotu příliš nízko, může se stát, že budou spolu se spamy zahazovány také legitimní zprávy. Z toho důvodu doporučujeme při testování a optimalizaci spamového filtru povolit možnost *Přeposlat zprávu do ka-*

rantény na adresu a doplnit účet, kam posílat kopie všech blokovaných zpráv. Potom bude kopie každé zprávy, která překročila hranici pro blokaci doručena do zadané schránky. Tuto schránku pak stačí jenom jednou za čas projít, zda v ní neuvízla legitimní zpráva.

Maximální hodnotou pro blokování zpráv je `9.9`. Nastavení hodnoty 10 blokování zpráv vypne, takže zprávy se budou pouze označovat jako spam, ale nikdy nebudou blokovány.

Poznámka: Budou-li hodnoty pro označení i blokování zprávy nastaveny na stejnou hodnotu, potom se všechny zprávy označené jako spam budou automaticky zahazovat.

Je-li hodnocení zprávy větší nebo rovno hodnocení ...

Zpráva bude označena hlavičkou `X-Spam-Flag` a doručena příjemci.

Kromě označení spamu speciální hlavičkou lze podle potřeby před předmět zprávy umístit text, podle kterého uživatel nebo případné sieve pravidlo na nevyžádanou poštu rozpozná, že zpráva je spam (takové pravidlo je možno založit přímo při vytváření uživatelských účtů v *Kerio Administration Console* — podrobnosti najdete v kapitole 13.2).

Výchozím textem v předmětu zprávy je řetězec `**SPAM**`. Tento řetězec lze libovolně změnit v poli *Označit zprávu jako spam* (více viz níže v textu).

TIP: Pokud je přidán do pole *Před předmět zprávy přidat tento text* zástupný znak `[%s]`, pak se do předmětu v podobě hvězdiček doplní počet bodů, které přidělila antispamová kontrola. Z toho vyplývá, že si uživatel může nastavit jedno nebo i více filtrovacích pravidel (podle počtu hvězdiček) pro nevyžádanou poštu na svém poštovním klientovi nebo v rozhraní *Kerio WebMail*.

Informovat odesílatele o odmítnutí zprávy

Server vrátí odesílateli DSN zprávu o nemožnosti doručení e-mailu.

Toto nastavení nedoporučujeme používat, protože většina spamů má zfalšovanou adresu odesílatele. To znamená, že zpráva s informací o odmítnutí nemůže být nikam doručena (adresa, na kterou je práva odeslána vůbec neexistuje). Zprávy s informací o odmítnutí pak zůstávají ve frontě, kde je nutno je buď explicitně smazat, nebo se je server pokouší odesílat podle nastavení fronty zpráv (standardně každých 30 minut po dobu 5 dnů). Poté nedoručitelnou zprávu zahodí.

Přeposlat zprávu do karantény na adresu

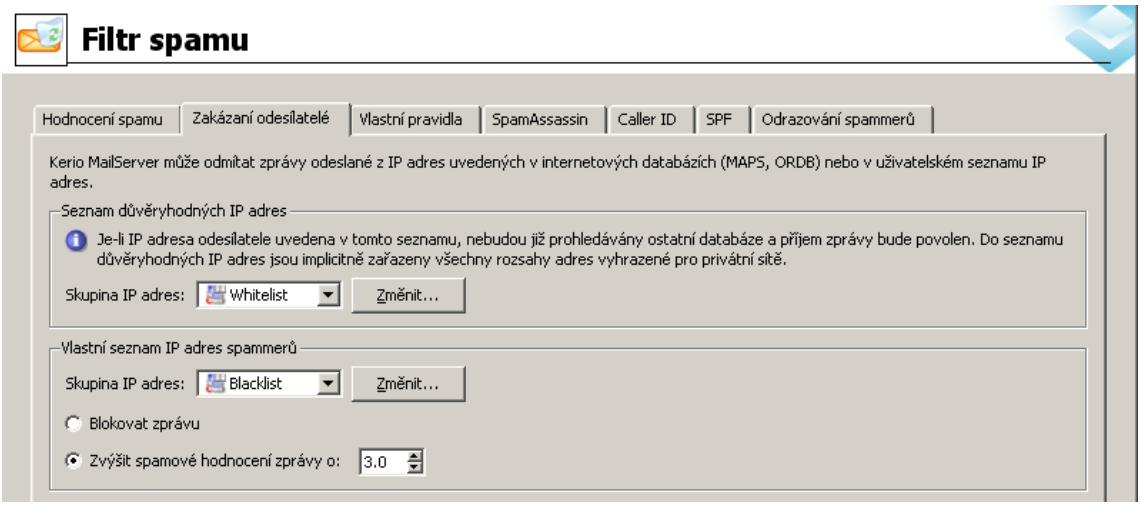
Adresa, na kterou budou zablokované zprávy přeposílány (bez ohledu na další nastavení spamového filtru). V hlavičce každé takové zprávy je zaznamenán seznam testů provedených na zprávě a skóre, které jednotlivé testy přidělily. Pokud se tedy do určené schránky dostane také legitimní zpráva, kterou testy zablokovaly, je možné na základě zjištění upravit chování testů tak, aby se situace příště neopakovala a zpráva se v pořádku dostala k uživateli.

Pro tento případ doporučujeme založit speciální schránku (například `spam@firma.cz`), kam budou kopie spamů doručovány.

16.2 Zakázaní odesílatelé

Kerio MailServer umožňuje blokovat příjem zpráv ze serverů, o nichž bylo zjištěno, že rozesílají nevyžádané e-maily. Přitom umí využít veřejné internetové databáze těchto serverů nebo databáze vlastní.

Definice parametrů této ochrany se provádí v sekci *Konfigurace* → *Filtr spamu*, záložka *Zakázaní odesílatelé*:



Obrázek 16.2 Zakázaní odesílatelé

Seznam důvěryhodných IP adres (whitelist)

Do databází spammerů (tzv. blacklistů) se mohou dostávat také servery doručující legitimní poštu. To se může stát poměrně snadno (například pokud není SMTP server dostatečně zabezpečen, spammer ho může zneužít k rozesílání spamu), a proto *Kerio MailServer* obsahuje seznam důvěryhodných IP adres (whitelist), kam lze zadávat IP adresy serverů, ze kterých chceme poštu přijímat i přesto, že jsou obsaženy v některém z blacklistů, který *Kerio MailServer* využívá ke kontrole pošty. Zprávy ze serverů zařazených do whitelistu nebudou testovány proti nastaveným blacklistům. Ostatní typy nastavených antispamových testů se však na ně vztahovat budou.

Pro založení whitelistu je třeba založit novou skupinu IP adres. Toto lze provést tlačítkem *Změnit*. Otevře se dialog, kde je možné vytvořit vlastní skupinu IP adres SMTP serverů (případně uživatelů).

Poznámka: Do whitelistu jsou standardně zařazeny všechny rozsahy IP adres vyhrazené pro privátní sítě:

`127.0.0.1`

`10.0.0.0/8`

`172.16.0.0/12`

`192.168.0.0/16`

Přesto, že jsou rozsahy privátních IP adres implicitně zařazeny do whitelistu, jsou na rozdíl od veřejných adres kontrolovány ještě proti blacklistu (*Vlastní seznam IP adres spammerů*). Důvodem je možnost potřeby některou z nich zakázat.

Vlastní seznam IP adres spammerů (blacklist)

Zde je možno vybrat vlastní skupinu IP adres SMTP serverů (případně uživatelů), o nichž víte, že rozesílají nevyžádanou poštu. Tlačítkem *Změnit* lze vybranou skupinu upravit nebo vytvořit novou.

Zprávu odeslanou ze SMTP serveru umístěného na seznamu spammerů je možno blokovat nebo jí zvýšit spamové hodnocení:

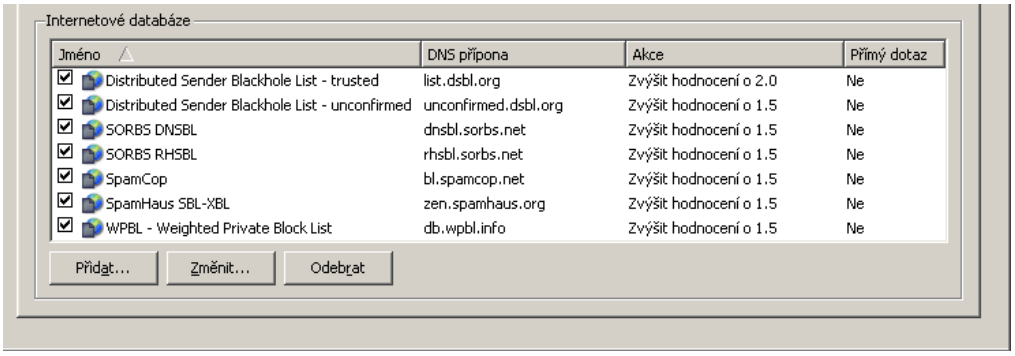
- *Blokovat zprávu*
  Zpráva bude blokována na SMTP úrovni a odesílateli dorazí oznámení o nemožnosti doručení zprávy příjemci.
- *Zvýšit spamové hodnocení zprávy o:*
  Nastavené spamové hodnocení bude připočteno k hodnocení zprávy.
  Doporučenou hodnotou pro skóre je v případě blacklistu 1 — 4 body.

Internetové databáze

Správce *Kerio MailServeru* může využívat různé internetové databáze spammerů (zdarma nebo placených). Databáze spammerů obsahují seznam SMTP serverů, které rozesílají spam. Internetových databází spammerů je více. Některé jsou dostupné zdarma a za některé je třeba platit. Obecně platí, že placené databáze poskytují kvalitnější služby a SMTP servery v jejich databázích ve velké většině opravdu rozesílají spam.

Internetové databáze spammerů jsou vzájemně nezávislé a je možné jich použít více současně.

Kerio MailServer standardně obsahuje několik databází, které jsou na Internetu k dispozici zdarma. Samozřejmě lze definovat jiné libovolné databáze. K tomuto účelu slouží dialog *Internetová databáze* (viz obrázek 16.4), který lze otevřít tlačítkem *Přidat* umístěným pod seznamem databází. Dialog obsahuje následující možnosti nastavení:



Obrázek 16.3 Internetové databáze

DNS doména

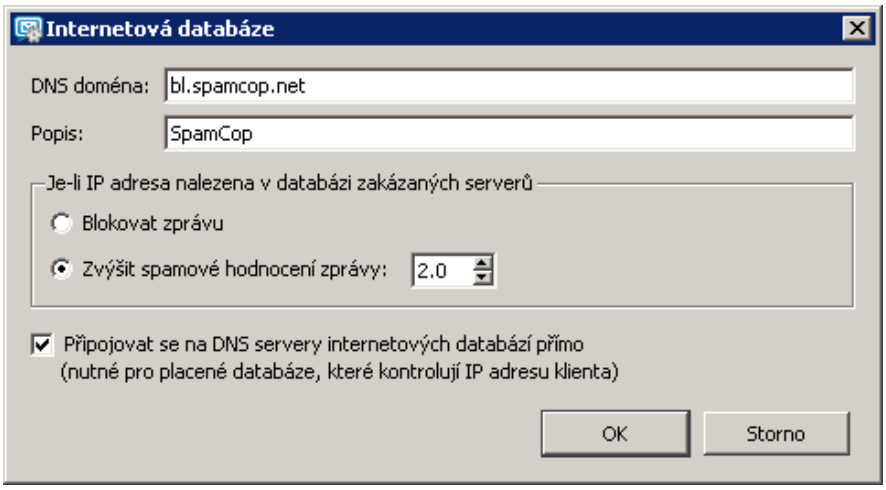
Do pole se doplňuje název DNS serveru, kterého se *Kerio MailServer* ptá.

Popis

Libovolný popis, nepovinná položka.

Blokovat zprávu

Připojí-li se ke *Kerio MailServeru* server nalezený v blacklistu, bude spojení s ním blokováno. Zpráva nebo zprávy nebudou do *Kerio MailServeru* přijaty. Zároveň budou odesílatelům doručována oznámení o nemožnosti přijetí zprávy.



Obrázek 16.4 Nastavení databáze

Zvýšit spamové hodnocení zprávy

Zprávy přijaté ze serveru, jehož název je umístěn v tomto blacklistu, budou mít zvýšené antispamové skóre o nastavenou hodnotu.

Doporučenou hodnotou pro skóre je v případě blacklistu 1 — 3 body. Hodnota přiděleného skóre závisí na důvěryhodnosti dané databáze. Obecně platí, že placené databáze spammerů si více ověřují, zda hlášený SMTP server skutečně rozesílá spam. Proto v případě placených databází si můžeme dovolit nastavit více bodů než u databází, které jsou poskytovány zdarma. To je ovšem

jen obecné pravidlo a výjimka jej může potvrzovat. Pokud máte s některou z databází poskytovaných zdarma výborné zkušenosti, můžete skóre nastavit vyšší.

Pokud používáte více databází spammerů najednou, nastavte nižší hodnotu spamového skóre, protože SMTP server se může vyskytovat ve více databázích zároveň a skóre ze všech databází se sčítá.

Připojovat se na DNS servery...

Doporučujeme zapnout v případě, že *Kerio MailServer* využívá placenou databázi spamserverů, jehož licence je vázána na konkrétní IP adresu. Dotazy na databázi se budou doručovat přímo, při doručování nebudou využívány nadřazené DNS servery.

Poznámka: Pokaždé, když adresa odesílatele doručené zprávy vyhovuje některému z nastavených blacklistů, objeví se tato informace v záznamu *Security* (více viz kapitolu 22.4).

Z toho vyplývá, že pokud si chcete otestovat spolehlivost nového blacklistu, zadejte ho do seznamu a do položky *Zvýšit spamové hodnocení zprávy* zadejte hodnotu 0. Zprávy nebudou nijak ovlivněny blacklistem a zároveň bude každá zpráva, která blacklistu vyhovuje, uvedena v záznamu *Security*.

Podporované databáze

SpamCop

Kerio MailServer podporuje databázi IP adres spammerů SpamCop. Více informací o SpamCop lze najít na stránkách `http://www.spamcop.net/`

SORBS

Spam and Open Relay Blocking System (SORBS) vytváří a udržuje sadu databází IP adres a doménových jmen spammerů. *Kerio MailServer* standardně obsahuje dvě agregované zóny databází spammerů, které obsahují všechny základní dílčí databáze zaměřující se na konkrétní typy serverů, ze kterých je šířen spam:

- *SORBS-DNSBL* — databáze IP adres spammerů.
- *SORBS-RHSBL* — databáze doménových jmen spammerů.

Více informací o SORBS lze najít na stránkách `http://www.de.sorbs.net/`

SpamHaus SBL-XBL

Databáze SpamHaus SBL-XBL spojuje klasickou databázi IP adres spammerů a databázi IP adres ilegálních "exploitů" třetích stran:

- *Spamhaus Block List* — SBL je databáze IP adres rozesílatelů spamu. Každý z těchto serverů je testován, zda se opravdu jedná o server, který rozesílá spam.
- *Spamhaus Exploit Block List* — XBL je databáze IP adres nelegálních exploitů třetích stran, včetně otevřených proxy serverů, červů/virů obsahujících škodlivý spustitelný kód a další typy trojských koní.

Více informací o SpamHAUS SBL-XBL lze najít na stránkách `http://www.spamhaus.org/`

Weighted Private Block List

Weighted Private Block List (WPBL) je databáze IP adres spammerů, kterou spravuje skupina členů, která vyhledává a posuzuje servery rozesílající spam. Databázi spamu, kterou tato skupina generuje, je volně k dispozici. Více informací o WPBL lze najít na stránkách `http://www.wpbl.info/`

Distributed Sender Blackhole List

Distributed Sender Blackhole List (DBSL) databází existuje několik typů, *Kerio MailServer* standardně obsahuje dva:

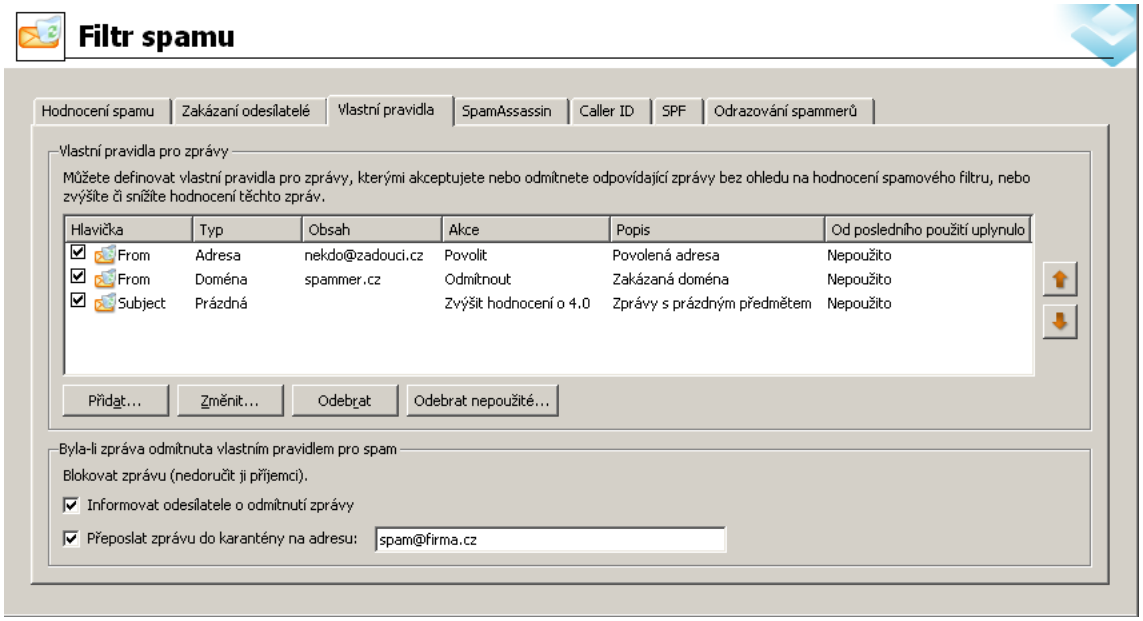
- *Distributed Sender Blackhole List — trusted* — seznam obsahuje všechny servery využívající jednostupňový relay pro rozesílání spamu. Každý z těchto serverů je testován, zda se opravdu jedná o server, který rozesílá spam.
- *Distributed Sender Blackhole List — unconfirmed* — seznam obsahuje všechna oznámení o serverech rozesílajících spam. Vyskytují se zde i servery, které nejsou ověřeny důvěryhodnými testery. Doporučujeme tomuto blacklistu nastavit nižší skóre.

Více informací o DSBL lze najít na stránkách `http://dsbl.org/`.

16.3 Vlastní pravidla

V případě, že vám vnitřní mechanizmy antispamového filtru *Kerio MailServeru* nestačí, lze pomocí ručně nastavených pravidel vytvořit filtr vlastní a upravit tak funkci celého spamového filtru. K tomuto účelu slouží záložka *Vlastní pravidla*.

Záložka se skládá ze dvou částí. První obsahuje seznam pravidel a nástroje pro jejich definici. Ve druhé části je možné nastavit, co má aplikace provést s těmi zprávami, které byly na základě definovaných pravidel serverem odmítnuty.



Obrázek 16.5 Vlastní pravidla

Nastavení pravidel

Každé filtrovací pravidlo se v záložce zobrazuje na jedné řádce (viz obrázek 16.5). Vlevo vedle pravidla je umístěno zaškrtávací pole, kterým lze pravidlo povolit či zakázat. Tímto způsobem je možné pravidlo dočasně vyřadit z činnosti, aniž by bylo nutné ho mazat, a poté znovu přidávat.

Při vytváření pravidel je třeba dbát na jejich pořadí. Jednotlivá pravidla jsou totiž serverem vykonávána v takovém pořadí, v jakém jsou umístěna v seznamu pravidel ve směru od shora dolů. Aby bylo možno pravidla po jejich vytvoření správně zařadit, jsou po pravé straně okna umístěny šipky. Těmito šipkami je možno každé z pravidel po označení kurzorem posunout v seznamu nahoru nebo dolů.

Kromě šipek lze pravidla posouvat také metodou Drag&Drop. To znamená, že lze pravidlo chytit kurzorem myši a přesunout ho na správné místo.

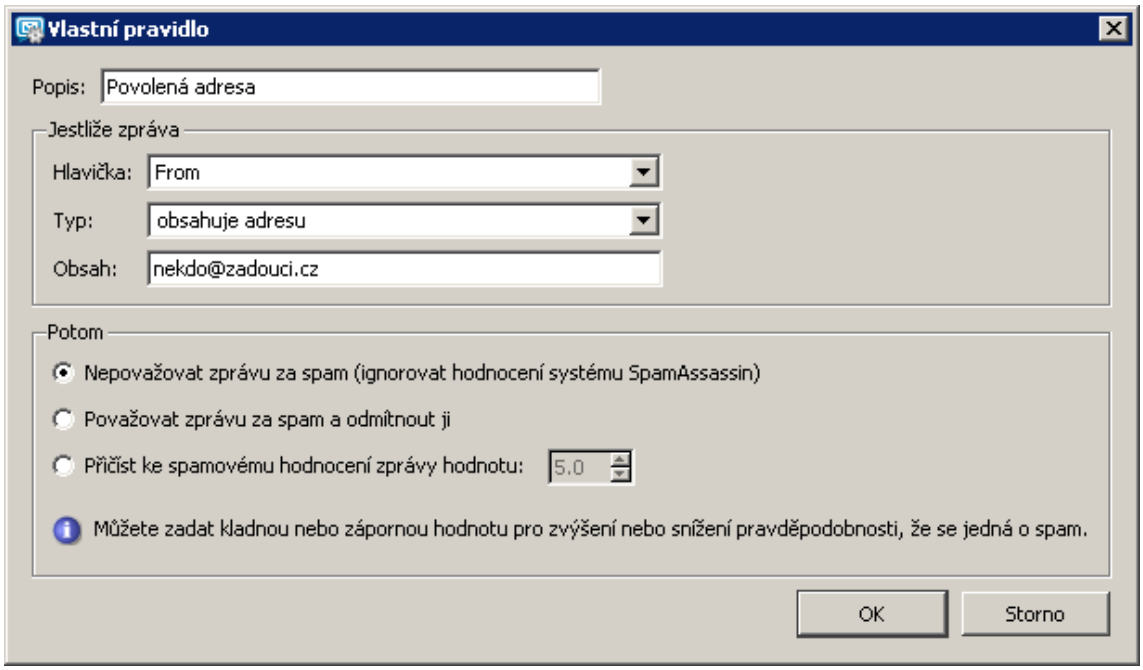
Správné řazení pravidel je nezbytně důležité zejména pro povolovací a zakazovací pravidla, protože po jejich vykonání již další pravidla nebudou brána v úvahu. Po pravidlech, která pouze zvyšují nebo snižují spamové skóre, jsou postupně vykonávána další pravidla v pořadí, dokud nejsou použita všechna, nebo dokud zpráva nevyhoví dalšímu povolovacímu nebo zakazovacímu pravidlu.

Poznámka: Pravidla testovaná proti hlavičkám `From` a `To` mají navíc jednu zvláštnost, respektive výhodu. Pokud tato pravidla umístíme před všechna ostatní, budou testována již na úrovni SMTP komunikace. U zakazovacích pravidel je potom zpráva vyhovující takovému pravidlu odmítnuta ještě před přijetím do fronty příchozích zpráv. Tímto

drobným opatřením lze snížit zatížení serveru, protože se server nemusí zprávou dále zabývat. To se týká zejména dalších testů antispamu a antivirové kontroly, která by na zprávě byla provedena po přijetí do fronty zpráv. Pro povolovací pravidla platí, že pokud jsou testována na úrovni SMTP komunikace, nejsou na ně aplikována ostatní pravidla. Podrobně je princip testování hlaviček vysvětlen níže v textu (položka *Hlavičky*).

Tlačítka *Odebrat* a *Odebrat nepoužité* umožňují vymazání pravidel ze seznamu.

Stisknutím tlačítka *Přidat* (resp. *Změnit*) se zobrazí dialog pro definici či úpravu pravidla.



Obrázek 16.6 Definice pravidla

Filtrovací pravidlo se skládá z následujících položek:

Popis
: Textový popis pravidla (pro snazší orientaci).

Hlavička
: Testovaná položka hlavičky e-mailu. Je možno vybrat z několika předdefinovaných (`From`, `To`, `Cc`, `Subject` a `Sender`) nebo zadat vlastní (např. `X-Mailer`). Zadává se vždy pouze název hlavičky bez dvojtečky.

  Položky `From` a `To` se od ostatních uvedených mírně liší. Tyto položky jsou testovány jak proti hlavičkám `From` a `To` v e-mailu, tak proti hlavičkám obsaženým v SMTP obálce. Položka `From` je testována proti `MAIL FROM:` a položka `To` proti `RCPT TO:`. Všechny ostatní položky jsou testovány pouze proti hlavičkám uvedeným přímo v e-mailu.

Z výše uvedeného vyplývá několik skutečností:
Na zprávy odmítnuté již na úrovni SMTP komunikace se nevztahují žádná další nastavení pro odmítnuté zprávy. Každá zpráva vyhovující zakazovacímu pravidlu bude zamítnuta se standardním chybovým kódem 553 (kód značí, že jde o trvalou chybu, a SMTP server se proto již nebude pokoušet zprávu doručit) a odesílateli bude doručena DSN zpráva.
Na pravidla na položky *From* a *To* se vztahuje zvláštní výjimka při řazení v seznamu pravidel (viz výše v textu). Pokud jsou pravidla *From* a *To* v seznamu umístěna na prvních místech a není před nimi žádné jiné pravidlo, jsou vykonávána proti hlavičkám `MAIL FROM:` a `RCPT TO:` na úrovni SMTP. Jakmile se před těmito pravidly objeví jediné, které se testuje proti jiné hlavičce, zpráva je automaticky přijata do fronty příchozích zpráv a pravidla *From* a *To* jsou testována proti hlavičkám `From:` a `To:` uvnitř zprávy.
Pro lepší pochopení problému si na toto téma uvedeme několik příkladů:

- *Příklad 1*
  První příklad (viz tabulku 16.1) zobrazuje pravidla seřazená tak, aby všechny zprávy odeslané z adresy `jnovak@nezadouci_domena.cz` byly propuštěny do *Kerio MailServeru*. Zároveň budou všechny ostatní zprávy z domény `nezadouci_domena.cz` zamítány na SMTP úrovni. Třetí pravidlo povoluje na SMTP úrovni všechny zprávy doručované do lokální domény `firma.cz`.
  Upozornění: Před spamovým testem na vlastní pravidla jsou aplikovány tyto typy testů:
  - *Odrazování spammerů*
  - *Caller ID* a *SPF*
  - Whitelisty/Blacklisty

  To znamená, že každá zpráva s adresou odesílatele `jnovak@nezadouci_domena.cz` musí nejprve projít těmito testy. Pokud není žádným z výše vyjmenovaných testů zablokována, a projde až k vlastním pravidlům, uplatní se povolovací pravidlo a na zprávu již nebudou aplikovány žádné další testy (respektive výsledky případných dalších testů budou nastaveny na 0 bodů).

Hlavička	Typ	Obsah	Akce
From	Adresa	jnovak@nezadouci_domena.cz	Povolit
From	Doména	nezadouci_domena.cz	Odmítnout
To	Doména	firma.cz	Povolit

Tabulka 16.1 Příklad 1

- *Příklad 2*

Druhý příklad (viz tabulku 16.2) je sestaven tak, aby byla na úrovni SMTP zamítána veškerá pošta pro adresu `admin@firma.cz`. Dále bude zamítána všechna pošta z domény `spam.cz` kromě takových zpráv, které mají v hlavičce `Subject` obsažen podřetězec `test`.

Hlavička	Typ	Obsah	Akce
To	Adresa	admin@firma.cz	Odmítnout
Subject	Podřetězec	test	Povolit
From	Doména	nezadouci_domena.cz	Odmítnout

Tabulka 16.2 Příklad 2

Upozornění: Z předchozího nepřímo vyplývá, že při tvoření pravidel je třeba dávat pozor také na nechtěné ovlivnění jednoho pravidla jiným. To se může stát například tehdy, když jsou uživatelé přihlášení do e-mailových konferencí a adresy v `MAIL FROM:` a `RCPT TO:` neodpovídají adresám v hlavičkách `From` a `To` uvnitř zprávy.

Typ

Typ podmínky, na níž bude položka testována. Možné typy jsou:

- *Je prázdná* — položka je prázdná.
- *Chybí* — zpráva neobsahuje uvedenou hlavičku.
- *Obsahuje adresu* — obsahuje konkrétní e-mailovou adresu.
- *Obsahuje doménu* — všechny e-mailové adresy z této domény. Do tohoto pole je nutné zadat poštovní doménu, to znamená celou část e-mailové adresy umístěné vpravo od znaku `@`.
- *Obsahuje řetězec* — obsahuje konkrétní znaky (slovo, text, číslo...).
- *Obsahuje binární data* — podmínka obsahuje konkrétní znaky podobně jako řetězec, navíc ovšem umožňuje použití binárních dat, která spam může obsahovat. Binární data jsou znaky, které v každé znakové sadě znamenají něco jiného (v češtině například ů, ř atd.).

Obsah

Požadovaný obsah položky (v závislosti na zvoleném typu).

Po nastavení pravidla je třeba zvolit jednu z následujících akcí:

Nepovažovat zprávu za spam

V případě, že přijímáte zprávy obsahující prvky spamu a nechcete, aby zpráva vyhovující tomuto pravidlu byla jako spam označena, zaškrtněte tuto volbu.

Považovat zprávu za spam a odmítnout ji

Zpráva vyhovující pravidlu bude bez ohledu na spamový filtr označena jako nevyžádaná a bude na ní aplikováno nastavení *Akce*.

Zvýšit spamové hodnocení zprávy o
: Číselné hodnocení zprávy, která vyhoví tomuto pravidlu (čím vyšší číslo, tím menší je možnost, že zpráva přes filtr projde). Číslice, kterou ohodnotíte zprávy vyhovující tomuto pravidlu, bude připočtena k celkovému skóre spamového filtru (záporně ohodnocené pravidlo chrání zprávy před tím, aby byly označeny jako spam).
Doporučenou hodnotou pro skóre je v tomto případě 1 — 3 body.

Příklady:

1. Chceme, aby server blokoval všechny e-maily odesílané z adresy `nekdo@nezadouci.cz`. Zadáme pravidlo, kde se bude testovat položka `From`. Typ podmínky zvolíme *obsahuje adresu* (tj. konkrétní e-mailová adresa) a do položky *Obsah* zadáme požadovanou e-mailovou adresu, tedy `nekdo@nezadouci.cz`. V poli *Hodnocení* buď nastavíme hodnotu, o kterou se má zvýšit spamové skóre, nebo využijeme volbu *Považovat zprávu za spam a odmítnout ji*.

2. Jeden z uživatelů si nechává pravidelně zasílat e-maily s nabídkami. Tyto zprávy jsou odesílány z adresy `info@nabidka.cz` a *SpamAssassin* je klasifikuje jako nevyžádané. Abychom tomu zabránili, vytvoříme pravidlo:

   - *Položka hlavičky* — zvolíme položku `From`
   - *Typ* — zvolíme položku *Obsahuje adresu*
   - *Obsah* — zadáme adresu `info@nabidka.cz`
   - *Přičíst k celkovému hodnocení ...* — nastavíme zápornou hodnotu, která sníží celkové hodnocení zprávy nebo použijeme volbu *Nepovažovat zprávu za spam (ignorovat hodnocení systému SpamAssassin)*.

Byla-li zpráva odmítnuta vlastním pravidlem pro spam

Nastavení se týká pouze těch vlastních pravidel, která mají nastavenu volbu *Považovat zprávu za spam a odmítnout ji*:

Blokovat zprávu (nedoručit ji příjemci)
: Odmítnutá zpráva bude bez upozornění zahozena. Tato akce se neprovede, pokud pravidlo filtruje položky `From` a `To` (více viz výše).

Informovat odesílatele o odmítnutí zprávy
: Server vrátí odesílateli DSN zprávu o nemožnosti doručení e-mailu.
Toto nastavení nedoporučujeme používat, protože většina spamů má falešnou adresu odesílatele. To znamená, že zpráva s informací o odmítnutí nemůže být nikam doručena (adresa, na kterou je práva odeslána vůbec neexistuje). Zprávy s informací o odmítnutí pak zůstávají ve frontě, kde je nutno je buď explicitně smazat, nebo se je server pokouší každých 30 minut odeslat a po lhůtě dvou až třech dnů teprve nedoručitelnou zprávu zahodí.

Přeposlat zprávu do karantény na adresu

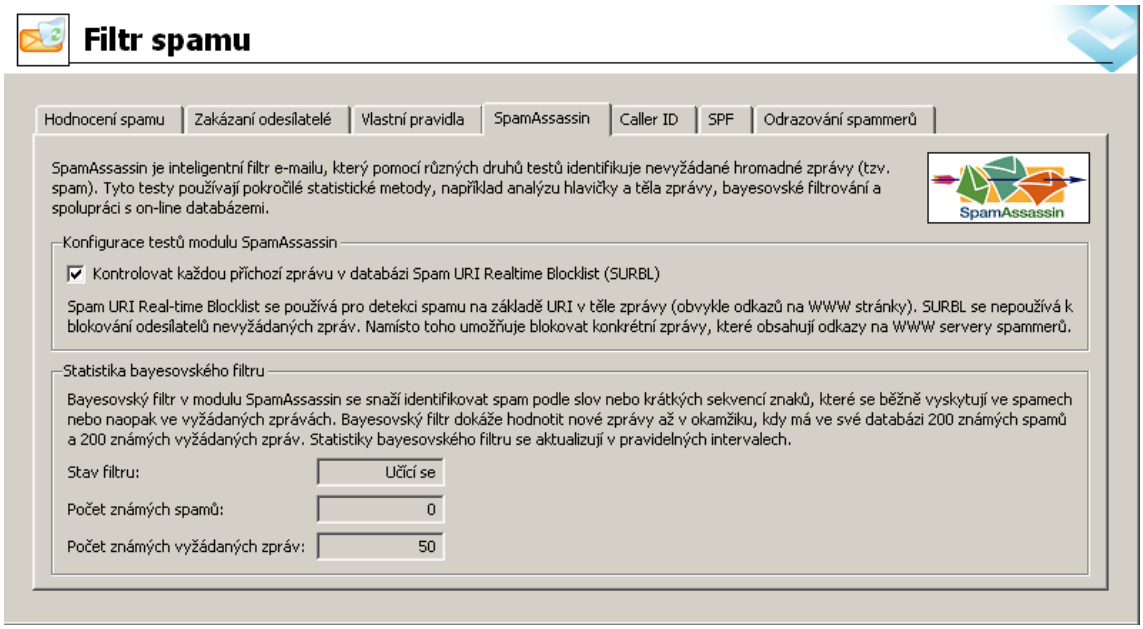
Adresa, na kterou budou označené zprávy přeposílány, a kde si administrátor nebo jiná pověřená osoba může čas od času zkontrolovat, zda mezi spamem není nějaká legitimní zpráva. Tuto volbu doporučujeme použít, aby bez jakéhokoli upozornění (ať už odesílatele nebo příjemce) nezmizel důležitý e-mail.

16.4 SpamAssassin

Kerio MailServer využívá v boji proti spamu také známý antispamový filtr *SpamAssassin*. *SpamAssassin* je složen z několika typů testů:

- filtr založený na statistickém hodnocení obsahu zpráv
- bayesovský filtr
- SURBL (Spam URI Realtime Blocklist) — metoda, která kontroluje případné odkazy na webové stránky umístěné uvnitř mailu proti speciálním on-line databázím.

Poznámka: Při řešení případných problémů se *SpamAssassinem* zapněte v záznamu *Debug* možnost *SpamAssassin Processing*. O záznamu *Debug* se dozvíte více v kapitole 22.8



Obrázek 16.7 SpamAssassin

Hodnocení obsahu zpráv

Filtr hodnocení obsahu zpráv funguje na principu statistického filtrování — podle obsahu zprávy (klíčových slov, počtu velkých písmen v textu, formátu zprávy a podobně) je každé zprávě přiděleno číselné hodnocení (spamové skóre), které čím je vyšší, tím vyšší je počet znaků obvyklých pro nevyžádanou poštu.

Bayesovský filtr

Druhou částí je takzvaný *Bayesovský filtr*. *Bayesovský filtr* je speciální antispamový filtr, který má schopnost se „učit“ co je a co není spam. Filtr sleduje charakteristiky spamu, a pak pro každou zprávu určuje pravděpodobnost, zda je či není nevyžádaná. Tato metoda obsahuje dva typy současně fungujících režimů:

- „Autolearn“ — režim pro vlastní učení spamového filtru.
- „Learn“ — tento režim vyžaduje spolupráci uživatelů. Každý uživatel musí zprávy, které jsou filtrem špatně určené, označit správně, aby se filtr naučil obdobné typy zpráv rozpoznat.

Aby byl filtr funkční, musí nejprve nasbírat vzorek alespoň 200 unikátních spamů a 200 unikátních hamů (legitimních zpráv). Unikátních znamená, že označené zprávy musí být různé. Pokud uživateli chodí každý den ten samý spam, do databáze se dostane pouze jednou. Další výskyty nebudou již brány v úvahu.

Bayesovský filtr sčítá spamy a hamy, které se učí metodami learn a autolearn. Záložka *SpamAssassin* obsahuje statistiku, která vypovídá o tom, kolik zpráv bylo označeno jako spam nebo ham, a zda se filtr ještě učí nebo už je aktivní. I po jeho aktivaci se však filtr samozřejmě učí dál.

Poznámka: SpamAssassin kontroluje pouze zprávy do velikosti 128 KB, neboť spamy mají v drtivé většině menší objem a kontrola příliš velkých e-mailů by zbytečně zatěžovala server.

Protože je v režimu „Learn“ nutné, aby zprávy posuzovali jednotliví uživatelé, musí nástroje na určování špatně rozpoznaných zpráv obsahovat poštovní klienti. Tyto nástroje standardně obsahují pouze *MS Outlook* s *Kerio Outlook Connectorem* a rozhraní *Kerio WebMail*. V těchto dvou případech mohou uživatelé využít speciálních tlačítek na panelu nástrojů, která umožňují označit špatně určenou zprávu.

Pro poštovní klienty s nastavenými IMAP účty a pro *MS Entourage* (platí pro IMAP a Exchange účty) existuje jiné řešení, jak učit bayesovský filtr. Tito uživatelé mohou označovat špatně určené zprávy pomocí přesunutí do určité složky. Chce-li uživatel označit zprávu jako spam, musí ji přesunout do složky *Nevyžádaná pošta* (*Junk E-mail*). Chce-li uživatel označit zprávu jako vyžádanou (byla systémem chybně označena jako spam), musí ji přesunout do složky *Doručená pošta* (*Inbox*).

TIP: Chcete-li tuto metodu využívat efektivně, nastavte uživatelům pravidlo pro nevyžádanou poštu (buď při zakládání uživatelských účtů v *Kerio MailServeru* nebo nastavením příslušného sieve pravidla pro příchozí poštu). Všechny zprávy označené *Kerio MailServerem* jako spam se budou automaticky přesouvat do složky *Nevyžádaná pošta*. Pokud filtr špatně označí zprávu jako spam, uživatel ji ručně přesune do složky *Doručená pošta*. A pokud server omylem propustí spam, uživatel ji ručně přesune do složky *Nevyžádaná pošta*. Tímto způsobem lze zajistit správné a efektivní učení bayesovského filtru.

On-line databáze SURBL

Třetí část filtru kontroluje obsah zpráv (případné odkazy na webové stránky umístěné uvnitř mailu) proti speciálním on-line databázím.

SpamAssassin umí spolupracovat s více on-line databázemi. V *Kerio MailServeru* však využívá pouze SURBL, protože s těmi ostatními již pracuje *Kerio MailServer* v rámci jiných testů.

16.5 Kontrola email policy záznamů

Velké procento nevyžádané pošty obsahuje podvrženou adresu odesílatele. Kontrola „email policy“ záznamů umožňuje odfiltrování zpráv s podvrženou adresou odesílatele.

Kontrola spočívá v možnosti zpětného ověřování IP adresy vzdáleného SMTP serveru, zda je oprávněn pro danou doménu odesílat poštu. Rozesílatelé spamu tak budou nuceni používat svoje skutečné adresy a bude jednodušší nevyžádané zprávy rozpoznat pomocí různých blacklistů.

Kerio MailServer umožňuje kontrolu „email policy“ záznamů pomocí dvou velmi podobných technologií. Tou první je *Caller ID* vytvořené společností *Microsoft*, druhou je open-source projekt nazvaný *SPF* (Sender Policy Framework). Obě technologie umožňují jednoznačné ověření odesílatele zprávy. Ověření funguje na základě zveřejnění IP adres SMTP serverů, které odesílají poštu z dané domény. Pro každou doménu podporující alespoň jednu z technologií je v DNS uložen záznam typu TXT, který obsahuje seznam IP adres serverů odesílajících poštu z dané domény. *Kerio MailServer* po přijetí zprávy porovná IP adresu SMTP serveru s IP adresami obsaženými v tomto DNS záznamu. Takto je pro každou zprávu ověřena důvěryhodnost odesílatele. Pokud DNS záznam neobsahuje IP adresu, ze které byla zpráva odeslána, pak je pravděpodobně zfalšovaná adresa odesílatele a jedná se o spam. Tímto způsobem lze velmi jednoduše rozlišit, zda je zpráva podvržená či nikoliv.

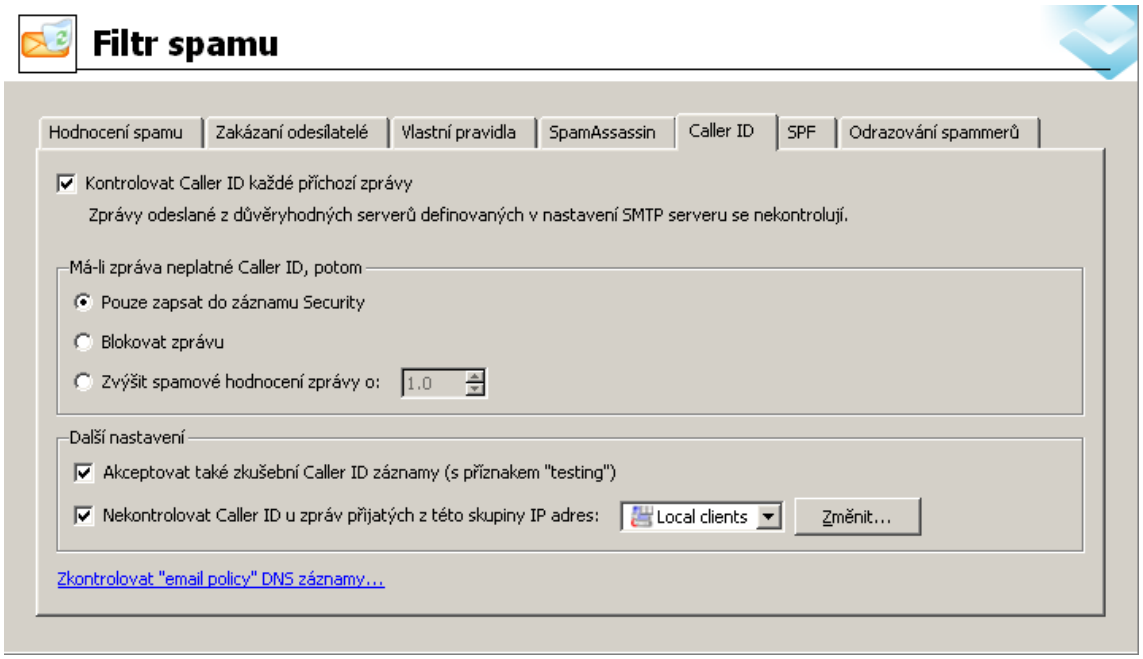
Pošta odeslaná ze serveru, který nemá v DNS záznamu obsažen příslušný seznam s IP adresami, bude vždy doručena. To znamená, že tato pošta pro kontrolu „email policy“ nebude brána v úvahu.

Nastavit *Caller ID* a *SPF* v *Kerio MailServeru* lze ve stejnojmenných záložkách *Caller ID* (*Filtr spamu* → *Caller ID*) a *SPF* (*Filtr spamu* → *SPF*).

Upozornění: SPF i Caller ID lze používat pouze v případě, že je pošta doručována protokolem SMTP. Pokud je pošta stahována z doménového koše pomocí POP3 protokolu, email policy záznamy nebudou fungovat.

Caller ID

Záložka *Caller ID* umožňuje provedení základního nastavení:



Obrázek 16.8 Caller ID

Kontrolovat Caller ID v každé ...
: Volba povoluje/zakazuje použití *Caller ID* kontroly.
V sekci *SMTP server* v záložce *Řízení přístupu* lze nastavit skupinu důvěryhodných IP adres. Zprávám, které byly odeslány z důvěryhodné adresy, nebude *Caller ID* kontrolováno (více viz kapitolu 15.2).

Pouze zaznamenat do záznamu Security
: Zprávy s neplatným *Caller ID* budou pouze zapsány do záznamu *Security*.

Blokovat zprávu
: Zpráva s neplatným *Caller ID* bude blokována na úrovni SMTP komunikace. Odesílateli bude doručeno oznámení o nedoručitelnosti zprávy.

Zvýšit hodnocení zprávy o
: Nastavená hodnota bude připočtena k celkovému hodnocení zprávy (viz sekci 16.1). Doporučená hodnota pro nastavení se v případě metody *Caller ID* pohybuje mezi 1 — 3 body.

Akceptovat také zkušební Caller ID ...
: V současné době technologie *Caller ID* není plně rozšířena. Proto ji mnoho domén používá v testovacím režimu (hlavička XML skriptu v DNS záznamu obsahuje příznak `testing`). Z toho důvodu doporučujeme volbu zapnout. Pokud volba nebude zapnuta, nebude konfigurace brána v úvahu, stejně jako kdyby DNS záznam příslušný XML skript neobsahoval.
Upozornění: Je-li zapnuta tato volba, nenastavujte pro zprávy s neplatným *Caller ID* možnost *Blokovat zprávu*.

Nekontrolovat Caller ID ...
: Volbu lze využít zejména pro nastavení záložních serverů. Pokud je zpráva poslána přes záložní server, IP adresa SMTP serveru neodpovídá doméně uvedené v hlavičkách zprávy, respektive povoleným adresám pro tuto doménu. Proto je nutné, aby zprávy z těchto adres nebyly kontrolovány.
Upozornění: Pokud má být zajištěna plná funkce *Caller ID*, nezařazujte mezi nekontrolované servery jiné než záložní.

Zkontrolovat „email policy“ ...
: Odkaz na stránku na WWW serveru firmy *Kerio Technologies*, kde je možno zkontrolovat DNS záznam „email policy“ pro zadanou doménu.

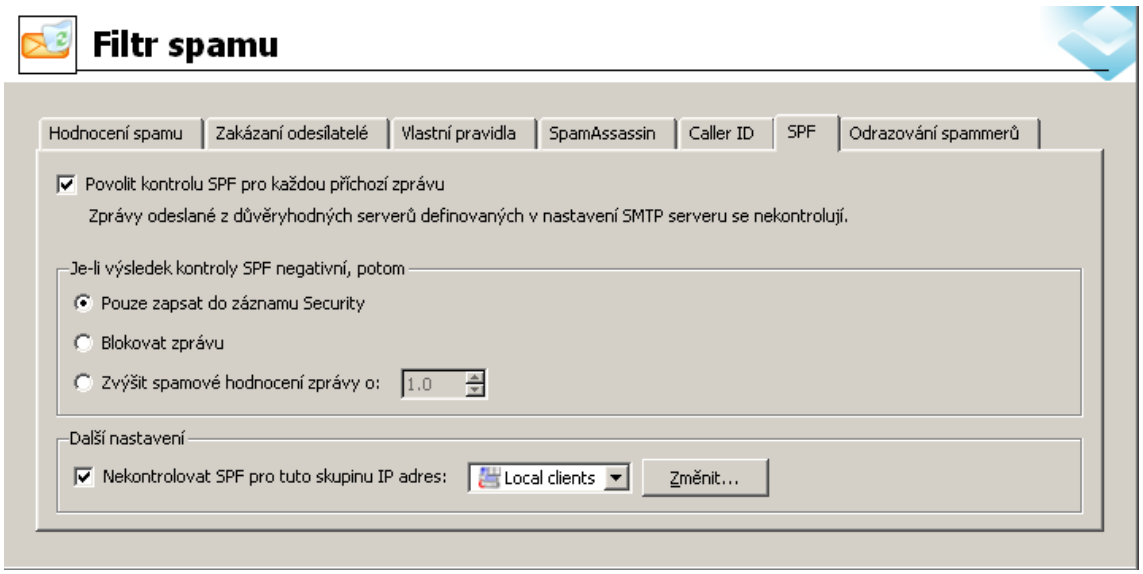
Poznámka: Podrobný návod na správné nastavení DNS záznamu pro *Caller ID* najdete na oficiálních webových stránkách společnosti *Microsoft*.

SPF

SPF je open-source ekvivalent ke *Caller ID* vyvinutým společností *Microsoft*. Obě tyto technologie lze používat v *Kerio MailServeru* zároveň.

Záložka *SPF* umožňuje provedení tohoto nastavení:

Povolit kontrolu SPF pro každou příchozí zprávu
: Volba povoluje/zakazuje použití *SPF*.
V sekci *SMTP server* v záložce *Řízení přístupu* lze nastavit skupinu důvěryhodných IP adres. Zprávy z důvěryhodných IP adres nebudou kontrole SPF podrobeny (více viz kapitolu 15.2).



Obrázek 16.9 SPF

Pouze zapsat do záznamu Security
Zprávy s neplatným *SPF* záznamem budou pouze zapsány do záznamu *Security*.

Blokovat zprávu
Zpráva s neplatným *SPF* záznamem bude blokována na úrovni SMTP komunikace. Odesílateli bude doručeno oznámení o nedoručitelnosti zprávy.

Zvýšit hodnocení zprávy o
Nastavená hodnota bude připočtena k celkovému hodnocení zprávy (viz sekci 16.1). Doporučená hodnota pro nastavení se v případě metody *SPF* pohybuje mezi 1 — 3 body.

Nekontrolovat *SPF* pro tuto skupinu IP adres
Volbu lze využít zejména pro nastavení záložních serverů. Pokud je zpráva poslána přes záložní server, IP adresa SMTP serveru neodpovídá doméně uvedené v hlavičkách zprávy, respektive povoleným adresám pro tuto doménu. Proto je nutné, aby zprávy z těchto adres nebyly kontrolovány.
Upozornění: Pokud má být zajištěna plná funkce *SPF*, nezařazujte mezi nekontrolované servery jiné než záložní.

Poznámka: Podrobnosti o *SPF* kontrole zobrazuje po příslušném nastavení záznam *Debug* (více viz kapitolu 22.8).

16.6 Odrazování spammerů

Jako další z antispamových zbraní nabízí *Kerio MailServer* možnost zpoždění odpovědi na SMTP pozdrav.

Kerio MailServer vyžaduje komunikaci podle RFC (viz slovníček pojmů), která definují komunikaci pomocí protokolu SMTP. Většina aplikací pro automatické rozesílání spamu RFC nedodržují. Díky tomu je *Kerio MailServer* může rozeznat od serverů, které rozesílají legitimní zprávy.

Kerio MailServer využívá k rozpoznání spamových serverů dvě provinění proti příslušnému RFC dokumentu. Tato provinění nastávají již při navazování SMTP spojení. Prvním proviněním je, že server navazující SMTP komunikaci by měl podle příslušného RFC čekat na odpověď po dobu trvající až 5 minut. Aplikace pro automatické rozesílání spamu mají tuto hodnotu značně zkrácenou, protože potřebují rozesílat zprávy pokud možno rychle a ve velkém množství. Dodržování čekací doby by je do značné míry omezovalo. Pokud tedy do určité doby *Kerio MailServer* nevyšle odpověď na SMTP pozdrav (má nastaveno zpoždění odpovědi), chovají se spamující servery obvykle dvěma způsoby. V prvním případě spamující server komunikaci s *Kerio MailServerem* vzdá a pokouší se kontaktovat jiný server. V druhém případě (a to je ono druhé provinění) začne do *Kerio MailServeru* odesílat poštu i bez přijetí SMTP pozdravu (v tomto případě *Kerio MailServer* komunikaci s daným serverem okamžitě ukončí).

Výhody vyplývající z nastavení zpoždění SMTP komunikace jsou dvě:

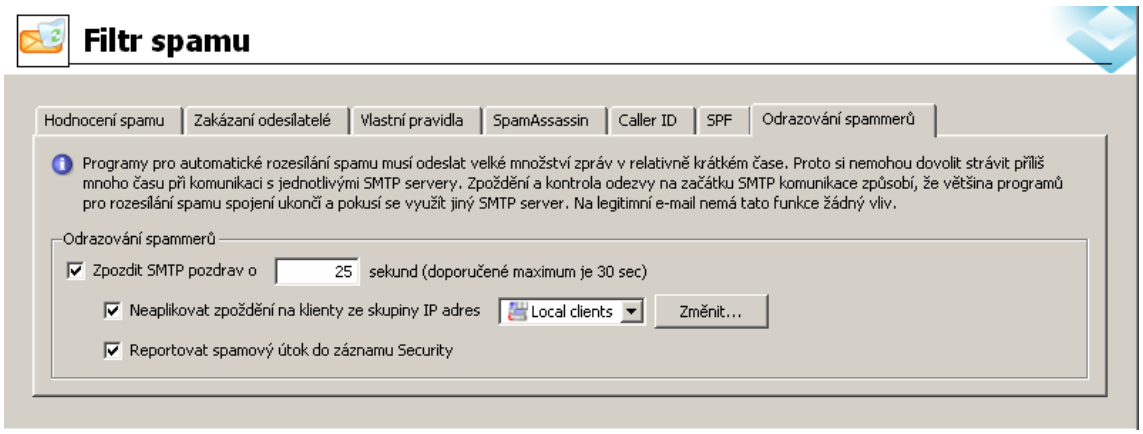
1. Nastavením se sníží příjem spamu do *Kerio MailServeru* o 60 — 70%. Protože jsou spamové testy náročné na výkon, snižuje se tímto opatřením zatížení serveru.

2. Druhou nespornou výhodou je, že tato metoda nepřináší tzv. false positives, neboť nemá žádný vliv na legitimně doručovanou poštu.

Nastavení zpoždění SMTP komunikace

Kerio MailServer ošetřuje zpoždění při navazování komunikace v záložce *Odrazování spammerů* (*Konfigurace* → *Filtrování obsahu* → *Filtr spamu*):

Zpozdit SMTP pozdrav o
: Volbou lze nastavit SMTP zpoždění. Optimální doba tohoto zpoždění je 25-30 sec. Kratší nastavená doba by nemusela stačit (programy pro rozesílání spamu mají obvykle nastavenou dobu 10-20 sec), delší nemá smysl, zbytečně by zdržovala komunikaci.



Obrázek 16.10 Odrazování spammerů

Neaplikovat zpoždění na klienty ze skupiny IP adres

Odrazování spammerů ošetřuje veškerou příchozí SMTP komunikaci, tedy také poštu z lokální sítě, záložních serverů apod. Z toho důvodu doporučujeme do této skupiny IP adres přidat všechny důvěryhodné IP adresy a sítě, aby zpoždění zbytečně nezdržovalo komunikaci v případech, kdy se nepředpokládá, že by se mohlo jednat o spam.

Reportovat spamový útok do záznamu Security

Položka umožňuje zápis všech rozpoznaných pokusů o tento typ útoku do záznamu *Security* (více viz kapitolu 22.4).

Pokud přes *Kerio MailServer* prochází velké množství e-mailů, bude pravděpodobně také vysoký počet pokusů o tento typ útoku, což může přeplnit záznam. V takovém případě zápis do záznamu vypněte.

Poznámka: Nastavení této záložky ošetřuje pouze nezabezpečenou verzi SMTP komunikace. Zabezpečenou verzi protokolu SMTP programy pro automatické šíření spamu nepoužívají.

16.7 Optimální nastavení spamových testů

Tato sekce dobře poslouží všem uživatelům, kteří si nejsou jisti správným nastavením spamových filtrů. Příklad dobře ukazuje, jak správně používat sčítání skóre z různých typů antispamových testů. Všimněte si, že téměř nikdy není preferováno blokování zpráv před nastavením dílčího zvýšení spamového skóre u konkrétního testu:

Hodnocení spamu

Základní a nejdůležitější nastavení, od kterého se posléze odvíjí nastavení ostatních testů, je nastavení záložky *Hodnocení spamu* (podrobnosti viz sekci 16.1). V této záložce vlastně nemusíme mnoho nastavovat, většinu parametrů ponecháme ve výchozím stavu:

1. Zkontrolujeme, zda je zaškrtnuta volba *Povolit hodnocení spamovým filtrem*. Pokud je volba neaktivní, zaškrtneme ji.

   Touto volbou povolujeme filtru, aby bral v úvahu výsledky jednotlivých hodnocení v podobě spamového skóre.

2. Zkontrolujeme, že volba *Povolit hodnocení zpráv odeslaných od důvěryhodných odesílatelů definovaných v nastavení SMTP serveru* je neaktivní (pokud však máte důvod kontrolovat i zprávy z důvěryhodných zdrojů, můžete ji zapnout).

3. Stupnici pro nastavení citlivosti spamového filtru nastavíme následovně:

   - *Hodnota pro označení zprávy* — hodnotu nastavíme na 5 bodů.
   - *Hodnota pro blokování zprávy* — hodnotu nastavíme na 9.9 bodů, aby jen skutečně „stoprocentní“ spamy byly serverem zahazovány, protože ani odesílatel ani příjemce v tomto případě nedostane žádnou zprávu o tom, že zpráva byla blokována (pokud není správcem nastavena alespoň jedna z položek *Informovat odesílatele o odmítnutí zprávy* nebo *Přeposlat zprávu do karantény na adresu*).
     Poznámka: Pokud nechcete, aby zprávy s jakýmkoliv skóre byly blokovány, zadejte do položky 10.0 bodů. Blokování zpráv se vypne a zprávy budou pouze označovány jako spam.

4. Zkontrolujeme, zda je neaktivní volba *Informovat odesílatele o odmítnutí zprávy*.

   Tuto volbu nebudeme využívat, protože většina spamů má v hlavičce neplatnou adresu odesílatele. Odpovědi na spamy by proto nemohly být odeslány a hromadily by se ve frontě odchozích zpráv.

5. Nakonec zaškrtneme volbu *Přeposlat zprávu do karantény na adresu* a doplníme adresu, která bude do nějaké vyhrazené schránky přeposílat všechny zprávy, které mají vyšší skóre než 10.

   Volba je užitečná zejména tehdy, pokud systém antispamové ochrany teprve nastavujeme a vylaďujeme. Pokud se stane, že příliš vysoké skóre bude mít i několik legitimních zpráv, odhalíme je při příležitostné kontrole schránky, do které budou kopie spamů doručovány. Později můžeme tuto volbu vypnout a spamovou schránku zrušit.

Zakázaní odesílatelé

Po nastavení obecného fungování filtru je třeba nastavit také jednotlivé typy testů. První z těchto testů obsahuje záložka *Zakázaní odesílatelé* (podrobnosti viz sekci 16.2). V této záložce nastavíme následující parametry:

1. *Seznam důvěryhodných IP adres* — položku není třeba nastavovat v případě, že nepotřebujeme žádný server vyjmout z antispamové kontroly. Pro náš příklad si ale můžeme vymyslet obchodního partnera, jehož SMTP server se omylem dostal do internetových databází spammerů, a proto je třeba adresu jeho SMTP serveru — alespoň než bude z této databáze vyjmut — do whitelistu nastavit:
   - V *Seznamu důvěryhodných IP adres* vytvoříme novou skupinu IP adres, která se bude jmenovat `Whitelist`. Jak se tvoří skupiny IP adres se dozvíte v sekci 12.1.
   - Do nově vytvořené skupiny zadáme IP adresu SMTP serveru, který se dostal do databáze spammerů. Po uložení nastavení všechny zprávy z nastaveného SMTP serveru nebudou procházet žádnou antispamovou kontrolou.
     Upozornění: Do whitelistu nikdy nezadávejte SMTP server, který by mohl být potenciálním distributorem spamu.

2. *Vlastní seznam IP adres spammerů* — nastavení této volby je obdobné jako v bodě 1, ale má opačný účinek. Po vytvoření příslušné skupiny IP adres do ní doplníme všechny SMTP servery, z nichž je rozesílán spam. A to zejména tehdy, pokud ostatní spamové testy nedokáží spamy z těchto serverů odhalit.

   Nyní pro vlastní seznam IP adres spammerů doplníme, co se má stát se zprávami doručenými ze SMTP serverů na blacklistu:

   - K dispozici máme v záložce *Zakázaní odesílatelé* dvě možnosti. Buď můžeme zprávu zablokovat nebo jí zvýšit spamové hodnocení. My si vybereme volbu druhou a zvýšíme spamové hodnocení zprávy o 3 body. 3 body jsou dostačující pro to, aby zpráva byla označena, pokud je skutečně nevyžádaná, protože se k těmto bodům připojí ještě hodnocení z ostatních testů.

3. *Internetové databáze* — zaškrtneme všechny databáze, které máme k dispozici. Otevřeme pomocí tlačítka *Změnit* postupně každou z databází a nastavíme spamové skóre na 2 body (viz obrázek 16.4).

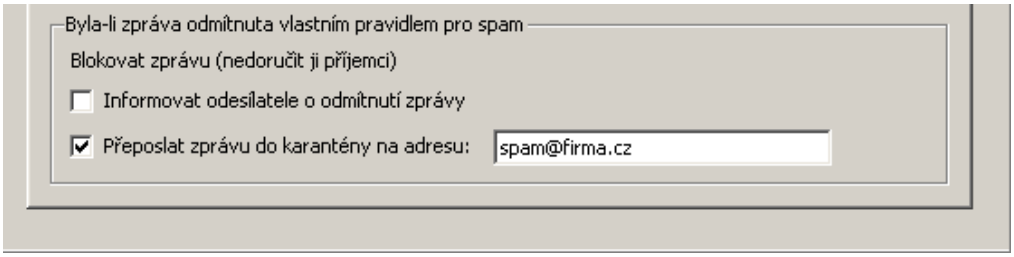
   Doporučení: U internetových databází, zvláště pak těch, které jsou pro použití k dispozici zdarma, nenastavujte blokování zpráv. Tyto databáze nemusí být nutně příliš rychle aktualizovány a informace o spam serverech nemusí být vždy důkladně ověřeny. Na jejich seznam se můžou dostat i nevinné servery. Z toho důvodu používejte tyto typy testů spíše pro zvyšování skóre zpráv.

Vlastní pravidla

Dalším testem pro příchozí zprávy je soubor ručně nadefinovaných pravidel (podrobnosti viz sekci 16.3). Vlastní pravidla lze vytvářet podle aktuální potřeby:

1. Nadefinujeme příslušná pravidla na SMTP servery. Všem pravidlům na nevyžádanou poštu opět pokud možno pouze zvýšíme spamové skóre o 2-3 body. Protože nastavujeme celou sadu testů, tak i ostatní testy, pokud je zpráva spam, připojí kladné skóre.

2. Pokud existuje pravidlo, kterému jsme nadefinovali blokování zpráv, nastavíme pro jistotu adresu, kam budou doručovány kopie blokovaných zpráv (viz obrázek 16.11). Nejlepší je si pro tyto účely vytvořit speciální uživatelskou schránku (jak založit uživatelskou schránku se dozvíte v kapitole 13).



Obrázek 16.11 Přeposlat zprávu do karantény na adresu

SpamAssassin

Spamový filtr *SpamAssassin* není nutné téměř nijak nastavovat. *SpamAssassinu* se věnuje záložka *SpamAssassin* (podrobnosti najdete v sekci 16.4).

Jediné nastavení, které provedeme v záložce *SpamAssassin* je zaškrtnutí volby *Kontrolovat každou příchozí zprávu v databázi Spam URI Realtime Blocklist (SURBL)*.

Caller ID

O technologii *Caller ID* se dozvíte více v kapitole 16.5. Pokud se rozhodnete technologii využívat, pak rozhodně doporučujeme nastavit záložku následujícím způsobem:

1. Otevřeme záložku *Caller ID* (*Konfigurace* → *Filtrování obsahu* → *Filtr spamu*).

2. Zaškrtneme volbu *Kontrolovat Caller ID každé příchozí zprávy*.

3. V sekci *Má-li zpráva neplatné Caller ID, potom* nastavíme spamové hodnocení na 3 body (jak jsme si vysvětlili dříve, pokud je zpráva spam, bude ohodnocena ještě dalšími testy, a proto není nutné zprávu blokovat nebo jí přiznat příliš vysoké skóre).

4. Zaškrtneme položku *Akceptovat také zkušební Caller ID záznamy (s příznakem "testing")*, protože většina serverů, které *Caller ID* technologii využívají, ji zatím má nastavenou na testovací provoz.

5. Používáme-li záložní SMTP server, zadáme jeho adresu do položky *Nekontrolovat Caller ID u zpráv přijatých z této skupiny IP adres*.

SPF

Technologii SPF nám blíže představuje kapitola 16.5. Doporučené nastavení testu SPF je v podstatě totožné s nastavením *Caller ID* a je následující:

1. Otevřeme záložku *SPF* (*Konfigurace* → *Filtrování obsahu* → *Filtr spamu*).

2. Zaškrtneme volbu *Povolit kontrolu SPF pro každou příchozí zprávu*.

3. V sekci *Má-li zpráva neplatné Caller ID, potom* nastavíme spamové hodnocení na 3 body (jak jsme si vysvětlili dříve, pokud je zpráva spam, bude ohodnocena ještě dalšími testy, a proto není nutné zprávu blokovat nebo jí přiznat příliš vysoké skóre).

4. Používáme-li záložní SMTP server, zadáme jeho adresu do položky *Nekontrolovat SPF pro tuto skupinu IP adres*.

Samozřejmě doporučujeme podílet se na *SPF* také aktivně a do svých DNS záznamů doplnit záznam o SMTP serverech, které mají povoleno odesílat poštu z vašich domén.

Odrazování spammerů

O technologii *Odrazování spammerů* v *Kerio MailServeru* se více dozvíte v kapitole 16.6. Na tomto místě se stačí o ní zmínit jen okrajově, protože nemá žádný podíl na hodnocení spamu. Její výhoda spočívá v tom, že dokáže vytřídit mnoho spamu ještě před přijetím do *Kerio MailServeru*, a tak výrazně snižuje zátěž, kterou mohou antispamové testy generovat.

Optimální nastavení *Odrazování spammerů* je následující:

1. Otevřeme záložku *Odrazování spammerů* (*Konfigurace* → *Filtrování obsahu* → *Filtr spamu*).

2. Zaškrtneme volbu *Zpozdit SMTP pozdrav o ... sekund* a do políčka doplníme 25 sekund.

3. Zaškrtneme volbu *Neaplikovat zpoždění na klienty ze skupiny IP adres* a jako skupinu IP adres zvolíme lokální privátní síť. Toto nastavení je důležité proto, aby nebylo

zbytečně zpožďováno odesílání pošty lokálních uživatelů a doručování interních zpráv.

4. Položku *Reportovat spamový útok do záznamu Security* necháme vypnutou (pokud nemáme zvláštní důvod ji zapnout). Zápisy o přerušení SMTP spojení by zbytečně zaplňovaly celý záznam.

16.8 Sledování funkčnosti a účinnosti spamového filtru

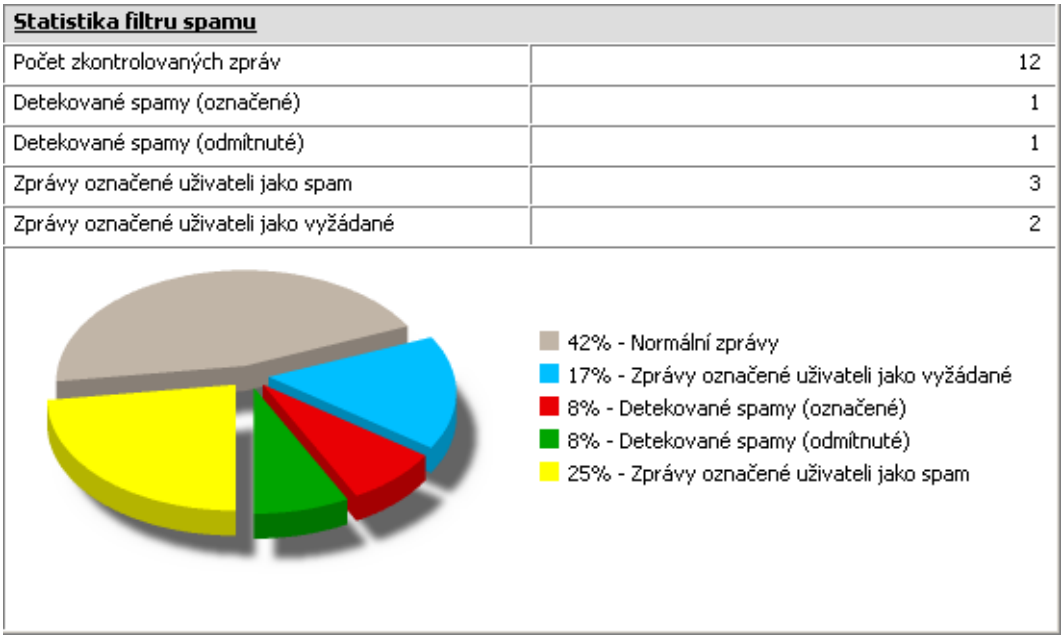
Kerio MailServer obsahuje několik možností, jak sledovat funkčnost spamového filtru. K tomuto účelu lze využít standardních nástrojů, které jsou k dispozici v *Kerio Administration Console*:

Statistika filtru spamu

Kerio MailServer vytváří statistiku spamového filtru. Tato statistika je umístěna spolu s ostatními statistikami v sekci *Stav* → *Statistiky* (viz kapitolu 21.6).

Statistika spamového filtru umožňuje zjistit, jaký je poměr hamu (legitimních zpráv) a spamu přicházejícího do *Kerio MailServeru*. Díky statistice lze snadno rozlišit, zda jsou jednotlivé metody spamového filtru správně nastaveny. Zda do uživatelských schránek neproniká příliš mnoho spamu, či zda není špatně označeno příliš mnoho korektních zpráv jako spam.

Statistika zobrazuje následující položky:



Obrázek 16.12 Statistika filtru spamu

Počet zkontrolovaných zpráv
Součet všech zpráv, které prošly spamovým filtrem (například zprávy doručené z domén ve whitelistu spamovým filtrem vůbec neprocházejí).

Detekované spamy (označené)
Všechny zprávy, které byly filtrem detekovány jako spam.

Detekované spamy (odmítnuté)
Všechny zprávy, které byly filtrem blokovány.

Zprávy označené uživateli jako spam
Zprávy, které spamovým filtrem nebyly rozpoznány jako spam (uživatelé museli zprávy ručně označit pomocí tlačítka *Je to spam* nebo pomocí ručního přesunutí příslušné zprávy do složky *Nevyžádaná pošta*).

Zprávy označené uživateli jako vyžádané
Regulérní zprávy, které byly spamovým filtrem nesprávně označeny jako spam — tzv. „false positives“.

Grafické zobrazení

Kerio MailServer zaznamenává do grafu některé parametry týkající se nevyžádané pošty. Grafů, které se týkají spamu je několik a jsou umístěny spolu s ostatními v sekci *Stav* → *Grafy* v *Kerio Administration Console* (viz kapitolu 21.5).

Grafy, které se týkají spamu, jsou čtyři:

Připojení/Odmítnuté SMTP
Graf zobrazuje v čase, kolik pokusů o SMTP spojení bylo odmítnuto pomocí funkce *Odrazování spammerů*.

Zprávy/Spam
Graf znázorní v čase, kolik spamu je doručováno do *Kerio MailServeru* v jakou dobu.

Záznamy

Při řešení případných problémů se spamovým filtrem lze využít záznamy *Kerio MailServeru*. Záznamům se podrobně věnuje kapitola 22.

Účinně mohou pomoci následující záznamy:

Spam
Do tohoto záznamu se průběžně zapisují všechny zprávy označené jako spam (více viz kapitolu 22.7).

Debug

Speciální záznam, ve kterém lze zapnout logování konkrétních informací. V případě spamu mohou pomoci položky:

- *Spam Filter* — volba zaznamenává hodnocení každé zprávy, která prošla spamovým filtrem *Kerio MailServeru*.
- *SPF Record Lookup* — volba vypisuje informace o *SPF* dotazech na SMTP servery. Lze využít při problémech s *SPF* kontrolou.
- *SpamAssassin Processing* — volba umožňuje sledování procesů, ke kterým dochází při testování zpráv spamovým filtrem *SpamAssassin*.

Kde a jak lze nastavit vypisování konkrétních informací do záznamu *Debug* najdete v kapitole 22.8.

Kapitola 17

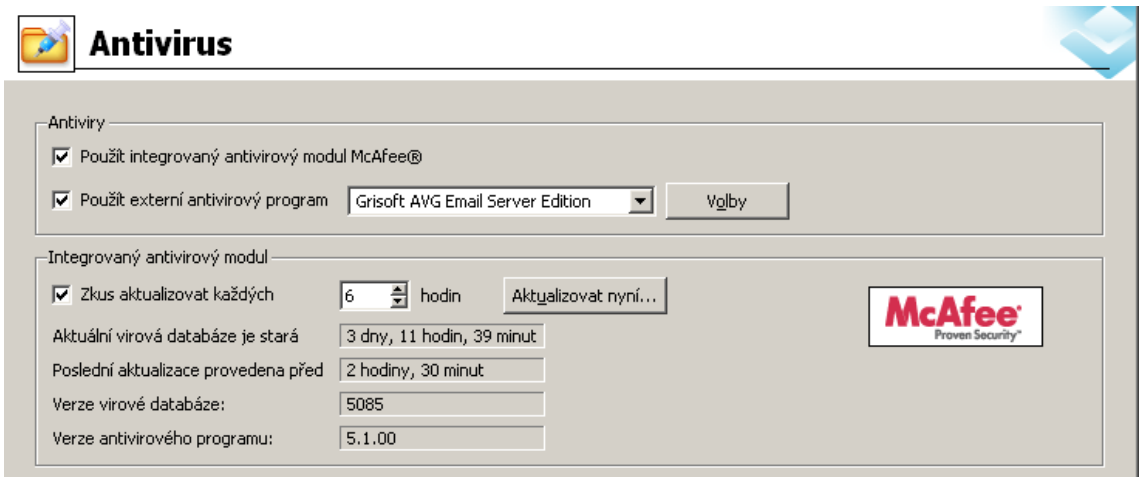
Antivirová kontrola a filtrování příloh

Kerio MailServer umožňuje nastavit antivirovou kontrolu všech příchozích zpráv. Tuto kontrolu lze provádět dvěma kombinovatelnými způsoby. První možností je využití integrovaného antivirového programu *McAfee*, druhá možnost spočívá v použití některého z podporovaných externích antivirů.

Bezprostředně po instalaci *Kerio MailServeru* je automaticky spuštěn integrovaný antivir *McAfee*. K němu je možné zapnout některý z podporovaných externích antivirů. Oba antiviry mohou být spuštěny současně. Dvojnásobná ochrana proti virům bude spolehlivěji chránit vaši lokální síť, protože bude zajišťovat rychlejší aktualizaci virových databází (jeden z antivirů může zareagovat na nově se šířící vir až o několik hodin rychleji než druhý), rychlost aktualizací proti novým virům je v ochraně proti infikované poště klíčová.

Samozřejmě je možné oba antiviry vypnout, ale tuto možnost důrazně nedoporučujeme, protože v tomto případě nebude uživatel před infikovanou poštou chráněn.

Kerio MailServer nezávisle na antiviru kontroluje v přílohách JPG souborů, zda nejsou poškozeny a neobsahují exploit pro knihovnu GDI+ (škodlivý kód způsobující pád operačního systému často navíc doplněný virem, který může exploit spustit při pádu systému). Všechny zprávy s takovou přílohou budou automaticky zahozeny.



Obrázek 17.1 Antivirus

Kromě spolupráce s antivirovým programem nabízí *Kerio MailServer* také možnost filtrování určitých typů e-mailových příloh (dle přípony souboru nebo MIME typu), bez ohledu na to, zda jsou virem infikovány, či nikoliv. Tato nastavení se provádějí v sekci *Konfigurace → Filtrování příloh*.

17.1 Integrovaný McAfee Anti-Virus

Chcete-li používat integrovaný antivirus, zaškrtněte v sekci *Antivirus* volbu *Použít integrovaný antivirový modul McAfee*.

Poznámka: Externí *McAfee Anti-Virus Kerio MailServer* nepodporuje.

Zkus aktualizovat každých

Nastavení intervalu automatické aktualizace virové databáze a vlastního antivirového programu (v hodinách). Informace o provedených aktualizacích naleznete v záznamu *Security* (viz kapitolu 22.4).

Poznámka: Automatická aktualizace vyžaduje funkční připojení do Internetu a nepodporuje automatické vytáčení. V případě vytáčené linky je vhodné provádět aktualizaci ručně (viz dále).

Aktualizační soubory se stahují standardním protokolem HTTP. Je-li ve vaší síti firewall nebo proxy server, nastavte jej tak, aby nebyla HTTP komunikace blokována (z počítače, kde *Kerio MailServer* běží).

Tlačítko *Aktualizovat nyní* umožňuje manuální spuštění aktualizace virové databáze a antivirového programu. Po stisknutí tohoto tlačítka se zobrazí okno znázorňující průběh aktualizace. Informace o provedených aktualizacích naleznete v záznamu *Security* (viz kapitolu 22.4).

Poznámka: Okno zobrazující průběh aktualizace je možno kdykoliv zavřít stisknutím tlačítka *OK* (není třeba čekat, až bude aktualizace dokončena).

Aktuální virová databáze je stará

Doba od poslední úspěšné aktualizace virové databáze (s přesností na minuty).

Poslední aktualizace provedena před

Doba, která uplynula od posledního úspěšného pokusu o aktualizaci. Nezáleží na tom, zda byla na serveru nová verze k dispozici, či nikoliv.

Upozornění: Je-li tato doba výrazně (několikanásobně) větší než nastavený interval automatické aktualizace, znamená to, že automatická aktualizace neprobíhá korektně. V tomto případě doporučujeme provést aktualizaci ručně a věnovat pozornost informacím v záznamech *Error* a *Security*.

17.2 Výběr externího modulu pro spolupráci s antivirovým programem

K nastavení parametrů antivirové kontroly slouží sekce *Konfigurace* → *Filtrování obsahu* → *Antivirus*. Pro použití externího antiviru je nutno zaškrtnout volbu *Použít externí antivirový program*. Volba obsahuje menu, které zobrazuje antivirové programy, které mohou být použity pro kontrolu pošty. Antivirový program musí být nainstalován dříve, než jej zde vyberete (před instalací antivirového programu doporučujeme zastavit službu *Kerio MailServer Engine*).

Může se stát, že nainstalovaný antivirus nebude automaticky spuštěn. V takovém případě můžete použít tlačítko *Volby*, které obsahuje možnost speciálního nastavení externího antiviru.

Upozornění: V případě výběru externího antiviru *Symantec Antivirus Scan Engine* je nutné zadat v okně *Volby* IP adresu a port počítače, kde je antivirus spuštěn.

Základní podmínky pro úspěšné spuštění antivirového programu jsou následující:

- Antivirový program musí být nainstalován na stejném počítači, kde je spuštěn *Kerio MailServer*.
- Licence antivirového programu musí splňovat licenční podmínky dané jeho výrobcem (typicky stejný nebo vyšší počet uživatelů, pro který je licencován *Kerio MailServer*, nebo speciální serverová licence).

Rozhraní mezi *Kerio MailServerem* a antivirovým programem vytvářejí speciální moduly (pro každý antivirus jeden modul). Správce poštovního serveru musí vybrat odpovídající modul podle toho, jaký antivirus chce pro kontrolu pošty používat. Bude-li nastaven určitý modul a odpovídající antivirus nebude nainstalován nebo nebude fungovat správně, *Kerio MailServer* administrátorovi nedovolí uložit toto nastavení. V záznamu *Error* se objeví chybové hlášení, že antivirová kontrola nefunguje.

Poznámka: Existují dvě výjimky z tohoto chování. Byl-li špatně proveden přenos konfigurace *Kerio MailServeru* (více viz kapitolu 28.2), nebo byl-li počet zakoupených uživatelských licencí v antiviru nižší než počet licencí *Kerio MailServeru*. V obou popsaných případech *Kerio MailServer* normálně funguje, ale přestanou se odesílat zprávy. Zprávy se neodesílají z toho důvodu, že *Kerio MailServer* je chce při přijetí kontrolovat antivirem, který nefunguje. V záznamu *Error* se objeví chybové hlášení, že antivirová kontrola není funkční.

Pro správnou spolupráci *Kerio MailServeru* a antivirového programu je nutné v rezidentním štítu antiviru vytvořit výjimku na adresář `store` (nebo v případě starších verzí některých antivirových programů na soubory `*.eml`), aby zprávy nebyly rezidentním štítem kontrolovány.

Je-li rezidentní štít nastaven špatně, pak se otevře okno s varovným hlášením, že nelze navázat spojení s externím antivirem. Zároveň rezidentní štít antiviru objeví virus `eicar.com` (testovací virus, který programově generuje *Kerio MailServer* pro kontrolu správného nastavení výjimky v rezidentním štítu).

17.3 Nastavení některých externích antivirových modulů

Kerio MailServer podporuje několik externích antivirových programů různých výrobců (např. *NOD32*, *Grisoft*, *Sophos Antivirus* atd.) pro operační systémy *Windows*, *Mac OS X* a *Linux*. Skupina podporovaných antivirů, stejně jako verze jednotlivých programů a obchodní podmínky, se však mohou často měnit, a proto tyto informace firma *Kerio Technologies* uveřejňuje pouze na WWW stránkách (`http://www.kerio.cz/`), kde jsou pravidelně aktualizovány.

Zde najdete několik poznámek ke zvláštnostem a případnému nastavení externích antivirů:

Symantec Scan Engine

Jedním z podporovaných antivirů je *Symantec Scan Engine* od firmy *Symantec*. Od verze *Kerio MailServer 6.1.2* byla provedena změna komunikačního protokolu mezi *Kerio MailServerem* a *Symantec Scan Engine* verzí 4 a 5. Původně spolu obě aplikace komunikovali pomocí protokolu Native, nyní používají protokol ICAP. Z tohoto důvodu je nutné v nastavení SAVSE přepnout protokol v *Configuration* → *Protocol* → *ICAP*.

Clam AntiVirus

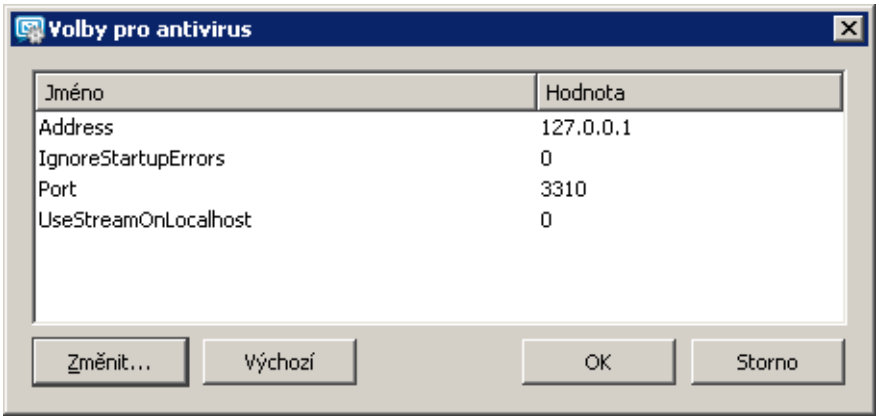
Kerio MailServer podporuje antivirus *Clam AV* pro linux, Mac OS X i pro Windows.

Upozornění: Clam AV existuje pro Windows ve dvou základních verzích, z nichž lze použít pouze *Clam AV for Windows* (také *ClamAV-win32*). Verze *ClamWin Antivirus* není ze strany *Kerio MailServeru* podporována). Produkt *Clam AV for Windows* lze získat zdarma na stránkách `http://www.sosdg.org/`.

Aby byla spolupráce *Clam AV* a *Kerio MailServeru* úplně funkční, je třeba zajistit následující:

- Komunikace mezi antivirem a *Kerio MailServerem* musí probíhat přes síťový socket (lze nastavit v konfiguračním souboru antiviru).
- V administrační konzoli *Kerio MailServeru* (*Konfigurace* → *Filtrování obsahu* → *Antivirus* → *tlačítko Volby*) v nastavení antiviru (viz obrázek 17.2) je třeba nastavit IP adresu a port pro komunikaci. V případě, že je *Clam AV* spuštěn na stejném počítači jako *Kerio MailServer*, není třeba měnit výchozí nastavení.
- *Kerio MailServer* je na systémech linux vždy spuštěn pod uživatelem root. Pokud je *Clam AV* nainstalován na stejném počítači jako *Kerio MailServer*, ale je spuštěný

pod jiným uživatelem, potom je nutno nastavit v konfiguraci antiviru v administrační konzoli (*Konfigurace* → *Filtrování obsahu* → *Antivirus* → *tlačítko Volby*) položku *UseStreamOutLocalhost* na hodnotu 1.

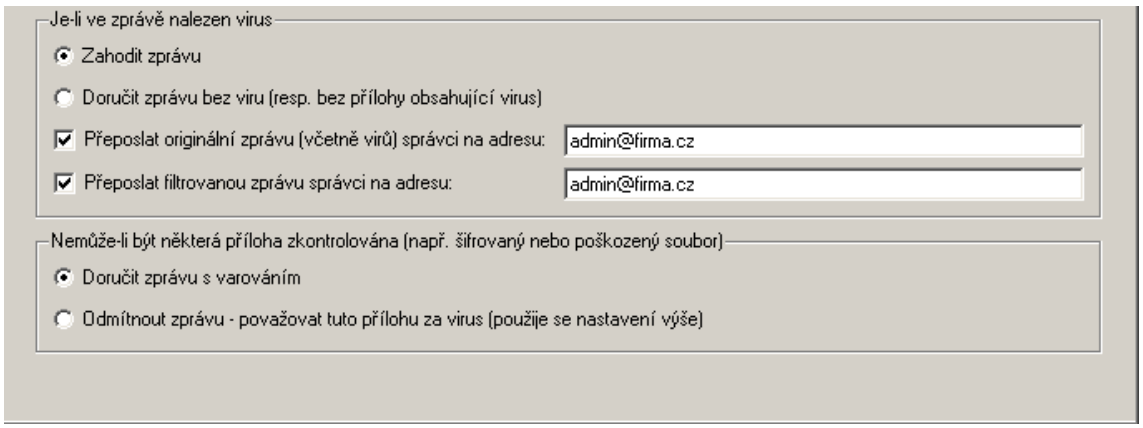


Obrázek 17.2 Volby pro antivirus Clam AntiVirus

Poznámka: Aktualizaci virové databáze je nutno nastavit pomocí utility *Freshclam*.

17.4 Chování serveru při nalezení viru nebo poškozené/šifrované přílohy

Správce *Kerio MailServeru* může poměrně detailně nastavit, jak se má server chovat, jestliže v e-mailu nalezne virus nebo poškozenou přílohu. K tomuto nastavení slouží poslední část sekce *Antivirus*:



Obrázek 17.3 Chování serveru při nalezení viru nebo poškozené/šifrované přílohy

Zahodit zprávu
Zpráva bude zahozena.

Doručit zprávu bez viru
Zpráva bude doručena příjemci, ale bez infikované či zakázané přílohy. Na její místo bude vložena zpráva serveru, že příloha byla odstraněna.

Přeposlat originální zprávu ...
Zpráva bude přeposlána (v původním tvaru — tedy i s infikovanou nebo zakázanou přílohou) na uvedenou e-mailovou adresu. Nezáleží na tom, zda zde bude uvedena lokální nebo externí adresa.

Přeposlat filtrovanou zprávu ...
Zpráva bez infikované či zakázané přílohy bude (kromě níže vybraných akcí) také přeposlána na uvedenou e-mailovou adresu. Toho lze využít např. pro ověření správné funkce antivirové kontroly a filtru příloh.

Nemůže-li být příloha zkontrolována ...
Specifikuje akci, která se má provést, jestliže antivirový program nemůže přílohu zprávy zkontrolovat (např. v případě, že se jedná o komprimovaný soubor chráněný heslem). Možnosti jsou:

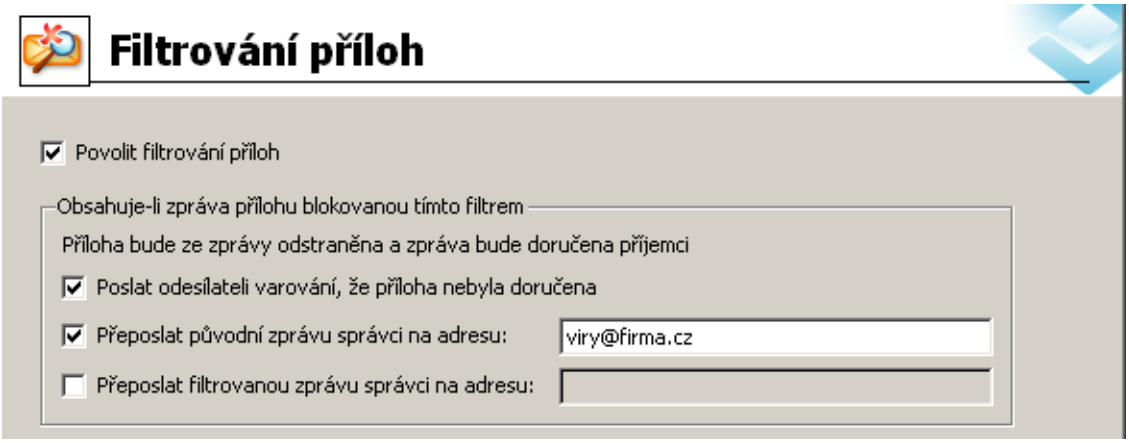
- *Doručit zprávu s varováním* — zpráva (resp. inkriminovaná příloha) bude doručena nezkontrolovaná. Ke zprávě bude připojeno varování (uživatel bude upozorněn na to, že zpráva může stále obsahovat viry).
- *Odmítnout zprávu* — se zprávou bude naloženo, jako by příloha byla infikována (tj. bude buď doručena bez této přílohy, nebo bude zahozena). Tato volba je bezpečná, ale prakticky znemožňuje posílání archivů chráněných heslem.

Každá zpráva je vyhodnocována nejprve antispamovou kontrolou, teprve poté antivirem. Důvodem této koncepce je ušetření strojového času serveru, protože antispamová kontrola je podstatně méně náročná než antivirová. Je-li v sekci *Filtr spamu* nastaveno, že zprávy vyhodnocené jako spam mají být automaticky zahazovány, budou samozřejmě zahozeny také všechny spamy obsahující vir.

17.5 Filtrování příloh e-mailů

Filtrování příloh je možno nastavit v záložce *Filtrování příloh*. Je-li zpráva zachycena tímto filtrem, bude automaticky doručena příjemci bez nepovolené přílohy.

Povolit filtrování příloh
Tato volba zapíná filtr příloh.



Obrázek 17.4 Filtrování příloh

Poslat odesílateli varování, ...
Odesílateli bude *Kerio MailServerem* posláno varování, že odeslal zprávu s infikovanou či nepovolenou přílohou.

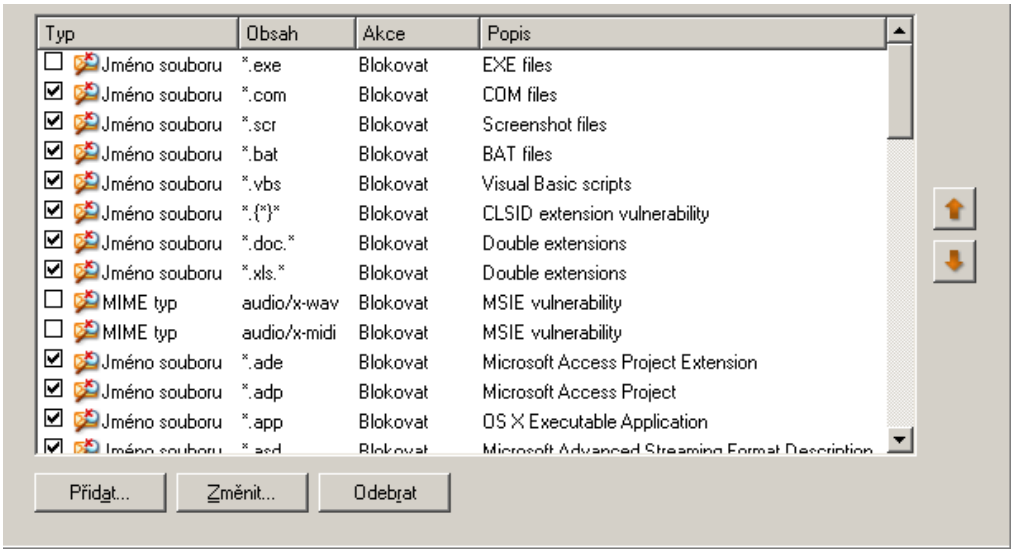
Přeposlat původní zprávu správci na adresu
Zpráva bude přeposlána (v původním tvaru — tedy i s infikovanou nebo zakázanou přílohou) na uvedenou e-mailovou adresu. Nezáleží na tom, zda zde bude uvedena lokální nebo externí adresa.

Přeposlat filtrovanou zprávu správci na adresu
Zpráva bez infikované či zakázané přílohy bude (kromě níže vybraných akcí) také přeposlána na uvedenou e-mailovou adresu. Toho lze využít např. pro ověření správné funkce antivirové kontroly a filtru příloh.

Seznam filtrů
Zobrazuje jednotlivé filtry. Vlevo vedle každého filtru se zobrazuje zaškrtávací pole, které určuje, zda je filtr aktivní či nikoliv. Chcete-li tedy (dočasně) vyřadit určitý filtr, nemusíte jej odebírat, ale stačí jej pouze vypnout.
Po instalaci *Kerio MailServeru* je v seznamu již uvedeno několik předdefinovaných filtrů (všechny jsou ale vypnuty, a záleží pouze na správci serveru, zda je použije či nikoliv, příp. smaže) — např. pro filtrování spustitelných souborů (`.com` a `.exe`), Visual Basic skriptů (`.vbs`) apod.

Tlačítkem *Přidat* lze přidat nový filtr:

Popis
Do položky lze zadat textový popis definovaného filtru (pro přehlednost).



Obrázek 17.5 Seznam filtrů

Typ filtru (MIME typ / Jméno souboru)
Určuje, zda má být filtrováno podle jména souboru nebo podle typu přílohy specifikovaného ve zprávě (MIME typ — Multi-purpose Internet Mail Extension).

Specifikace typu nebo jména souboru
Zadejte (dle nastaveného typu) buď jméno souboru (lze použít hvězdičkovou konvenci, typicky pro filtrování souborů s určitou příponou — např. `*.exe`) nebo název MIME typu (např. `application/x-msdownload` nebo `application/*`). Rovněž je možno vybrat některý z přednastavených typů souborů nebo MIME typů.

Blokovat přílohu ...
Bude provedena akce definovaná nad seznamem zakázaných příloh (viz výše).

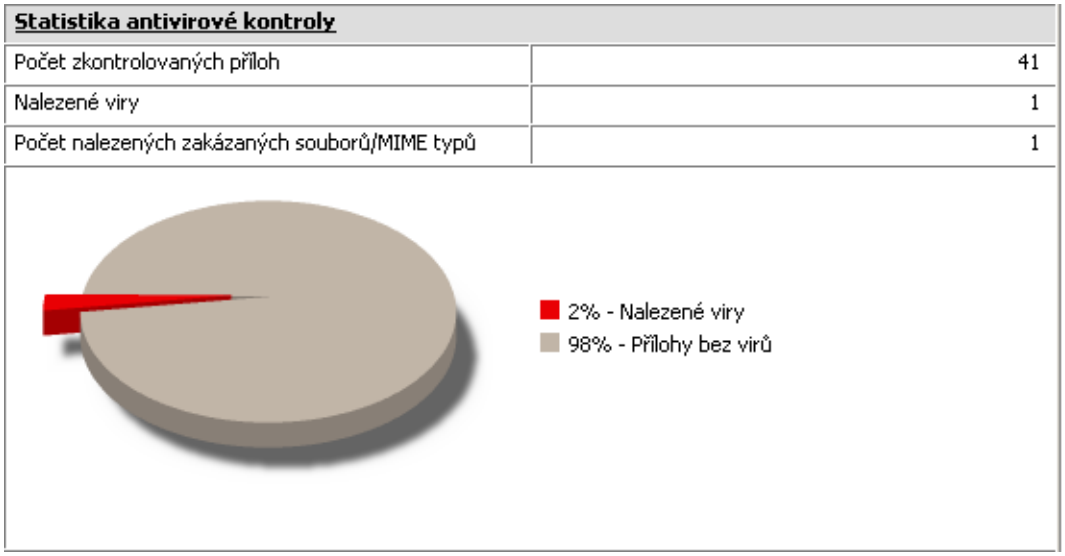
Akceptovat přílohu
Příloha bude ve zprávě ponechána a další pravidla již nebudou brána v úvahu.

17.6 Statistika antivirové kontroly

Kerio MailServer vytváří statistiku zachycování virů v e-mailových zprávách. Tato statistika je umístěna spolu s ostatními statistikami v sekci *Stav* → *Statistiky* (viz kapitolu 21.6).

Statistika antivirové kontroly umožňuje zjistit, jaký je počet zavirovaných zpráv přicházejících do *Kerio MailServeru*.

Statistika zobrazuje následující položky:



Obrázek 17.6 Statistika filtru spamu

- *Počet zkontrolovaných příloh* — Počet všech e-mailových zpráv s přílohami, které byly kontrolovány antivirem.
- *Nalezené viry* — Počet nalezených virů.
- *Počet nalezených zakázaných souborů/MIME typů* — Počet všech nalezených zakázaných typů příloh (viz kapitolu 17.5).

Poznámka: Statistika je vytvářena vždy od posledního startu serveru.

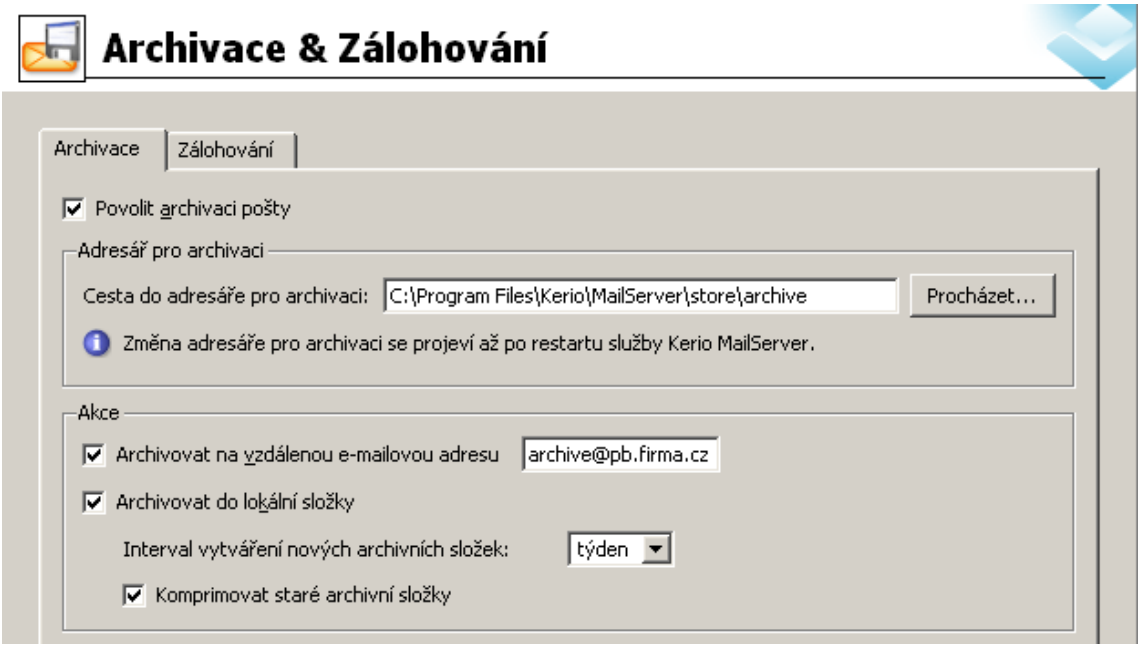
Kapitola 18

Archivace a zálohování pošty

18.1 Archivace pošty

Kerio MailServer může ukládat kopie všech zpráv (nebo pouze zpráv odeslaných do Internetu) do speciálních archivačních složek nebo je přeposílat na jiný SMTP server. Tak je možné uchovávat zálohu zpráv pro případ, že je nutné dohledat konkrétní nebo omylem smazanou zprávu (k tomuto účelu se lépe hodí tzv. obnova zpráv jejíž nastavení se provádí v nastavení domény — více viz kapitolu 7.2).

Nastavit parametry archivace lze v sekci *Konfigurace* → *Archivace & Zálohování* v záložce *Archivace*.



Obrázek 18.1 Archivace zpráv

Povolit archivaci pošty

Zapnutí/vypnutí archivace. Po povolení archivace pošty a nastavení příslušných parametrů v záložce *Archivace* se při doručení první zprávy vytvoří archivační složka s názvem odvozeným od intervalu vytváření složek (denní, týdenní nebo měsíční), který lze v záložce také nastavit.

Po restartu *Kerio MailServeru* se vždy vytváří nová archivační složka (bezprostředně po přijetí první zprávy po restartu). Dále se archivační cyklus chová podle nastavení v záložce *Archivace*.

Cesta do adresáře pro archivaci

Úplná cesta k adresáři určenému pro archiv (dle konvence operačního systému, na kterém *Kerio MailServer* běží). Z technických důvodů je třeba adresář pro archivaci umístit lokálně (na serveru kde je *Kerio MailServer* spuštěn).
Upozornění: Cestu k adresáři nelze zadat jako UNC cestu.

Archivovat na vzdálenou adresu

Kopie všech zpráv budou přeposílány na tuto e-mailovou adresu.

Zálohovat do archivní složky

Kopie zpráv budou ukládány do lokálních složek, automaticky vytvářených v jmenném prostoru *#archive* (na disku je reprezentován podadresářem `mail/archive` v adresáři, kde je *Kerio MailServer* nainstalován) podle definovaného formátu.

Interval vytváření nových ...

Položka umožňuje vybrat vyhovující interval (den, týden, měsíc). Podle nastavení intervalu se tvoří názvy archivních složek:

`2005-Jan` — formát měsíčního archivu. Název obsahuje rok a měsíc, během kterého byly zprávy archivovány. Nová složka se vytvoří každých 30 dní, vždy po přijetí první zprávy po půlnoci serverového času.

`2005-W03` — formát týdenního archivu. Název obsahuje rok a číslo týdne. Číslo týdne je počítáno vždy od 1. ledna daného roku. Týdny nemusí být shodné s počítáním týdnů v kalendáři (1. ledna může spadat ještě do 52. týdne a celé počítání týdnů se tak může posunout). Nová složka se vytvoří každých sedm dní, vždy po přijetí první zprávy po půlnoci serverového času.

`2005-Jan-12` — formát denního archivu. Název obsahuje rok, měsíc a den v běžném kalendáři. Nová složka se vytvoří každý den vždy po přijetí první zprávy po půlnoci serverového času.

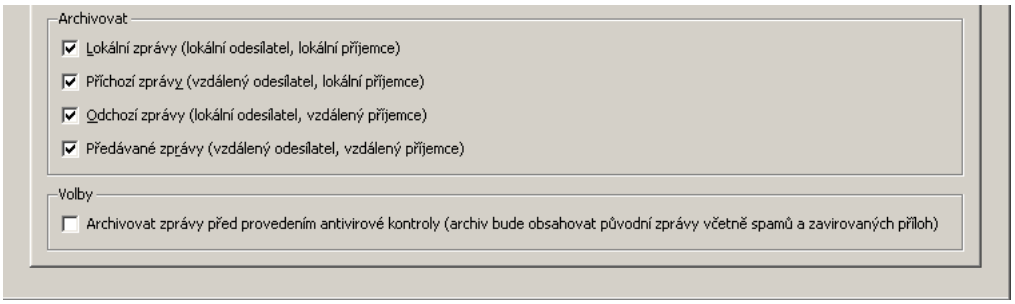
Poznámka: Nastavení intervalu vytváření nových archivních složek (vyplývajícího z formátu jmen) záleží pouze na vůli správce *Kerio MailServeru*. Doporučujeme zohlednit počet zpráv, které přes server procházejí (příp. počet lokálních uživatelů, kteří jej využívají). Větší počet složek, z nichž každá obsahuje menší počet zpráv, zajišťuje rychlejší přístup a je přehlednější.

Komprimovat staré archivní složky

Volba umožňuje komprimaci archivu kromě aktuální (poslední vytvořené) složky. Nevýhodou této volby je nemožnost prohlížení komprimovaných složek přes poštovního klienta.

První komprimace archivní složky se provádí hned po spuštění *Kerio MailServeru*. Každá následující komprimace proběhne za 24 hodin od vytvoření nové složky.

Lokální zprávy (lokální odesílatel, lokální příjemce)
Archivovat se budou všechny zprávy lokální, tedy zprávy odeslané z domény, která je lokální na tomto serveru.



Obrázek 18.2 Výběr typu zpráv pro archivaci

Příchozí zprávy (vzdálený odesílatel, lokální příjemce)
Archivovat se budou všechny příchozí zprávy (od vzdáleného odesílatele k lokálnímu příjemci).

Odchozí zprávy (lokální odesílatel, vzdálený příjemce)
Archivovat se budou všechny odchozí zprávy (od lokálního odesílatele k vzdálenému příjemci).

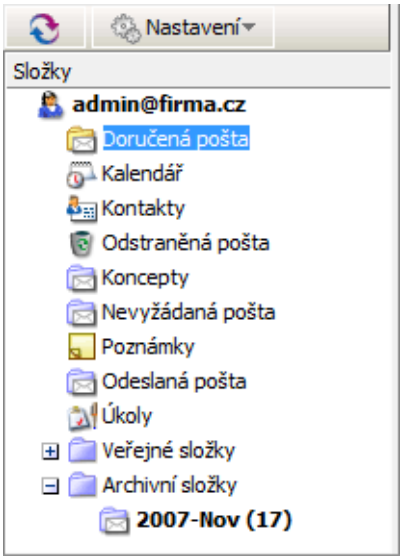
Předávané zprávy (vzdálený odesílatel, vzdálený příjemce)
Po zaškrtnutí se budou archivovat všechny zprávy předávané na nadřazený server (od vzdáleného odesílatele k vzdálenému příjemci).

Archivovat zprávy před provedením...
Zapnutím této volby se budou archivovat všechny zprávy ještě před spuštěním antivirové kontroly, tzn. v záloze najdete všechny zprávy v originální podobě (včetně virů).

Přístup k archivním složkám je standardně umožněn uživateli `admin` primární domény (kapitola 13.1). `Admin` může nastavit přístupová práva k archivním složkám i dalším uživatelům. Lze tak učinit v rozhraní *Kerio WebMail* nebo v aplikaci *MS Outlook* doplněné *Kerio Outlook Connectorem*. Je třeba si uvědomit, že do těchto složek se zálohují zprávy všech uživatelů, a proto by k nim měl mít přístup pouze důvěryhodný správce (nanejvýš malá skupina osob).

Zobrazení archivních složek

Archivní složky se zobrazují pouze uživatelům s příslušnými právy. Standardně má přístup k archivním složkám pouze uživatel `admin` primární domény (první účet vytvořený v konfiguračním průvodci při instalaci *Kerio MailServeru*).



Obrázek 18.3 Archivní složky v rozhraní Kerio WebMail

Archivní složku lze nasdílet jiným uživatelům. Sdílení probíhá stejně jako u všech ostatních typů složek. Je ovšem třeba si uvědomit, že do těchto složek se zálohují zprávy všech uživatelů, a proto by k nim měl mít přístup pouze důvěryhodný správce (nanejvýš malá skupina osob).

18.2 Zálohování poštovních složek a konfiguračních souborů

Kerio MailServer umožňuje pravidelné zálohování uživatelských složek a konfiguračních souborů na médium, které je k těmto účelům určené. K zálohování může být využit výměnný disk nebo síťový disk tvořený jakýmkoliv zálohovacím médiem.

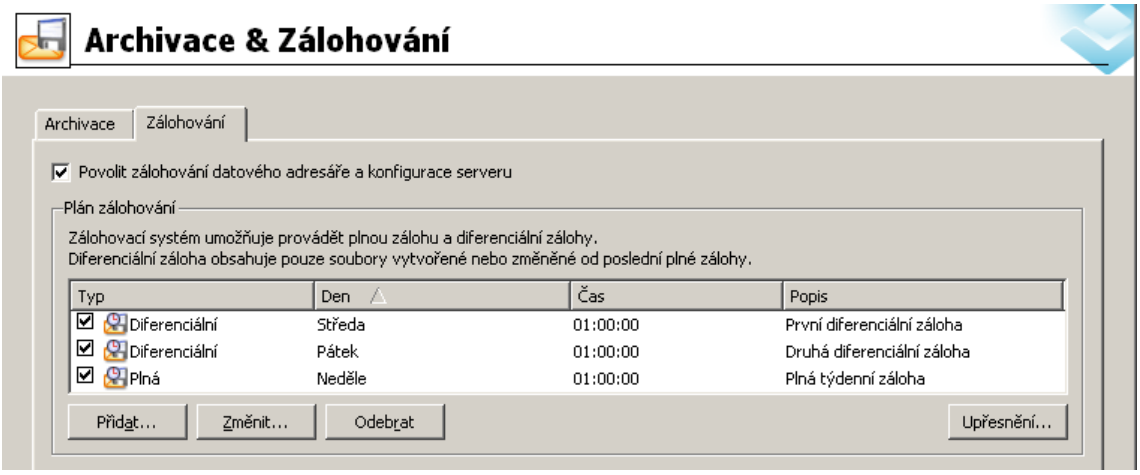
Kerio MailServer provádí zálohu celého datového adresáře `store` a konfiguračních souborů `users.cfg` a `mailserver.cfg`.

Zálohování uživatelských složek obsahuje různá nastavení. Tato nastavení lze provést v sekci *Konfigurace* → *Archivace & Zálohování*, v záložce *Zálohování*:

Povolit zálohování datového adresáře ...

Volba umožňuje zálohovat všechny uživatelské složky spolu s aktuální konfigurací *Kerio MailServeru*. Konkrétně je to celý datový adresář `store` a konfigurační soubory `users.cfg` a `mailserver.cfg`.

Pokud nechcete využít zálohování v *Kerio MailServeru*, potom je třeba deaktivovat (odškrtnout) volbu *Povolit zálohování datového adresáře a konfigurace serveru*. Vymažete-li všechny položky plánu zálohování, a zároveň necháte volbu *Povolit zálohování datového adresáře a konfigurace serveru* aktivní, potom se po restartu *Kerio MailServeru* automaticky načte a použije výchozí příkladový plán zálohování.



Obrázek 18.4 Zálohování uživatelských složek

Upozornění:

- Systém zálohování v *Kerio MailServeru* nezahrnuje všechny konfigurační soubory serveru. Je-li nutno například přenést konfiguraci a uživatelské složky na jiný server nebo přeinstalovat *Kerio MailServer*, je třeba provést kromě standardní zálohy také ruční zálohu adresářů `sslcert` (obsahuje SSL certifikáty) a `license` (obsahuje soubory s licencemi). O této problematice se dozvíte více v kapitole 28.2.
- Adresáře `sslcert` a `license` doporučujeme ručně zazálohovat bezprostředně po instalaci a registraci *Kerio MailServeru*, a také po každé změně jejich obsahu (například po zvýšení počtu uživatelských licencí nebo po importu nového důvěryhodného certifikátu).

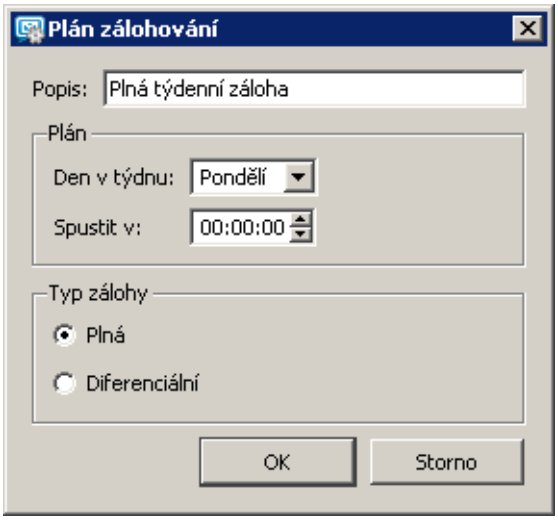
Plán zálohování

Záložka *Zálohování* obsahuje možnost detailního nastavení plánu zálohování. Plán zálohování mohou tvořit dva typy záloh:

- *Plná záloha* — kompletní záloha všech souborů.
- *Diferenciální záloha* — částečná záloha, která ukládá všechny změněné a nově vytvořené soubory. Předností částečné zálohy je její menší objem. Částečná záloha obvykle v plánu zálohování doplňuje zálohu plnou. Pokud je v plánu více diferenciálních záloh za sebou, nová záloha vždy přepíše předchozí. Takže na zálohovacím disku je vždy po plné záloze uložena maximálně jedna diferenciální záloha.
  Poznámka: Pokud využijete možnosti zálohování pomocí diferenciálních záloh, potom je při případné obnově ze zálohy nutno obnovit vždy poslední plnou a diferenciální zálohu.

Plán zálohování je tvořen jednotlivými úlohami zálohování. Každá úloha sestává z jednoho z výše popsaných typů zálohování a času, kdy se má vybraný typ zálohy spustit.

Zadat novou úlohu do plánu zálohování lze tlačítkem *Přidat*. Otevře se okno (viz obrázek 18.5), které obsahuje následující možnosti nastavení:



Obrázek 18.5 Úloha zálohování

Popis
: Popis zálohy není nutnou položkou, slouží pouze k lepší orientaci v plánu zálohování.

Plán
: Rámeček obsahuje dvě menu, kde lze nastavit den a přesný čas spuštění zálohy. Jednotlivé úlohy zálohování, a to zejména plné zálohy, doporučujeme spouštět v nočních hodinách, protože proces zálohování může značně zatížit poštovní server.

Typ zálohy
: Nastavení plné nebo diferenciální zálohy.

Tlačítkem *Přidat* lze tedy nastavit novou úlohu zálohování. Tlačítkem *Změnit* je možno editovat kteroukoliv vybranou úlohu a tlačítkem *Odebrat* je možno vybranou úlohu z plánu odstranit.

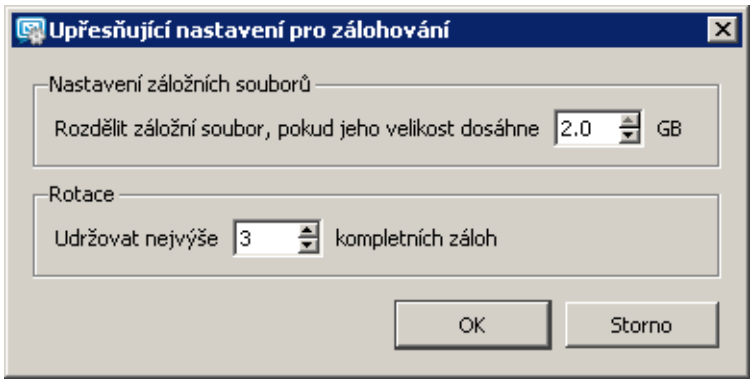
Při vytváření plánu zálohování je možno podle potřeby využít oba výše jmenované typy záloh. V plánu lze nastavit libovolné množství úloh zálohování. Někomu může vyhovovat plná záloha jednou týdně, někomu každý den. Počet úloh zálohování je obvykle závislý na:

1. velikosti datového úložiště a tedy na tom, jak dlouho bude záloha trvat a jak bude velká. Přičemž jak problém s časovou náročností, tak problém s místem se dá řešit využitím diferenciální zálohy.

2. míře důležitosti dat, o která by uživatelé mohli přijít. Jinými slovy, ve společnostech

kde je pro uživatele pošta velmi důležitá, tam se zálohy provádí častěji. Uživatelé potom v případě problému ztratí minimum dat.

Tlačítko *Upřesnění* umístěné pod plánem zálohování umožňuje provést další nastavení (viz obrázek 18.6):



Obrázek 18.6 Upřesnění plánu zálohování

Nastavení záložních souborů

Zálohy jsou ukládány v komprimovaných souborech (`.zip`), jejichž velikost nesmí přesáhnout 2 GB. Tato položka umožňuje rozdělení zálohy na několik menších částí. Maximální hranice pro dělení je standardně nastavena na hodnotu 2 GB (maximální velikost souboru). Pokud je soubor větší než hodnota nastavená v dialogu, pak tento soubor nebude zálohován.

Rotace

Každá záloha uživatelských složek je velmi náročná na místo na zálohovacím médiu a správce *Kerio MailServeru* může být v případě jeho nedostatku nucen zálohy často mazat. Po nastavení rotace záloh odpadne práce s pravidelným ručním mazáním souborů. Do pole *Udržovat nejvýše ... kompletních záloh* stačí zadat číslicí počet záloh, které mají být na zálohovacím médiu udržovány. Jakmile se počet záloh naplní, nejstarší záloha bude vždy přemazána tou nejnovější.

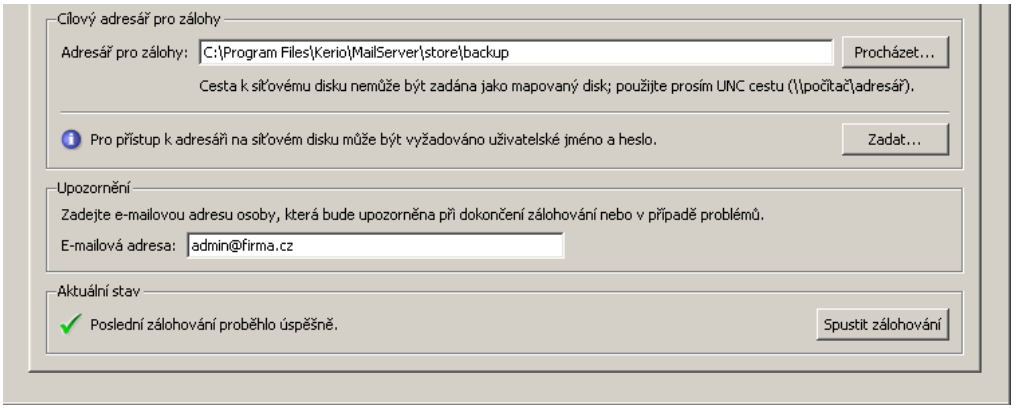
Ostatní nastavení

Adresář pro zálohu

Úplná cesta k adresáři určenému pro zálohy (dle konvence operačního systému, na kterém *Kerio MailServer* běží).

Výchozí úložiště záloh se standardně nachází v adresáři, kde je *Kerio MailServer* nainstalován:

```
Kerio\MailServer\store\backup
```



Obrázek 18.7 Cílový adresář pro zálohy

Upozornění: Úložiště záloh doporučujeme změnit a nastavit cestu k výměnnému zálohovacímu disku nebo jinému zálohovacímu médiu, pokud je k dispozici.
Pokud je *Kerio MailServer* spuštěn na systému Windows, pak je nutno cestu k serveru pro zálohování zadat ve tvaru UNC (viz obrázek 18.7).
Pokud je *Kerio MailServer* spuštěn na linuxu nebo systému Mac OS, potom jsou k dispozici tyto možnosti:

- Server určený pro zálohování připojíme jako adresář a do pole *Adresář pro zálohu* zadáme cestu k tomuto adresáři. Výsledek může vypadat například takto:

  `/mnt/server-backup`

- Zálohu uložíme do lokálního adresáře, a teprve poté necháme odeslat na server (například pomocí synchronizační utility `rsync`). Výsledek může vypadat například následovně:

  `/backup/kms/backup`

Název každého archivu se zálohou je složen z typu zálohy a data, kdy byla pořízena:

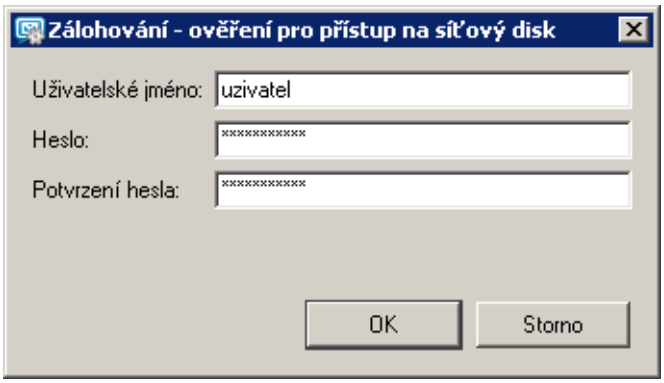
- Plná záloha — `F20060118T220007Z.zip`
  F — plná záloha
  2006 — rok
  01 — měsíc
  18 — den
  T220007Z — časová značka v GMT (22:00:07), vždy je uvozena T a končí Z.
- Diferenciální záloha — `I20060106T220006Z.zip`
  I — diferenciální záloha
  2006 — rok
  01 — měsíc
  06 — den
  T220006Z — časová značka v GMT (22:00:06), vždy je uvozena T a končí Z.

- Kopie zálohy (ruční spuštění zálohování) — `C20060117T084217Z.zip`
  2006 — rok
  01 — měsíc
  17 — den
  T084217Z — časová značka v GMT (08:42:17), vždy je uvozena T a končí Z.

Ověření pro přístup na síťový disk

Kromě výměnného zálohovacího média je samozřejmě možné ukládat zálohy na síťový disk. Má-li síťový disk chráněný přístup, musí být umožněno ověření pomocí uživatelského jména a hesla, který má přístup na disk povolen.

Jméno a heslo pro přístup k disku lze použít pouze v případě, že je *Kerio MailServer* nainstalován na operačních systémech *MS Windows*.



Obrázek 18.8 Ověření pro přístup na disk

Notifikace

Na uvedenou adresu budou *Kerio MailServerem* zasílány e-maily o průběhu zálohování.

Kromě záloh nastavených v plánu zálohování lze v případě potřeby ihned pořídit také tzv. kopii zálohy. Kopie zálohy je de facto plná záloha, která ovšem v ničem nenarušuje nastavený plán zálohování. Kopii zálohování lze zapnout tlačítkem *Spustit zálohování*. Vlevo od tlačítka se objeví aktuální stav průběhu zálohování. Při obnově ze zálohy je kopie brána jako standardní plná záloha, a proto pokud je kopie poslední provedenou zálohou, provede se obnova z ní.

Obnova ze zálohy

Pro obnovu dat ze zálohy slouží speciální aplikace *Kerio MailServer Recover*. Tato aplikace samostatně rozbalí zálohu a uloží ji do adresáře `store`.

Kerio MailServer Recover je součástí instalace a spouští se v příkazové řádce příkazem `kmsrecover` z adresáře, kde je *Kerio MailServer* nainstalován.

Použití:

```
kmsrecover <nazev_adresare>|<nazev_souboru>
```

Upozornění: Na operačních systémech Mac OS X a Linux je nutné zapsat příkaz v následujícím formátu, pokud není zanesen do souboru systémové proměnné `path`:

```
./kmsrecover <directory_name>|<file_name>
```

To znamená, že před název utility je třeba připojit znaky `./`, které systému řeknou, že se má příkaz spustit z aktuálního adresáře.

Podrobnosti a příklady k parametrům obsahuje nápověda, kterou lze spustit příkazem `kmsrecover`.

Upozornění:

- Před obnovou zálohy je nutné zastavit *Kerio MailServer Engine*.
- Po spuštění aplikace *Kerio MailServer Recover* budou přepsány soubory s konfigurací a data v úložišti *Kerio MailServeru*.

Obnovu ze zálohy si nejlépe vysvětlíme na jednoduchém příkladu:

Windows

Obnovu provádíme na počítači s operačním systémem *MS Windows*. Adresář s konfigurací je uložen ve výchozím umístění (standardní nastavení při instalaci), adresář store je umístěn na samostatném disku (pole RAID nebo jakýkoliv rychlejší disk) na stejném počítači, kde je umístěn adresář s konfigurací a adresář se zálohou je pro případ ztráty adresáře store umístěn na výměnném disku určeném k provádění zálohování. Pro obnovu ze zálohy použijeme zálohu plnou.
Podmínky:

1. Konfigurace je uložena v adresáři

   ```
   C:\Program Files\Kerio\MailServer
   ```

2. Adresář *store* je uložen na disku

   ```
   D:\store
   ```

3. Adresář se zálohou je z bezpečnostních důvodů uložen na výměnném zálohovacím disku

   ```
   E:\backup
   ```

Řešení:
Příkaz je nutno spustit z adresáře, kde je *Kerio MailServer* nainstalován. V našem případě je to adresář

```
C:\Program Files\Kerio\MailServer
```

Nyní mohou nastat dva různé případy zápisu:

1. Chceme obnovit poslední uloženou kompletní zálohu (poslední plná a poslední diferenciální záloha nebo poslední kopie zálohy). V takovém případě bude zá-

pis příkazu i s parametry vypadat takto:

```
kmsrecover E:\backup
```

2. Chceme obnovit konkrétní zálohu (starší než poslední):

   ```
   kmsrecover E:\backup\F20051009T220008Z.zip
   ```

Cestu k úložišti (`D:\store`) najde `kmsrecover` automaticky v konfiguračním souboru *Kerio MailServeru* a použije ji.
Upozornění: Obsahuje-li parametr mezeru v názvu adresáře, je třeba jej celý opatřit uvozovkami. Pro příklad si uveďme výše uvedený zápis:

```
kmsrecover "E:\backup 2"
```

Mac OS X

Obnovu provádíme na počítači s operačním systémem *Mac OS X*. Adresář s konfigurací je uložen ve výchozím umístění (standardní nastavení při instalaci), adresář store je umístěn na samostatném disku na stejném počítači, kde je umístěn adresář s konfigurací a adresář se zálohou je pro případ ztráty adresáře store umístěn na výměnném disku určeném k provádění zálohování. Pro obnovu ze zálohy použijeme poslední plnou zálohu.
Podmínky:

1. Konfigurace je uložena v adresáři

   ```
   /usr/local/kerio/mailserver
   ```

2. Adresář *store* je uložen na disku

   ```
   /store
   ```

3. Adresář se zálohou je z bezpečnostních důvodů uložen na výměnném zálohovacím disku

   ```
   /Volume/backup
   ```

Řešení:
Příkaz je nutno spustit z adresáře, kde je *Kerio MailServer* nainstalován, proto se přesuneme do adresáře:

```
/usr/local/kerio/mailserver
```

Chceme obnovit poslední uloženou kompletní zálohu (poslední plná a poslední diferenciální záloha nebo poslední kopie zálohy). Zápis příkazu se nyní bude lišit podle toho zda je cesta k adresáři *Kerio MailServeru* zapsána do proměnné path či nikoliv. Pokud jste cestu nenastavili, bude zápis vypadat takto:

```
./kmsrecover /Volume/backup
```

pokud ano, bude vypadat následovně:

```
kmsrecover /Volume/backup
```

Cestu k úložišti (`/store`) najde `kmsrecover` automaticky v konfiguračním souboru *Kerio MailServeru* a použije ji.

Řešení případných problémů

Pokud je třeba vyřešit v souvislosti se zálohováním problém, lze v *Kerio MailServeru* nastavit záznam průběhu zálohování:

1. Otevřeme v *Kerio Administration Console* sekci *Záznamy* a vybereme záznam *Debug*.
2. V okně záznamu pravým tlačítkem myši otevřeme kontextové menu a vybereme položku *Zprávy*.
3. Otevře se okno *Zaznamenávané informace*, kde zaškrtneme volbu *Store Backup*.
4. Změnu potvrdíme tlačítkem OK.

Po vyřešení problému doporučujeme logování opět vypnout.

Kapitola 19

LDAP server

Vestavěný LDAP server (je možno použít nezabezpečený i zabezpečený přístup — viz kapitolu 6) umožňuje přístup ke kontaktům uloženým na serveru standardním protokolem LDAP (*Lightweight Directory Access Protocol*). Tento protokol je podporován v naprosté většině běžných e-mailových klientů. Klient pak umožňuje vyhledávání informací o osobách (typicky e-mailových adres), případně automatické doplňování adres přímo při psaní.

LDAP server umožňuje přístup k osobním kontaktům uživatele (tj. kontaktům uloženým v jeho vlastních složkách typu *Kontakty*) a kontaktům ve všech sdílených veřejných složkách typu *Kontakty*, které má daný uživatel přihlášeny.

19.1 Konfigurace LDAP serveru

Použití služby *LDAP* v *Kerio MailServeru* je velmi jednoduché. Stačí splnit následující dvě podmínky:

- V *Kerio MailServeru* musí být spuštěna alespoň jedna ze služeb *LDAP* nebo *Zabezpečený LDAP*.
- Uživatel musí mít definovány kontakty ve svých složkách kontaktů a/nebo přihlášenu alespoň jednu veřejnou či sdílenou složku kontaktů. Při nesplnění této podmínky bude komunikace s LDAP serverem fungovat, ale žádné kontakty nebudou nalezeny.

Poznámka: Je-li *Kerio MailServer* chráněn firewallem a služba LDAP má být přístupná zvenčí, je třeba zpřístupnit příslušný port (standardně `389` pro službu *LDAP* a `636` pro *Zabezpečený LDAP*). V tomto případě by měla být preferována zabezpečená verze služby *LDAP*.

19.2 Nastavení poštovních klientů

Aby mohl poštovní klient přistupovat ke kontaktům uloženým na *Kerio MailServeru* protokolem LDAP, je třeba uvést následující informace:

LDAP server
: DNS jméno (např. `mail.firma.cz`) nebo IP adresa (např. `192.168.1.10`) počítače, na němž *Kerio MailServer* běží.

Uživatelské jméno a heslo
Údaje pro přihlášení uživatele k LDAP serveru (shodné s jménem a heslem pro poštu). LDAP server v *Kerio MailServer* nepodporuje anonymní přístup — vždy je vyžadováno přihlášení uživatele.

Zabezpečení, Port
Zvolte, zda má být používána nezabezpečená či zabezpečená (SSL) verze protokolu LDAP. Případně zadejte odpovídající číslo portu (není-li použit standardní port).
Poznámka: Protokol TLS (tzn. přepnutí do zabezpečeného módu příkazem *STARTTLS*) není podporován.

Výchozí bod hledání (Search base)
Chcete-li mít přístup do všech vlastních a přihlášených sdílených i veřejných složek, ponechte ji prázdnou nebo zadejte do této položky:

```
fn=ContactRoot
```

Bližší specifikací prohledávané větve LDAP databáze je možno omezit vyhledávání pouze na určité složky. Jednotlivé možnosti budou vysvětleny na následujících příkladech:

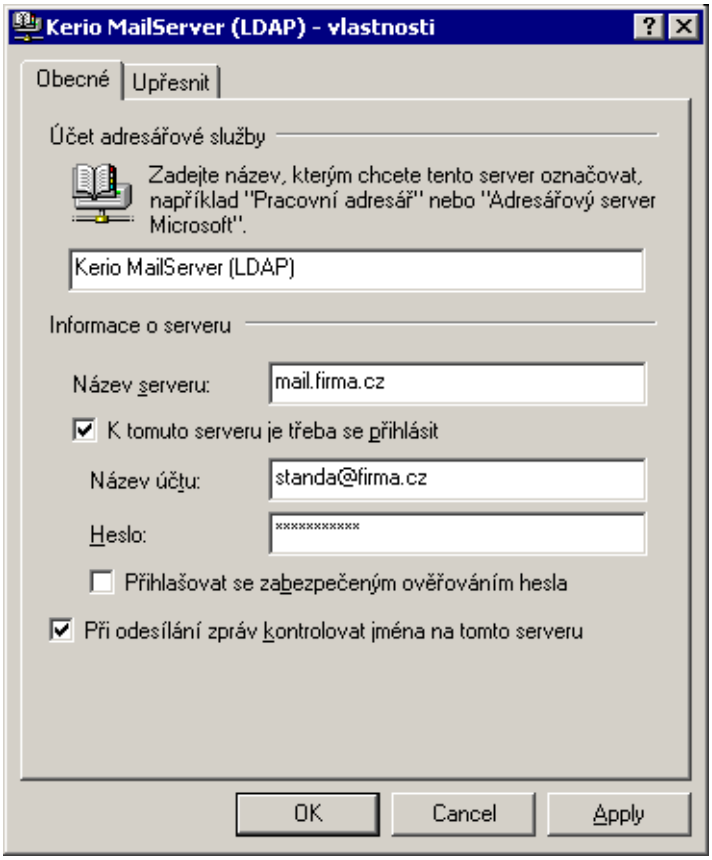
- `cn=jnovak@firma.cz,fn=ContactRoot`
  budou prohledávány pouze složky kontaktů uživatele `jnovak@firma.cz`
- `fn=personal,fn=ContactRoot` budou prohledávány pouze složky kontaktů uživatele, který je na LDAP server přihlášen. Tato volba je v podstatě shodná s předchozí, rozdíl je však v tom, že není nutné vypisovat jméno (resp. e-mailovou adresu) příslušného uživatele. Toto lze s výhodou použít např. při hromadné konfiguraci více klientů nebo v obecném návodu, jak si mají uživatelé své klienty nastavit, apod.
- `fn=public,fn=ContactRoot`
  budou prohledávány pouze veřejné složky kontaktů
- `fn=Contacts,cn=jnovak@firma.cz,fn=ContactRoot`
  bude prohledávána pouze složka `Contacts` uživatele `jnovak@firma.cz`
- `fn=Public Folders,fn=public,fn=ContactRoot`
  bude prohledávána pouze veřejná složka `Public Folders`

Příklad nastavení — Outlook Express

Jako příklad uveďme nastavení LDAP serveru v poštovním klientovi *Microsoft Outlook Express*.

Nastavení LDAP účtu se provádí v menu *Nástroje* → *Účty* → *Adresářová služba*. Přidání nového účtu probíhá pomocí průvodce, který však umožňuje zadat pouze základní parametry. Poté je třeba účet vybrat, stisknout tlačítko *Vlastnosti* a provést detailní nastavení.

Záložka Obecné:



Obrázek 19.1 Nastavení LDAP serveru — obecné

Název účtu
: Libovolné pojmenování účtu (slouží pouze pro orientaci).

Název serveru
: DNS jméno nebo IP adresa počítače, na němž *Kerio MailServer* běží (např. `mail.firma.cz` nebo `192.168.1.10`).

K tomuto serveru je třeba se přihlásit
: Tuto volbu je nutno zaškrtnout, protože LDAP server v *Kerio MailServeru* nepodporuje anonymní přístup.

Název účtu, Heslo
: Zadejte vaše uživatelské jméno a heslo pro přihlášení k serveru (shodné s jménem a heslem pro přístup k poště).

Přihlašovat se zabezpečeným ověřováním hesla
: Tato volba zapíná bezpečné ověřování hesla v NT doméně (SPA/NTLM). Tento způsob ověřování LDAP server v *Kerio MailServeru* nepodporuje, a proto je třeba ponechat tuto volbu vypnutou!

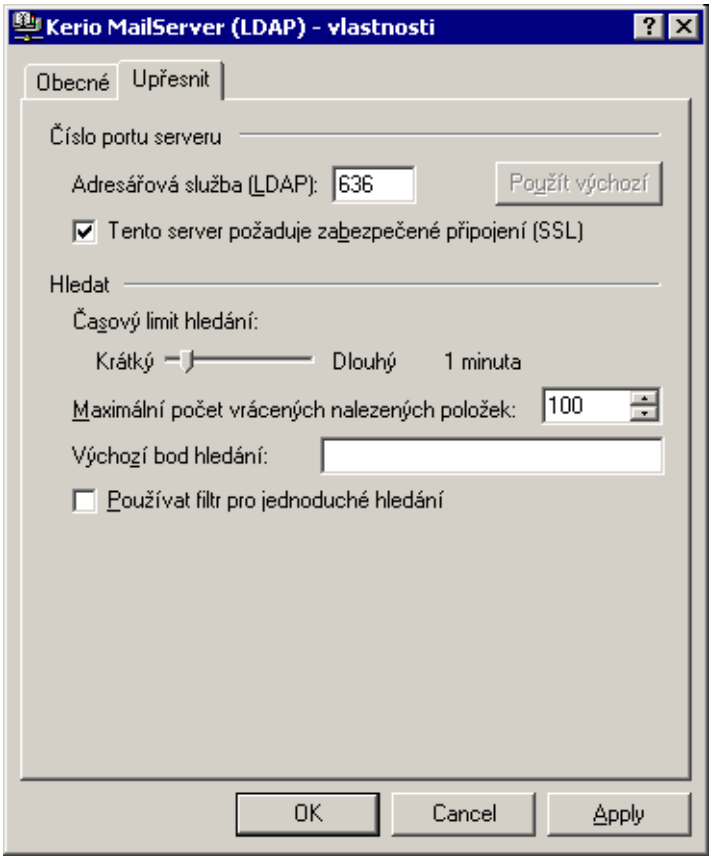
Poznámka: Pro bezpečné ověření uživatele doporučujeme použít zabezpečenou verzi služby *LDAP* (režim SSL).

Při odesílání zpráv kontrolovat jména...

Zapnutím této volby budou při odesílání zpráv automaticky vyhledávány e-mailové adresy osob. V praxi to znamená, že je možno do položky *Komu* (resp. *Kopie* či *Skrytá kopie*) zadávat namísto e-mailových adres jména osob — příslušné e-mailové adresy budou načteny z LDAP serveru.

Poznámka: Nebude-li některé ze zadaných jmen nalezeno, *Outlook Express* nepovolí odeslání zprávy (uživatel jej bude muset opravit nebo zadat e-mailovou adresu ručně). Pokud bude zadanému jménu vyhovovat více záznamů, zobrazí se dialog pro výběr správné osoby/adresy.

Záložka Upřesnit:



Obrázek 19.2 Nastavení LDAP serveru — upřesňující

Číslo portu serveru

Port, na němž služba LDAP běží. Tlačítko *Použít výchozí* dosazuje standardní port (v závislosti na tom, zda je či není zapnuto používání SSL — viz dále).

Tento server požaduje zabezpečení SSL

Tato volba zapíná/vypíná používání zabezpečeného spojení. Zabezpečení SSL nastavte podle konfigurace služeb *Kerio MailServeru* (podrobnosti najdete v kapitole 6), resp. v závislosti na nastavené bezpečnostní politice (viz kapitolu 15.6).

Časový limit hledání

Je-li LDAP databáze rozsáhlá, a/nebo spojení se serverem pomalé, může prohledávání databáze trvat velmi dlouhou dobu. Tato volba umožňuje nastavit maximální dobu prohledávání databáze. Po této době bude hledání ukončeno (bez ohledu na to, zda byl nalezen nějaký záznam či nikoliv).

Poznámka: Je-li LDAP server umístěn v téže lokální síti jako klient, trvá vyhledávání zpravidla několik sekund.

Maximální počet nalezených položek

V případě, že je specifikace hledané položky nedostatečná (např. pouze část křestního jména osoby), může výsledek hledání obsahovat velké množství položek. Omezení maximálního počtu slouží především ke snížení doby vyhledávání a zátěže sítě. Je-li vrácen takto vysoký počet položek, je zpravidla nutné hledaný výraz upřesnit a provést nové hledání.

Výchozí bod hledání

Do této položky může být zadáno umístění kontaktů v LDAP databázi (viz výše). Zůstane-li pole prázdné, budou prohledávány všechny přihlášené složky kontaktů (vlastní i sdílené).

Používat filtr pro jednoduché hledání

Zapnutí této volby způsobí, že bude prohledáván menší počet položek záznamů databáze. Hledání bude sice rychlejší (což běžný uživatel téměř nepozná), ale sníží se hledací schopnosti. Z tohoto důvodu *nedoporučujeme zapínat tuto volbu.*

Kapitola 20

E-mailové konference

Kerio MailServer teoreticky umožňuje zřídit v každé lokální doméně libovolný počet e-mailových konferencí. Prakticky je počet omezen na počet uživatelských licencí, protože každá e-mailová konference je v *Kerio MailServeru* brána jako jedna licence.

Základem konference je skupinová e-mailová adresa — e-mail poslaný na tuto adresu je doručen všem členům skupiny (konference). Na rozdíl od prosté skupiny uživatelů však konference umožňuje i následující funkce:

- přihlášení a odhlášení členů skupiny e-mailem
- moderování konference (moderátoři řídí přihlašování a odhlašování členů skupiny a zasílání příspěvků do konference)
- automatickou úpravu předmětu, resp. textu zprávy (přidávání definovaného textu do všech zpráv)
- záměnu položek v hlavičce zprávy (za účelem skrytí e-mailové adresy odesílatele zprávy)
- blokování zpráv s určitými vlastnostmi (např. s prázdným předmětem)

Veškeré akce (přihlašování, odhlašování, moderování...) se provádějí zasíláním e-mailů na speciální adresy. V programu *Kerio Administration Console* stačí konferenci pouze založit — vše ostatní už může probíhat pomocí e-mailů, které jsou odesílány a samozřejmě také doručovány pomocí protokolu SMTP.

Upozornění: Nedoporučujeme zpracování zpráv e-mailových konferencí v případě stahování pošty přes POP3. Chcete-li provozovat e-mailové konference pro Internet, je nutné zajistit si MX záznam pro váš server.

Pokud se při provozování e-mailových konferencí objeví problémy, může vám s jejich vyřešením pomoci záznam *Debug* (viz kapitolu 22.8). V tomto záznamu je třeba povolit záznam *Mailing Lists Processing*.

20.1 Klasifikace uživatelů

Uživatelé e-mailové konference mohou mít následující funkce (tzv. role):

Administrátor

Uživatel, který má práva ke správě *Kerio MailServeru* (tj. právo pro čtení i zápis — viz kapitolu 13). Administrátor v programu *Kerio Administration Console* konferenci vytváří a nastavuje její parametry (moderátory, politiku atd.). Detaily najdete v kapitole 20.2).

Moderátor

Každá konference by měla mít alespoň jednoho moderátora (též nazýván vlastníkem konference). Moderátor konference má následující pravomoci:

- může potvrdit nebo odmítnout požadavek uživatele na přihlášení do konference (pokud to politika konference vyžaduje)
- může povolit nebo zamítnout přidání příspěvku do konference (pokud to politika konference vyžaduje)
- přijímá chybové zprávy (např. o nedoručitelnosti e-mailů)
- může být kontaktován přímo pomocí adresy

  `<název_konference>-owners@<doména>`

Člen

Členem konference je libovolný uživatel, který se do konference přihlásí. Jeho e-mailová adresa může být z libovolné domény — konference není omezena pouze na uživatele z domény, v níž je vytvořena. Člen konference má následující práva:

- přihlásit se a odhlásit (je-li člen přihlášen, jsou mu doručovány všechny příspěvky — tedy zprávy zaslané na adresu konference)
- požadovat nápovědu
- zasílat příspěvky do konference (pokud to politika konference vyžaduje, musí být každý zaslaný příspěvek odsouhlasen některým z moderátorů konference)

Poznámka: Jednotlivé role se mohou vzájemně překrývat — např. moderátor konference může být i jejím členem, administrátor může být zároveň moderátorem apod.

20.2 Vytvoření a nastavení konference

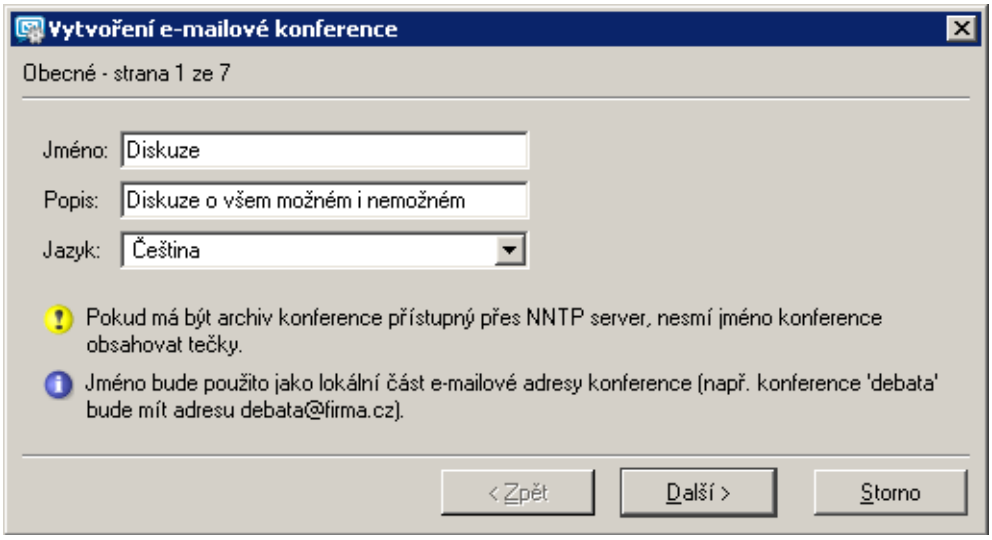
Definice e-mailové konference se provádí v sekci *Nastavení domény* → *E-mailové konference*. Toto může provést pouze administrátor (tj. uživatel s přístupem pro čtení i zápis).

Nejprve je nutno v poli *Doména* (v horní části okna) zvolit doménu, v níž má být konference vytvořena. Tlačítko *Přidat* otevírá dialog pro definici konference.

Základní parametry (záložka Obecné)

Jméno

Název konference. Tento název bude zároveň tvořit e-mailovou adresu konference v dané doméně.
Příklad: Konference nazvaná `diskuze` vytvořená v doméně `firma.cz` bude mít e-mailovou adresu `diskuze@firma.cz`.
Upozornění:



Obrázek 20.1 Vytvoření konference — základní parametry

- Název konference nesmí obsahovat přípony (tj. výrazy uvozené pomlčkou), které se používají pro speciální funkce (např. `-subscribe` — přihlášení do konference). Detaily najdete v kapitole 20.7, sekce *Aliasy v rámci konference*.
- Název konference nesmí obsahovat znak `.` (tečka), protože tento znak v NNTP konferencích funguje jako dělítko struktury konferencí. Takovou konferenci je sice možno vytvořit, ale nebude možno v ní číst pomocí služby NNTP.
- Název konference se nesmí ve stejné doméně shodovat s žádným uživatelským jménem nebo aliasem. V opačném případě má vždy přednost alias a uživatel před e-mailovou konferencí a zprávy do konference nebudou vůbec doručovány.

Popis

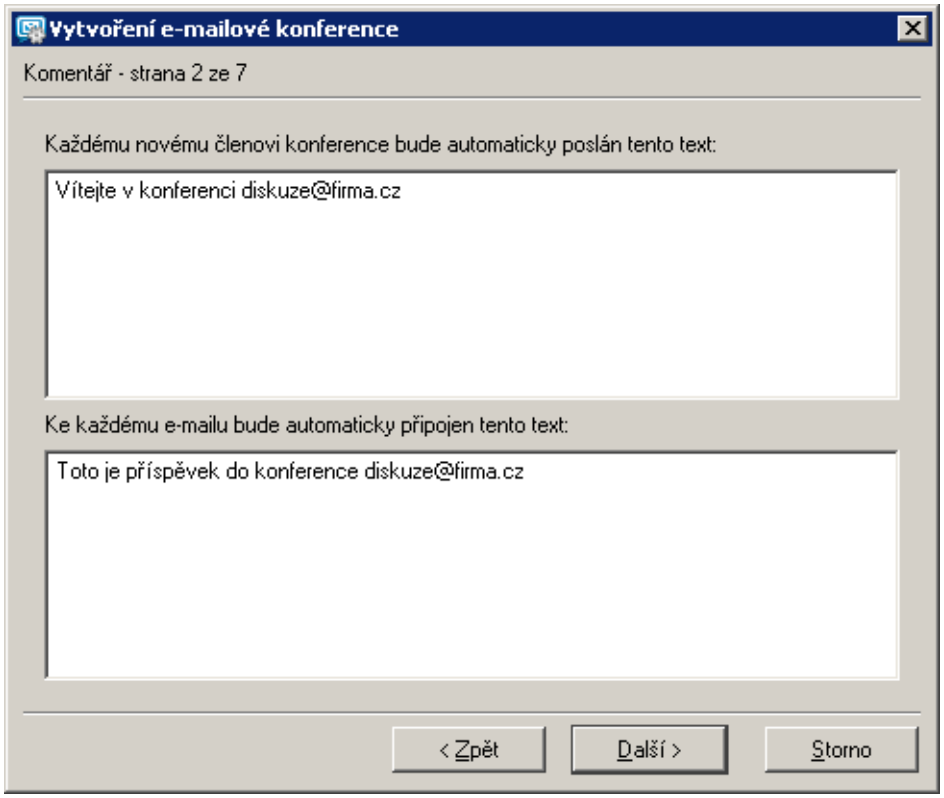
Libovolný textový popis konference.

Jazyk

Výběr jazyka, v němž budou zobrazovány informativní a chybové zprávy týkající se této konference. Díky této volbě je možno na jednom serveru zřizovat konference v různých jazycích. Šablony těchto zpráv pro jednotlivé jazyky jsou uloženy v podadresáři `reports` adresáře, kde je *Kerio MailServer* nainstalován. Soubory používají kódování znaků UTF-8. Zkušený správce tak může jednotlivá hlášení modifikovat, případně vytvořit vlastní jazykovou variantu.

Komentář

Krok 2 umožňuje zadat libovolný text, který bude zaslán každému nově přihlášenému členovi konference (horní pole). Dále obsahuje text, který bude připojen jako zápatí ke každé zprávě (příspěvku) zaslané do této konference (dolní pole). Texty jsou nepovinné — tato pole (resp. některá z nich) mohou zůstat nevyplněna.



Obrázek 20.2 Vytvoření konference — komentáře

Poznámka: Uvítací text je novému členovi zaslán pouze v případě, že se do konference přihlásil e-mailem (podrobnosti najdete v sekci 20.7). Pokud byl do konference zařazen administrátorem v programu *Kerio Administration Console*, uvítací zpráva mu poslána nebude.

Přihlášení

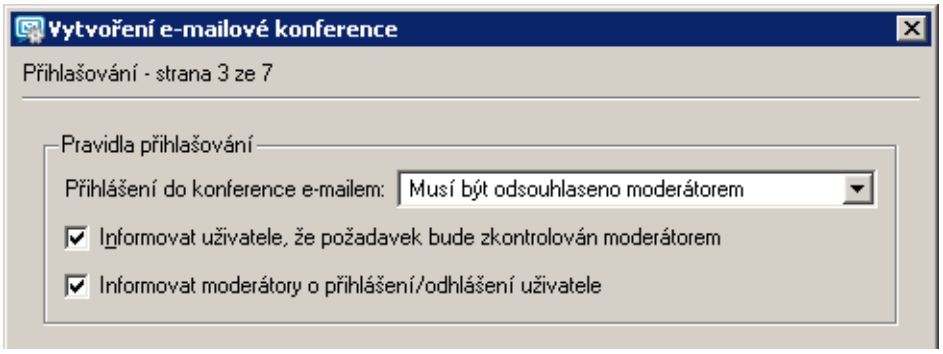
Krok 3 definuje pravidla přihlašování nových členů do konference.

Poznámka: Detaily o přihlašování do konference najdete v kapitole 20.7.

Přihlášení do konference e-mailem

Konference může povolovat přihlašování nových členů zasláním e-mailu na speciální adresu. Možnosti jsou následující:

- *Povoleno* — uživatel je přihlášen automaticky prostým zasláním e-mailu na přihlašovací adresu
- *Musí být odsouhlaseno moderátorem* — požadavek nového člena na přihlášení je předán moderátorům konference. Uživatel je přihlášen až tehdy, pokud některý z moderátorů požadavek potvrdí. Pokud moderátor požadavek zamítne nebo na



Obrázek 20.3 Vytvoření konference — nastavení parametrů pro přihlašování

něj žádný z moderátorů neodpoví ve stanovené době (7 dní), uživatel nebude do konference přihlášen a obdrží informativní zprávu.

- *Zakázáno* — přihlášení e-mailem není možné. Členy konference musí zadat administrátor v tomto dialogu (viz dále).

Informovat uživatele, že...

Uživatel, který požaduje přihlášení, bude informován o tom, že jeho požadavek byl předán moderátorům konference. Tato zpráva je mu zaslána bezprostředně po přijetí požadavku. Bude-li tato volba vypnuta, uživatel obdrží zprávu až v okamžiku, kdy bude jeho požadavek potvrzen či zamítnut (případně vyprší).

Informovat moderátory o přihlášení / odhlášení...

Po zapnutí této volby budou moderátoři konference informováni o každém přihlášení / odhlášení člena konference.

Toto má význam zejména v případě, že je povoleno automatické přihlašování (jinak moderátoři obdrží požadavek — tato informace je pak nadbytečná). Odhlašování je však vždy automatické — tato informace může mít pro moderátora význam.

Poznámka: Je-li uživatel do konference přidán či odstraněn administrátorem v programu *Kerio Administration Console*, moderátor o tom není informován (bez ohledu na to, zda je tato volba zapnuta či nikoliv).

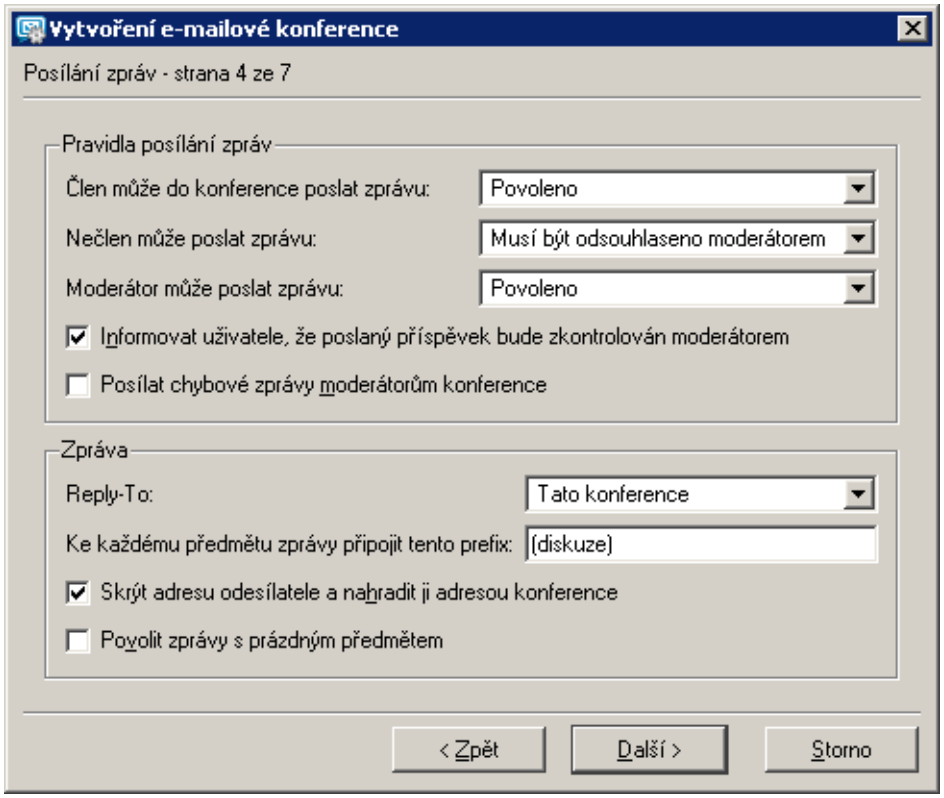
20.3 Pravidla pro posílání zpráv

V kroku 4 je možné nastavení pravidel pro posílání zpráv do konference a pro automatickou úpravu těchto zpráv.

Člen může do konference poslat zprávu

Volba obsahuje několik možností:

- *Povoleno* — příspěvek zaslaný na adresu konference bude ihned doručen všem jejím členům (včetně odesílatele).
- *Musí být odsouhlaseno moderátorem* — příspěvek zaslaný na adresu konference je předán moderátorům k odsouhlasení. Členům konference je rozeslán



Obrázek 20.4 Vytvoření konference — posílání zpráv

až tehdy, pokud jej některý z moderátorů povolí. V opačném případě je odesílatel informován o tom, že zaslání příspěvku bylo odmítnuto.

- *Zakázáno* — členové konference nemají povoleno do ní zasílat příspěvky.
- *Pouze moderátoři* — příspěvky mohou zasílat pouze moderátoři příslušné konference.

Nečlen může poslat zprávu

Volba umožňuje posílat do této konference zprávy i uživatelům, kteří do ní nejsou přihlášeni. Tato volba je dále omezena výběrovým menu, jehož možnosti jsou následující:

- *Povoleno* — příspěvek zaslaný na adresu konference bude ihned doručen všem jejím členům (včetně odesílatele).
- *Musí být odsouhlaseno moderátorem* — příspěvek zaslaný na adresu konference je předán moderátorům k odsouhlasení. Členům konference je rozeslán až tehdy, pokud jej některý z moderátorů povolí. V opačném případě je odesílatel informován o tom, že zaslání příspěvku bylo odmítnuto.
- *Zakázáno* — členové konference nemají povoleno do ní zasílat příspěvky.
- *Pouze moderátoři* — příspěvky mohou zasílat pouze moderátoři příslušné kon-

ference.

Poznámka: Příspěvek v tomto případě nebude zaslán odesílateli, protože není členem konference.

Moderátor může poslat zprávu

Volba, zda a jakým způsobem může posílat moderátor příspěvky do konference. Je zde opět několik možností:

- *Povoleno* — volbu je dobré použít v případě, že z bezpečnostních důvodů musí být zakázán přístup členům i nečlenům. Příspěvky do konference může posílat pouze moderátor.
- *Musí být odsouhlaseno moderátorem* — tato volba je obdobou předchozí, ale má vyšší bezpečnost. Pokusí-li se odesílatel zprávy obejít zákaz tím, že jako odesílatele dosadí adresu moderátora, zpráva se do konference nepošle, ale bude předána (skutečnému) moderátorovi k odsouhlasení.
- *Použít pravidla pro člena/nečlena* — výběrem této položky budou moderátorovi nastavena práva pro členy nebo nečleny konference (v závislosti na tom, zda je zároveň členem konference či nikoliv).

Informovat uživatele, že poslaný příspěvek...

Uživatel, který posílá příspěvek do konference, bude informován o tom, že jeho požadavek byl předán moderátorům konference. Tato zpráva je mu zaslána bezprostředně po přijetí požadavku. Bude-li tato volba vypnuta, uživatel obdrží zprávu až v okamžiku, kdy bude jeho požadavek zamítnut, případně vyprší.

Posílat chybové zprávy...

Po zapnutí této volby budou moderátorům konference posílány veškeré chybové zprávy týkající se této konference. Bude-li tato volba vypnuta, obdrží chybovou zprávu pouze odesílatel příslušného e-mailu. Takovým hlášením může být např. informace o tom, že byl odeslán neplatný požadavek nebo, že e-mailová schránka jednoho z členů konference přesáhla diskovou kvótu nastavenou v *Kerio MailServeru* a zpráva odeslaná do e-mailové konference tudíž nemohla být tomuto členovi doručena.

Reply-To

Tato položka určuje, jaká adresa bude uváděna v příspěvcích do konference jako adresa pro odpověď (položka `Reply-To:` v hlavičce e-mailu):

- *Odesílatel* — v hlavičce bude zachována adresa původního odesílatele. Odpověď na příspěvek bude doručena pouze této osobě. V případě použití této volby nebude zpráva zaslaná do konference nijak upravována.
- *Tato konference* — adresa původního odesílatele bude nahrazena adresou konference. Odpověď na příspěvek tak obdrží všichni členové konference.

- *Jiná adresa* — adresa původního odesílatele bude nahrazena zadanou e-mailovou adresou. Odpovědi na příspěvky tak mohou být posílány určité osobě, do jiné konference apod.
- *Odesílatel + tato konference* — nastavení umožňuje doručování odpovědí na zprávy také nečlenům konference. Mohou zde nastat dva stavy:
  1. Odesílatel je členem konference — odpověď bude doručena na adresu konference. Odesílateli přijde odpověď pouze jednou.
  2. Odesílatel není členem konference — odpověď bude doručena na adresu konference a zároveň na adresu odesílatele. V opačném případě by odesílateli (nečlenovi konference) nebyla odpověď vůbec doručena.

  Z předchozího vyplývá, že volbu je výhodné využít tehdy, pokud je konference určena jak pro její členy, tak pro případné nečleny.
  Poznámka: Tuto možnost nekombinujte s volbou *Skrýt adresu odesílatele a nahradit ji adresou konference*. Kombinace *Odesílatel + tato konference* spolu s *Skrýt adresu odesílatele a nahradit ji adresou konference* je nesmyslná a *Kerio MailServer* nepovolí její uložení na server.

Ke každému předmětu zprávy připojit tento prefix

Prefix, který bude přidán k předmětu každé zprávy zaslané do této konference. Při založení konference je do této položky automaticky dosazeno jméno konference v hranatých závorkách. Obsah této položky však lze libovolně měnit a může zůstat i prázdná (pak se k předmětu zprávy nebude nic připojovat).
Poznámka: Prefix není k předmětu zprávy přidáván, pokud je v něm již obsažen — např. v odpovědích na zprávy z konference má předmět typicky tvar:

```
Re: [jméno] Původní předmět
```

— bez tohoto omezení by byl prefix `[jméno]` duplikován.

Skrýt adresu odesílatele...

Po zapnutí této volby bude v každé zprávě zaslané do konference nahrazena adresa odesílatele (položka `From`) adresou této konference. Příspěvky tak budou víceméně anonymní (pokud se uživatel do zprávy nepodepíše).
Poznámka: Je-li tato volba zapnuta, musí být položka *Reply-To* nastavena na *Tato konference* nebo *Jiná adresa*.

Povolit zprávy s prázdným předmětem

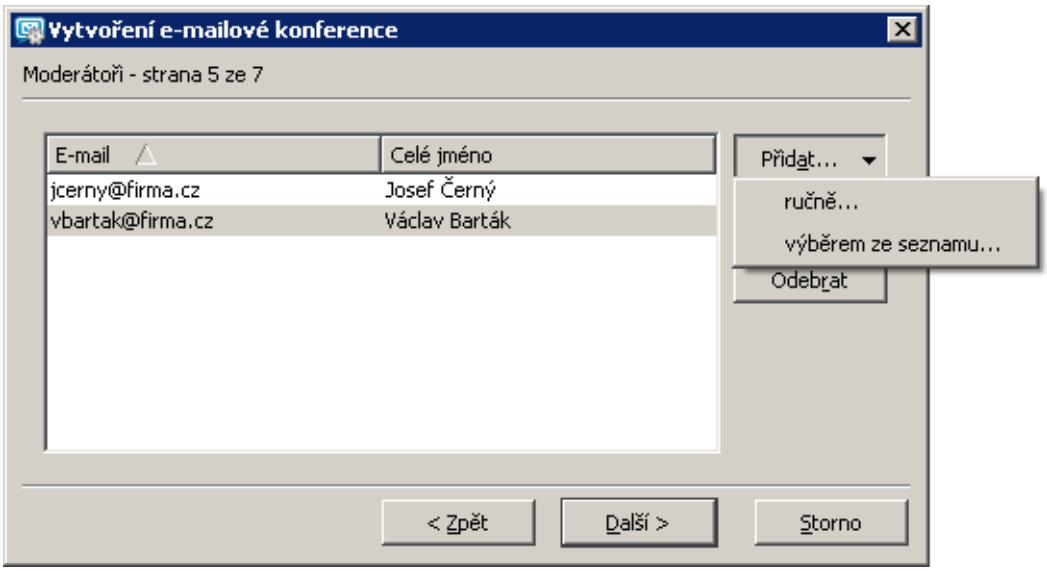
Vypnutí této volby způsobí, že budou akceptovány pouze příspěvky s vyplněnou položkou `Předmět` (`Subject`). Rozhodnutí závisí na administrátorovi (hlavním důvodem je, že takové zprávy mohou být pro některé uživatele obtěžující).

20.4 Moderátoři a členové

V těchto dvou krocích je možno definovat moderátory a členy konference. Moderátory i členy lze přidat stejnými způsoby, proto si obě záložky popíšeme najednou.

Moderátory a členy konference mohou být libovolní uživatelé — zadaná e-mailová adresa nemusí patřit do žádné z domén definovaných v *Kerio MailServeru*. Moderátory konference může definovat pouze administrátor v tomto dialogu. Členy konference může buď přidávat administrátor, nebo se mohou přihlašovat sami prostřednictvím e-mailu (pokud to politika konference dovoluje — viz výše).

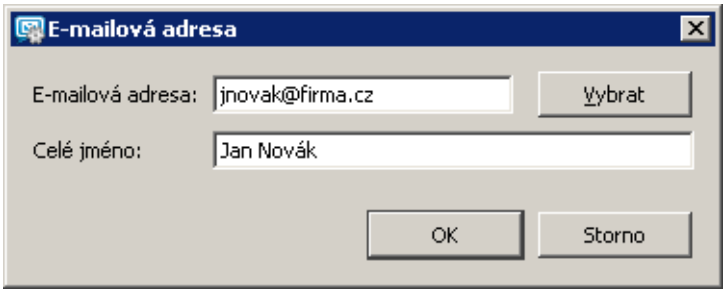
Nového moderátora/člena, lze přidat ručně nebo výběrem ze seznamu (viz obrázek 20.5):



Obrázek 20.5 Vytvoření konference — zadávání moderátorů konference

Ruční přidání moderátora/člena konference

Ručně je možno moderátora/člena konference přidat takto:



Obrázek 20.6 Ruční přidání moderátora/člena konference

1. Klikneme na tlačítko *Přidat*.

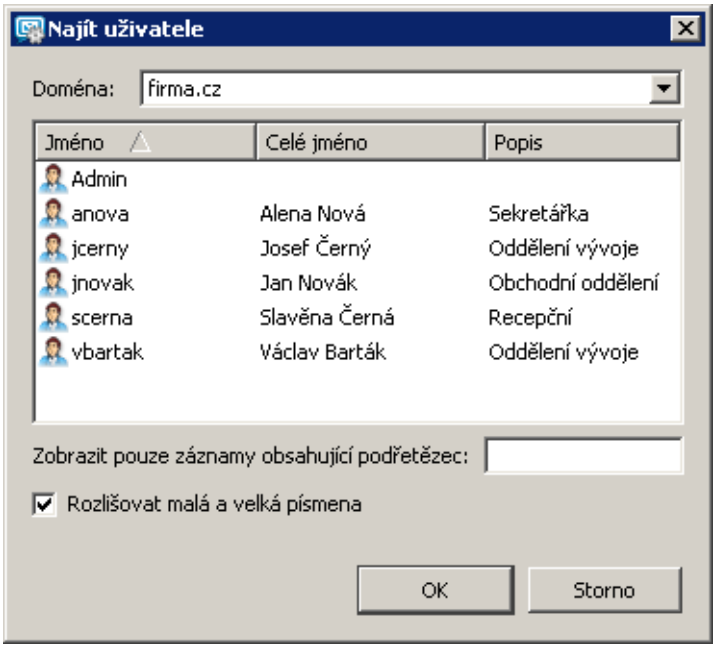
2. Vybereme možnost *ručně...*

3. Otevře se okno, kam přímo zadáme e-mailovou adresu, případně také celé jméno uživatele (doplnění celého jména uživatele je nepovinné). Jedná-li se o uživatele v některé z lokálních domén, lze jej zvolit v dialogu *Najít uživatele*, který otevřeme pomocí tlačítka *Vybrat*.

4. Nastavení potvrdíme tlačítkem *OK*.

Přidání moderátora/člena konference výběrem ze seznamu

Tuto možnost doporučujeme v případě, že přidávaní uživatelé mají schránku v některé z lokálních domén a je jich více najednou.



Obrázek 20.7 Přidání moderátora/člena konference výběrem ze seznamu

Moderátora/člena konference lze výběrem ze seznamu přidat takto:

1. Klikneme na tlačítko *Přidat*.

2. Vybereme možnost *výběrem ze seznamu...* (viz obrázek 20.5).

3. Otevře se dialog *Najít uživatele*, který obsahuje seznam domén a uživatelů (viz obrázek 20.7). Pro vybranou doménu můžeme vybrat více uživatelů najednou pomocí

standardní klávesy `Ctrl` (v případě *Kerio MailServeru* na systému Mac OS použijte samozřejmě klávesu `Command`).

Pokud nemůžete najít správného uživatele, nebo pokud je seznam uživatelů příliš dlouhý, lze použít pole *Zobrazit pouze záznamy obsahující podřetězec*.

4. Nastavení potvrdíme tlačítkem *OK*.

Import nových členů konference z CSV souboru

Jak už bylo řečeno v úvodu kapitoly, členy konference se mohou stát i uživatelé, kteří nemají založen účet v *Kerio MailServeru*. Do konference se uživatelé mohou hlásit pomocí přihlašovacího e-mailu sami, nebo je moderátor konference přidá ručně, a nebo — zejména pokud je takových uživatelů více — je importuje ze souboru.

Aby bylo možné import ze souboru provést, je třeba zajistit několik technických detailů:

1. Soubor s uživateli musí být uložen ve formátu CSV (takový soubor lze vytvořit v kterémkoliv tabulkovém editoru).
2. Oddělovačem dat v souboru musí být čárka (,) nebo středník (;).
3. Nadpisy jednotlivých sloupců musí korespondovat s položkami v *Kerio MailServeru*. Podporovány jsou následující:
   - Email — e-mailová adresa uživatele. Povinná položka.
   - FullName — celé jméno uživatele. Volitelná položka.

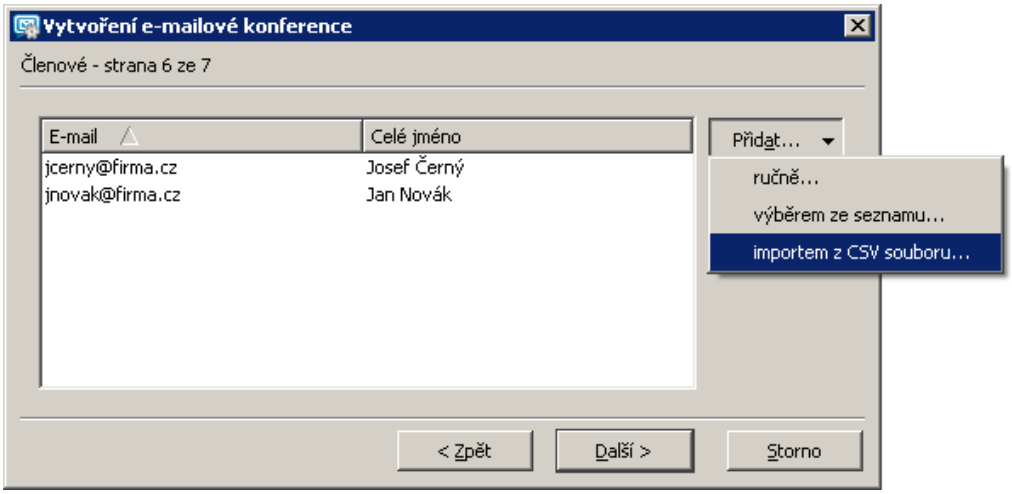
Email	FullName
ebila@yahoo.com	Eva Bílá
lnova@atlas.cz	Lenka Nová
dbilek@seznam.cz	David Bílek
lopletal@hotmail.com	Lubomír Opletal

Tabulka 20.1 Příklad obsahu CSV souboru

Sloupce lze do tabulky poskládat podle potřeby, na jejich pořadí nezáleží. Také je možné využít pouze sloupec Email, FullName je nepovinná položka.

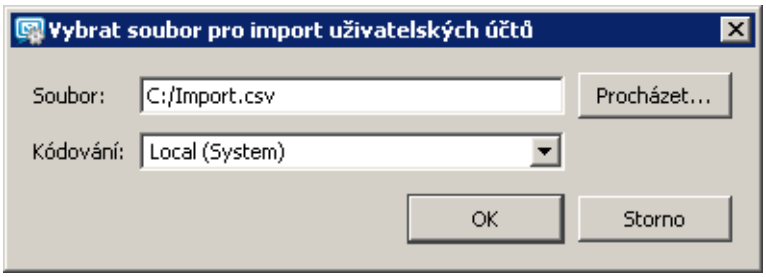
Po správném vytvoření a uložení souboru můžeme buď pokračovat v zakládání konference, nebo pokud už byla konference založena a uložena, otevřeme ji pomocí tlačítka *Změnit* a přepneme se do záložky *Členové*:

1. Klikneme na tlačítko *Přidat* a z menu tlačítka vybereme možnost *importem z CSV souboru* (viz obrázek 20.8).



Obrázek 20.8 Vytvoření konference — zadávání členů konference

2. Otevře se dialog (viz obrázek 20.9), kam zadáme cestu k souboru a nastavíme typ kódování, ve kterém jsou data uložena — ve většině případů stačí nechat v položce standardní *Local (System)*.



Obrázek 20.9 Import ze souboru — výběr souboru

3. Klikneme na tlačítko *OK* a uživatelé se zkopírují do seznamu členů konference.

   Pokud se nepodaří data načíst, důvody mohou být následující:

   - Soubor není uložen ve formátu CSV.
   - Sloupce v souboru nejsou správně označeny nebo nejsou označeny vůbec. CSV soubor musí obsahovat úvodní řádek s názvy sloupců, jinak *Kerio MailServer* data nepřečte.

     Správně:

     ```
     Email;FullName
     ebila@yahoo.com;Eva Bílá
     lnova@atlas.cz;Lenka Nová
     ```

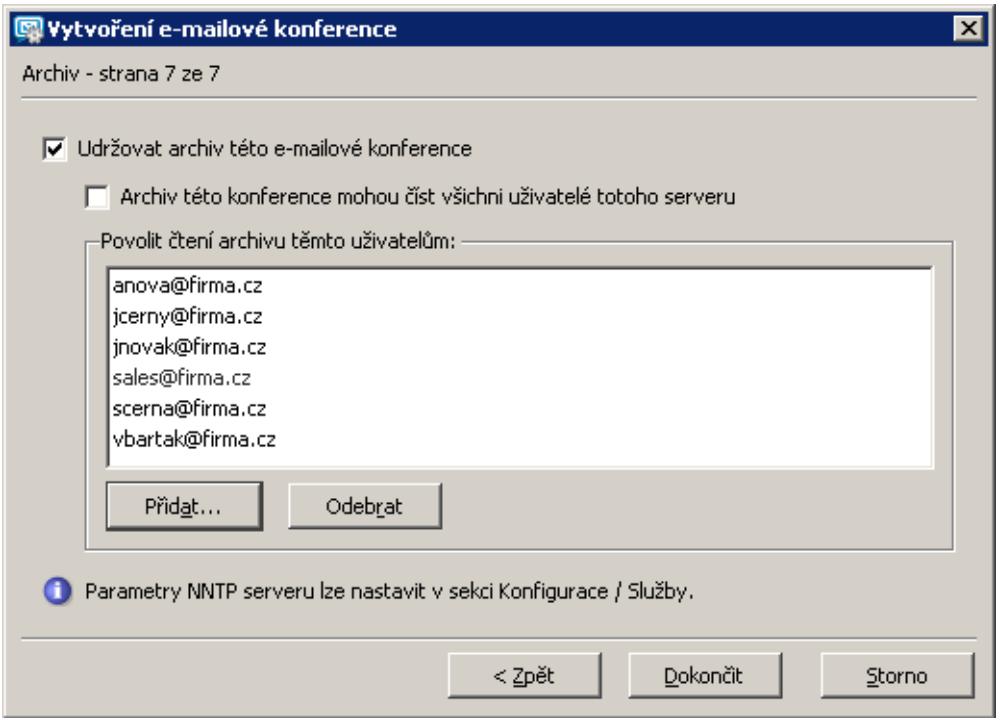
     Špatně:

     ```
     ebila@yahoo.com;Eva Bílá
     lnova@atlas.cz;Lenka Nová
     ```

- Jako oddělovač pro data je použit jiný znak než čárka (,) nebo středník (;).

20.5 Archivace konference

Poslední krok průvodce nastavení konference umožňuje archivaci příspěvků. Archiv je speciální složka, ke které lze přistupovat přes službu NNTP.



Obrázek 20.10 Vytvoření konference — povolení archivace konference

Udržovat archiv této e-mailové konference
Volba aktivuje archivaci konference. K archivu konference budou mít standardně přístup všichni uživatelé příslušné konference.

Archiv této konference mohou číst všichni uživatelé tohoto serveru
Po zaškrtnutí volby bude povoleno čtení archivu všem uživatelům, kteří mají založen v *Kerio MailServeru* účet.

Povolit čtení archivu těmto uživatelům
Čtení archivu konference bude povoleno pouze uživatelům explicitně zadaným do seznamu.

Je-li povolen službě NNTP anonymní přístup (více viz kapitolu 6), bude mít povoleno čtení archivu libovolný uživatel (nemusí mít založen účet v *Kerio MailServeru*).

20.6 Zprávy serveru

V e-mailových konferencích je použita celá řada automaticky generovaných zpráv (informativní zprávy, chybové zprávy, požadavky moderátorům atd.). Každá konference umožňuje nastavit jazyk, v němž budou tyto zprávy zobrazovány (výběr z několika jazyků, které jsou definovány). Šablony těchto zpráv jsou uloženy v podadresáři `reports` adresáře, kde je *Kerio MailServer* nainstalován. Adresář `reports` obsahuje další podadresáře podle jazyků (např. `cs` pro češtinu, `en` pro angličtinu atd.). V těchto podadresářích jsou již uloženy jednotlivé šablony zpráv.

Šablony zpráv je možno upravovat v libovolném editoru podporujícím kódování UTF-8 (v něm jsou zprávy uloženy). Správce *Kerio MailServeru* tak může dát těmto zprávám novou podobu, případně dle popsaného schématu vytvořit novou jazykovou verzi.

20.7 Používání konference

Přihlášení a odhlášení člena konference

Pokud to politika konference (viz kapitolu 20.2) povoluje, mohou se členové přihlašovat do konference pomocí e-mailu. Přihlášení se provede zasláním prázdného e-mailu (resp. e-mailu libovolného obsahu) na adresu v následujícím formátu:

`<jméno_konference>-subscribe@<doména>`

Příklad: Uživatel se chce přihlásit do konference `diskuze` v doméně `firma.cz`. Ze své e-mailové adresy pošle prázdný e-mail na adresu

`diskuze-subscribe@firma.cz`.

Bezprostředně po odeslání této zprávy uživatel obdrží zprávu, v níž je požadováno ověření přihlášení. Důvodem je ochrana proti nežádoucímu odeslání požadavku (např. cizí osobou, která zfalšovala e-mailovou adresu odesílatele). Na tuto zprávu stačí jednoduše odpovědět — pak bude požadavek uživatele přijat ke zpracování.

V závislosti na nastavené politice konference bude uživatel buď přímo přihlášen, nebo bude muset vyčkat na potvrzení přihlašovacího požadavku některým z moderátorů konference. Po úspěšném přihlášení obdrží nový člen uvítací zprávu.

Odhlášení člena z konference e-mailem je možné vždy, bez ohledu na nastavenou politiku přihlašování. Odhlášení se provede zasláním prázdného e-mailu (resp. e-mailu s libovolným obsahem) na adresu v následujícím formátu:

`<jméno_konference>-unsubscribe@<doména>`.

Příklad: Uživatel se chce odhlásit z konference `diskuse` v doméně `firma.cz`. Ze své e-mailové adresy pošle prázdný e-mail na adresu

`diskuze-unsubscribe@firma.cz`.

Bezprostředně po odeslání této zprávy uživatel obdrží zprávu, v níž je požadováno ověření odhlášení. Důvodem je ochrana proti nežádoucímu odeslání požadavku (např. cizí osobou, která zfalšovala e-mailovou adresu odesílatele). Na tuto zprávu stačí jednoduše odpovědět — pak bude požadavek uživatele na odhlášení vyřízen a uživatel obdrží informaci, že byl z konference odhlášen.

Posílání zpráv

Chce-li uživatel přidat do konference příspěvek, odešle jej na adresu konference (např.: `diskuze@firma.cz`). V závislosti na nastavené politice bude příspěvek buď ihned zaslán všem členům konference (včetně odesílatele, pokud je rovněž členem), nebo předán moderátorům k odsouhlasení. V tomto případě odesílatel obdrží informativní zprávu (je-li to nastaveno — viz kapitolu 20.2) a příspěvek bude do konference zaslán, až jej některý z moderátorů potvrdí. Bude-li zaslání příspěvku zamítnuto nebo žádný z moderátorů na požadavek neodpoví ve stanoveném čase (7 dní), bude o tom odesílatel rovněž informován.

Aliasy v rámci konference

V každé e-mailové konferenci jsou automaticky vytvořeny určité e-mailové adresy, které slouží pro speciální funkce (např. přihlášení člena, kontakt na moderátory konference atd.). Všechny tyto adresy mají následující formát:

`<konference>-<přípona>@<doména>`

(např. pro žádost o nápovědu ke konferenci `diskuze` v doméně `firma.cz` pošleme e-mail na adresu: `diskuze-help@firma.cz`).

Zde uvádíme přehled přípon, které může uživatel v adrese konference použít:

- `subscribe` — požadavek na přihlášení uživatele do konference,
- `unsubscribe` — požadavek na odhlášení uživatele z konference,
- `help` — žádost o nápovědu pro použití konference,
- `owner`, `owners` — zaslání zprávy moderátorům konference (uživatel nemusí znát jejich e-mailové adresy).

Kapitola 21

Stavové informace

Kerio MailServer umožňuje správci (popř. jiné oprávněné osobě) poměrně detailně sledovat jeho činnost. V podstatě se jedná o tři druhy informací: sledování stavu, záznamy a statistiky.

- Sledovat je možno stav fronty odchozích e-mailů, připojení k jednotlivým službám *Kerio MailServeru* a doručující procesy (tj. procesy odesílající jednotlivé zprávy z fronty na cílové SMTP servery).
- Záznamy jsou soubory, do nichž se postupně přidávají informace o určitých událostech (např. chybová či varovná hlášení, ladicí informace atd.). O záznamech se dozvíte více v kapitole 22.
- Statistiky obsahují podrobné informace o používání jednotlivých služeb *Kerio MailServeru*, přijatých a odmítnutých zprávách, chybách atd. *Kerio MailServer* také umí graficky vyhodnocovat počet připojení k jednotlivým službám a počet zpracovaných zpráv za určité časové období.

Jaké informace lze sledovat a jak lze přizpůsobit sledování potřebám uživatele je popsáno v následujících kapitolách.

21.1 Fronta zpráv

Veškeré e-maily, které přes *Kerio MailServer* procházejí, jsou řazeny do tzv. fronty zpráv. Fyzicky se jedná o adresář `store/queue` v adresáři, kde je *Kerio MailServer* nainstalován. Do tohoto adresáře je každá zpráva uložena jako dva soubory:

- Soubor s příponou `.eml` je vlastní odesílaný e-mail
- Soubor s příponou `.env` je jeho SMTP obálka. Ta se používá pouze při komunikaci mezi SMTP servery a při uložení zprávy do cílové schránky je oříznuta (tj. zahozena).

Oba tyto soubory mají shodný název, představující jednoznačný identifikátor zprávy.

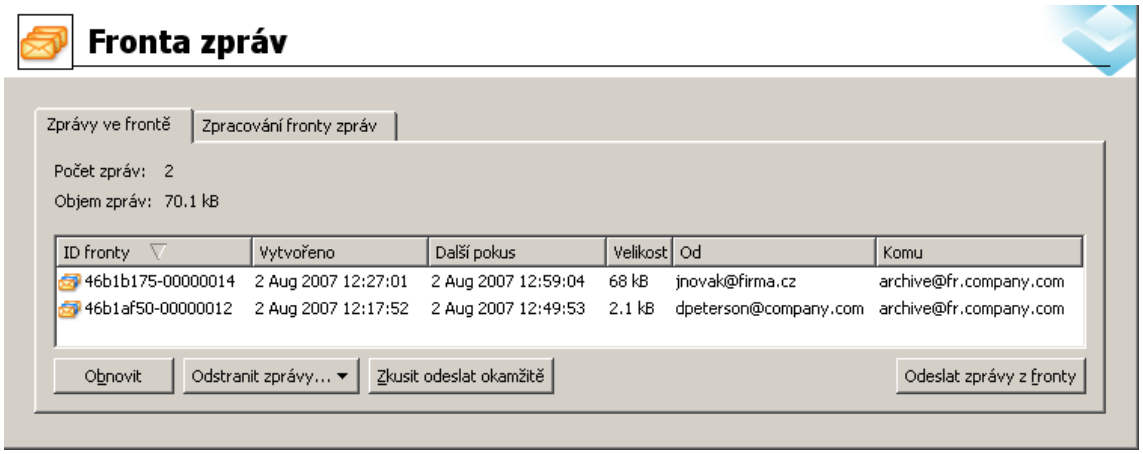
Odeslání zprávy z fronty se provádí buď bezprostředně po jejím příchodu do fronty, nebo v časech řízených plánovačem — dle nastaveného typu internetového připojení — viz kapitolu 8. Odesílá-li SMTP server zprávy přímo do cílových domén (tzn. nepoužívá se žádný nadřazený SMTP server), může také nastat situace, že zprávu nelze odeslat (žádný ze serverů cílové domény není dostupný). V tomto případě se zpráva vrací do fronty a její odeslání je přeplánováno na pozdější dobu.

Poznámka: Pracuje-li server v režimu *Offline*, pak se zpráva zařadí zpět do fronty a další pokus o odeslání zprávy se provede až v nejbližším čase stanoveném plánovačem (*Další pokus* se tedy nastavuje na konkrétní čas pouze v režimu *Online*). V režimu *Offline* (který se používá typicky u připojení vytáčenou linkou) je proto výhodnější odesílat zprávy přes nadřazený SMTP server.

Prohlížení fronty zpráv

Potřeba zkontrolovat frontu zpráv vzniká typicky při podezření, že zprávy ze serveru neodcházejí. Prohlížení fronty přímo v adresáři na disku není příliš komfortní, navíc zpravidla vůbec není možné, jestliže je *Kerio MailServer* spravován vzdáleně (musel by být k dispozici nějaký další nástroj pro vzdálený přístup na počítač, na němž *Kerio MailServer* běží). Z tohoto důvodu je možné sledovat frontu také přímo v *Kerio Administration Console*, a to v sekci *Stav* → *Fronta zpráv*.

Záložka kromě fronty zpráv obsahuje také statistické údaje o aktuálním počtu zpráv ve frontě a jejich celkové velikosti.



Obrázek 21.1 Fronta zpráv

Na každé řádce tohoto okna je zobrazena jedna zpráva ve frontě. Sloupce obsahují následující informace:

ID fronty
: Jedinečný identifikátor zprávy. Tento identifikátor také tvoří názvy souborů, v nichž je zpráva a její obálka uložena v adresáři `mail/queue`.

Vytvořeno
: Datum a čas uložení zprávy do fronty.

Další pokus
Datum a čas dalšího pokusu o odeslání zprávy (interval pokusů a dobu, po níž budou prováděny, lze nastavit v sekci *Konfigurace* → *Vlastnosti SMTP* — viz kapitolu 15.2). Zkratka *ASAP* znamená *As Soon As Possible* — čili „ihned, jakmile to bude možné“. Takto je plánováno odeslání zpráv, které jsou do fronty zařazeny poprvé — v módu *Online* jsou odeslány okamžitě a v módu *Offline* v nejbližším čase daném plánovačem.

Velikost
Velikost zprávy (nezahrnuje SMTP obálku).

Od, Komu
E-mailová adresa odesílatele a příjemce zprávy. Pokud je položka *Od* prázdná, pak je to systémová DSN zpráva odeslaná *Kerio MailServerem*.

Stav
Sloupec popisuje stav odeslání zprávy, resp. důvod, proč zpráva nebyla odeslána.

Manipulace se zprávami ve frontě

Tlačítky po oknem *Fronta zpráv* je možno ručně spustit následující akce:

Obnovit
K obnovení informací v okně *Fronta zpráv* dochází vždy, když nastane ve frontě nějaká změna. Kromě toho je možné zobrazení obnovit ručně tlačítkem *Obnovit*.

Odstranit zprávy
Odstranění zpráv z fronty. Tlačítko obsahuje menu, kde je možné vybrat, zda mají být odstraněny z fronty vybrané zprávy, všechny zprávy nebo zprávy odpovídající kritériím (elektronické adresy odesílatele a příjemce).

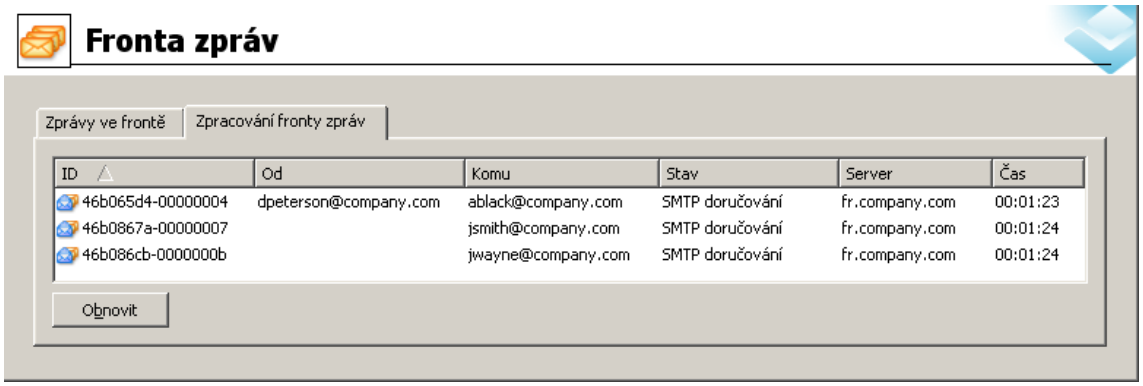
Zkus odeslat okamžitě
Pokus o okamžité odeslání vybrané zprávy.

Odeslat zprávy z fronty
Zahájení odesílání zpráv z odchozí fronty.

21.2 Zpracování fronty zpráv

Při zpracování fronty zpráv vytvoří *Kerio MailServer* pro každou zprávu nový proces, který provede její zpracování (doručení do lokální schránky nebo na vzdálený SMTP server, antivirovou kontrolu atd.), a poté se ukončí. Takovýchto procesů může běžet několik současně (paralelně) — z toho vyplývá, že *Kerio MailServer* je schopen odesílat více odchozích zpráv současně. Maximální počet odesílajících procesů lze nastavit v sekci *Konfigurace* → *Vlastnosti SMTP*, záložka *Volby*, parametr *Maximální počet doručujících procesů* (výchozí hodnota je *32*).

V sekci *Stav* → *Fronta zpráv* v záložce *Zpracování fronty zpráv* je možno tyto procesy sledovat (kdy byl proces vytvořen, jakou zprávu zpracovává, na který SMTP server je odesílána...) a zjišťovat jejich stav (antivirová kontrola, odesílání, lokální doručování...).



Obrázek 21.2 Zpracování fronty zpráv

Jednotlivé sloupce okna *Doručující procesy* mají následující význam:

ID
: Jednoznačný identifikátor zprávy, kterou proces zpracovává (odpovídá ID zprávy ve frontě a názvu souboru v adresáři `mail/queue`).

Velikost
: Velikost doručované zprávy (v bytech).

Od, Komu
: E-mailová adresa odesílatele a příjemce zprávy.

Stav
: Stav procesu: *Spouští se*, *Zálohování*, *Filtrování obsahu* (kontrola na zakázané typy příloh), *Antivirová kontrola*, *Lokální doručování* (jestliže se zpráva ukládá do lokální schránky), *SMTP doručování* (jestliže se odesílá na jiný SMTP server), *Ukončuje se* (závěrečná fáze, ukončení procesu). Proces nemusí nutně projít všemi uvedenými fázemi — je-li např. vypnuto zálohování pošty, fáze *Zálohování* se přeskočí.

Server
: SMTP server, na nějž je zpráva doručována (pouze ve fázi *SMTP doručování*).

Čas
: Doba běhu procesu (čas od jeho vytvoření).

Procent
: Informace o průběhu odesílání zprávy (jaká část zprávy již byla odeslána).

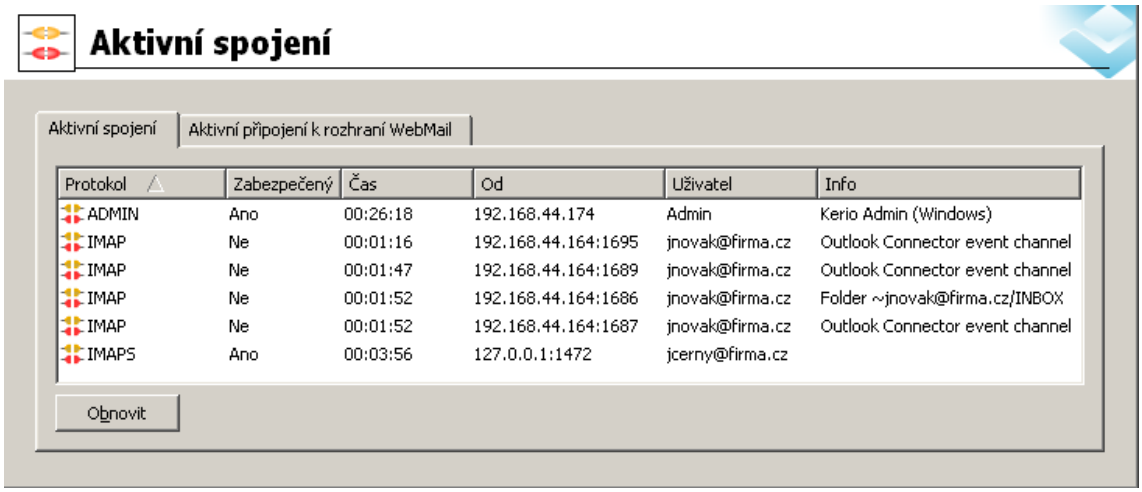
Informace v okně *Doručující procesy* jsou automaticky obnovovány, navíc je také možno je aktualizovat ručně tlačítkem *Obnovit*.

21.3 Aktivní spojení

V sekci *Stav* → *Aktivní spojení* lze sledovat veškerá síťová připojení ke *Kerio MailServeru*, a to jednak k jeho službám (*SMTP*, *POP3* atd.), a jednak ke správě (programem *Kerio Administration Console*).

Aktivní spojení

Na každé řádce této záložky je zobrazeno jedno spojení. Jedná se o síťová spojení, nikoliv připojení uživatelů (každý klientský program může např. z důvodu přijímání a odesílání zpráv najednou navázat více spojení současně). Sloupce zobrazují následující informace:



Obrázek 21.3 Aktivní spojení

Protokol
: Typ protokolu, který klient používá (resp. služby, k níž je připojen). Pojmenování koresponduje s názvy služeb v sekci *Konfigurace* → *Služby*, *ADMIN* znamená připojení ke správě programem *Kerio Administration Console*.

Zabezpečený
: Volba umožňuje zabezpečení spojení protokolem SSL (*technická poznámka:* vzdálená správa umožňuje pouze zabezpečené připojení).

Čas
: Doba připojení klienta. U některých služeb funguje timeout — automatické odpojení klienta při nečinnosti (jestliže se spojením nepřenášejí žádná data).

Od
: IP adresa, z níž se klient připojuje. Namísto IP adresy je zde možné zobrazit DNS jméno klienta získané reverzním DNS dotazem, jestliže je zapnuta volba *Provádět reverzní DNS dotazy na příchozí spojení* v sekci *Konfigurace → Upřesňující nastavení* (viz též kapitolu 15.6). Doporučujeme zapínat tuto volbu pouze v případě, chcete-li cíleně sledovat, odkud se klienti připojují — reverzní dotazy zpomalují činnost serveru.

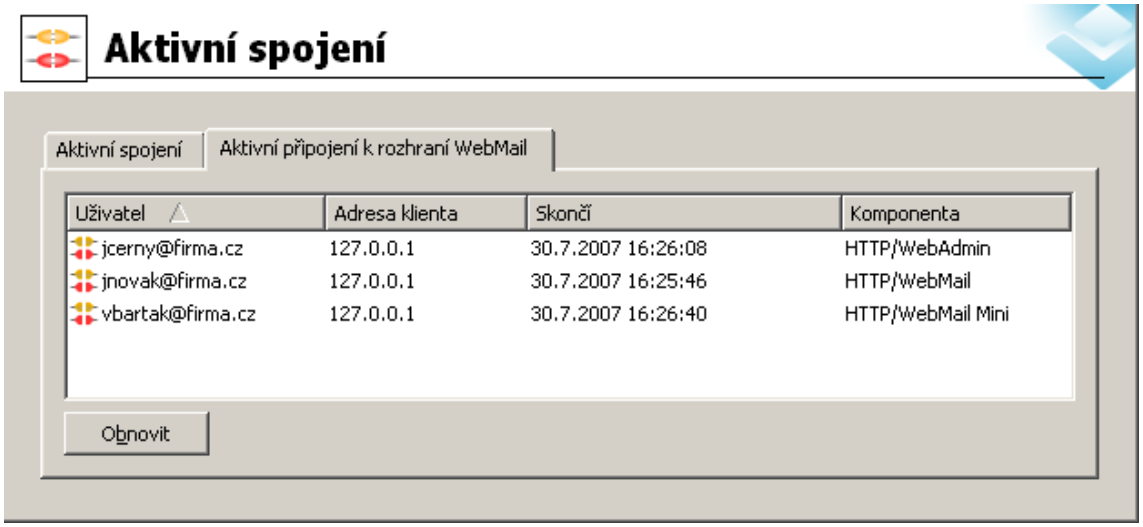
Uživatel
: Jméno přihlášeného uživatele. V některých případech se jméno nezobrazuje (např. připojení k SMTP serveru, není-li vyžadováno ověření uživatele — klient je anonymní).

Informace
: Další informace o připojení (např. IMAP složka, verze administračního programu atd.).

Informace v okně *Aktivní spojení* jsou automaticky obnovovány, navíc je také možno je obnovit ručně tlačítkem *Obnovit*.

Aktivní připojení k rozhraní WebMail

V této záložce jsou zobrazováni uživatelé připojení k rozhraní *Kerio WebMail*. Každý řádek zaznamenává jednoho uživatele (jeho elektronickou adresu), IP adresu, ze které se připojuje ke *Kerio MailServeru* a čas automatického konce připojení.



Obrázek 21.4 Aktivní připojení k webovému rozhraní

Uživatel
Uživatel připojený přes *Kerio WebMail* ke *Kerio MailServeru*.

Adresa klienta
IP adresa počítače, ze kterého se uživatel připojuje ke *Kerio MailServeru*.

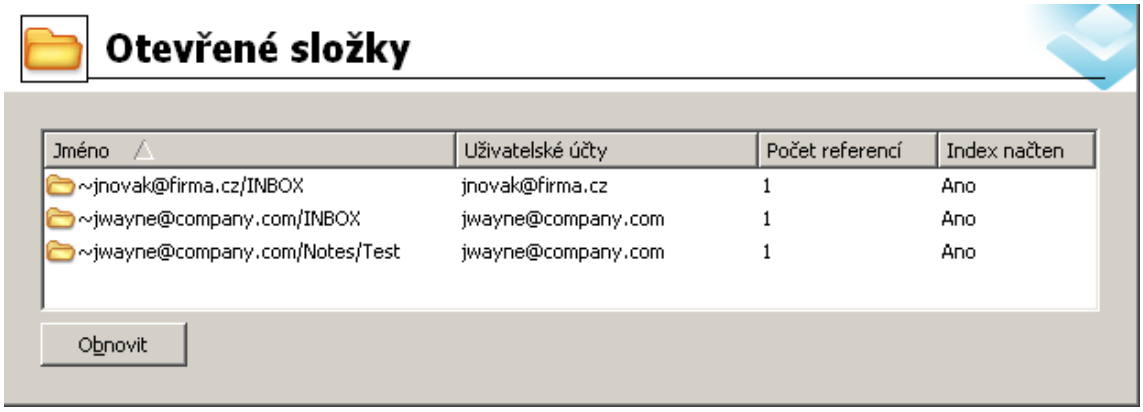
Skončí
Rozhraní *Kerio WebMail* provádí z bezpečnostních důvodů automatické odhlášení uživatele po určité době nečinnosti (1 hodina).

Komponenta
Uživatel může být k serveru připojen třemi různými komponentami — *Kerio WebMailem* (HTTP/WebMail), *Kerio WebMailem Mini* (HTTP/WebMail Mini) a *Kerio Web Administration* (HTTP/WebAdmin).

21.4 Otevřené složky

Sekce *Stav* → *Otevřené složky* zobrazuje všechny uživatele, kteří mají ve svých poštovních klientech otevřeny nějaké složky.

Tato sekce zobrazuje o složkách následující informace:



Obrázek 21.5 Otevřené složky

Jméno
Název uživatelské složky ve tvaru `~uzivatelske_jmeno@domena/nazev slozky`

Uživatelské účty
Položka obsahuje všechny uživatele, kteří mají v daném čase složku otevřenou. Uživatelů může být více najednou v případě veřejných nebo sdílených složek.

Počet referencí
: Položka zobrazuje počet uživatelů, kteří mají v daném čase složku otevřenou. Uživatelů může být více najednou v případě veřejných nebo sdílených složek. Stejně tak může být jedna složka otevřena vícekrát jedním uživatelem.

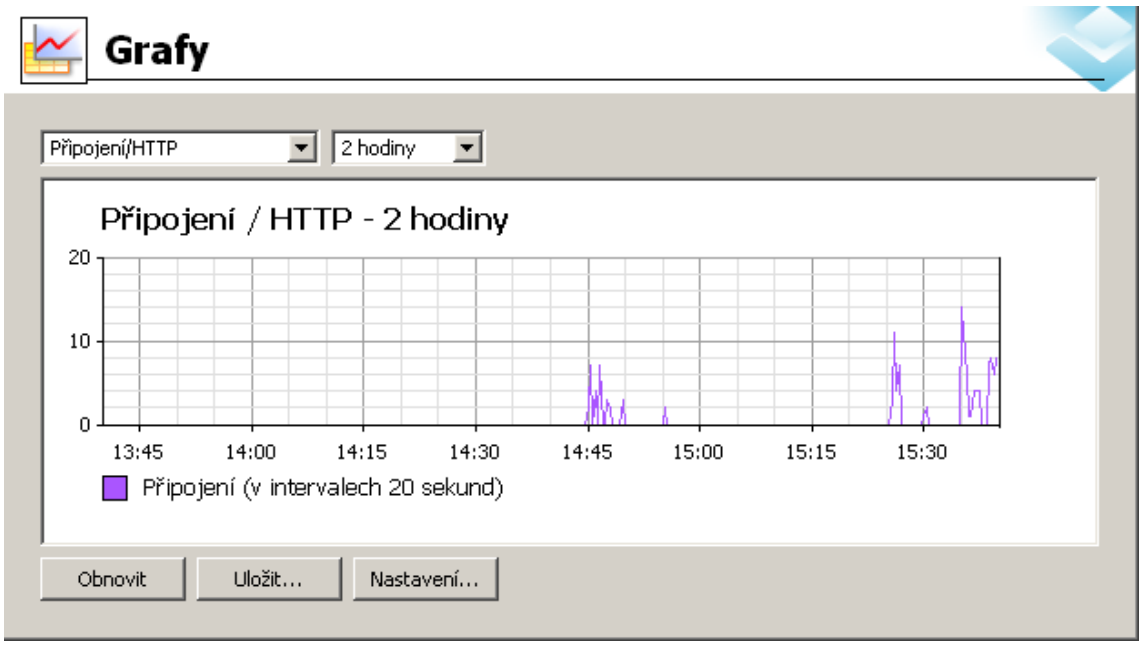
Index načten
: Položka signalizuje, zda byl serverem načten soubor `index.fld`, díky kterému se uživateli správně zobrazují různé informace ke zprávám (příznaky, informace o tom, zda je zpráva označena jako smazaná nebo přečtená, atd.).

Tlačítko *Obnovit* v levém dolním rohu sekce ručně aktualizuje zobrazení otevřených složek.

Poznámka: Obnovu zobrazení je možné nastavit také periodicky v určených časových intervalech. Zapnout a nastavit automatické obnovování lze přes kontextové menu (nabídka vyvolaná pravým tlačítkem myši).

21.5 Grafy

V sekci *Stav* → *Grafy* je možno graficky sledovat počet připojení k jednotlivým službám *Kerio MailServeru* a počet zpracovaných zpráv (příchozích i odchozích) za určité časové období.



Obrázek 21.6 Grafy v Kerio MailServeru

Graf umožňuje nastavení následujících parametrů:

Sledovaný parametr

První pole slouží pro výběr sledovaného parametru:

- *Připojení / HTTP* — počet připojení ke službě *HTTP*
- *Připojení / IMAP* — počet připojení ke službě *IMAP*
- *Připojení / LDAP* — počet připojení ke službě *LDAP*
- *Připojení / NNTP* — počet připojení ke službě *NNTP*
- *Připojení / Odchozí SMTP* — počet odchozích spojení služby *SMTP*
- *Připojení / Odmítnuté SMTP* — počet odmítnutých připojení ke službě *SMTP* (připojení odmítnutá spamovým filtrem *Odrazování spammerů*)
- *Připojení / POP3* — počet připojení ke službě *POP3*
- *Připojení / SMTP* — počet připojení ke službě *SMTP*
- *Zprávy / Přijaté* — počet zpráv zpracovaných poštovním serverem (součet odchozích a příchozích SMTP zpráv a zpráv stažených ze vzdálených POP3 schránek)
- *Zprávy / Spam* — počet zpráv označených antispamovým filtrem jako spam

Časové období

Ve druhém poli je možno vybrat časové období, ve kterém má být sledování prováděno (v rozsahu 2 hodiny — 30 dní). Zvolené časové období je vždy bráno od aktuálního času do minulosti („poslední 2 hodiny“, „posledních 30 dní“, apod.).

Komentář pod grafem zobrazuje interval vzorkování (tj. interval, za který se hodnoty sečtou a zaznamenají do grafu).

Příklad: Je-li zvoleno časové období *2 hodiny*, provádí se vzorkování po 20 sekundách. To znamená, že se každých 20 sekund zaznamená do grafu počet připojení (resp. zpráv) za uplynulých 20 sekund.

Pod grafem jsou umístěna tři tlačítka:

- Tlačítko *Obnovit* umožňuje okamžitou aktualizaci grafu.
- Pomocí tlačítka *Uložit* umístěného pod grafem lze tento graf uložit jako obrázek ve formátu PNG.
- Tlačítko *Nastavení* otevírá dialog pro detailní nastavení vlastností grafu.

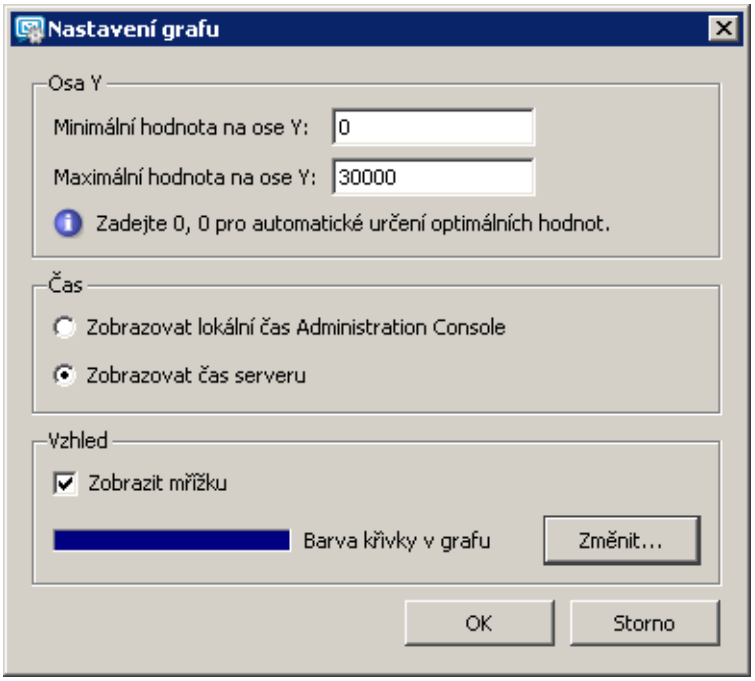
  Osa Y

  Nastavení minimální a maximální hodnoty na ose *y*

  Poznámka: Měřítko osy *x* je pevně dáno vybraným časovým intervalem.

  Čas

  Volba, který čas má být v grafu zobrazován (čas serveru nebo lokální čas počítače, na němž běží *Kerio Administration Console*). Obecně platí následující:



Obrázek 21.7 Nastavení grafu

- Je-li *Kerio Administration Console* spuštěna přímo na počítači, kde je *Kerio MailServer* nainstalován, jsou tyto časy vždy shodné.
- Totéž platí, pokud je čas na obou počítačích synchronizován (např. protokolem NTP či ve Windows NT doméně).
- Není-li čas synchronizován, ale oba počítače jsou ve stejném časovém pásmu, doporučujeme používat čas serveru.
- Je-li každý z těchto počítačů v jiném časovém pásmu, zvolte čas serveru nebo administrační konzoly podle potřeby.

Zobrazit mřížku

Volba umožňuje zobrazit nebo skrýt mřížku v příslušném grafu.

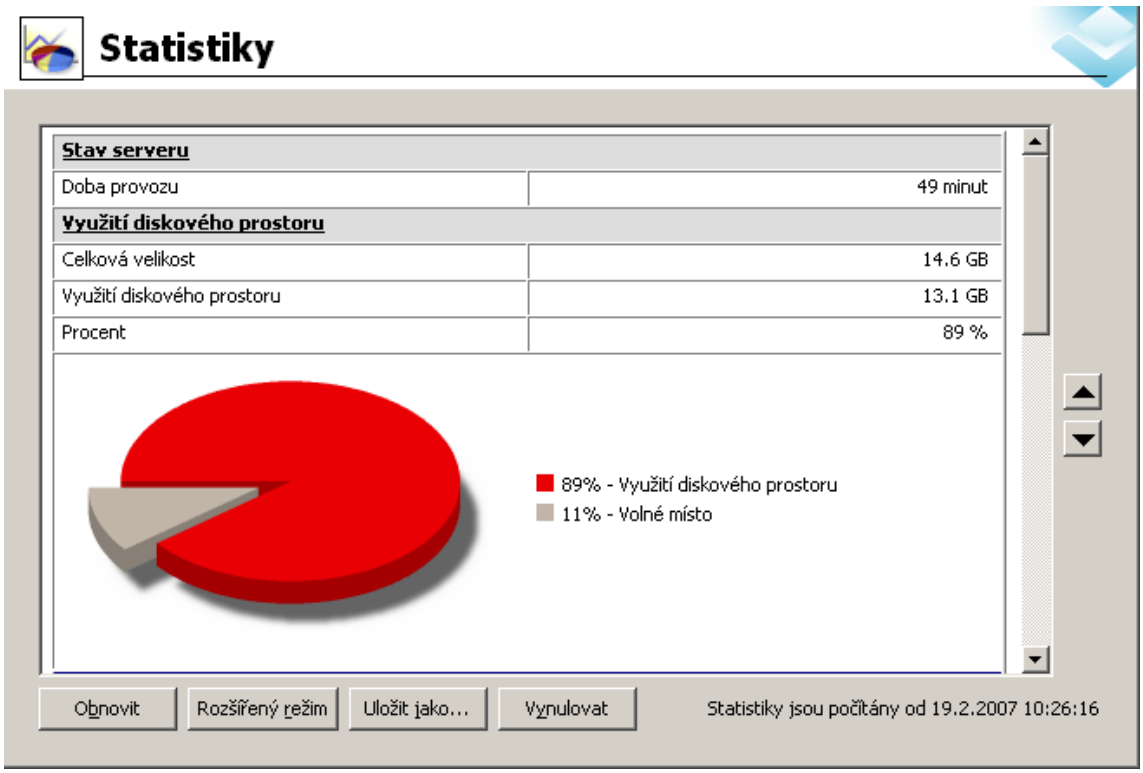
Barva křivky v grafu

Volba barvy křivky, která má být v grafu použita. Tlačítkem *Změnit* lze otevřít standardní okno s paletou a vybrat zde vyhovující barvu.

21.6 Statistiky

K zobrazení statistických údajů slouží sekce *Stav* → *Statistiky*. Pro lepší přehlednost jsou informace v této sekci rozděleny do tabulek (např. „Využití diskového prostoru“, „Zprávy odeslané na nadřazený SMTP server“, „Statistika POP3 klienta“ apod.). Každá tabulka zobrazuje data, která k sobě tématicky patří.

Sekce *Statistiky* obsahuje několik tlačítek:



Obrázek 21.8 Zobrazení statistik

Obnovit

Tlačítko slouží k průběžným obnovám dat ve statistikách.

TIP: Konkrétní statistika se obnoví také v případě, že klikneme na její záhlaví.

Základní režim/Rozšířený režim

Statistiky mají dva režimy:

- *Základní režim* — obsahuje pouze čtyři nejpoužívanější statistiky: *Stav serveru*, *Využití diskového prostoru*, *Statistika antivirové kontroly* a *Statistika spamového filtru*.
- *Rozšířený režim* — obsahuje všechny statistiky.

Uložit jako

Tlačítko slouží k uložení statistiky v HTML formátu.

Vynulovat

Tlačítko umožňuje restart počítání údajů. To znamená, že se všechny statistiky začnou počítat znovu od začátku.

Upozornění: Všechny statistiky jsou měřeny vždy od prvního spuštění *Kerio MailServeru* nebo od posledního restartu statistik. Vpravo dole v sekci *Statistiky* jsou zobrazeny datum a čas počátku počítání statistik.

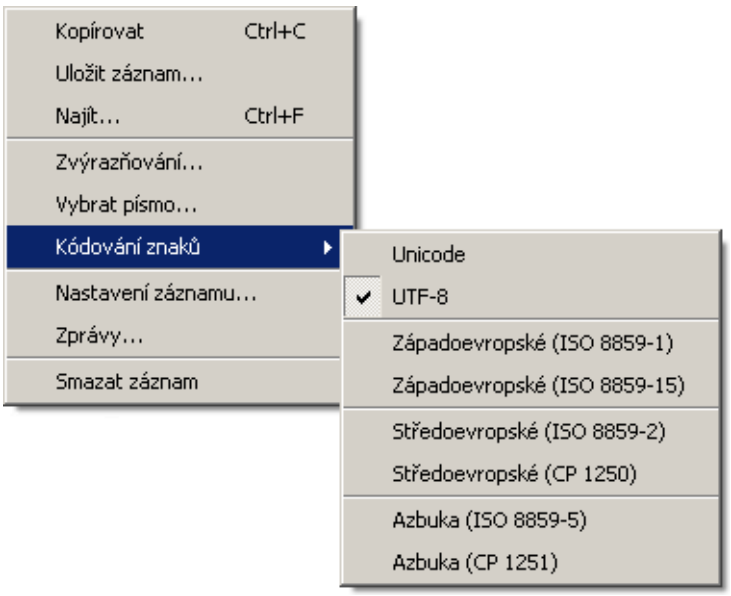
Kapitola 22

Záznamy

Záznamy jsou soubory, do nichž se postupně přidávají informace o určitých událostech (např. chybová či varovná hlášení, ladicí informace atd.). Každá položka je zapsána na jedné řádce a uvozena časovou značkou (datum a čas, kdy událost nastala, s přesností na sekundy). Zprávy vypisované v záznamech jsou ve všech jazykových verzích *Kerio MailServeru* anglicky (generuje je přímo *Kerio MailServer Engine*).

22.1 Nastavení záznamů

V okně každého záznamu se po stisknutí pravého tlačítka myši zobrazí kontextové menu, v němž lze zvolit různé funkce nebo změnit parametry záznamu (zobrazení, příp. sledované informace).



Obrázek 22.1 Kontextové menu v záznamech

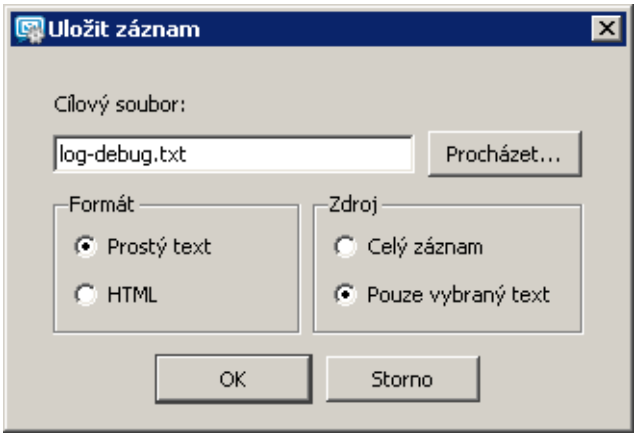
Kopírovat

Zkopírování označeného textu do schránky (clipboardu). Pro tuto funkci lze využít také klávesové zkratky operačního systému (např. ve Windows *Ctrl+C* nebo *Ctrl+Insert*).

Uložit záznam

Pomocí volby *Uložit záznam* je možno celý záznam nebo jeho část uložit do libovolného souboru na disku.

Volby dialogu jsou následující:



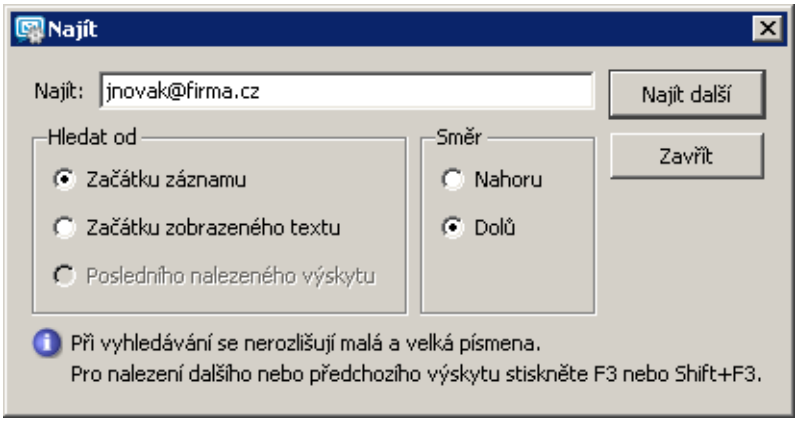
Obrázek 22.2 Uložit záznam

- *Formát* — Záznam může být uložen buď formou prostého textu (TXT) nebo ve formátu HTML. Bude-li záznam uložen v HTML formátu, zůstane zachováno nastavené kódování a také barva, pokud bylo nastaveno zvýrazňování. Záznam v textovém formátu může být lepší volbou, pokud bude záznam dále zpracováván nějakým skriptem.
- *Zdroj* — Volba umožní uložit buď celý záznam nebo také vybraný text záznamu označený kurzorem.
  Volba *Pouze vybraný text* standardně není aktivní. Pouze v případě, že je část záznamu označena kurzorem, bude možné vyznačenou část uložit.

Najít

Umožní vyhledat konkrétní řádek záznamu. Do pole *Najít* zadejte řetězec, který má být vyhledán.

- *Hledat od* — Vyhledávání lze nastavit buď od začátku záznamu, nebo od začátku zobrazeného textu (vyhledávat se bude pouze v textu, který je zobrazen v okně), a nebo od posledního nalezeného výskytu.
- *Směr* — Touto položkou lze nastavit směr prohledávání textu (*Nahoru*, *Dolů*).

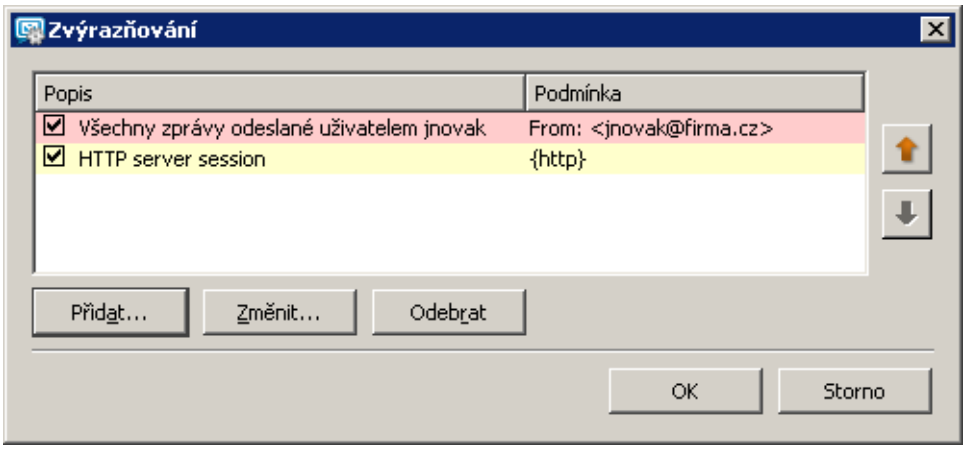


Obrázek 22.3 Vyhledávání

Zvýrazňování

Kerio MailServer umožňuje zvýraznit jakýkoliv text v záznamu. Toto zvýraznění slouží především ke zlepšení orientace v záznamu.

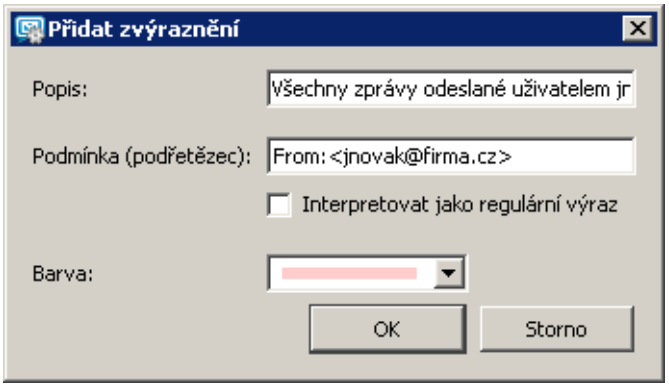
Po kliknutí na volbu *Zvýraznění* se otevře okno, kde je možno zadávat, měnit a mazat zvýraznění pomocí standardních tlačítek *Přidat*, *Změnit* a *Odebrat*.



Obrázek 22.4 Zvýrazňování

Nastavit parametry nového zvýraznění lze v okně *Přidat zvýraznění* (viz obrázek 22.5):

- *Popis* — zvýraznění může být libovolné množství, a proto lze pro lepší orientaci každé výstižně popsat.
- *Podmínka (podřetězec)* — v záznamu bude barevně odlišen každý řádek, který bude obsahovat řetězec zadaný do tohoto pole.
  Po zaškrtnutí možnosti *Interpretovat jako regulární výraz*, lze do pole zapsat libovolný regulární výraz (komplexní definice, pro zkušené uživatele).
  Regulární výrazy (regular expression) jsou speciální jazyky standardu POSIX pro popis řetězce. Jsou tvořeny sadou flexibilních vzorů, které programy porovnávají



Obrázek 22.5 Přidat zvýraznění

s různými řetězci.

- *Barva* — menu obsahuje barevnou škálu, kterou je možno použít ke zvýraznění textu.

Každé nastavené zvýraznění platí pro všechny typy záznamu. Nastavené zvýraznění se projeví na všech řádcích vyhovujících podmínce v celém záznamu.

Vybrat písmo

Volba umožňuje otevření standardního okna pro nastavení velikosti, stylu a typu písma záznamu.

Kódování znaků

Nastavení kódování pro příslušný záznam.

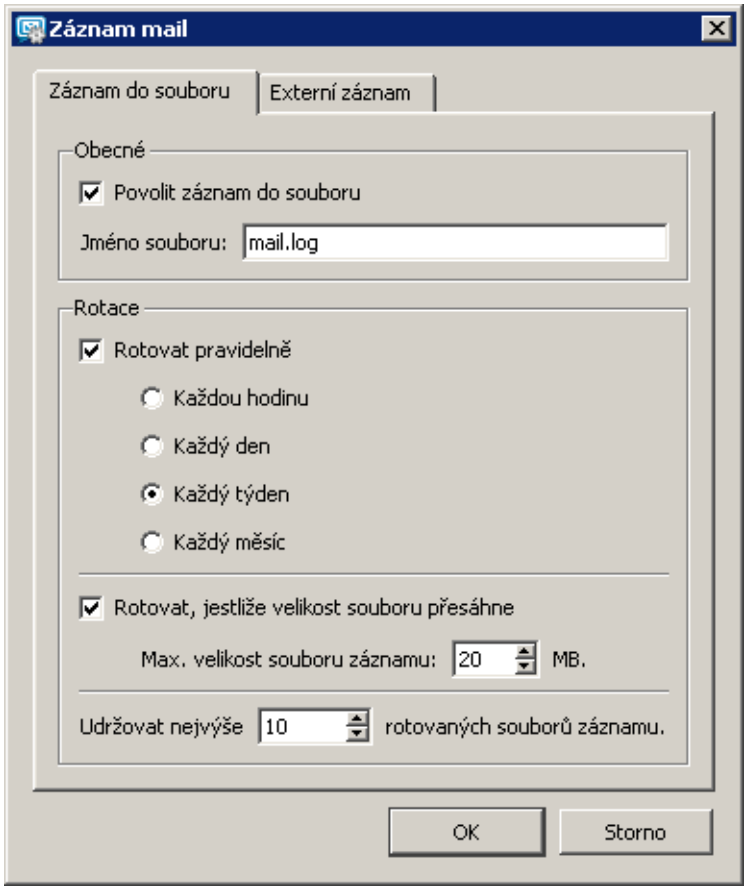
Nastavení záznamu

Tato volba otevírá dialog *Záznam debug*, kde je možné nastavit podmínky, za jakých bude záznam vymazán nebo uložen, a kam bude uložen.

Záložka Záznam do souboru

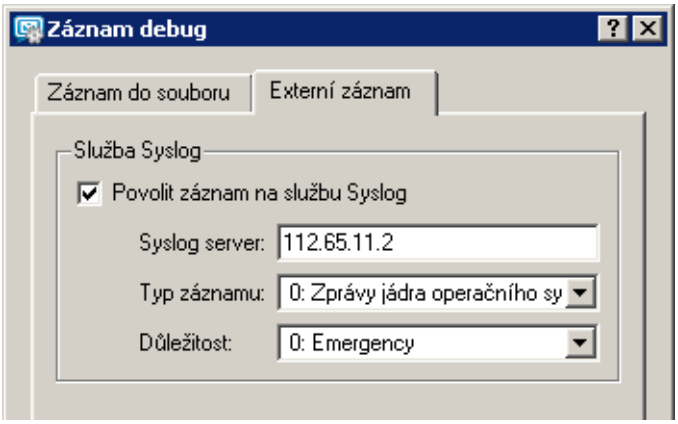
- *Povolit záznam do souboru* — volba umožní zápis záznamu do souboru. Do pole *Cesta* lze zapsat cestu k souboru, kam se budou záznamy zapisovat.
- *Rotovat pravidelně* — vyberete jeden z následujících časových údajů:
  - *Každou hodinu* — záznam je každou hodinu archivován a začne se zapisovat do nového souboru.
  - *Každý den* — záznam je rotován každých 24 hodin.
  - *Každý týden* — záznam je rotován vždy jednou týdně.
  - *Každý měsíc* — záznam je rotován každý měsíc.
- *Rotovat, jestliže velikost souboru přesáhne* — v poli *Max. velikost souboru záznamu* lze nastavit archivaci záznamů podle velikosti souboru (v KB).
- *Uchovávat nejvýše ... souborů záznamu.* — počet souborů záznamu, které mají zůstat uchovány. Při každé rotaci záznamu se vždy nejstarší soubor smaže.

Záložka Externí záznam



Obrázek 22.6 Ukládání záznamů

Záložka *Externí záznam* umožňuje nastavení parametrů pro odesílání záznamu na *Syslog server*.



Obrázek 22.7 Ukládání logu na Syslog server

- *Povolit záznam na Syslog server* — volba umožňuje zapnout/vypnout záznam na server *Syslog*.
- *Syslog server* — DNS jméno nebo IP adresa *Syslog* serveru.
- *Typ záznamu* — slouží mimo jiné k rozlišení, odkud záznam přišel (*Syslog* server může přijímat záznamy z mnoha různých zdrojů).
- *Důležitost* — nastavení důležitosti záznamu (*Syslog* server umožňuje filtrování záznamů podle stupně důležitosti).

Smazat záznam
Smazání okna záznamu (informace se smažou i z příslušného souboru).

Zprávy
Možnost detailního nastavení informací, které mají být sledovány (podrobnosti viz dále). Pouze v sekci *Debug*.

22.2 Config

Záznam *Config* uchovává kompletní historii komunikace *Kerio Administration Console* s *Kerio MailServer Engine* — z tohoto záznamu lze zjistit, který uživatel kdy prováděl jaké administrační úkony.

Do okna *Config* jsou zapisovány tři druhy záznamů:

Informace o přihlašování uživatelů ke správě *Kerio MailServeru*
Příklad:

```
[30/Jun/2004 09:09:18] Admin - session opened for host 127.0.0.1
```

- `[30/Jun/2004 09:09:18]` — datum a čas, kdy byl záznam zapsán
- `Admin` — jméno uživatele přihlášeného ke správě *Kerio MailServeru*.
- `session opened for host 127.0.0.1` — informace o zahájení komunikace a IP adrese počítače, ze kterého se uživatel připojuje

Změny v konfigurační databázi
Jedná se o změny provedené uživatelem v *Kerio Administration Console*. Pro příklad si uveďme založení nového uživatelského účtu.

```
[30/Jun/2004 13:09:48] Admin - insert User set
Name='tjandak', Domain='firma.cz', Account_enabled='1',
Auth_type='0', Password=xxxxxx, Rights='1',
ForwardMode='0', Qstorage='10485760', Qmessage='5000'
```

- `[30/Jun/2004 13:09:48]` — datum a čas, kdy byl záznam zapsán
- `Admin` — jméno uživatele přihlášeného ke správě *Kerio MailServeru*.
- `insert User set Name='tjandak'...` — zápis parametrů, které byly novému uživatelskému účtu nastaveny

Ostatní konfigurační změny

Typickým příkladem je zálohovací cyklus. Po stisknutí tlačítka *Použít* v sekci *Konfigurace* → *Zálohování* se do záznamu *Config* vypíše datum a čas každé zálohy.

```
[30/Jun/2004 09:29:08] Admin - Store backup started
```

- `[30/Jun/2004 09:29:08]` — datum a čas začátku zálohování
- `Admin` — jméno uživatele přihlášeného ke správě *Kerio MailServeru*.
- `Store backup started` — informace o spuštění zálohy

22.3 Mail

Záznam *Mail* obsahuje informace o jednotlivých zprávách, které byly *Kerio MailServerem* zpracovány. Záznam obsahuje všechny typy zpráv:

- příchozí zprávy,
- odchozí zprávy,
- zprávy e-mailových konferencí,
- DSN (Delivery Status Notification) — zprávy automaticky generované serverem (tzv. systémové zprávy — např. informace o tom, že zpráva je nedoručitelná, že ji nebylo možné doručit v definované době, že uživatel odeslal zprávu s virem nebo zakázanou přílohou apod.).

Příchozí a odchozí zprávy

Všechny zprávy, které byly přijaty serverem přes protokoly SMTP, HTTP nebo byly staženy protokolem POP3. Pro příklad můžeme uvést dva řádky patřící k jedné zprávě a blíže si rozebereme jejich jednotlivé položky:

```
[30/Nov/2005 17:57:14] Recv: Queue-ID: 438dd9ea-00000000,
[30/Nov/2005 17:57:14] Recv: Queue-ID: 438dd9ea-00000000,
Service: SMTP, From: <jnovak@firma.cz>, To: <jcerny@firma.cz>,
Size: 1229, User: jnovak@firma.cz, Sender-Host: 195.39.55.2,
SSL: yes

[30/Nov/2005 17:57:15] Sent: Queue-ID: 438dd9ea-00000000,
Recipient: <jcerny@firma.cz>, Result: delivered, Status: 2.0.0
```

- `[30/Nov/2005 17:57:14]` — datum a čas, kdy byla doručena nebo odeslána zpráva.
- `Recv/Sent` — toto pole obsahuje informaci, zda server zprávu přijal, či zda ji odesílá. Proto se zde mohou vyskytovat dvě položky: `Sent` nebo `Recv` (received).
- `Queue-ID: 438d6fb6-00000003` — číslo, které od serveru zpráva obdržela ve frontě odchozích zpráv. Slouží jako identifikátor, který označuje stejným číslem všechny řádky patřící k jedné zprávě. Každá zpráva je serverem nejprve přijata,

a poté odeslána. V záznamu se tedy objeví ke každé zprávě nejméně dva řádky (příjem zprávy a její odeslání). Nejméně proto, že zpráva může být doručena více příjemcům (každý další příjemce znamená další řádek v záznamu).

- `Service: HTTP` — protokol, přes který byla zpráva přijata serverem (HTTP, SMTP). Tuto informaci lze najít pouze u příchozích zpráv. U odchozích zpráv se tato informace nezobrazuje, protože nemá smysl. Všechny odchozí zprávy jsou odesílány protokolem SMTP.
- `From: <jwayne@company.com>` — elektronická adresa odesílatele.
- `To: <jnovak@firma.cz>` — elektronická adresa příjemce.
- `Size: 378` — velikost zprávy v bytech.
- `User: jnovak@firma.cz` — uživatelský účet, ze kterého byla zpráva odeslána.
- `Sender-Host: 195.39.55.2` — IP adresa počítače, ze kterého byla zpráva odeslána.
- `SSL: yes` — informuje o použití šifrovaného spojení (zobrazuje se pouze u protokolu SMTP).
- `Recipient: <jcerny@firma.cz>` — elektronická adresa příjemce.
- `Result: delivered` — výsledek pokusu o doručení zprávy.
- `Status: 2.0.0` — kód odpovědi protokolu SMTP (více viz RFC 821 a 1893). Pokud kód začíná číslicí 2, zpráva byla úspěšně doručena. Začíná-li kód číslicí 4 nebo 5, pak zpráva doručena nebyla.

Zprávy generované serverem

Tento typ zprávy generuje *Kerio MailServer*. Například pokud zpráva nemůže být doručena, server tuto skutečnost formou DSN sdělí odesílateli.

```
[30/Nov/2005 15:31:40] Recv: Queue-ID: 438db7cc-00000000,
Service: DSN, From: <>, To: <jnovak@firma.cz>, Size: 1650,
Report: failed
```

- `[30/Nov/2005 15:31:40]` — datum a čas, kdy byla zpráva vygenerována
- `Recv:` — toto pole obsahuje informaci, zda server zprávu přijal, či zda ji odesílá. Proto se zde mohou vyskytovat dvě položky: `Sent` nebo `Received`.
- `Queue-ID: 438db7cc-00000000` — číslo, které od serveru zpráva obdržela ve frontě odchozích zpráv.
- `Service: DSN` — *Delivery Status Notification*; zprávy generované *Kerio MailServerem*.
- `From: <>` — položka je prázdná, protože zpráva je generována serverem.
- `To: <jnovak@firma.cz>` — elektronická adresa příjemce.
- `Size: 1650` — velikost zprávy v bytech.
- `Report: failed` — typ hlášení.

Zprávy konferencí

Mail záznam obsahuje všechny zprávy e-mailových konferencí. Zaznamenány jsou jak jednotlivé příspěvky do konferencí, tak řídící zprávy konference.

```
[30/Nov/2005 19:09:11] Recv: Queue-ID: 438deac7-00000009,
Service: List, From: <Diskuze-bounce@firma.cz>, To:
<jnovak@firma.cz>, Size: 3302, Answer: subscribe response
```

- `[30/Nov/2005 19:09:11]` — datum a čas přijetí zprávy.
- `Recv:` — toto pole obsahuje informaci, zda server zprávu přijal, či zda ji odesílá. Proto se zde mohou vyskytovat dvě položky: `Sent` nebo `Received`.
- `Queue-ID: 438deac7-00000009` — číslo, které od serveru zpráva obdržela ve frontě odchozích zpráv.
- `Service: List` — příznak konference.
- `<Diskuze-bounce@firma.cz>` — elektronická adresa odesílatele.
- `To: <jnovak@firma.cz>` — elektronická adresa příjemce.
- `Size: 1397` — velikost zprávy v bytech.
- `Answer: subscribe response` — typ zprávy.

Sieve

Zprávy generované uživatelským filtrem (např. autoreplay).

22.4 Security

Záznam *Security* obsahuje informace, které souvisejí s bezpečností *Kerio MailServeru*. Také obsahuje záznam o všech zprávách, které nebylo možno doručit. Jedná se zejména o tyto typy událostí:

Nalezené viry a zakázané přílohy

Pro příklad uveďme zprávu, v níž byl obsažen vir:

```
[16/Jun/2004 18:37:17] Found virus in mail from
<missgold18@hotmail.com> to <support@kerio.com>:
W32/Netsky.p@MM
```

- `[16/Jun/2004 18:37:17]` — datum a čas, kdy byl virus nalezen.
- `Found virus in mail` — provedená akce (zpráva o nalezení viru).
- `from <missgold18@hotmail.com>` — elektronická adresa odesílatele.
- `to <support@kerio.com>` — elektronická adresa příjemce.
- `W32/Netsky.p@MM` — typ nalezeného viru.

Odmítnutí spam filtrem

Zpráva s příliš vysokým hodnocením spamového filtru:

```
[16/Jun/2004 18:37:17] Message from <missgold18@hotmail.com>
```

```
to <support@kerio.com> rejected by spam filter: score 9.74,
threshold 5.00
```

- `[16/Jun/2004 18:37:17]` — datum a čas, kdy byla zpráva odmítnuta.
- `from <missgold18@hotmail.com>` — elektronická adresa odesílatele.
- `to <support@kerio.com>` — elektronická adresa příjemce.
- `rejected by spam filter` — provedená akce (odmítnutí zprávy spamovým filtrem).
- `score 9.74, threshold 5.00` — hodnocení spamového filtru *SpamAssassin*.

Neúspěšné pokusy o přihlášení

Záznam obsahuje neplatné pokusy o přihlášení. Obvyklou příčinou bývá neplatné jméno/heslo nebo nepovolená IP adresa. Důvod neúspěšného pokusu o přihlášení můžete nalézt také v záznamu *Warning* (kapitola 22.5).

```
[13/Apr/2004 17:35:49] Failed IMAP login from 192.168.36.139,
missing parameter in AUTHENTICATE header
```

- `[13/Apr/2004 17:35:49]` — datum a čas neúspěšného pokusu o přihlášení.
- `Failed IMAP login` — provedená akce (neúspěšný pokus o přihlášení).
- `from 192.168.36.139` — IP adresa, ze kterého byl pokus učiněn.

Důvodů neúspěchu přihlášení může být několik:

- `missing parameter in AUTHENTICATE header` — byla poslána špatná nebo neplatná hlavička s přihlašovacími informacemi,
- `authentication method PLAIN is disabled` — použitá autentizační metoda je v *Kerio MailServeru* vypnutá,
- `authentication method CRAM_MD5 is invalid or unknown` — *Kerio MailServer* neumí nebo nezná tuto metodu ověřování,
- `error during authentication with method CRAM-MD5` — došlo k chybě při ověřování hesla, např. chyba při komunikaci s ověřovacím serverem,
- `authentication with method CRAM-MD5 cancelled by user` — uživatel (klient) přerušil ověřování,
- `(Failed IMAP login from 127.0.0.1), authentication method PLAIN` — uživatel nebyl ověřen (uživatel neexistuje, špatně zadané heslo, uživatelský účet v *Kerio MailServeru* je vypnutý nebo nelze ověřit jméno a heslo uživatele, protože daná metoda ověřování neposkytuje dostatek údajů pro ověření uživatele v *Active Directory*).

Pokusy o zneužití serveru (relaying)

Pro příklad pokusu o relaying si uveďme:

```
[11/Jun/2004 00:36:07] Relay attempt from IP address
61.216.46.197, mail from <wgiwknovry@hotmail.com> to
```

```
<fodder@falls.igs.net> rejected
```

- `[11/Jun/2004 00:36:07]` — datum a čas pokusu o zneužití serveru.
- `Relay attempt` — provedená akce (neúspěšný pokus relaying).
- `61.216.46.197` — IP adresa, ze které byl pokus o relaying učiněn.
- `from <wgiwknovry@hotmail.com>` — adresa odesílatele.
- `to <fodder@falls.igs.net>` — adresa adresáta.
- `rejected` — provedená akce (odmítnutí zprávy).

Antibombing

Ochrana proti zahlcení serveru — viz kapitolu 15.2, sekce *Bezpečnostní volby*.

```
[16/Jun/2004 18:53:43] Directory harvest attack from
213.7.0.87 detected
```

- `[16/Jun/2004 18:53:43]` — datum a čas neúspěšného útoku.
- `Directory harvest attack` — typ útoku.
- `from 213.7.0.87` — IP adresa, ze které byl pokus o útok učiněn.
- `detected` — provedená akce (zjištěno a zakázáno).

Nalezení odesílatele v databázích zakázaných serverů

Odesílatel byl nalezen v databázi zakázaných serverů (*ORDB*, vlastní skupina IP adres).

```
[13/Apr/2004 17:44:02] IP address 212.76.71.93 found in DNS
blacklist ORDB, mail from <emily.macdonald@nmc-uk.org> to
<support@kerio.com>
```

- `[13/Apr/2004 17:44:02]` — datum a čas přijetí zprávy.
- `212.76.71.93` — IP adresa, ze které byla zpráva odeslána.
- `found in DNS blacklist ORDB` — typ akce (adresa byla nalezena v databázi zakázaných serverů).
- `from <emily.macdonald@nmc-uk.org>` — elektronická adresa odesílatele.
- `to <support@kerio.com>` — elektronická adresa příjemce.

Vzdálené vyčištění mobilního zařízení

Uživateli bylo odcizeno mobilní zařízení (nebo ho ztratil) a správce odstranil ze zařízení všechna data uživatele (více viz sekci 36.5).

V záznamu *Security* se mohou objevit v podstatě tři typy záznamu o vyčištění mobilního zařízení. První záznam se týká zahájení vyčištění. Tento záznam se při vyčištění zařízení objevuje vždy. V této fázi lze obvykle vyčištění ještě stornovat. Druhý typ záznamu se tedy objeví právě při stornování vyčištění zařízení. Třetí záznam se vyskytne, pokud vyčištění nebylo stornováno a vyčištění se skutečně provede. To proběhne při prvním následujícím připojení zařízení k serveru.

- První příklad záznamu zobrazuje jeho iniciaci:

  ```
  [22/Aug/2006 12:30:23] Device with id
  C588E60FCF2FB2C107FBF2ABE09CA557(user: jnovak@firma.cz)
  will be wiped out by request Admin
  ```

- Druhý příklad záznamu zobrazuje jeho stornování:

  ```
  [22/Aug/2006 12:36:51] Wiping out of the device
  C588E60FCF2FB2C107FBF2ABE09CA557 (user: jnovak@firma.cz)
  has been cancelled by Admin
  ```

- Třetí příklad zobrazuje oznámení o vymazání zařízení:

  ```
  [22/Aug/2006 12:31:11] Device C588E60FCF2FB2C107FBF2ABE09CA557
  (user: jnovak@firma.cz), connected from: 192.168.44.178
  has been irrecoverable wiped out
  ```

22.5 Warning

Záznam *Warning* zobrazuje varovná hlášení, což jsou ve své podstatě chyby, které nemají závažný charakter. Typickým příkladem takového varování může být např. zpráva, že uživatel s administrátorskými právy má prázdné heslo, že uživatelský účet tohoto jména neexistuje, nebo že vzdálený POP3 server je nedosažitelný.

Události, které způsobují varovná hlášení v tomto záznamu, nemají zásadní vliv na činnost *Kerio MailServeru*, mohou však signalizovat určité (případně potenciální) problémy, např. u konkrétních uživatelů. Záznam *Warning* může pomoci např. v případě, jestliže si jeden uživatel stěžuje na nefunkčnost některých služeb.

22.6 Error

Na rozdíl od záznamu *Warning*, záznam *Error* zobrazuje závažné chyby, které mají zpravidla vliv na chod celého serveru. Správce *Kerio MailServeru* by měl tento záznam pravidelně sledovat a zjištěné chyby v co nejkratší možné době napravit. V opačném případě hrozí nejen nebezpečí, že uživatelé nebudou moci využívat některé (či dokonce všechny) služby, ale může dojít také ke ztrátě zpráv či k bezpečnostním problémům (např. ke zneužití serveru k rozesílání nevyžádaných e-mailů nebo doručování zpráv obsahujících viry).

Typickým chybovým hlášením v záznamu *Error* bývá například: problém se spuštěním některé služby (většinou z důvodu kolize na příslušném portu), problém se zápisem na disk, s inicializací antivirové kontroly, s externím ověřením uživatele apod.

22.7 Spam

Do záznamu *Spam* jsou zapisovány informace o veškeré nevyžádané poště, která je uložena v *Kerio MailServeru*. Každý řádek záznamu obsahuje informace o jednom konkrétním spamu. Jednotlivé záznamy se liší podle toho, jak bylo zjištěno, že je zpráva nevyžádaná. Záznam *Spam* zaznamenává také zprávy, které byly z nějakého důvodu *Kerio MailServerem* označeny jako spam, ale uživatel je určil jako korektní.

Nevyžádaná zpráva detekovaná filtrem

Zpráva vyhodnocená jako nevyžádaná spamovým filtrem *Kerio MailServeru*:

```
[06/Sep/2004 08:43:17] Message marked as spam with score:
8.00, To: jnovak@firma.cz, Message size: 342,
From: jcerny@firma.cz, Subject:
```

- `[06/Sep/2004 08:43:17]` — datum a čas detekce spamu.
- `Message marked as spam with score: 8.00` — typ akce (zpráva byla označena jako spam, protože jí bylo spamovým filtrem přiděleno příliš vysoké skóre).
- `To: jnovak@firma.cz` — elektronická adresa příjemce.
- `Message size: 342` — velikost zprávy v bytech.
- `From: jcerny@firma.cz` — elektronická adresa odesilatele.
- `Subject:` — předmět zprávy (v tomto případě prázdný).

Nevyžádaná zpráva detekovaná uživatelem

Zpráva, která byla uživatelem označena jako nevyžádaná:

```
[06/Sep/2004 08:40:39] User jcerny@firma.cz marked a message
as spam, Folder: ~jcerny@firma.cz/INBOX, Size: 462,
From: "Jan Novák" <jnovak@firma.cz>, Subject: Hallo
```

- `[06/Sep/2004 08:40:39]` — datum a čas, kdy byla zpráva označena jako spam.
- `User jcerny@firma.cz` — elektronická adresa uživatele, kterému byla zpráva doručena.
- `marked a message as spam` — typ akce (zpráva byla uživatelem označena jako spam).
- `Folder: ~jcerny@firma.cz/INBOX` — složka, ve které je zpráva uložena
- `Size: 462` — velikost zprávy v bytech.
- `From: "Jan Novák" <jnovak@firma.cz>` — elektronická adresa odesilatele .
- `Subject: Hallo` — předmět zprávy.

Zpráva není spam

Zpráva, která byla uživatelem označena jako korektní:

```
[06/Sep/2004 08:43:32] User jnovak@firma.cz marked a message
as not spam, Folder: ~jnovak@firma.cz/Junk E-mail, Size: 500,
From: "Jan Černý" <jcerny@firma.cz>, Subject: *SPAM*
```

- `[06/Sep/2004 08:43:32]` — datum a čas, kdy byla zpráva označena, že není spam.
- `User: jnovak@firma.cz` — elektronická adresa uživatele, kterému byla zpráva doručena.
- `marked a message as not spam` — typ akce (zpráva byla uživatelem označena jako korektní).
- `Folder: ~jnovak@firma.cz/Junk E-mail` — složka, ve které je zpráva uložena (v tomto případě je to vždy složka pro nevyžádanou poštu).
- `Size: 500` — velikost zprávy v bytech.
- `From: "Jan Černý" <jcerny@firma.cz>` — elektronická adresa, ze které byla zpráva odeslána.
- `Subject: **SPAM**` — předmět zprávy.

22.8 Debug

Debug (ladicí informace) je speciální záznam, který slouží zejména k detailnímu sledování určitých informací. Proto může významně pomoci při odstraňování problémů. Standardně obsahuje informace o startu a ukončení *Kerio MailServeru*, výpis služeb s informací o adresách a portech, na kterých navazují spojení. Dále zapisuje zprávy zpracovávající se ve frontě a podobně.

Ostatní informace se týkají služeb a procesů, které provádějí veškerou činnost serveru. Těchto informací je poměrně velké množství, což by způsobilo naprostý nepřehled, pokud by byly zobrazovány všechny najednou. Zpravidla je však třeba sledovat pouze informace týkající se konkrétní služby či funkce.

Upozornění: Zobrazování velkého množství informací navíc zpomaluje činnost *Kerio MailServeru*. Doporučujeme tedy zapínat sledování pouze těch informací, které vás skutečně zajímají, a to pouze po dobu nezbytně nutnou.

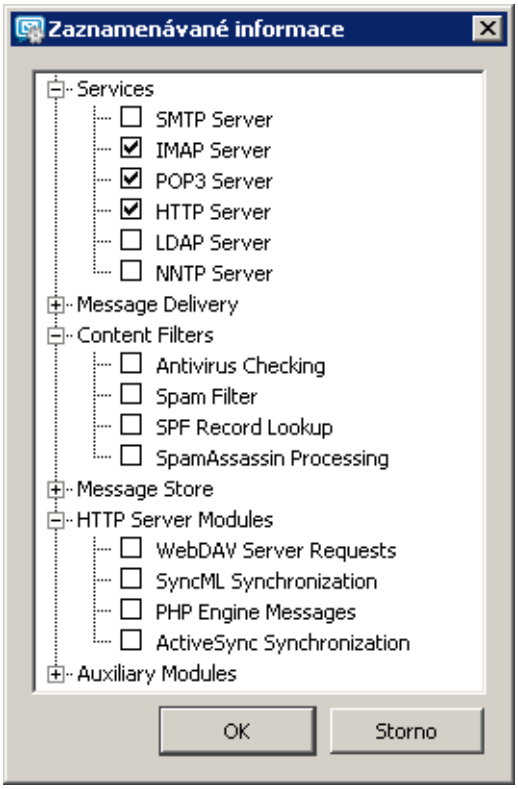
Nastavení záznamu Debug

Z výše uvedených důvodů umožňuje záznam *Debug* nastavit, jaké informace v něm mají být zobrazovány. Toto se provádí volbou *Zprávy* v kontextovém menu okna *Debug*.

Otevře se okno *Zaznamenávané informace*, kde je k dispozici mnoho voleb pro zapnutí konkrétních záznamů:

Services

Sekce *Services* obsahuje možnost zapnutí záznamů týkajících se služeb spuštěných v *Kerio MailServeru*:



Obrázek 22.8 Nastavení záznamu Debug

- SMTP Server — Detailní výpis komunikace klientů a SMTP serveru. Záznam je vhodné použít při problémech s příjmem pošty přes MX záznamy.
- IMAP Server — Detailní výpis komunikace klientů s IMAP serverem. Záznam také poskytuje informace o komunikaci přes rozhraní MAPI.
- POP3 Server — Detailní výpis komunikace klientů s POP3 serverem. Spolu s následujícími dvěma záznamy (*IMAP server session*, *HTTP server session*) napomáhá řešení problémů s vybíráním schránek.
- HTTP Server — Komunikace klientů s HTTP serverem pro rozhraní *Kerio WebMail*.
- LDAP Server — Detailní sledování komunikace klientů s LDAP serverem a vyhledávání kontaktů v databázi.
- NNTP Server — Detailní výpis komunikace klientů s news serverem.

Message Delivery

Sekce *Message Delivery* obsahuje volby pro zaznamenávání průběhu doručování zpráv:

- Queue Processing — Zpracování odchozí fronty (odesílání a příjem zpráv, plánování apod.).
- Remote POP3 Download — Vybírání vzdálených POP3 schránek (*Kerio MailServer*

je v roli POP3 klienta) a třídicích pravidel (při přijetí zprávy či jejím stažení ze vzdálené POP3 schránky). Záznam *Remote POP3 download* slouží spolu se záznamem *Alias Expansion* k řešení problémů s tříděním doménového koše.
- SMTP Client — Odesílání odchozích zpráv (komunikace *Kerio MailServeru* s nadřazeným SMTP serverem nebo serverem cílové domény). Záznam obsahuje příkazy a odezvy serveru a klienta přesně podle pořadí jednotlivých událostí. Proto tento záznam může pomoci při problémech s odesíláním pošty.
- Mailing List Processing — Sledování e-mailových konferencí (přihlašování a odhlašování členů, posílání zpráv, akce moderátorů apod.).
- Alias Expansion — Zpracování aliasů (při přijetí zprávy či jejím stažení ze vzdálené POP3 schránky). Záznam *Alias processing* slouží spolu se záznamem *Remote POP3 download* k řešení problémů s tříděním doménového koše.
- Sieve Filters — Filtrování zpráv dle uživatelských filtrů.

Content Filters

Sekce *Content Filters* obsahuje volby k zapnutí/vypnutí záznamů o průběhu antivirové a antispamové kontroly:

- Antivirus Checking — Antivirová kontrola zpráv (komunikace s antivirovým programem, zpracování jednotlivých příloh zprávy). Záznam lze použít, pokud zavirované zprávy nejsou rozpoznávány antivirovým programem a prochází až k uživateli.
- Spam Filter — Zaznamenává hodnocení každé zprávy hodnocené spamovým filtrem *Kerio MailServeru*.
- SPF Record Lookup — Volba vypisuje informace o *SPF* dotazech na SMTP servery. Lze využít při problémech s *SPF* kontrolou.
- SpamAssassin Processing — volba umožňuje sledování procesů, ke kterým dochází při testování zpráv spamovým filtrem *SpamAssassin*.

Message Store

Sekce *Message Store* umožňuje zaznamenávat operace týkající se úložiště dat, vyhledávání, zálohování, atd.:

- Message Folder Operation — Operace s uživatelskými a veřejnými složkami (otevírání, ukládání zpráv, uzavírání).
  Tento záznam lze použít například při problémech s mapováním veřejných složek.
- Searching and Sorting — záznam obsahuje operace, které server provádí při vyhledávání v poštovních, kalendářových, kontaktních nebo úkolových složkách. Zaznamenávají se také operace, které jsou prováděny při třídění (např. emailů podle abecedy nebo data přijetí).
- Quota and Login Statistics— záznam lze dobře využít zejména v případě, že se objevuje nějaký problém s nastavenými uživatelskými kvótami a podobně.

- Store Backup — Výpis mapuje průběh zálohy, procházení a zálohovaní všech složek. Pomocí tohoto záznamu lze získat informaci, zda záloha probíhá správně, a zda nebyla přerušena.
- Messages decoding — Tento záznam může pomoci při identifikaci problémů s dekódováním TNEF a uuencode zpráv.

HTTP Server Modules

Sekce *HTTP Server Modules* poskytuje volby, které umožňují zaznamenávat informace o komunikaci přes rozhraní HTTP:

- WebDAV Server Requests — Záznam vypisuje všechny akce rozhraní WebDAV. Tento záznam je užitečný při řešení problémů v komunikaci mezi *Kerio MailServerem* a *MS Entourage*, *NotifyLink*, *Kerio Sync Connector* a iCal klienty.
- SyncML Synchronization — Zobrazuje veškerou aktivitu vyvíjenou mezi *Kerio MailServerem* a *Kerio Synchronization Plug-inem* při synchronizaci.
- PHP Engine Messages — Záznam zapisuje informace z rozhraní *Kerio WebMail*. Tyto informace jsou rozšířením záznamu *Error* a lze je využít při řešení problémů v *Kerio WebMailu*.
- *ActiveSync Synchronization* — Záznam vypisuje komunikaci protokolu *ActiveSync* mezi mobilními zařízeními a *Kerio MailServerem*.

Auxiliary Modules

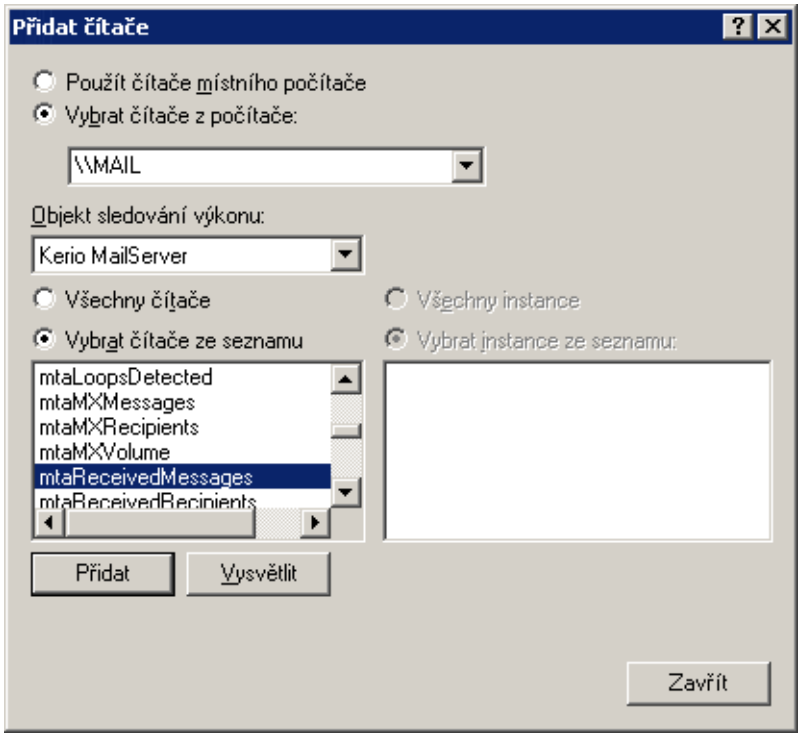
Sekce *Auxiliary Modules* obsahuje následující možnosti zaznamenávání informací:

- User Authentication — Externí ověřování uživatelů (NT doména, Kerberos, PAM).
- Network Connections and SSL — Navazování spojení na vzdálené servery (na úrovni TCP), DNS dotazy, SSL šifrování apod.
- DNS Resolver— Zjišťování serverů cílových domén z DNS MX záznamů, záznamy nalezené v interní DNS cache.
- Directory Service Lookup — Dotazy do externí databáze uživatelů (*Active Directory*). Tento záznam může pomoci při řešení problémů s importem uživatelů z domény.
- Update Checker Activity — Vypisuje komunikaci se serverem *update.kerio.com*, kde se nacházejí nové verze *Kerio MailServeru*.
- Thread Pool Activity — vypisuje navazování, průběh i ukončení všech vláken, která *Kerio MailServer* zpracovává.
- Administration Console Connections — zaznamenává připojení a činnost *Kerio Administration Console*.

22.9 Sledování výkonu (Windows)

Je-li *Kerio MailServer* instalován na operační systém *Windows* řady 2000, nebo XP, je možno také nainstalovat volitelnou komponentu *Performance Monitor* (detaily naleznete v kapitole 2.4). *Performance Monitor* je modul do systémového nástroje *Výkon* (*Performance*), který naleznete v *Nástrojích pro správu* (*Administrative Tools*).

V aplikaci *Performance Monitor* se přepneme do sekce *System Monitor*. Tlačítkem + v nástrojovém panelu této sekce otevřeme dialog pro přidání nových sledovaných objektů.



Obrázek 22.9 Performance Monitor

V položce *Performance object* vybereme položku *Kerio MailServer*. V levém dolním poli je pak možno vybrat statistiky, které chceme sledovat. K dispozici jsou všechny ukazatele, které *Kerio MailServer* sleduje (viz též kapitolu 21.6, resp. sekce *Stav* → *Statistiky* programu *Kerio Administration Console*). Tlačítkem *Explain* lze získat podrobnější informace o vybraném objektu.

Poznámky:

- Pokud se v seznamu objektů v poli *Performance object* neobjeví položka *Kerio MailServer*, pak zřejmě není komponenta *Performance Monitor* nainstalována, nebo je

poškozena. V tom případě doporučujeme znovu spustit instalační program *Kerio MailServeru* (viz kapitolu 2.4).

- Detailní informace o aplikaci *Performance Monitor* naleznete v nápovědě systému Windows.

Kapitola 23

Veřejné složky

Veřejná složka je speciální typ složky. K této složce mají automaticky přístup pro čtení všichni uživatelé z domény nebo celého *Kerio MailServeru*.

Veřejné složky může vytvářet pouze uživatel s příslušnými právy. Tato práva jsou standardně přidělena uživateli `admin` primární domény v *Kerio MailServeru*. `Admin` může přidělit administrátorská práva dalším uživatelům.

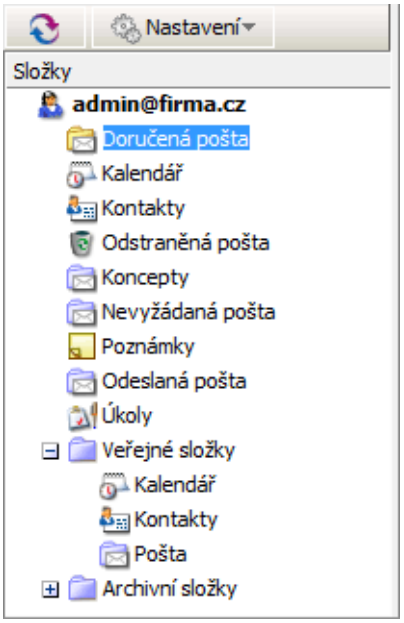
Veřejné složky lze spravovat z následujících rozhraní a poštovních klientů:

- Kerio WebMail
- Kerio Outlook Connector (Offline Edition)
- Kerio Outlook Connector

Pro vytvoření nové veřejné složky je třeba kliknout na složce *Veřejné složky* pravým tlačítkem myši a vybrat v kontextovém menu položku *Nová složka*. Otevře se dialog pro zadání jména a typu složky.

Po založení nové složky jsou automaticky nastavena práva pro čtení pro všechny uživatele v doméně nebo v celém *Kerio MailServeru*. Zda budou veřejné složky přístupné pro celý server, nebo budou vytvořeny zvláštní složky pro každou doménu, záleží na nastavení v administrační konzoli v sekci *Konfigurace* → *Domény*. V této sekci klikneme na tlačítko *Upřesnění*, kde je nastavení umístěno.

Každá veřejná složka bude všem nasdíleným uživatelům zobrazena automaticky jako podsložka složky *Veřejné složky* (viz obrázek 23.1).



Obrázek 23.1 Veřejné složky v rozhraní Kerio Webmail

23.1 Zobrazení veřejných složek v jednotlivých typech účtů

Jednoduchá tabulka zobrazuje, které veřejné složky se uživateli zobrazí v závislosti na typu používaného poštovního účtu, potažmo klienta.

Účet	Pošta	Kontakty	Kalendář	Úkoly	Poznámky
Kerio Outlook Connector (Offline Edition)	ANO	ANO	ANO	ANO	ANO
Kerio Outlook Connector	ANO	ANO	ANO	ANO	ANO
Kerio WebMail	ANO	ANO	ANO	ANO	ANO
Kerio Synchronization Plug-in + IMAP	ANO[a]	ANO	ANO	NE	NE
Kerio Synchronization Plug-in + POP3	NE	ANO	ANO	NE	NE
Účet typu Exchange v MS Entourage	ANO	ANO[b]	ANO[b]	NE	NE
Účet typu Exchange v Apple Mail[c]	ANO	ANO	ANO	ANO	ANO
IMAP (libovolný klient podporující protokol IMAP)	ANO (pokud je klient umí zobrazit)	NE	NE	NE	NE
POP3 (libovolný klient podporující protokol POP3)	NE	NE	NE	NE	NE

[a] Po přihlášení k odběru.

[b] Pouze verze *MS Entourage 2004 sp2*.

[c] Platí pouze v případě nastavení plné podpory IMAP v konfiguračním souboru *Kerio MailServeru* (více viz kapitolu 41).

Tabulka 23.1 Zobrazení veřejných složek v jednotlivých typech účtů

Kapitola 24

Ověřování přes Kerberos

Tato kapitola slouží jako jednoduchý a přehledný průvodce nastavením ověřování uživatelů přes systém Kerberos.

Kerberos je systém založený na architektuře klient — server, která umožňuje autentizaci a autorizaci uživatelů a zvyšuje tak bezpečí při využívání zdrojů v počítačové síti. Kerberos je popsán standardem IETF RFC 4120.

Kerio MailServer má implementovánu podporu pro Kerberos V5.

Poznámka: Při řešení případných problémů s konfigurací vám mohou pomoci následující záznamy:

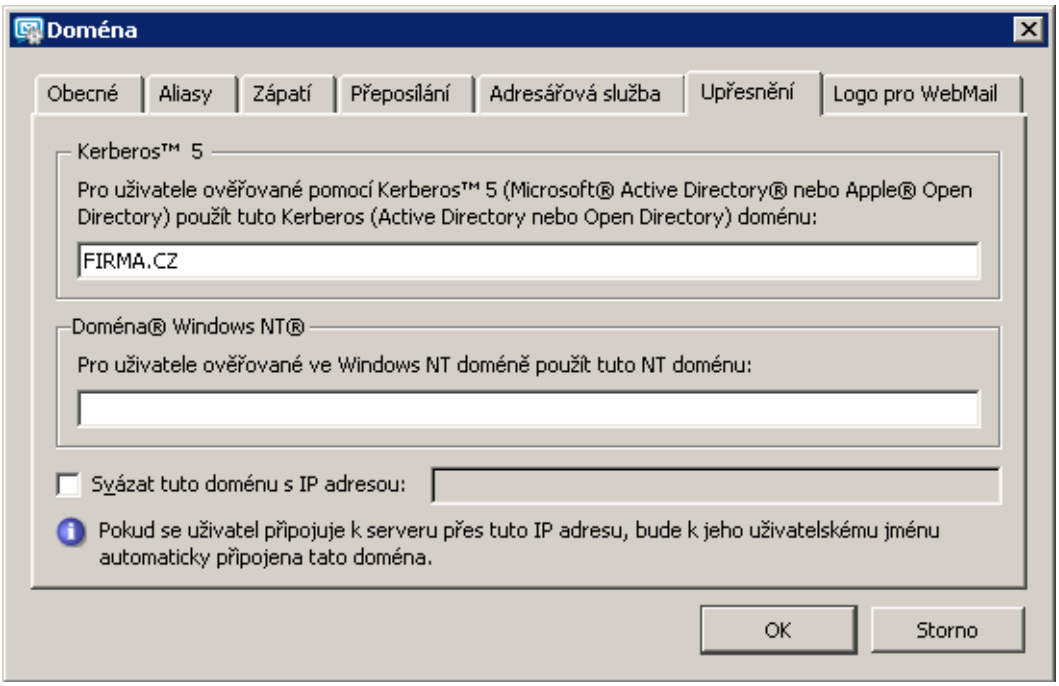
- *MS Windows* — logy jsou umístěny v menu *Start* → *Nastavení* → *Ovládací panely* → *Nástroje pro správu* → *Prohlížeč událostí*
- *Linux* — logy ve standardním adresáři `/var/log/syslog`
  To se ovšem týká pouze Kerberos klienta. Logování komunikace na straně serveru lze zajistit přidáním následující konfigurace do souboru `/etc/krb5.conf`:
  ```
  [logging]
      default = FILE:/var/log/krb5libs.log
      kdc = FILE:/var/log/krb5kdc.log
      admin_server = FILE: /var/log/kadmind.log
  ```
  Poznámka: Nastavení logování na straně serveru se týká Kerberos MIT (US implementace Kerberosu aplikovaná v *Active Directory* a *Apple Open Directory*). Nastavení logování Kerberos Heimdal (evropská implementace Kerberosu, kterou můžete nalézt v některých linuxových distribucích) se může lišit.[3]
- *Mac OS X Server* — záznamy v aplikaci *Server Admin* (více viz kapitolu 24.4)
- *Kerio MailServer* — záznamy najdete v administrační konzoli, v sekci *Záznamy*. Relevantní jsou v tomto případě záznamy *Warning*, *Error* a *Debug* (musí být spuštěno sledování modulu *User Authentication*). Bližší popis jednotlivých záznamů obsahuje kapitola 22.

[3] Klient Kerberos Heimdal je také standardní součástí instalace *Kerio MailServeru* pro linuxové distribuce. Není ovšem podstatné, jaká z obou forem je použita na serveru (Key Distribution Center), a jaká na klientovi (v tomto případě *Kerio MailServer*), protože protokol je tentýž a server i klientská část budou bez problémů spolupracovat.

24.1 Kerio MailServer na systému Windows

Ověřování proti Active Directory

V případě ověřování v *Active Directory* je třeba uvést název *Active Directory* domény v *Kerio MailServeru*. Toto lze nastavit v *Kerio Administration Console* v nastavení domény (viz obrázek 24.1).



Obrázek 24.1 Doplnění Active Directory domény do Kerio MailServeru

Kromě uvedení názvu domény v dialogu *Upřesnění* (viz obrázek 24.1) je třeba zajistit aby:

1. *Kerio MailServer* byl členem domény, proti které se ověřuje. Pokud *Kerio MailServer* nebude členem domény, pak Kerberos nebude fungovat a uživatelé budou muset používat lokální heslo — tedy jiné než mají nastaveno v doméně.

2. *Kerio MailServer* používal jako primární DNS server doménový řadič (*Active Directory Controller*) — to by mělo být automaticky zajištěno přidáním počítače do domény (viz bod 1).

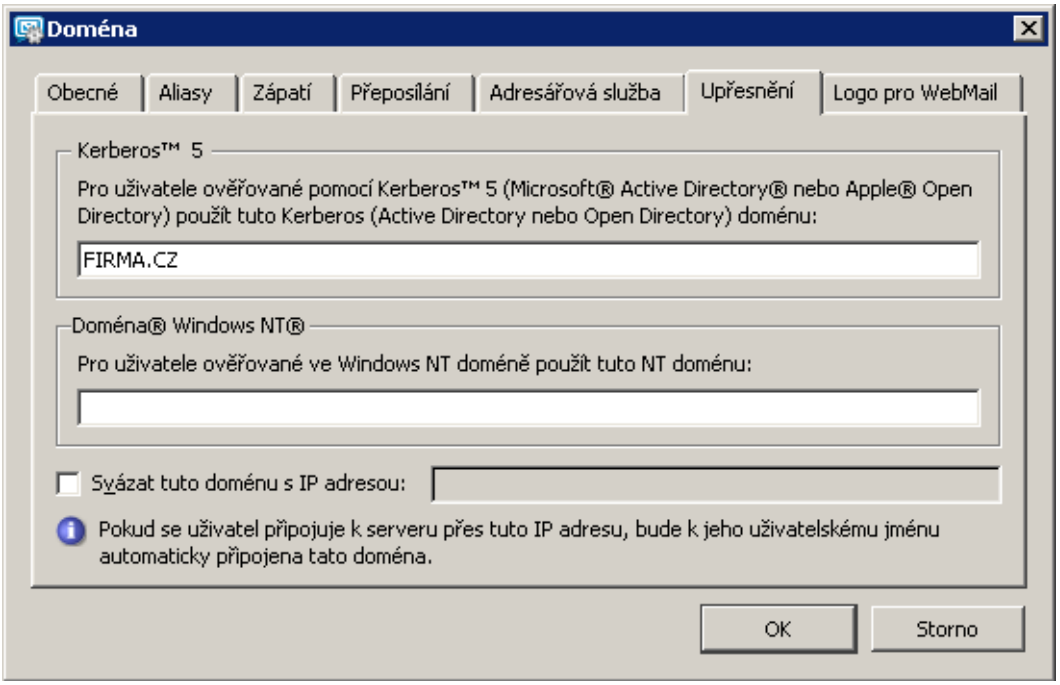
   Pokud konfigurace sítě vyžaduje ověřování proti více doménovým řadičům zároveň, potom přidáme jako DNS servery všechny doménové řadiče, proti kterým se bude *Kerio MailServer* ověřovat. V tomto případě je však vyžadována speciální konfigurace DNS serverů. Buď je třeba nastavit DNS servery tak, že si budou navzájem

dotazy přeposílat (pokud daný dotaz není nalezen ve vlastní databázi, je přeposlán dalšímu doménovému řadiči) nebo musí mít všechny DNS servery nadřazený společný primární DNS server.

3. byl synchronizován čas *Kerio MailServeru* a *Active Directory* — to by mělo být automaticky zajištěno přidáním počítače do domény (viz bod 1).

Ověřování proti Open Directory

V případě ověřování v *Open Directory* je třeba uvést Kerberos realm v *Kerio MailServeru* (např. `FIRMA.CZ`).



Obrázek 24.2 Doplnění Kerberos realm do Kerio MailServeru

Kromě uvedení názvu *Open Directory* domény (Kerberos realm) v *Kerio MailServeru* je třeba zajistit aby:

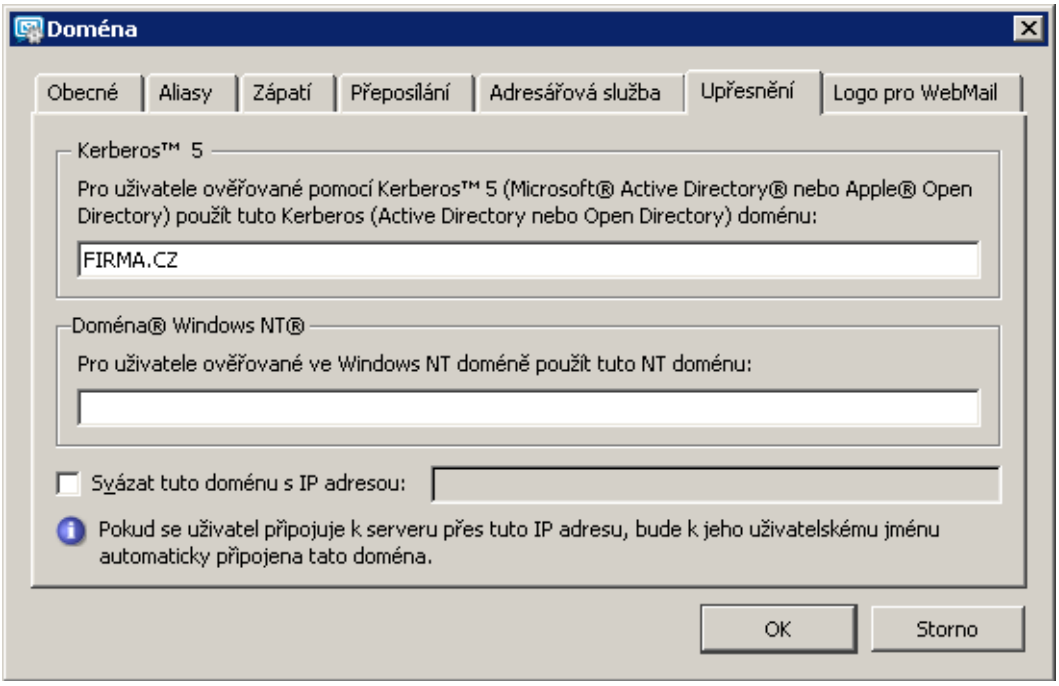
1. byl *Kerio MailServer* členem *Open Directory* domény, proti které se ověřuje. Pokud *Kerio MailServer* nebude členem domény, pak Kerberos nebude fungovat a uživatelé budou muset používat lokální heslo — tedy jiné než mají nastaveno v doméně.

2. počítač s *Kerio MailServerem* měl správně nastavený DNS server (IP adresa nebo DNS jméno počítače, na kterém je spuštěn *Apple Open Directory*).

3. byl synchronizován čas *Kerio MailServeru* a *Open Directory* — to by mělo být automaticky zajištěno přidáním počítače do domény (viz bod 1).

Ověřování proti samostatnému Kerberos serveru

Chcete-li použít pro ověřování samostatný Kerberos server (*Key Distribution Center*), potom bude nutno udržovat databázi uživatelských jmen a hesel v *Key Distribution Center* i v *Kerio MailServeru*.



Obrázek 24.3 Doplnění Kerberos realm do Kerio MailServeru

Kromě uvedení názvu Kerberos oblasti (Kerberos realm) v *Kerio MailServeru* je třeba zajistit následující:

1. *Kerio MailServer* musí být členem Kerberos oblasti, proti které se ověřuje. Jména a hesla všech uživatelů založených v *Kerio MailServeru* musí být definována v *Key Distribution Center* (pokud se mají ověřovat přes Kerberos).

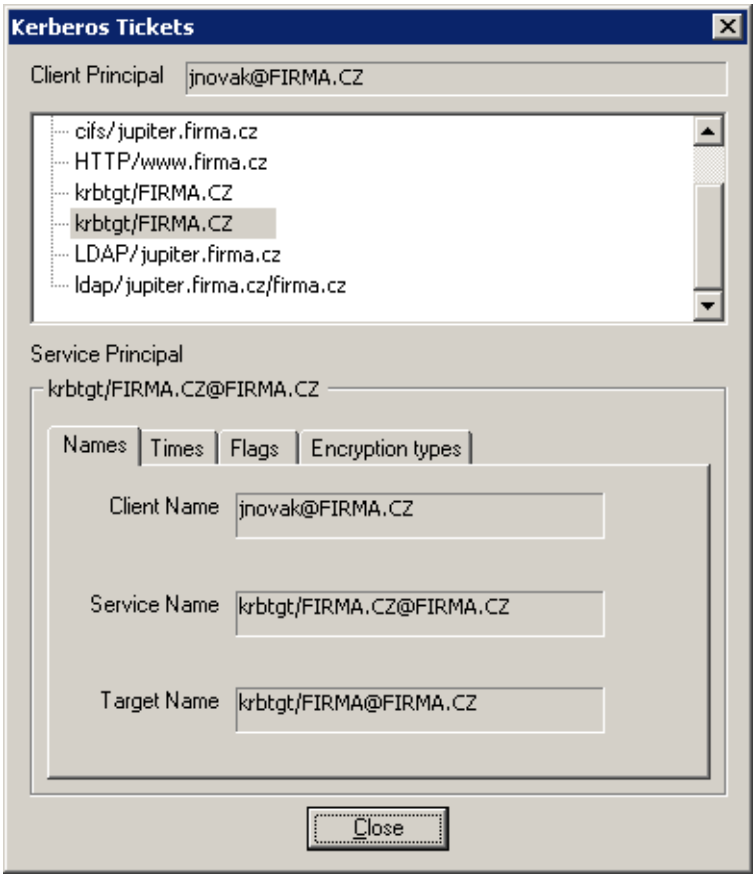
2. Počítač s *Kerio MailServerem* musí mít správně nastavený DNS server (*Key Distribution Center* vyhledává na základě DNS dotazů).

3. Počítač s *Kerio MailServerem* musí mít synchronizován čas s *Key Distribution Center* (všechny počítače v Kerberos oblasti musí mít synchronizován čas).

Vyzkoušet si, že *Kerio MailServer* je schopen ověřovat se proti *Key Distribution Center*, je možné pomocí utility *Kerbtray*.

Kontrolu lze provést z počítače, kam budete instalovat *Kerio MailServer*. Ze systému *MS Windows* zkontrolujeme ověřování pomocí utility *Kerbtray* (viz obrázek 24.4), která

je k dispozici zdarma na stránkách firmy *Microsoft*. Pokud po instalaci a spuštění aplikace *Kerbtray* nenalezne žádné přidělené lístky (tickety), potom ověřování funkční není a je třeba jej v KDC nastavit a spustit.



Obrázek 24.4 Kerberos lístky zobrazené v aplikaci Kerbtray

Teprve poté doporučujeme nastavit ověřování v *Kerio MailServeru* v sekci *Konfigurace* → *Domény*, v záložce *Upřesnění* (více viz kapitolu 7.7).

24.2 Kerio MailServer na systému Linux

Ověřování proti Active Directory

Před nastavením přihlašování uživatelů do Linuxu přes Kerberos doporučujeme nejprve zkontrolovat správnou funkci ověřování proti doméně (přihlášením se do systému účtem definovaným v *Active Directory*).

Dále je nutno zajistit následující:

1. Počítač s *Kerio MailServerem* musí mít nastavený jako primární DNS server doménový řadič *Active Directory* domény.

   Pokud konfigurace sítě vyžaduje ověřování proti více doménovým řadičům zároveň, přidáme jako DNS servery všechny doménové řadiče, proti kterým se bude *Kerio MailServer* ověřovat.

2. Na počítači s *Kerio MailServerem* musí být synchronizován čas s *Active Directory*.

Dále je nutné pro správnou funkci ověřování nastavit soubor `/etc/krb5.conf`

Příklad nastavení souboru `krb5.conf`:

```
[logging]
  default = FILE:/var/log/krb5libs.log
  kdc = FILE:/var/log/krb5kdc.log
  admin_server = FILE:/var/log/kadmind.log

[libdefaults]
  ticket_lifetime = 24000
  default_realm = FIRMA.CZ
  dns_lookup_realm = false
 dns_lookup_kdc = yes

[realms]
 FIRMA.CZ = {
  kdc = server.firma.cz
  admin_server = server.firma.cz
  default_domain = firma.cz
 }

[domain_realm]
 .firma.cz = FIRMA.CZ
 firma.cz = FIRMA.CZ

[kdc]
 profile = /var/kerberos/krb5kdc/kdc.conf

[appdefaults]
 pam = {
  debug = false
```

```
  ticket_lifetime = 36000
  renew_lifetime = 36000
  forwardable = true
  krb4_convert = false
 }
```

Pokud je ověřování proti Kerberos serveru plně funkční, potom je možné nastavit ověřování v *Kerio MailServeru*. Tato nastavení lze provést v sekci *Konfigurace* → *Domény*, v záložkách *Adresářová služba* a *Upřesnění* (více viz kapitoly 7.6 a 7.7).

Ověřování proti Open Directory

Před nastavením přihlašování uživatelů do Linuxu přes Kerberos doporučujeme nejprve zkontrolovat správnou funkci ověřování proti doméně (přihlášením se do systému účtem definovaným v *Open Directory*). Pokud se toto nepodaří, zkontrolujte prosím následující:

1. *Kerio MailServer* musí být členem Kerberos oblasti (Open Directory domény), proti které se ověřuje. Pokud *Kerio MailServer* nebude členem oblasti, pak Kerberos nebude fungovat a uživatelé budou muset používat lokální heslo — tedy jiné než mají nastaveno v doméně.

2. počítač s *Kerio MailServerem* musí mít správně nastavenou službu DNS.

3. na počítači s *Kerio MailServerem* musí být synchronizován čas s *Open Directory*.

Dále je nutné pro správnou funkci ověřování nastavit soubor `/etc/krb5.conf`

Příklad nastavení souboru `krb5.conf`:

```
[logging]
  default = FILE:/var/log/krb5libs.log
  kdc = FILE:/var/log/krb5kdc.log
  admin_server = FILE:/var/log/kadmind.log

[libdefaults]
  ticket_lifetime = 24000
  default_realm = FIRMA.CZ
  dns_lookup_realm = false
 dns_lookup_kdc = yes

[realms]
 FIRMA.CZ = {
  kdc = server.firma.cz
  admin_server = server.firma.cz
```

```
  default_domain = firma.cz
 }

[domain_realm]
 .firma.cz = FIRMA.CZ
 firma.cz = FIRMA.CZ

[kdc]
 profile = /var/kerberos/krb5kdc/kdc.conf

[appdefaults]
 pam = {
  debug = false
  ticket_lifetime = 36000
  renew_lifetime = 36000
  forwardable = true
  krb4_convert = false
 }
```

Je-li ověřování proti Kerberos serveru plně funkční, potom je možné nastavit ověřování v *Kerio MailServeru*. Tato nastavení lze provést v sekci *Konfigurace* → *Domény*, v záložkách *Adresářová služba* a *Upřesnění* (více viz kapitoly 7.6 a 7.7).

Ověřování proti samostatnému Kerberos serveru (KDC)

Chcete-li použít pro ověřování samostatný Kerberos server (*Key Distribution Center*), potom bude nutno udržovat databázi uživatelských jmen a hesel v *Key Distribution Center* i v *Kerio MailServeru*.

Před nastavením přihlašování uživatelů do Linuxu přes Kerberos doporučujeme nejprve zkontrolovat správnou funkci ověřování proti Kerberos oblasti (přihlášením se do systému účtem definovaným v *Key Distribution Center*. Pokud se toto nepodaří, zkontrolujte prosím následující:

1. *Kerio MailServer* musí být členem Kerberos oblasti, proti které se ověřuje:
   - na stanici musí být nainstalován Kerberos klient,
   - jména a hesla všech uživatelů založených v *Kerio MailServeru* musí být definována v *Key Distribution Center* (pokud se mají ověřovat přes Kerberos).
2. Počítač s *Kerio MailServerem* musí mít správně nastavenou službu DNS (*Key Distribution Center* se orientuje na základě DNS dotazů).
3. Na počítači s *Kerio MailServerem* musí být synchronizován čas s *Key Distribution Center* (všechny počítače v Kerberos oblasti musí mít synchronizovaný čas).

Dále je nutné pro správnou funkci ověřování nastavit soubor `/etc/krb5.conf`

Příklad nastavení souboru `krb5.conf`:

```
[logging]
  default = FILE:/var/log/krb5libs.log
  kdc = FILE:/var/log/krb5kdc.log
  admin_server = FILE:/var/log/kadmind.log

[libdefaults]
  ticket_lifetime = 24000
  default_realm = FIRMA.CZ
  dns_lookup_realm = false
 dns_lookup_kdc = yes

[realms]
 FIRMA.CZ = {
  kdc = server.firma.cz
  admin_server = server.firma.cz
  default_domain = firma.cz
 }

[domain_realm]
 .firma.cz = FIRMA.CZ
 firma.cz = FIRMA.CZ

[kdc]
 profile = /var/kerberos/krb5kdc/kdc.conf

[appdefaults]
 pam = {
  debug = false
  ticket_lifetime = 36000
  renew_lifetime = 36000
  forwardable = true
  krb4_convert = false
 }
```

Vyzkoušet si, že je *Kerio MailServer* schopen ověřovat se proti *Key Distribution Center*, je možné pomocí utility `kinit`. Stačí otevřít terminál (příkazovou řádku) a zadat následující příkaz:

```
kinit -S host/nazev_KMS@KERBEROS_REALM uzivatelske_jmeno
```

například:

```
kinit -S host/mail.firma.cz@FIRMA.CZ jnovak
```

Pokud dotaz proběhl v pořádku, budete požádáni o heslo zadaného uživatele. Pokud ne, jako odpověď bude doručeno chybové hlášení.

Teprve poté doporučujeme provést příslušná nastavení v *Kerio MailServeru* (více viz kapitolu 7.7).

24.3 Kerio MailServer na systému Mac OS

Ověřování proti Active Directory

Pokud je *Kerio MailServer* nainstalován na systému Mac OS X a uživatelské účty jsou mapovány z *Active Directory*, potom je nutno provést následující nastavení:

Konfigurace DNS

Aby se mohl systém Mac OS X připojit do *Active Directory*, nastavíme převod DNS jmen počítačů z *Active Directory*. Z tohoto důvodu nastavíme *Active Directory* jako primární DNS server:

1. Otevřeme aplikaci *System Preferences* a klikneme na ikonku *Network* (viz obrázek 24.5).

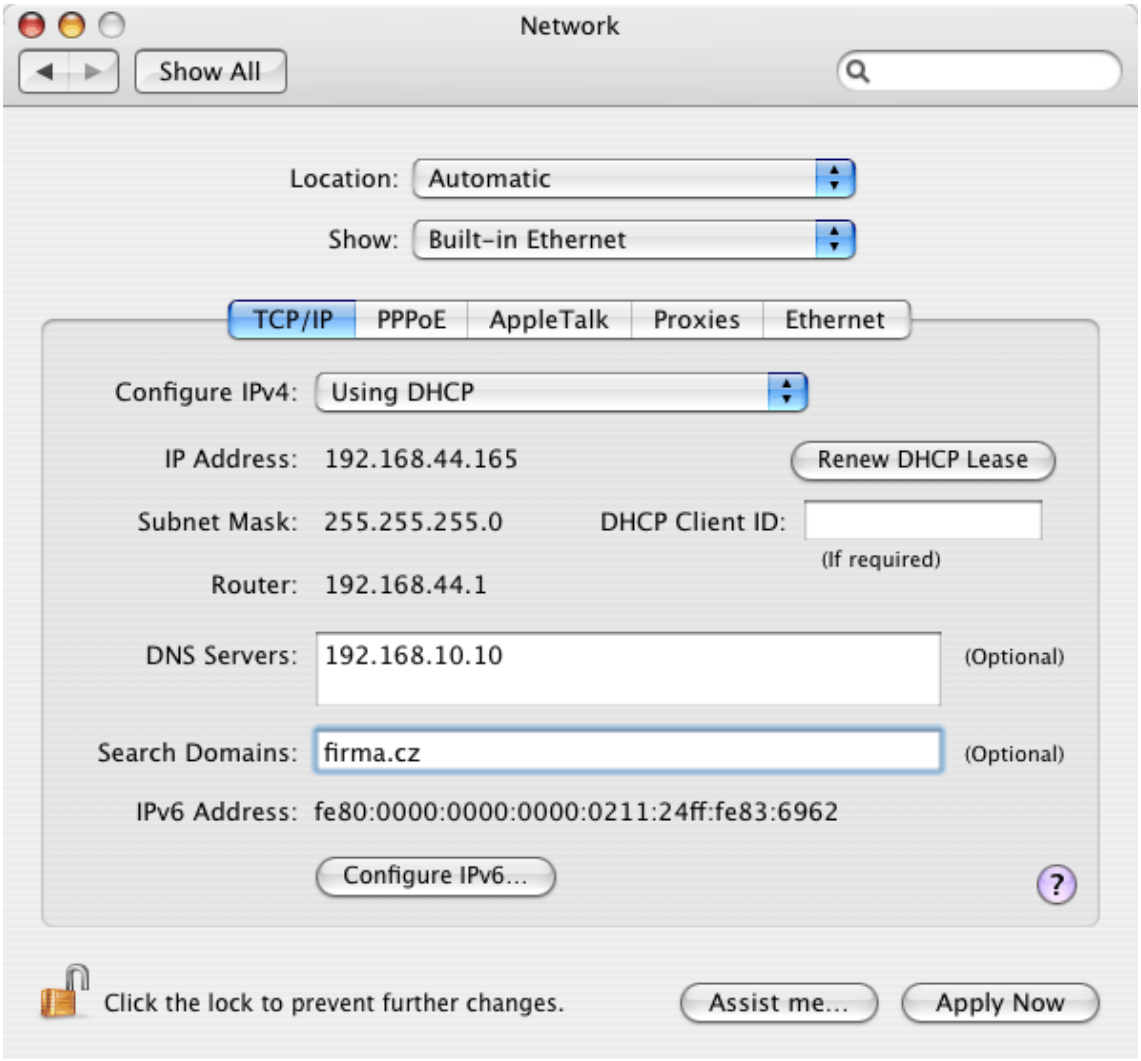
2. Otevře se okno *Network*. V záložce TCP/IP doplníme do položky *DNS servers* IP adresu *Active Directory* serveru.

   Pokud konfigurace sítě vyžaduje ověřování proti více doménovým řadičům zároveň, potom přidáme jako DNS servery všechny doménové řadiče, proti kterým se bude *Kerio MailServer* ověřovat.

Připojení počítače s Kerio MailServerem do Active Directory domény

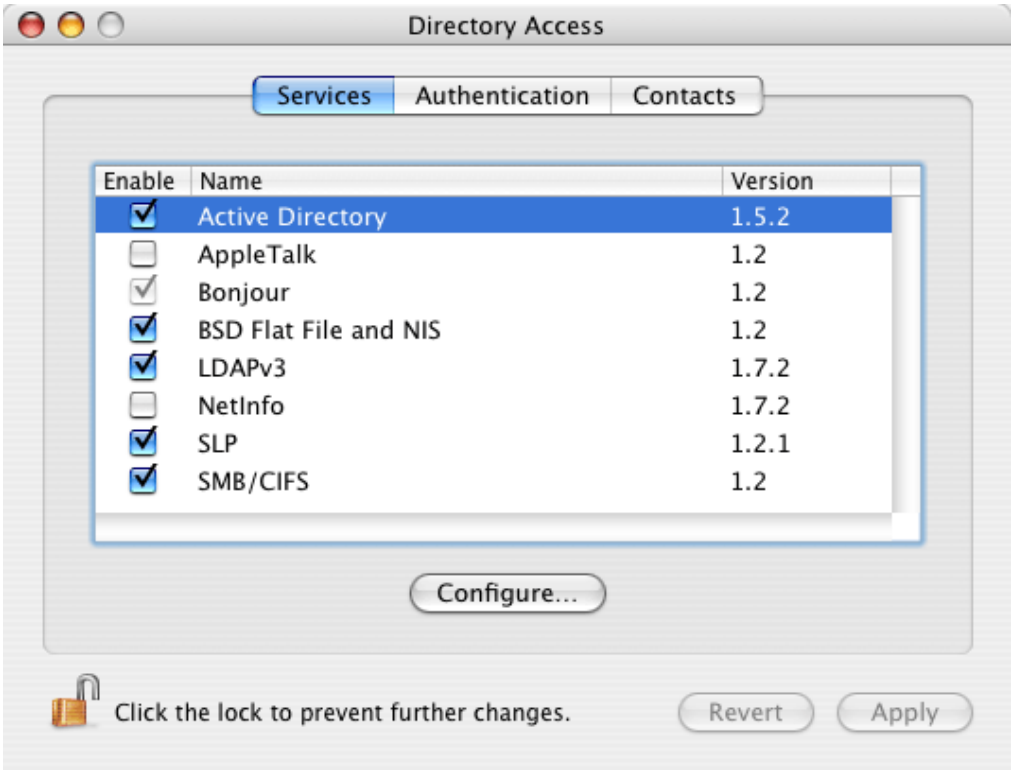
Počítač do *Active Directory* domény připojíme pomocí utility *Directory Access* (*Applications* → *Utilities*), která je standardní součástí systémů *Apple Mac OS X*. Konfigurace je následující:

1. Otevřeme aplikaci *Directory Access* a zaškrtneme v záložce *Services* službu *Active Directory* (více viz obrázek 24.6). Nejprve ovšem zadáme jméno a heslo pro ověření. Uživatel, který bude provádět v aplikaci změny, musí mít nastavena práva k administraci systému.

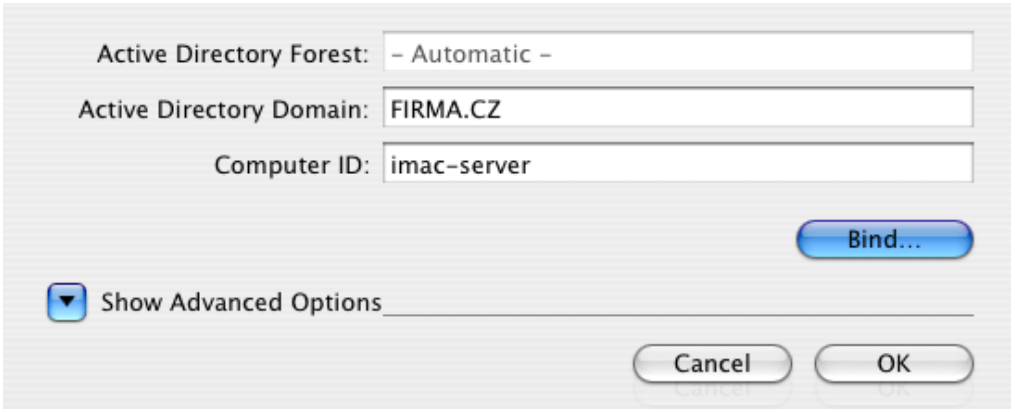


Obrázek 24.5 Konfigurace DNS

2. Po zaškrtnutí služby klikneme na tlačítko *Configure* a do dialogu doplníme název *Active Directory* domény (viz obrázek 24.7).



Obrázek 24.6 Directory Access — záložka Services

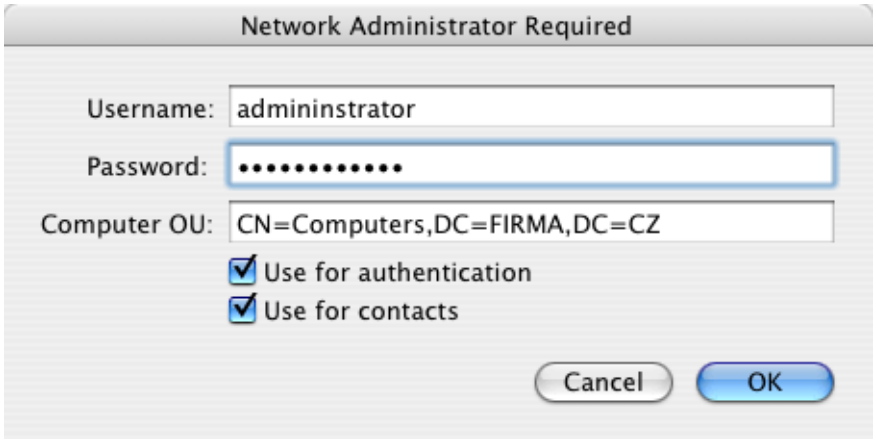


Obrázek 24.7 Directory Access — konfigurace

3. Klikneme na tlačítko *Bind* a nastavíme jméno a heslo administrátora *Active Directory*, který může přidat počítač do *Active Directory* domény (viz obrázek 24.8).

Je-li vše nastaveno správně, počítač se po několika vteřinách do domény úspěšně připojí.

Nastavení Kerberosu



Obrázek 24.8 Directory Access — zadání jména a hesla administrátora

Jakmile se Mac OS X úspěšně připojí k *Active Directory* doméně, vytvoří se v adresáři `/Library/Preferences/` speciální soubor `edu.mit.Kerberos`. Přesvědčte se, že soubor byl vytvořen, a že byl vytvořen správně. Pro porovnání uvádíme následující příklad obsahu souboru:

```
# WARNING This file is automatically created by Active Directory
# do not make changes to this file;
# autogenerated from : /Active Directory/firma.cz
# generation_id : 0
[libdefaults]
        default_realm = FIRMA.CZ
    ticket_lifetime = 600
        dns_fallback = no
[realms]
        FIRMA.CZ = {
                    kdc = server.firma.cz.:88
                    admin_server = server.firma.cz.
        }
```

Vyzkoušet si, že *Kerio MailServer* je schopen ověřovat se proti *Active Directory*, je možné pomocí utility `kinit`. Stačí otevřít terminál (příkazovou řádku) a zadat následující příkaz:

```
kinit -S host/nazev_KMS@KERBEROS_REALM uzivatelske_jmeno
```

například:

```
kinit -S host/mail.firma.cz@FIRMA.CZ jnovak
```

Pokud dotaz proběhl v pořádku, budete požádáni o heslo zadaného uživatele. Pokud ne, jako odpověď bude doručeno chybové hlášení.

Ověřování proti Open Directory

Kerio MailServer je možno nainstalovat buď na stejný server, kde je umístěna také adresářová služba *Apple Open Directory* nebo je možno *Kerio MailServer* nainstalovat na jakýkoliv jiný server.

Je-li *Kerio MailServer* umístěn na stejném serveru jako *Open Directory*, potom není nutné kromě instalace *Kerio Open Directory Extensions* provádět jakoukoliv další konfiguraci. Je-li však fyzicky umístěn na jiném stroji, pak je třeba nastavit externí ověřování přes *Kerberos* do *Open Directory*.

Kerio MailServer je možno nainstalovat na server se systémem *Mac OS X 10.3* a vyšší. Nastavení probíhá na obou verzích systému velmi podobně. Z toho důvodu zde bude popsán postup pouze pro verzi *Mac OS X 10.4* s tím, že případné odchylky nastavení na systému *Mac OS X 10.3* budou explicitně zmíněny.

Nastavení externího ověřování se provádí pomocí speciální aplikace *Directory Access*, která se nachází v *Applications* → *Utilities* → *Directory Access*. Tato aplikace v podstatě slouží k vytvoření speciálního ověřovacího souboru `edu.mit.Kerberos`, který najdete v adresáři `/Library/Preferences`. Aby ověřování fungovalo správně, je třeba provést následující nastavení:

1. Otevřeme aplikaci *Directory Access*.

2. V první záložce *Services* zaškrtneme položku LDAPv3 (viz obrázek 24.9).

3. V záložce *Services* označíme kurzorem položku LDAPv3 a stiskneme tlačítko *Configure* umístěné pod seznamem služeb.

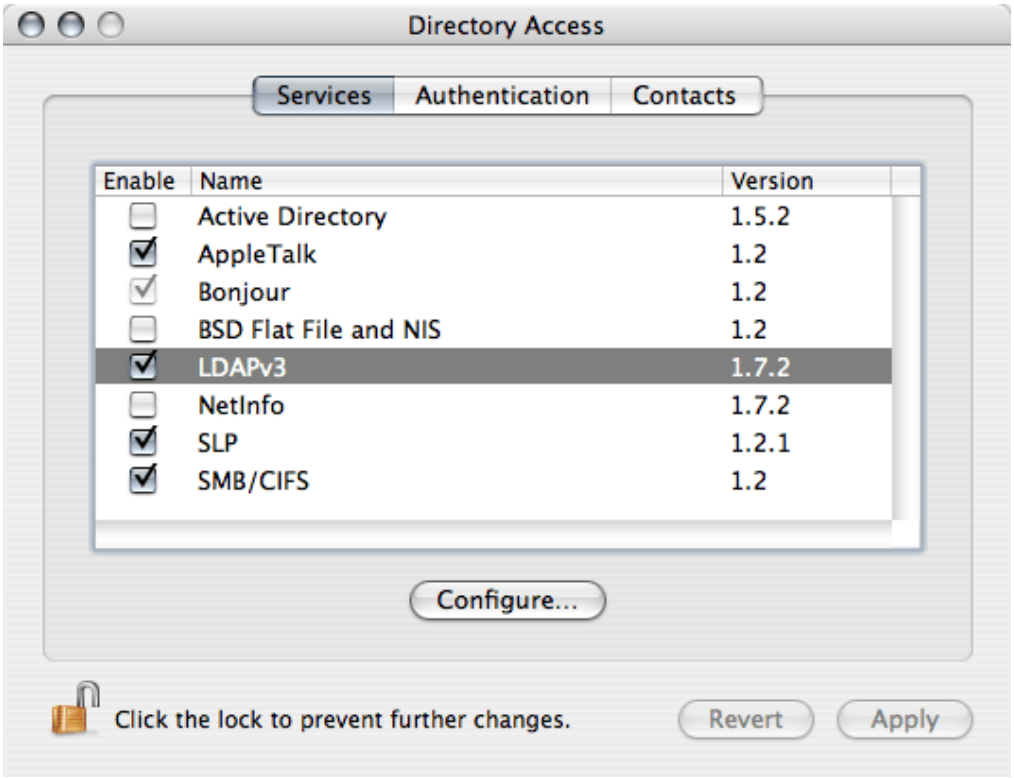
4. V dialogu, který se otevřel, najdeme tlačítko *New* a stiskneme ho.

5. Otevře se okno pro zadání názvu nebo IP adresy serveru. Doplníme IP adresu nebo DNS název serveru, kde je spuštěna služba *Apple Open Directory*. Po zadání serveru klikneme v levém dolním rohu na tlačítko *Manual* (v systému *Mac OS X 10.3* toto není potřeba) a doplníme libovolný název do pole *Configuration name* (položka slouží pouze pro lepší orientaci).

6. Konfiguraci uložíme a v menu *LDAP Mappings* nastavíme *Open Directory Server*.

7. Po zvolení *Open Directory Server* se automaticky otevře okno pro zadání přípony pro hledání (*Search Base Suffix*). Příponu pro hledání je třeba vyplnit tak, jak to zobrazuje příklad na obrázku 24.10:

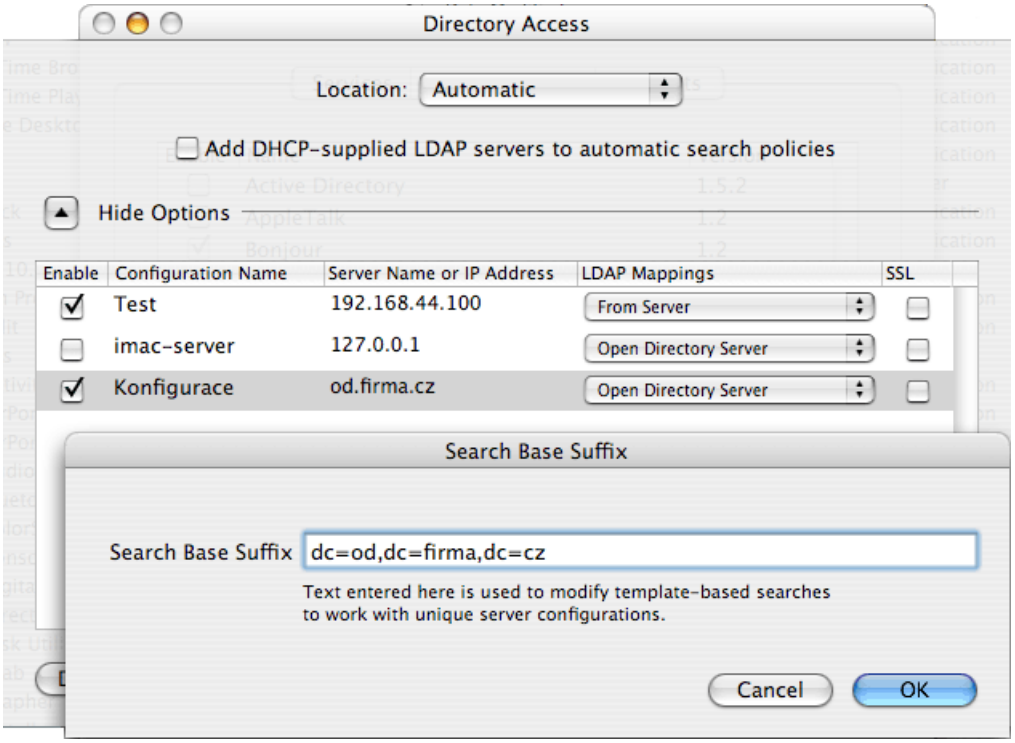
   `od.firma.cz` → `dc=od,dc=firma,dc=cz`



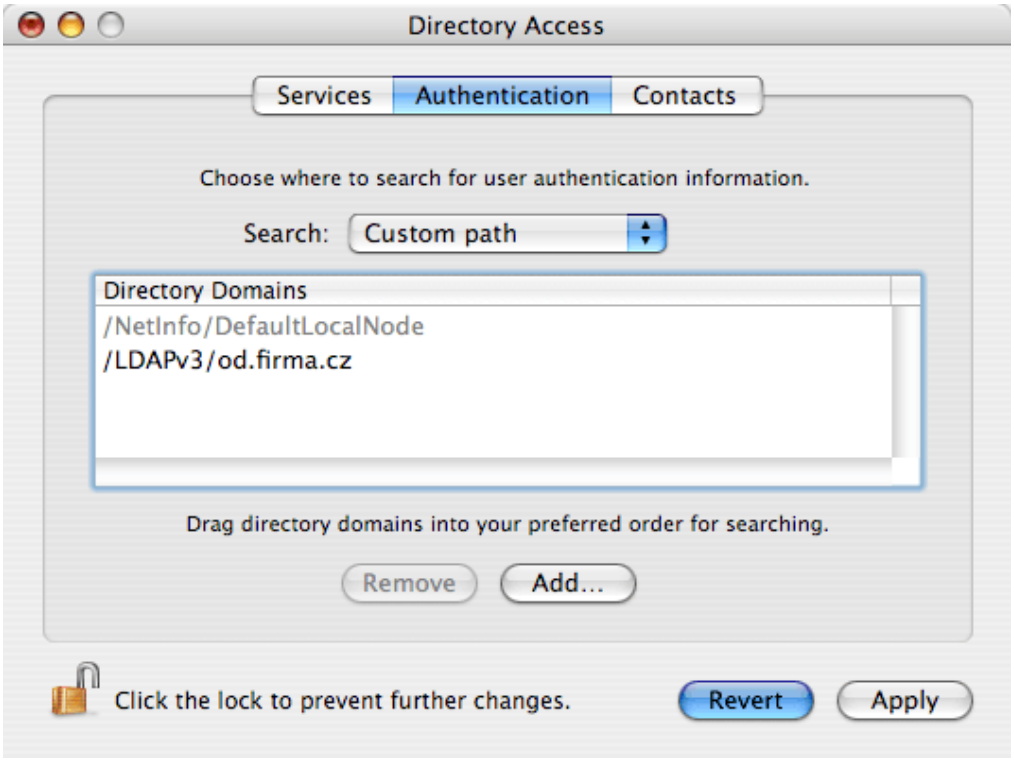
Obrázek 24.9 Directory Access — Výběr služby LDAP

Z výše uvedeného příkladu tedy vyplývá, že příponu je třeba vždy zapsat ve tvaru `dc=subdomena,dc=domena`. Kolik subdomén v názvu server obsahuje, tolik jich je nutno do přípony zapsat.

8. Nyní je třeba nastavit serveru s *Open Directory* ověřování. K tomuto účelu nám dobře poslouží záložka *Authentication* (viz obrázek 24.11).



Obrázek 24.10 Directory Access — Nastavení serveru s Open Directory



Obrázek 24.11 Directory Access — Nastavení ověřování

9. V menu *Search* musí být zvolena možnost *Custom path*.

10. Do seznamu *Directory Domains* je třeba zadat název serveru s *Open Directory*. Klikneme na tlačítko *Add*. Aplikace *Directory Access* automaticky doplní název *Open Directory*, který jsme zadali v předchozí záložce. Nabídnutý název serveru stačí pouze potvrdit.

11. Celé nastavení uložíme tlačítkem *Apply*.

Directory Access vytvoří v adresáři `/Library/Preferences` soubor `edu.mit.Kerberos`. Tento soubor je nutno zkontrolovat, zda jsou v něm uvedena správná data. Soubor by měl obsahovat následující parametry:

```
# WARNING This file is automatically created by Open Directory
# do not make changes to this file;
# autogenerated from : /Open Directory/firma.cz
# generation_id : 0
[libdefaults]
        default_realm = FIRMA.CZ
        ticket_lifetime = 600
        dns_fallback = no
```

```
[realms]
        FIRMA.CZ = {
                kdc = server.firma.cz.:88
                admin_server = server.firma.cz.
        }
```

Vyzkoušet si, že je *Kerio MailServer* schopen ověřovat se proti Kerberos serveru, je možné pomocí utility `kinit`. Stačí otevřít terminál (příkazovou řádku) a zadat následující příkaz:

```
kinit -S host/KMS_hostname@KERBEROS_REALM username@REALM
```

například:

```
kinit -S host/od.firma.cz@FIRMA.CZ jnovak@FIRMA.CZ
```

Pokud dotaz proběhl v pořádku, budete požádáni o heslo zadaného uživatele. Pokud ne, jako odpověď bude doručeno chybové hlášení.

Nyní stačí provést nastavení v *Kerio MailServeru*:

- V administrační konzoli *Kerio MailServeru* v sekci *Domény* nastavíme záložky *Adresářová služba* a *Upřesnění* (v poli *Kerberos 5* musí být zadán realm *Apple Open Directory*).
  Upozornění: Kerberos realm doplněný v záložce *Upřesnění* musí být shodný s názvem Kerberos oblasti, který je uveden v souboru `/Library/Preferences/edu.mit.Kerberos`. Konkrétně musí souhlasit s hodnotou `default_realm` v tomto souboru. Příslušný řádek tedy může vypadat například takto `default_realm = FIRMA.CZ`
- V administrační konzoli *Kerio MailServeru* nastavíme uživatelským účtům typ ověřování *Apple Open Directory*.

Ověřování proti samostatnému Kerberos serveru (KDC)

Chcete-li použít pro ověřování samostatný Kerberos server (*Key Distribution Center*), potom bude nutno udržovat databázi uživatelských jmen a hesel v *Key Distribution Center* i v *Kerio MailServeru*.

Před nastavením přihlašování uživatelů do *Kerio MailServeru* přes Kerberos doporučujeme nejprve zkontrolovat správnou funkci ověřování proti Kerberos oblasti (přihlášením se do systému účtem definovaným v *Key Distribution Center* na počítači, kam budete *Kerio MailServer* instalovat. Pokud se toto nepodaří, zkontrolujte prosím následující:

1. *Kerio MailServer* musí být členem Kerberos oblasti, proti které se ověřuje:

- na stanici musí být nainstalován Kerberos klient,
- jména a hesla všech uživatelů založených v *Kerio MailServeru* musí být definována v *Key Distribution Center* (pokud se mají ověřovat přes Kerberos).

2. Počítač s *Kerio MailServerem* musí mít správně nastavenou službu DNS (*Key Distribution Center* se orientuje na základě DNS dotazů).

3. Na počítači s *Kerio MailServerem* musí být synchronizován čas s *Key Distribution Center* (všechny počítače v Kerberos oblasti musí mít synchronizovaný čas).

Ověřit správnou funkci Kerberosu lze zkontrolováním souboru `/Library/Preferences/edu.mit.Kerberos`. Tento soubor by měl obsahovat následující parametry:

```
# WARNING This file is automatically created by KERBEROS
# do not make changes to this file;
# autogenerated from : /KERBEROS/firma.cz
# generation_id : 0
    [libdefaults]
            default_realm = FIRMA.CZ
      ticket_lifetime = 600
            dns_fallback = no
    [realms]
            FIRMA.CZ = {
                    kdc = server.firma.cz.:88
                    admin_server = server.firma.cz.
           }
```

Vyzkoušet si, že *Kerio MailServer* je schopen ověřovat se proti Kerberosu, je možné pomocí utility `kinit`. Stačí otevřít terminál (příkazovou řádku) a zadat následující příkaz:

```
kinit -S host/KMS_hostname@KERBEROS_REALM username@REALM
```

například:

```
kinit -S host/mail.firma.cz@FIRMA.CZ jnovak@FIRMA.CZ
```

Pokud dotaz proběhl v pořádku, budete požádáni o heslo zadaného uživatele. Pokud ne, jako odpověď bude doručeno chybové hlášení.

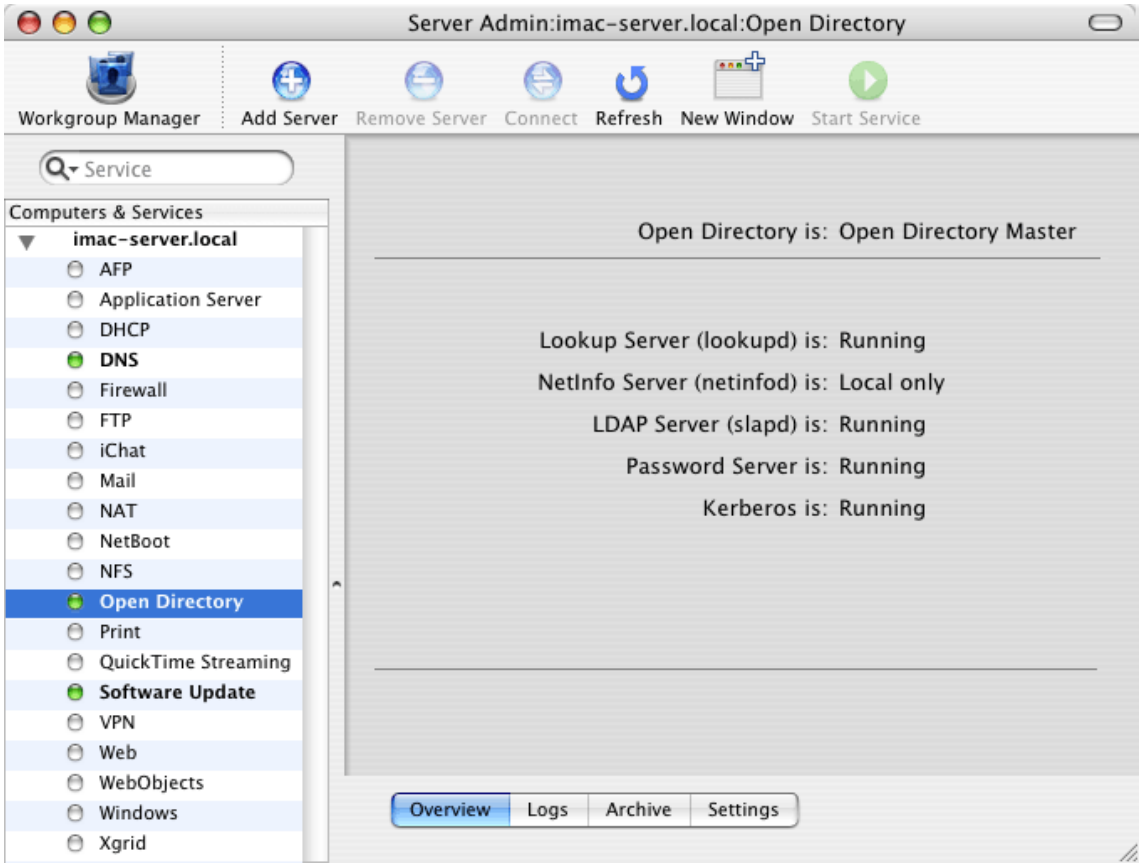
Potom teprve doporučujeme nastavit ověřování v *Kerio MailServeru* v sekci *Konfigurace* → *Domény*, v záložce *Upřesnění* (více viz kapitolu 7.7).

24.4 Spuštění služby Open Directory a nastavení systému Kerberos

V *Open Directory* je možné ověřovat uživatele proti password serveru (více viz kapitolu 7.6) nebo proti Kerberos serveru (více viz kapitolu 24). Jak již bylo řečeno v kapitole 7.6, ověřování proti password serveru nevyžaduje téměř žádná nastavení, zatímco ověřování přes Kerberos není vždy snadné nakonfigurovat. Tato kapitola se tedy bude věnovat správnému nastavení ověřování proti Kerberos serveru v *Open Directory*.

Po spuštění Mac OS X Serveru je třeba důkladně se přesvědčit, zda je spuštěna adresářová služba *Open Directory* a zároveň, zda je spuštěn Kerberos server. To lze učinit v aplikaci *Server Admin* (*Applications* → *Server* → *Server Admin*).

Úvodní okno aplikace *Server Admin* je rozděleno na dvě základní části. Levá obsahuje seznam počítačů a služeb, které jsou na těchto počítačích spuštěny. V této části je zobrazen počítač, kde je, nebo má být spuštěna služba *Open Directory*. Pokud je služba spuštěna, je zvýrazněna tučným písmem a zeleným symbolem (viz obrázek 24.12).

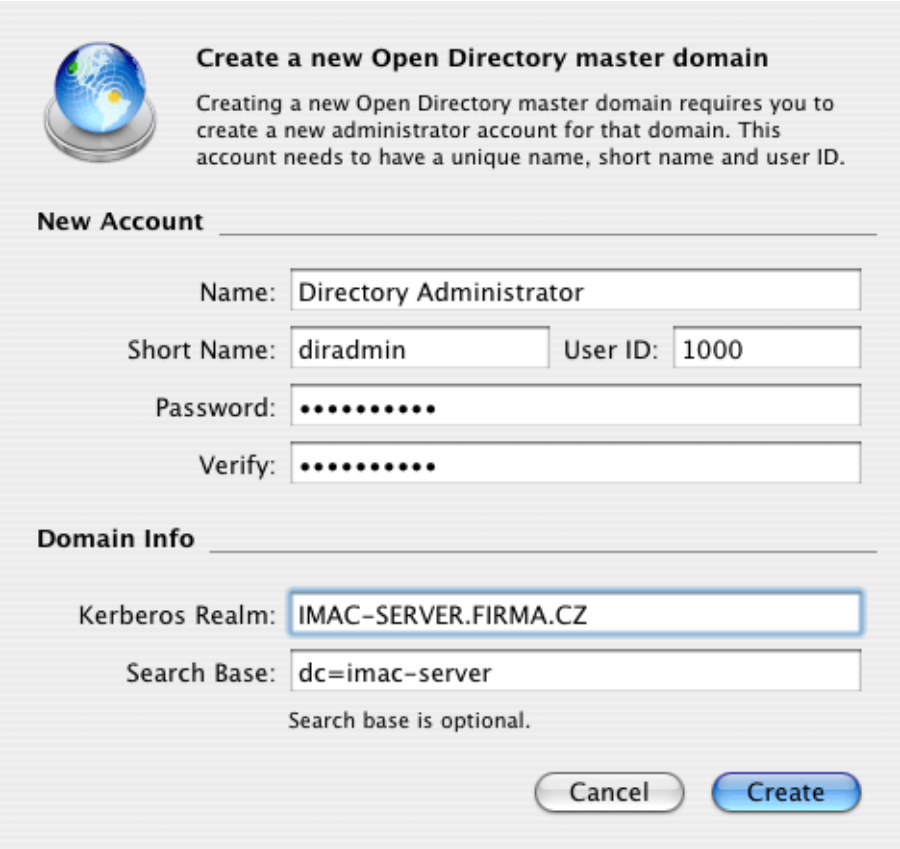


Obrázek 24.12 Služba Open Directory

Pravá strana okna obvykle obsahuje informace o službě, záznamy a případná nastavení vybrané služby.

Adresářová služba by měla být spuštěna automaticky po prvním startu Mac OS X Serveru. Pokud spuštěna není, označíme ji kurzorem a použijeme tlačítko *Start Service* umístěné na panelu nástrojů. V pravé části okna se přesvědčíme, které služby *Open Directory* jsou spuštěny, a které nikoliv (viz obrázek 24.12). Důležitá je poslední položka Kerberos. Je-li Kerberos server spuštěn, vše je v pořádku a není třeba provádět další nastavení. Není-li služba spuštěna, zkontrolujte prosím následující:

1. V pravé části okna v záložce *Settings* musí být server nastaven jako *Open Directory Master*. Toto nastavení vyžaduje ověření. Je nutno použít jméno a heslo administrátora, který je založen v *Open Directory*, například uživatel `diradmin` (viz obrázek 24.13).



Obrázek 24.13 Nastavení jména a hesla administrátora

2. Musí být správně nastavena služba DNS.

3. Musí být správně nastaveno DNS jméno (hostname) serveru, kde je spuštěna *Open Directory*.

Po úspěšném spuštění Kerberos serveru doporučujeme přesvědčit se o jeho správném nastavení utilitou `kinit`. Stačí otevřít terminál (příkazovou řádku) a zadat následující příkaz:

```
kinit -S host/nazev_KMS@KERBEROS_REALM uzivatelske_jmeno
```

například:

```
kinit -S host/mail.firma.cz@FIRMA.CZ diradmin
```

Pokud dotaz proběhl v pořádku, budete požádáni o heslo zadaného uživatele. Pokud ne, jako odpověď bude doručeno chybové hlášení.

Poznámka: S odstraňováním případných potíží při nastavování ověřování přes Kerberos vám mohou pomoci záznamy v záložce *Logs*.

Kapitola 25

Nastavení NTLM ověřování

NTLM (NT LAN Manager) je název pro typ ověřování, kterým je možné se na systémech Windows ověřovat proti Active Directory (případně NT) doméně.

Nejprve musíme dodržet následující podmínky:

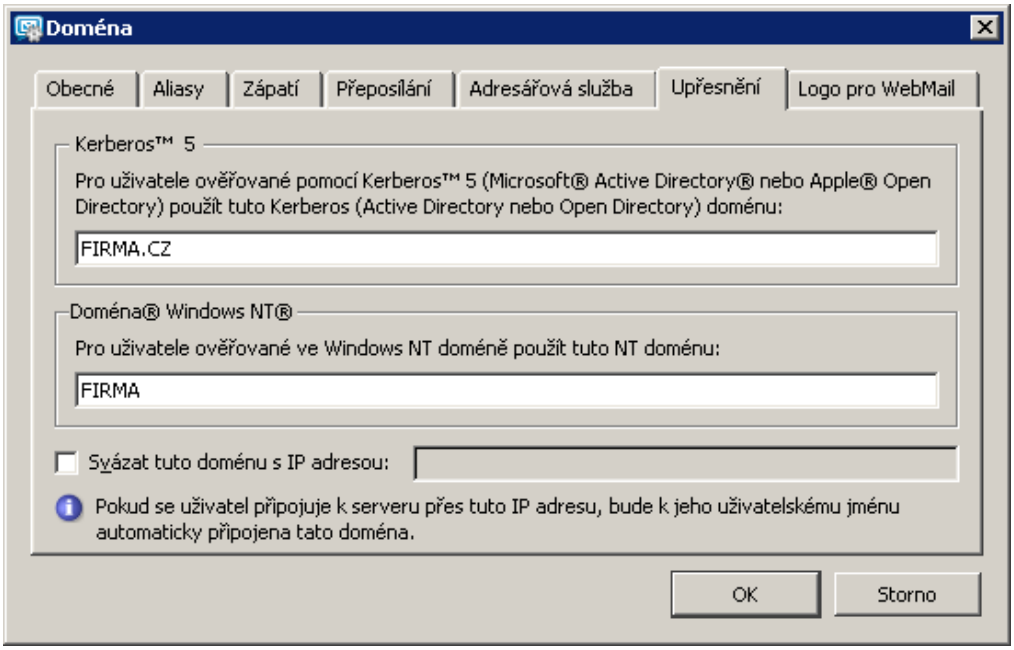
- NTLM ověřování je možno v *Kerio MailServeru* využít pouze v případě, že se uživatelé ověřují proti *Active Directory* doméně. To znamená, že lze takto ověřovat pouze účty, které jsou buď mapovány nebo importovány z *Active Directory* (viz kapitoly 7.6 a 13.10).
- Aby bylo NTLM ověřování funkční, musí být počítače i uživatelské účty součástí domény, proti které se uživatelé ověřují.
- Aby mělo nastavení NTLM ověřování smysl, musí uživatelé používat poštovní klienty, které podporují NTLM (SPA) ověřování (např. *MS Outlook*).

Upozornění: NTLM ověřování nelze používat v případě, že uživatelé využívají *MS Outlook* rozšířený o *Kerio Synchronization Plug-in*.

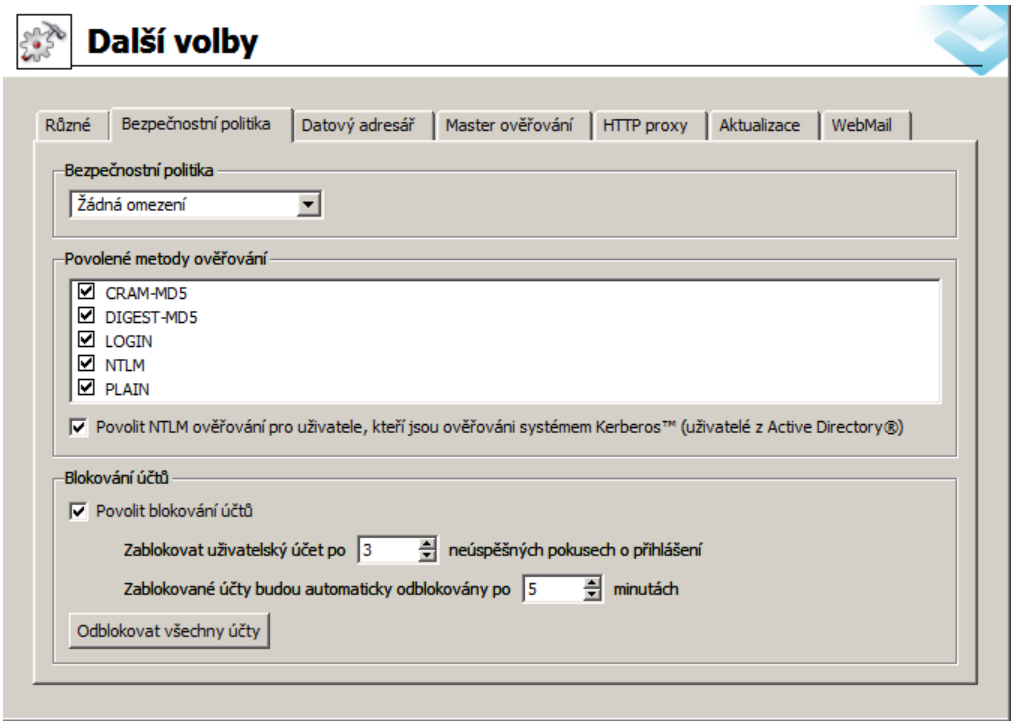
Správné nastavení NTLM ověřování v *Kerio MailServeru* je následující:

1. V administrační konzoli otevřeme sekci *Domény* (*Konfigurace* → *Domény*) Otevřeme dialog s podrobnostmi nastavení domény a přepneme se do záložky *Upřesnění* (viz obrázek 25.1). Do řádku *Doména Windows NT* je třeba nejprve doplnit název NT domény (obvykle název Active Directory domény bez domény první úrovně — CZ, COM, atd.).

2. V administrační konzoli se přepneme do sekce *Konfigurace* → *Další volby* do záložky *Bezpečnostní politika* a zde zaškrtneme volbu *Povolit NTLM ověřování pro uživatele, kteří jsou ověřováni systémem Kerberos*. Zaškrtnutím této volby bude uživatelům z *Active Directory* domény umožněno ověřovat se při přihlášení ke *Kerio MailServeru*.



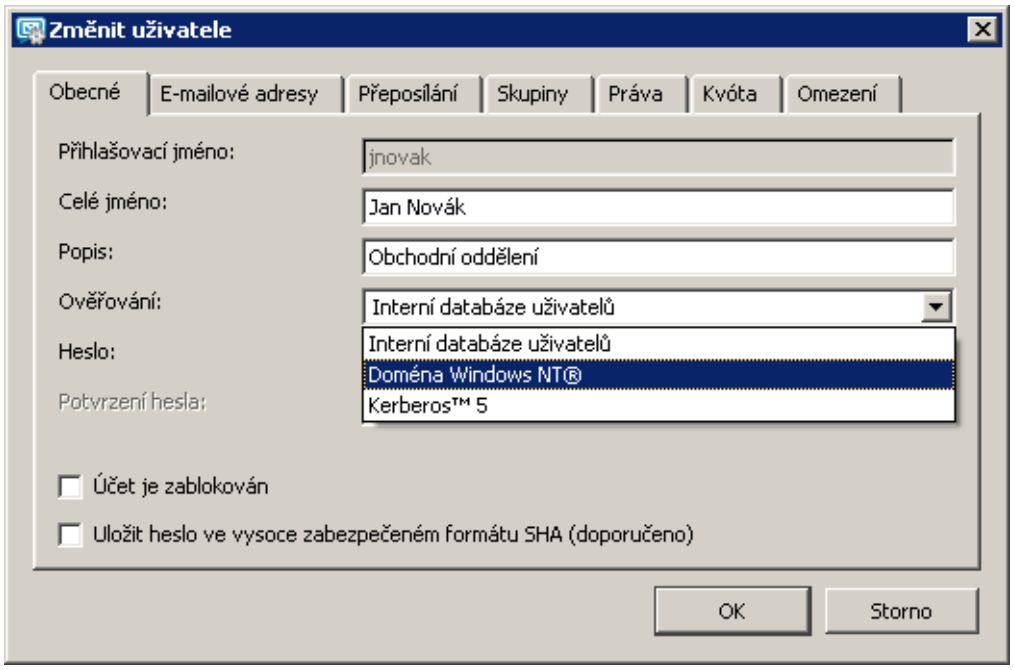
Obrázek 25.1 Nastavení názvu Windows NT domény



Obrázek 25.2 Zaškrtnutí volby Povolit NTLM ověřování pro uživatele, kteří jsou ověřováni systémem Kerberos

3. V administrační konzoli se přepneme do sekce *Nastavení domény* → *Uživatelské*

účty a uživatelům nastavíme jako typ ověřování volbu *Doména Windows NT*. Toto nastavení se v uživatelských účtech provádí v záložce *Obecné* (viz obrázek 25.3).



Obrázek 25.3 Nastavení ověřování uživatele

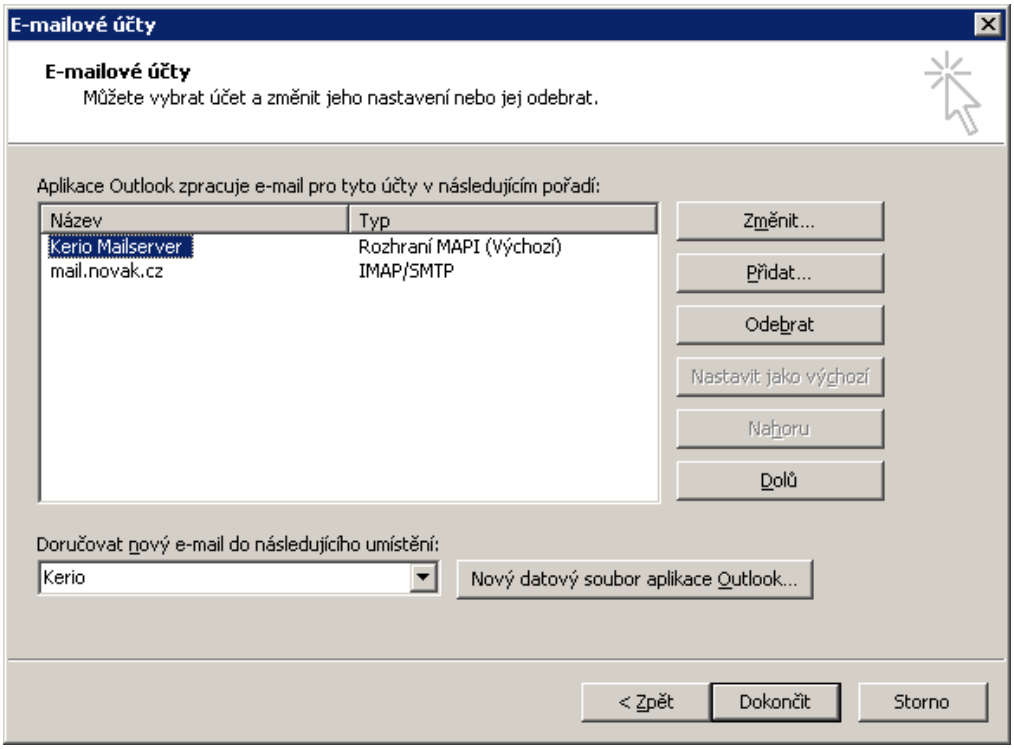
25.1 Nastavení NTLM v aplikaci MS Outlook s Kerio Outlook Connectorem

Kromě nastavení na serveru je třeba povolit NTLM (SPA) ověřování v poštovních klientech. Obvykle se toto nastavení provádí v nastavení e-mailového účtu uživatele. Jak nastavit například *MS Outlook* s *Kerio Outlook Connectorem* se dozvíme v následujícím návodu:

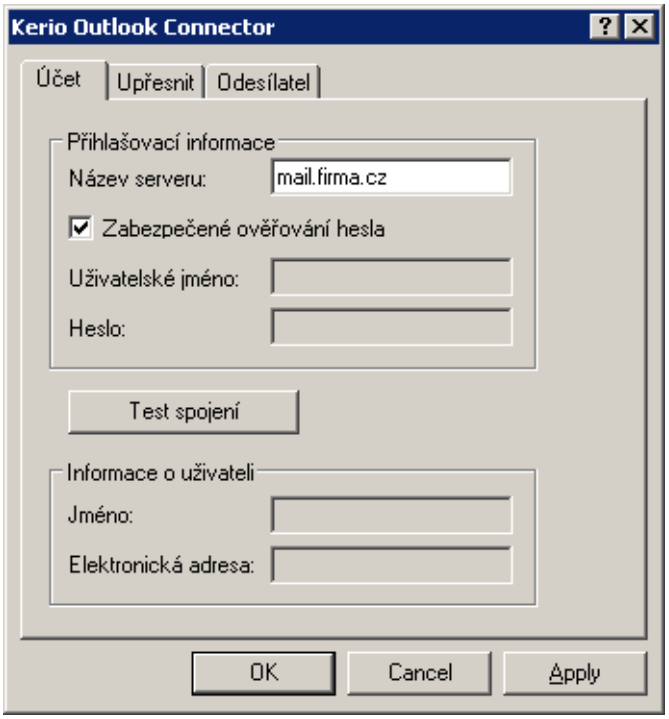
1. V menu *Nástroje* → *E-mailové účty* vybereme možnost *Zobrazit nebo změnit existující e-mailové účty*.

2. Vybereme Kerio (MAPI) účet a stiskneme tlačítko *Změnit* (viz obrázek 25.4).

3. Otevře se nastavení účtu, kde v záložce *Účet* zaškrtneme volbu *Zabezpečené ověřování hesla* (viz obrázek 25.5).



Obrázek 25.4 Změna e-mailového účtu



Obrázek 25.5 Nastavení NTLM ověřování

Kapitola 26

Nastavení poštovních klientů a firewallu

26.1 Nastavení poštovních klientů

Tato kapitola obsahuje základní informace o tom, jak nastavit poštovní klienty (tj. programy, které slouží ke čtení a psaní e-mailových zpráv). Nezaměřuje se na konkrétního klienta, ale uvádí obecné zásady, které by měly být dodrženy, aby klient spolupracoval správně s *Kerio MailServerem*.

Poštovní účet

Poštovní účet je skupina parametrů, které popisují server příchozí a odchozí pošty a podmínky jejich použití. Většina poštovních klientů umožňuje přepínat mezi více účty. Vytvoříme tedy nový účet, který bude používán pro příjem zpráv a odesílání zpráv přes *Kerio MailServer*.

Poznámka: Následující popis nastavení byl vytvořen podle klienta *MS Outlook Express 6.0*. Základní nastavení účtu jsou však ve všech poštovních klientech velmi podobná.

Odchozí (osobní) e-mailová adresa
: Tato adresa by měla být tvořena jménem uživatele a doménou tak, jak je účet nastaven v *Kerio MailServeru*, tedy např. `novak@firma.cz`.

Jméno uživatele
: Může být nastaveno libovolně, slouží pouze pro zobrazení v hlavičce zprávy v klientovi. Doporučujeme ale nepoužívat v tomto jméně diakritiku, zejména pokud je známo, že uživatel bude komunikovat s partnery v zahraničí.
Toto jméno nemá žádnou souvislost s plným jménem či popisem uživatele v *Kerio MailServeru*. Slušný uživatel ale odesílá zprávy výhradně pod svým vlastním jménem!

Server odchozí pošty (SMTP)
: IP adresa nebo DNS jméno počítače, na němž *Kerio MailServer* běží (např. `192.168.1.1` nebo `mail.firma.cz`).

Server příchozí pošty
: Rovněž IP adresa nebo DNS jméno počítače, na němž *Kerio MailServer* běží (např. `192.168.1.1` nebo `mail.firma.cz`).

Typ serveru příchozí pošty
POP3 nebo IMAP. Běží-li na *Kerio MailServeru* obě služby, může si uživatel dle vlastního uvážení vybrat, který protokol bude používat (podle toho, co je pro něj výhodnější). Typ protokolu nelze již později změnit, pouze smazáním účtu a vytvořením nového. Je však třeba si uvědomit, že pokud bylo ke schránce dříve přistupováno protokolem IMAP, a nyní má být používán protokol POP3, nebude možno stáhnout zprávy z jiné složky než *INBOX*.

Uživatelské jméno a heslo
Jméno a heslo k uživatelskému účtu vytvořenému v *Kerio MailServeru*. Není-li účet vytvořen v primární doméně, musí se jako uživatelské jméno použít celá e-mailová adresa.

Ověření na odchozím (SMTP) serveru
Toto ověření je třeba nastavit, jestliže je v *Kerio MailServeru* zapnuta antispamová ochrana (kapitola 16) a řízení přístupu — z IP adresy klienta není povoleno odesílání pošty do libovolné domény (viz kapitolu 15.2). Jinak by klient mohl odesílat zprávy pouze do lokálních domén.

Odchozí, resp. příchozí server vyžaduje zabezpečení
Tyto volby určují, zda má být při odesílání, resp. příjmu pošty použito nešifrované spojení nebo spojení zabezpečené SSL. S *Kerio MailServerem* je možno použít v obou případech zabezpečené spojení (běží-li příslušné služby), což je doporučeno.

Bezpečné ověřování hesla (SPA/NTLM)
Tuto funkci je možno použít, jestliže se uživatel klientského počítače přihlašuje do NT domény a jeho účet v *Kerio MailServeru* je nastaven tak, aby byl ověřován v této doméně. Pak není nutné zadávat v klientovi heslo, místo něj se použijí stejné ověřovací údaje jako při přihlášení do domény.

Adresářová služba

Jako adresářovou službu je možno využít LDAP server v *Kerio MailServeru* (podrobnosti v kapitole 19).

Práce s IMAP složkami

Po vytvoření poštovního účtu používajícího protokol IMAP klient stáhne ze serveru seznam složek a zobrazí jej. Uživatel si může vybrat složky, které se mají zobrazovat (toto nastavení lze i později změnit). V klientovi může uživatel vytvářet, přejmenovávat a mazat složky, stejně jako v rozhraní *Kerio WebMail*. Vždy je ale třeba si uvědomit, že se jedná o složky na serveru, nikoliv o lokální složky klienta, jak je tomu při použití protokolu POP3!

Dále je třeba zajistit, aby poštovní klient i rozhraní *Kerio WebMail* používali stejné názvy složek pro odeslanou poštu (*Sent Items*) a koncepty zpráv (*Drafts*).

Poštovní klient také umožňuje nastavit u každé složky tzv. synchronizaci. Je-li složka synchronizována se serverem, znamená to, že každá nově příchozí zpráva se okamžitě zobrazí také na klientovi. To ale vyžaduje trvalé připojení klienta k serveru. Je-li klient např. připojen vytáčenou linkou, je možno provádět jednorázovou synchronizaci složek ručně nebo v určitých intervalech.

26.2 WWW prohlížeče

Podporované prohlížeče pro plnou verzi *Kerio WebMailu* jsou:

- *Internet Explorer* 6 a 7
- *Firefox* 1.5 a 2
- *Safari* 1.3, 2 a 3 na Mac OS X 10.5 Leopard

Ve starších verzích výše jmenovaných prohlížečů a ve všech ostatních typech není možné z technických důvodů spustit plnou verzi *Kerio WebMailu*, lze však spustit jeho zjednodušenou verzi *Kerio WebMail Mini*. *Kerio WebMail Mini* se automaticky spouští na všech typech starších prohlížečů, v prohlížečích založených na textovém režimu jako jsou například *Lynx* nebo *Links*, na PDA zařízeních, v mobilních telefonech, atd. *Kerio WebMail Mini* pro zobrazení nevyužívá CSS a JavaScript.

Chcete-li využívat zabezpečený přístup k rozhraní *Kerio WebMail* (protokolem HTTPS), musí prohlížeč podporovat zabezpečení SSL. Je-li možno jej konfigurovat (např. v prohlížeči Microsoft Internet Explorer), doporučuje se zapnout podporu verzí SSL 3.0 a TLS 1.0.

26.3 Firewall

Poměrně častým případem bývá, že je *Kerio MailServer* nainstalován v lokální síti chráněné firewallem, případně přímo na počítači, kde firewall běží. Správce systému pak musí, kromě vlastní konfigurace poštovního serveru, provést ještě některá doplňující nastavení.

Porty

Má-li být poštovní server přístupný z Internetu, je třeba ve firewallu otevřít (tzv. mapovat) některé porty. Obecně lze říci, že každý mapovaný port znamená díru v zabezpečení, a tedy čím méně mapovaných portů, tím lépe.

Při mapování portů pro *Kerio MailServer* je vhodné dodržet následující pravidla a doporučení:

- Port 25 musí být mapován, jestliže má být zvenčí přístupný SMTP server. To je nutné, je-li na tento server nasměrován primární MX záznam pro danou doménu (či více domén). V tomto případě je bezpodmínečně nutné nastavit antispamovou ochranu (viz kapitolu 16) a řízení přístupu (viz kapitolu 15.2), aby nemohlo dojít ke zneužití serveru. Na port SMTP serveru se může legálně připojit libovolný SMTP server v Internetu, chce-li odeslat e-mail do některé z lokálních domén. Z tohoto důvodu nesmí být na mapovaný port 25 omezen přístup pouze z vybrané skupiny IP adres.
  Je-li veškerá příchozí pošta pouze vybírána ze vzdálených POP3 schránek, není třeba port 25 mapovat.
- Porty ostatních služeb (*POP3*, *IMAP*, *HTTP*, LDAP a Secure LDAP) je třeba mapovat tehdy, pokud chtějí klienti přistupovat ke svým schránkám odjinud než z chráněné lokální sítě (typický případ je mobilní uživatel s notebookem). V tomto případě je silně doporučeno používat výhradně zabezpečené verze všech služeb a na firewallu povolit pouze porty pro tyto služby (tedy 636, 443, 993, 995).
- Je-li možné definovat subsítě či rozsahy IP adres, odkud se vzdálení klienti připojují, doporučuje se také omezit přístup k mapovaným portům pouze z těchto adres. Toto je bohužel nerealizovatelné, pokud se zmíněný mobilní uživatel pohybuje po celém světě a připojuje se náhodně k různým poskytovatelům Internetu.

Telefonické připojení

Běží-li *Kerio MailServer* a firewall na tomtéž počítači, který je připojen do Internetu vytáčenou linkou, může vzniknout požadavek, aby poštovní server používal jiné telefonické připojení (např. k jinému poskytovateli) než firewall pro přístup do Internetu. Pak ale firewall musí znát obě tato připojení — v opačném případě by blokoval pakety jdoucí připojením, které využívá poštovní server (firewall nesmí propustit žádný neznámý paket v žádném směru).

Kapitola 27

Příklady nastavení

Tato kapitola ukazuje na několika modelových příkladech praktické nasazení *Kerio MailServeru* v konkrétních podmínkách. Každý příklad je v podstatě aplikací postupu *Rychlé nastavení* (viz kapitolu 1.2) na danou situaci. Tyto příklady by vám měly pomoci rychle a jednoduše nasadit *Kerio MailServer* ve vaší firmě.

27.1 Trvalé připojení k Internetu

Informace a požadavky

1. Firma má vlastní doménu `firma.cz`, primární MX záznam je nasměrován na počítač, kde bude nainstalován *Kerio MailServer* (ten má v DNS přiřazeno jméno `mail.firma.cz`).

2. Připojení do Internetu je realizováno pevnou linkou.

3. Nadřazený SMTP server není k dispozici.

4. Firma má NT doménu `DOMENA`, uživatelé mají být ověřováni v této doméně.

5. Výrobní oddělení má mít speciální adresu `vyroba@firma.cz`, obchodní oddělení `obchod@firma.cz`

6. Někteří uživatelé si přejí, aby *Kerio MailServer* vybíral jejich soukromé schránky v Internetu a doručoval je do lokálních schránek.

7. Pro antivirovou kontrolu pošty má být použit program AVG 7.0, nesmějí být posílány žádné přílohy typu `EXE`, `COM`, `BAT` a `VBS`.

8. Vzdálená správa *Kerio MailServeru* smí být povolena pouze z adresy `67.34.112.2` (externí správce).

Realizace

1. V sekci *Konfigurace* → *Domény* vytvoříme primární lokální doménu `firma.cz` a zadáme internetové jméno serveru `mail.firma.cz`. V záložce *Ověřování* zadáme jméno NT domény `DOMENA`.

2. V sekci *Nastavení domény* → *Uživatelské účty* tlačítkem *Importovat* importujeme požadované uživatele z domény `DOMENA`. Tak nebude nutno definovat účty ručně.

3. V sekci *Nastavení domény* → *Skupiny* vytvoříme skupiny `Vyroba` a `Obchod` a zařadíme do nich příslušné uživatele.

4. V sekci *Nastavení domény* → *Aliasy* definujeme aliasy `vyroba` a `obchod` doručované příslušným skupinám uživatelů.

5. Připojení do Internetu je trvalé. V sekci *Konfigurace* → *Internetové připojení* tedy vybereme volbu *Online*.

6. Odchozí pošta bude odesílána přímo do cílových domén. V sekci *Konfigurace* → *SMTP server* v záložce *SMTP doručování* vybereme volbu *Doručovat přímo dle DNS MX záznamů*.

7. V sekci *Konfigurace* → *Stahování POP3 schránek* definujeme vybírání požadovaných externích schránek. U každé z nich vybereme uživatele, kterému má být její obsah doručován.

8. Nastavíme plánování pro vybírání vzdálených schránek. Pevná linka je rychlá a za připojení se nic neúčtuje, proto mohou být schránky vybírány poměrně často. Nastavíme plánování: *Každých 10 minut*. Odchozí e-maily jsou odesílány okamžitě a pomocí ETRN se žádná pošta nepřijímá — stačí tedy zaškrtnout akci *Stáhnout zprávy ze vzdálených POP3 schránek*.

9. V sekci *Konfigurace* → *Filtrování obsahu* → *Antivirus* povolíme antivirovou kontrolu a vybereme modul *AVG 7.0*. V sekci *Konfigurace* → *Filtrování obsahu — Filtrování příloh* povolíme filtrování a nastavíme názvy zakázaných souborů — tedy `*.exe`, `*.com`, `*.bat` a `*.vbs`.

10. V sekci *Konfigurace* → *Definice* → *Skupiny IP adres* vytvoříme skupinu `Vzdálená správa` a přidáme do ní jedinečnou IP adresu (*Počítač*) `67.34.112.2`.

11. V sekci *Konfigurace* → *Vzdálená správa* zaškrtneme volbu *Povolit vzdálenou správu po síti* i volbu *Pouze z této skupiny IP adres*. Zde vybereme vytvořenou skupinu *Vzdálená správa*.

27.2 Vytáčená linka + doménový koš

Informace a požadavky

1. Firma má vlastní doménu `jinafirma.cz`, veškeré zprávy poslané na tuto adresu jsou ukládány do doménové schránky `jinafirma` na serveru `pop3.poskytovatel.cz` s přístupovým heslem `heslo`.

2. Připojení do Internetu je realizováno vytáčenou linkou.

3. Poskytovatel Internetu umožňuje odesílat odchozí poštu přes svůj server

   `smtp.poskytovatel.cz`,

   jestliže se na něm odesílatel ověří jménem a heslem (shodné jako pro POP3).

4. V pracovní době (pondělí až pátek 8:00-17:00 hod) se má pošta stahovat každou hodinu, mimo pracovní dobu ve 20:00, 0:00 a 5:00 hod.

Realizace

1. V sekci *Konfigurace* → *Domény* vytvoříme primární lokální doménu `jinafirma.cz` a zadáme internetové jméno serveru `mail.jinafirma.cz` (to je v tomto případě víceméně fiktivní, ale obsahuje název naší domény). Tím, že je zde doména definována jako lokální, se dosáhne toho, že pošta posílaná mezi lokálními uživateli nebude odesílána do Internetu a odtud stahována zpět.

2. V sekci *Nastavení domény* → *Uživatelské účty* vytvoříme uživatelské účty všem lokálním uživatelům.

3. Server se bude připojovat do Internetu vytáčeným připojením (které je již v systému vytvořeno). V sekci *Konfigurace* → *Internetové připojení* vybereme volbu *Offline*, zaškrtneme volbu *Použít vytáčené připojení do Internetu*, vybereme požadovanou položku telefonického připojení (RAS) a zadáme příslušné jméno a heslo pro toto připojení.

4. Veškerá odchozí pošta bude odesílána přes nadřazený SMTP server. V sekci *Konfigurace* → *SMTP server* v záložce *SMTP doručování* vybereme volbu *Použít nadřazený SMTP server* a zadáme jeho jméno — `smtp.poskytovatel.cz`. Server vyžaduje ověření, proto zapneme volbu *Nadřazený server vyžaduje ověřování* a vyplníme zde příslušné jméno a heslo. Typ ověřování nastavíme *Příkaz SMTP AUTH* (přihlášení na SMTP server).

5. V sekci *Konfigurace* → *Stahování POP3 schránek*, záložka *Účty*, definujeme vybírání doménové schránky jinafirma na serveru `pop3.poskytovatel.cz`. Zprávy z této schránky mají být rozdělovány podle třídicích pravidel — zvolíme *Použít třídicí pravidla*. Výběr preferované hlavičky doporučujeme konzultovat se správcem serveru, na němž schránka leží. Výchozí hlavička *Received* by ale měla vyhovět ve většině situací.

6. V sekci *Konfigurace* → *Stahování POP3 schránek*, záložka *Třídicí pravidla*, nastavíme třídicí pravidla pro e-mailové adresy jednotlivých uživatelů.

7. V sekci *Konfigurace* → *Definice* → *Časové intervaly* si vytvoříme časový interval *Pracovní doba*, obsahující rozsah hodin 8:00-17:00 a platný ve dnech Po-Pá, který využijeme při definici plánování.

8. Nastavíme plánování pro vybírání POP3 schránky a odesílání zpráv z odchozí fronty: Přidáme jedno plánování pro každou hodinu (*Každých 1 hodin*) platné v intervalu *Pracovní doba* a tři plánování pro konkrétní časy (*V*), platné vždy. U všech plánování zaškrtneme nejen volbu *Stáhnout zprávy ze vzdálených POP3 schránek*, ale také *Odeslat zprávy z odchozí fronty*, aby se odeslaly všechny případné odchozí zprávy.

27.3 Vytáčená linka + ETRN

Informace a požadavky

1. Firma má vlastní doménu `tretifirma.cz`, primární MX záznam je nasměrován na počítač, kde bude nainstalován *Kerio MailServer* (ten má v DNS přiřazeno jméno `mail.tretifirma.cz`).

2. Sekundární MX záznam pro doménu je nasměrován na SMTP server

   `etrn.poskytovatel.cz`,

   který podporuje příkaz ETRN a vyžaduje ověření jménem a heslem.

3. Připojení do Internetu je realizováno vytáčenou linkou (přiděluje se pevná IP adresa, na niž je v DNS nastaveno jméno `mail.tretifirma.cz`).

4. Poskytovatel Internetu umožňuje odesílat odchozí poštu přes svůj server

   `smtp.poskytovatel.cz`,

   jestliže se na něm odesílatel ověří jménem a heslem.

5. V pracovní době (pondělí až pátek 8:00-17:00 hod) se má pošta stahovat každou hodinu, mimo pracovní dobu ve 20:00, 0:00 a 5:00 hod.

Realizace

1. V sekci *Konfigurace* → *Domény* vytvoříme primární lokální doménu `tretifirma.cz` a zadáme internetové jméno serveru `mail.tretifirma.cz`. V době, kdy bude linka vytočena, bude *Kerio MailServer* fungovat jako primární server této domény. Bude-li linka zavěšena, e-maily budou posílány na sekundární server.

2. V sekci *Nastavení domény* → *Uživatelské účty* vytvoříme uživatelské účty všem lokálním uživatelům.

3. Server se bude připojovat do Internetu vytáčeným připojením (které je již v systému vytvořeno). V sekci *Konfigurace* → *Internetové připojení* vybereme volbu *Offline*, zaškrtneme volbu *Použít vytáčené připojení k Internetu*, vybereme požadovanou položku telefonického připojení (RAS) a zadáme příslušné jméno a heslo pro toto připojení.

4. Veškerá odchozí pošta bude odesílána přes nadřazený SMTP server. V sekci *Konfigurace* → *SMTP server* v záložce *SMTP doručování* vybereme volbu *Použít nadřazený SMTP server* a zadáme jeho jméno — `smtp.poskytovatel.cz`. Server vyžaduje ověření, proto zapneme volbu *Nadřazený server vyžaduje ověřování* a vyplníme zde příslušné jméno a heslo. Typ ověřování nastavíme *Příkaz SMTP AUTH* (přihlášení na SMTP server).

5. V sekci *Konfigurace* → *Příjem pomocí ETRN*, definujeme položku:

   server: `etrn.poskytovatel.cz`,

   doména: `tretifirma.cz`,

   Server vyžaduje ověření, zadáme příslušné jméno a heslo.

6. V sekci *Konfigurace* → *Definice* → *Časové intervaly* si vytvoříme časový interval *Pracovní doba*, obsahující rozsah hodin 8:00:00-17:00:00 a platný ve dnech pondělí až pátek, který využijeme při definici plánování.

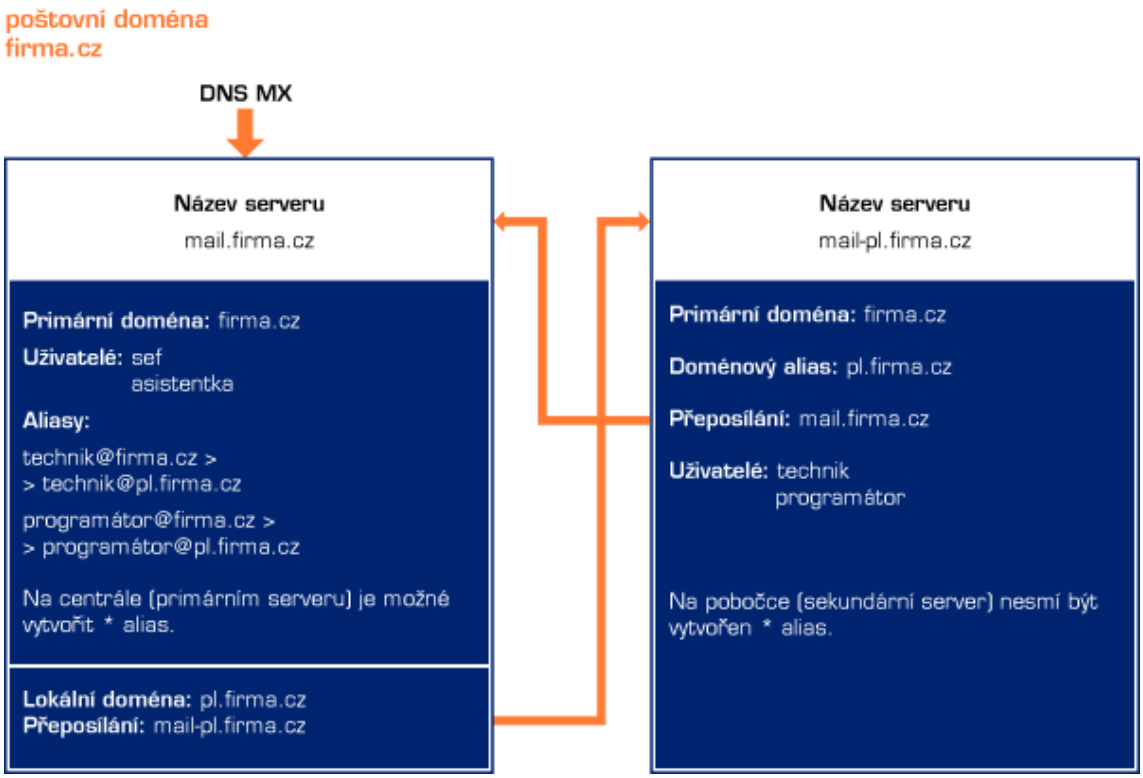
7. Nastavíme plánování pro příjem a odesílání zpráv: Přidáme jedno plánování pro každou hodinu (*Každých 1 hodin*) platné v intervalu *Pracovní doba* a tři plánování pro konkrétní časy (*V*), platné vždy. U všech plánování zaškrtneme nejen volbu *Poslat příkaz ETRN na definované SMTP servery*, ale také *Odeslat zprávy z odchozí fronty*, aby se odeslaly všechny případné odchozí zprávy.

27.4 Firma s pobočkou

Informace a požadavky

Firma má jednu doménu `firma.cz`. Centrála firmy sídlí v Praze a pobočka v Plzni. V centrále i na pobočce je nainstalován *Kerio MailServer* (dvě samostatné licence). Server v centrále firmy má DNS jméno `mail.firma.cz`, server pobočky jméno `mail-pl.firma.cz`.

Základním požadavkem je, aby pošta posílaná mezi lokálními uživateli na pobočce byla doručována lokálně, zatímco pošta určená uživatelům v centrále byla správně odesílána na centrálu. Stejná funkčnost musí být zajištěna i v opačném směru — tedy zpráva odeslaná z centrály na pobočku musí být doručena na server pobočky.



Obrázek 27.1 Firma s pobočkou

Poznámka: Pro jednoduchost a větší názornost předpokládejme, že v centrále budou pracovat uživatelé `sef` a `asistentka` a na pobočce uživatelé `technik` a `programator`. Následující popis se zabývá pouze kroky nutnými pro splnění těchto požadavků — není zde tedy popsáno detailní nastavení parametrů SMTP serveru, vzdálené správy apod.

Realizace

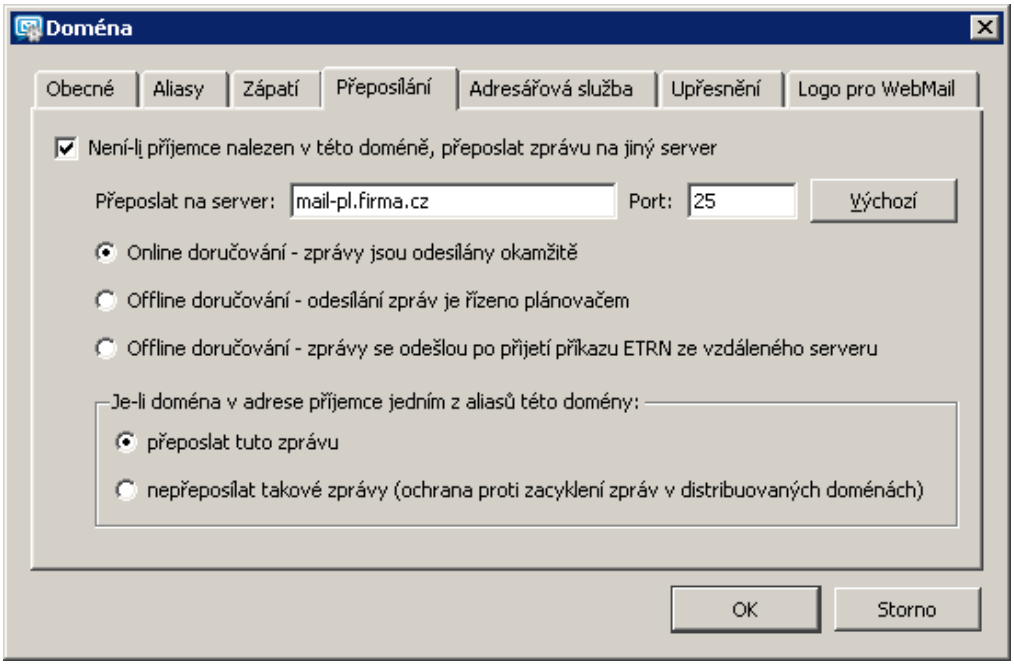
Centrála (nastavení na primárním serveru `mail.firma.cz`)

1. V *Kerio MailServeru* v centrále firmy (tedy na primárním serveru `mail.firma.cz`) definujeme doménu `firma.cz` jako lokální primární.

2. V této doméně definujeme účty lokálním uživatelům (tj. těm, kteří pracují v centrále).

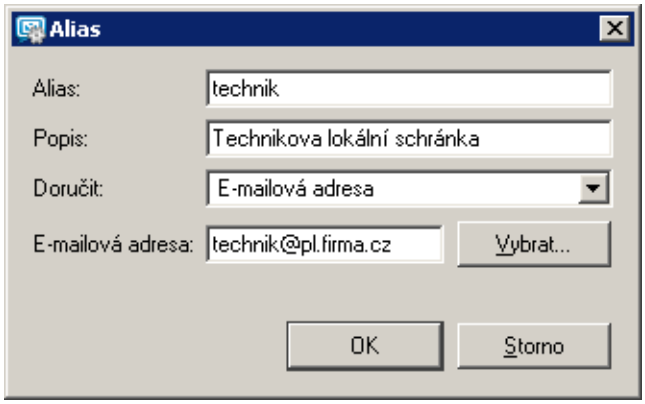
3. Je-li *Kerio MailServer* chráněn firewallem, je třeba zpřístupnit port `25` pro službu SMTP.

4. Vytvoříme doménu `pl.firma.cz`, kde nebudou definováni uživatelé ani aliasy. Nastavením záložky *Přeposílání* v sekci *Domény* zajistíme, aby pošta pro doménu `pl.firma.cz` byla přeposílána na server pobočky `mail-pl.firma.cz` (viz obrázek 27.2).



Obrázek 27.2 Nastavení přeposílání

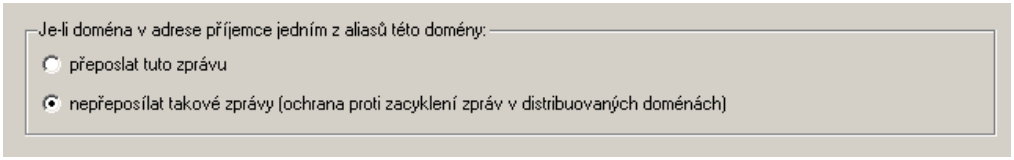
5. Dále nastavíme aliasy pro všechny uživatele na pobočce (*Nastavení domény* → *Aliasy*), v našem případě uživatele `technik` a `programator`. Tyto aliasy zajistí, aby pošta pro příslušné uživatele byla doručována do domény `pl.firma.cz`.



Obrázek 27.3 Nastavení aliasu

Pobočka (nastavení na serveru `mail-pl.firma.cz`)

1. Vytvoříme lokální primární doménu `firma.cz`, která bude mít alias `pl.firma.cz`.
2. V lokální primární doméně vytvoříme účty všem uživatelům z této pobočky (tzn. těm, kteří mají mít na pobočce lokální schránku).
3. Nastavíme, aby pošta pro doménu `firma.cz` byla přeposílána na server centrály `mail.firma.cz`, přičemž nastavíme, že zprávy s doménovým aliasem v adrese příjemce se nemají přeposílat. Tato volba umožňuje zachytit zprávy, které nemají v adrese příjemce správně uvedeno uživatelské jméno nebo jeho alias.



Obrázek 27.4 Nastavení ochrany proti zacyklení zpráv

Upozornění: Na pobočkových serverech nesmí být použit hvězdičkový alias, jinak se pošta pro centrálu nebude přeposílat.

Doporučení: Na pobočkový server nastavte sekundární DNS MX záznam, čímž vyřešíte případný výpadek centrály (primárního serveru).

Poznámky:

- Budou-li uživatelé chtít přistupovat k poště vzdáleně (např. pomocí rozhraní *Kerio WebMail*), budou vždy přistupovat na ten server, kde mají vytvořeny své lokální schránky (tj. uživatelé z centrály na server `mail.firma.cz` a uživatelé z pobočky na server `mail-pl.firma.cz`).
- *Free/Busy* kalendář bude zobrazovat pouze informace o lokálních uživatelích daného serveru.

27.5 Nastavení záložního poštovního serveru

Informace a požadavky

1. Firma má vlastní doménu `firma.cz`, primární MX záznam je nasměrován na počítač, kde je nainstalován primární poštovní server. Ten má v DNS přiřazeno jméno `mail1.firma.cz`.

2. K primárnímu poštovnímu serveru je třeba vytvořit a nastavit záložní (ten bude mít v DNS přiřazeno jméno `mail2.firma.cz`). K těmto účelům použijeme základní verzi *Kerio MailServeru*, protože zde není nutné vytvářet žádné uživatelské účty.

Realizace

1. V DNS je nutno poštovní doméně `firma.cz` vytvořit sekundární MX záznam (s nižší prioritou) pro jméno záložního serveru (`mail2.firma.cz`).

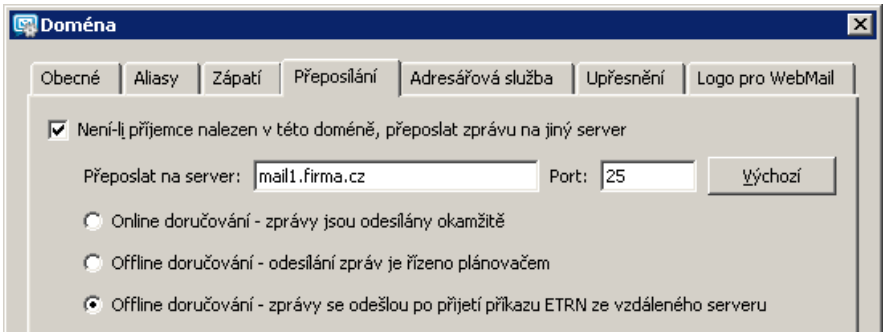
2. Po instalaci záložního *Kerio MailServeru* vytvoříme v konfiguračním průvodci primární doménu a nazveme ji stejně jako na primárním poštovním serveru, tedy `firma.cz`.

3. Této doméně nenastavujeme žádné uživatelské účty.

4. V administrační konzoli *Kerio MailServeru* v sekci *Konfigurace* → *Domény* (kapitola 7.5) je nutno nastavit přeposílání pošty na primární poštovní server `mail1.firma.cz` (viz obrázek 27.5).

   Přeposílání pošty je možno provádět několika způsoby:

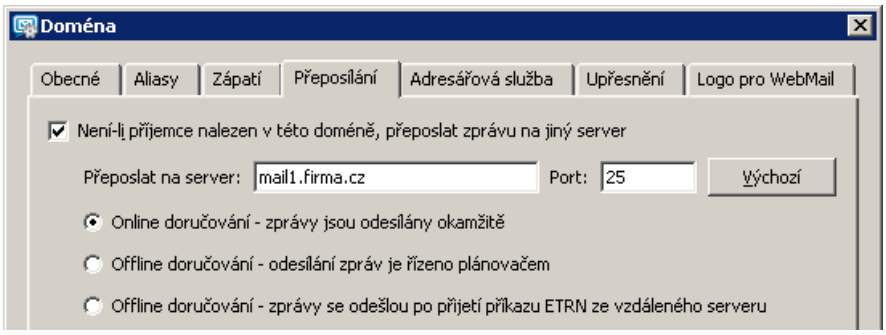
   - Doporučeným způsobem, jak nastavit přeposílání pošty ze záložního serveru je nastavení primárního serveru tak, aby se pravidelně dotazoval na sekundární server příkazem ETRN. Tato varianta nezatěžuje servery zbytečným připojováním k nedostupnému primárnímu serveru. Jedinou podmínkou je, aby primární server podporoval příjem pošty pomocí příkazu ETRN.
     Kerio MailServer podporuje příkaz ETRN pro vyžádání pošty (viz kapitolu 15.5), takže pokud používáte *Kerio MailServer* jako primární poštovní server, důrazně doporučujeme tuto variantu nastavení. *Kerio MailServer* navíc vysílá ETRN příkaz na nastavené servery při každém spuštění serveru, čímž je zajištěno, že se pošta na server dostane v nejkratší možné době po výpadku.
     Chcete-li využít tuto metodu přeposílání pošty, pak na záložním serveru stačí v administrační konzoli (*Konfigurace* → *Domény*) povolit pro doménu `firma.cz` volbu *Offline doručování — zprávy se odešlou po přijetí příkazu ETRN ze vzdáleného serveru* (viz obrázek 27.5).



Obrázek 27.5 Nastavení záložního serveru — příkaz ETRN

Na primárním poštovním serveru je samozřejmě nutné nastavit používání příkazu ETRN (viz kapitolu 15.5) a plánování vysílání příkazu ETRN (viz kapitolu 9).

- Méně výhodnou možností je nastavení pravidel pro odchozí frontu zpráv (viz kapitolu 15.2). Negativem tohoto nastavení je, že v případě nedostupnosti primárního serveru se bude server v nastavených intervalech snažit opakovaně doručovat poštu, dokud nebude primární server opět dostupný, což může v některých případech způsobit i zahlcení primárního serveru.
  Preferujete-li i přes výše zmíněný nedostatek tento způsob nastavení sekundárního SMTP serveru, doporučujeme prodloužení intervalu opakování odesílání zpráv. Nastavení lze provést v sekci *Konfigurace* → *SMTP Server* v záložce *Volby pro frontu zpráv*.

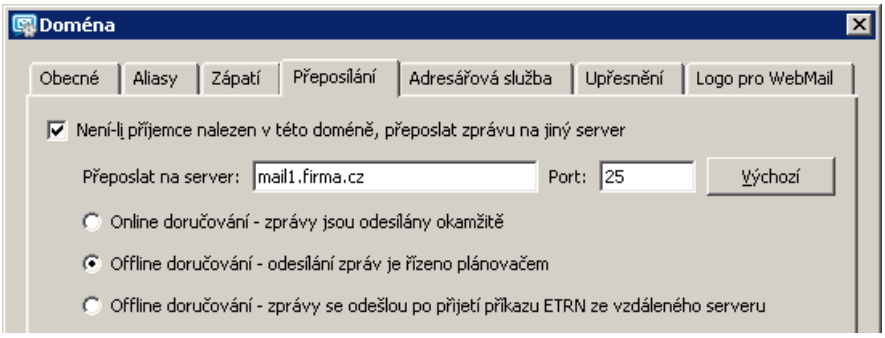


Obrázek 27.6 Nastavení záložního serveru —doručování pošty je řízeno pravidly pro odchozí frontu zpráv

V okně pro konfiguraci domény je nutné nastavit jméno nebo adresu primárního serveru, port pro komunikaci a volbu *Online doručování — zprávy jsou odesílány okamžitě* (viz obrázek 27.6).

- Třetí řešení je pouze obměnou předcházejícího. Server pro odesílání pošty použije, stejně jako v předchozím případě, pravidla pro odchozí frontu zpráv, ale interval opakování doručování pošty bude definován pomocí plánovače. Výhodou tohoto řešení je možnost vytvořit podrobný plán odesílání pošty.
  Pro tento způsob doručování pošty musí být povolena v sekci *Konfigurace* → *Domény* možnost *Offline doručování — odesílání zpráv je řízeno plánovačem* (viz

obrázek 27.7) a zároveň je nutno správně nastavit plánovač (nastavení plánovače popisuje kapitola 9.)



Obrázek 27.7 Nastavení záložního serveru — doručování pošty je řízeno plánovačem

5. Je-li jako primární poštovní server používán *Kerio MailServer*, doporučujeme v sekci *Konfigurace* → *SMTP server* v záložce *Bezpečnostní volby* přidat adresu sekundárního SMTP serveru do seznamu, pro který neplatí omezení nastavená v této záložce (více viz kapitolu 15.2).

Kapitola 28

Řešení možných problémů v Kerio MailServeru

28.1 Reindexace poštovních složek

Problém

Uživatel má problém se zobrazením poštovní složky nebo dokonce celého mailboxu. Poškozená složka se jeví jako prázdná nebo jsou v ní zobrazeny jen některé zprávy.

Velmi pravděpodobnou příčinou tohoto problému je nesouhlasící obsah speciálního souboru `index.fld` s adresářem `#msgs` v některé z poštovních složek *Kerio MailServeru*.

Pro lepší orientaci v celém problému si musíme nejprve vysvětlit, jak *Kerio MailServer* pracuje se zprávami. E-mailové zprávy, kontakty, události, úkoly a poznámky jsou fyzicky ukládány do úložiště ve formě stromové struktury složek. Tímto úložištěm je adresář `\store`, který se dále člení na domény, poštovní schránky uživatelů a složky v těchto schránkách. Každá poštovní složka obsahuje několik adresářů a souborů, kam jsou fyzicky ukládány e-mailové zprávy a také různé informace o nich.

Pro nás je důležitý adresář `#msgs`, kam jsou fyzicky ukládány zprávy ve formátu `.eml` souborů a speciální soubor `index.fld`, pomocí kterého se *Kerio MailServer* orientuje v adresáři `#msgs` při komunikaci s poštovními klienty. Tento soubor se vytváří pro každou poštovní složku hned při prvním spuštění *Kerio MailServeru*.

Soubor `index.fld` obsahuje seznam zpráv, které daná složka obsahuje, a specifické informace k nim. Každý řádek v souboru představuje záznam o jedné e-mailové zprávě, která je ve složce uložena.

Soubor `index.fld` a adresář `#msgs` jsou oba uloženy v každé složce, kterou má uživatel ve schránce vytvořenu. Jako příklad si můžeme uvést následující cestu:

```
\Kerio\MailServer\store\mail\firma.cz\jnovak\INBOX
```

Řešení

Následující řešení je velmi jednoduché:

1. Zastavíme *Kerio MailServer Engine*.
2. V úložišti *Kerio MailServeru*, v adresáři `store` najdeme doménu uživatele, který má problémy s některou ze svých složek. V této složce najdeme a otevřeme složku nazvanou jeho/jejím uživatelským jménem. Tato složka fyzicky obsahuje celou poštovní schránku. Podsložky, které si uživatelé sami vytvořili jsou vnořeny do hlavních

složek — jsou uspořádány ve stejné hierarchii jako se zobrazují v rozhraní *Kerio WebMail*.

3. Ze složek vybereme tu, se kterou měl uživatel problémy, otevřeme ji a přejmenujeme soubor `index.fld` na `index.bad`

4. Spustíme *Kerio MailServer Engine*.

Při prvním následném přihlášení uživatele k jeho schránce se soubor automaticky znovu vytvoří — tentokráte podle aktuálního stavu složky a zároveň převezme flagy (příznaky zpráv, které zobrazují například zda zpráva nebyla označena jako smazaná, nebo zda byla přeposlána) z původního souboru přejmenovaného na `index.bad`.

Po spuštění *Kerio MailServeru* se v záznamu *Error* objeví záznam:

```
[23/Jun/2005 12:12:47] mail_folder.cpp: Folder
~jnovak@firma.cz/Contacts has corrupted status and index files,
going to restore them. Some flag information may be lost
```

28.2 Zálohování a přenos konfigurace

Veškeré konfigurační informace *Kerio MailServeru* jsou nezávislé na operačním systému a jsou uloženy ve dvou souborech v adresáři, kde je *Kerio MailServer* nainstalován:

users.cfg a users.cfg.bak
: Informace o uživatelských účtech, skupinách a aliasech. Je-li soubor poškozen a *Kerio MailServer* jej již nedovede přečíst, je možné nahradit jej zálohou `users.cfg.bak`. Stačí pouze přejmenovat jej na `users.cfg`.

mailserver.cfg a mailserver.cfg.bak
: Všechny ostatní konfigurační parametry. Je-li soubor poškozen a *Kerio MailServer* jej nedovede přečíst, je možné nahradit jej zálohou `mailserver.cfg.bak`. Stačí pouze přejmenovat ho na `mailserver.cfg`.

Upozornění: Na systémech *Mac OS X* a *Linux* lze s konfiguračními soubory manipulovat pouze pokud je uživatel přihlášen jako root.

Údaje v těchto dvou souborech jsou uloženy ve formátu XML v kódování UTF-8. Zkušený uživatel je tedy může poměrně snadno ručně modifikovat, případně automaticky generovat vlastní aplikací. Zálohu či přenos konfigurace lze provést pouhým zkopírováním těchto souborů.

Před přenosem konfigurace doporučujeme zazálohovat také adresáře `sslcert` a `license` (standardně jsou uloženy v adresáři, kde je *Kerio MailServer* nainstalován). Adresář `license` obsahuje soubor `license.key` s licenčním klíčem *Kerio MailServeru*. Zapomenete-li pořídit kopii zálohy, lze licenční klíč znovu stáhnout na produktových

stránkách společnosti *Kerio Technologies*. Ke stažení licenčního klíče je potřeba pouze zadat na stránce `https://secure.kerio.com/reg` registrační číslo produktu. Toto řešení nedoporučujeme využívat příliš často, protože počet stažení licenčního klíče je omezen. Dále je potřeba zálohovat také adresář `myspell`, pokud využíváte jiné než výchozí slovníky pro kontrolu pravopisu v rozhraní *Kerio WebMail* (o slovnících myspell se dozvíte více v sekci 11.3).

Adresář `sslcert` obsahuje údaje o SSL certifikátu, který je používán. Nepořídíte-li zálohu tohoto adresáře před přenosem konfigurace, nebude možno v nové instalaci spustit žádnou ze zabezpečených služeb. V tomto případě volejte technickou podporu společnosti *Kerio Technologies* (kontakt na technickou podporu najdete v kapitole 43.1).

Upozornění: Před jakoukoliv manipulací s konfiguračními soubory je doporučeno zastavit *Kerio MailServer Engine*! Konfigurační soubory jsou totiž načítány pouze při jeho spuštění. Ukládány jsou při provedení jakékoliv změny v konfiguraci a při zastavení *Engine*. Změny, které byly v konfiguračních souborech provedeny za běhu *Engine*, budou při jeho zastavení přepsány konfigurací v operační paměti.

Obnovení konfigurace ze zálohy

Chceme-li použít dříve uloženou zálohu konfigurace *Kerio MailServeru* (typicky při přenosu na jiný počítač nebo po přeinstalování operačního systému) budeme postupovat následovně:

1. Na vybraný počítač nainstalujeme *Kerio MailServer* (viz kapitolu 2.4)
2. Zastavíme *Kerio MailServer Engine*
3. Do instalačního adresáře *Kerio MailServeru* zkopírujeme ze zálohy soubory `mailserver.cfg` a `users.cfg`, případně adresáře `sslcert`, `license` a soubory adresáře `myspell`.
4. Spustíme *Kerio MailServer Engine*

Kapitola 29

Kerio Active Directory Extensions

Active Directory Extensions je rozšíření adresářové služby *Microsoft Active Directory* (dále jen *Active Directory*) o položky obsahující specifické informace pro *Kerio MailServer*. Instalací rozšíření lze integrovat část *Kerio MailServeru* do *Active Directory*, a zjednodušit tak administrační úkony spojené se správou uživatelů.

V praxi přinese instalace *Kerio Active Directory Extensions* následující výhody:

Jednotná správa účtů
: *Kerio MailServer* může kromě vlastní (interní) databáze uživatelských účtů pracovat také s účty a skupinami, které jsou uloženy v LDAP databázi (v současné době *Microsoft Active Directory*). Výhodou použití LDAP je, že jsou uživatelské účty udržovány na jednom místě, čímž se výrazně snižuje administrativní náročnost a pravděpodobnost vzniku chyb.

Online spolupráce *Kerio MailServer* a *Microsoft Active Directory*
: Vytvoření, změna nebo zrušení uživatelského účtu (resp. skupiny) v databázi *Microsoft Active Directory* se okamžitě promítnou do aplikace *Kerio MailServer*.

Příklad: Firma používá *Windows 2000* doménu a *Kerio MailServer*. Do firmy byl přijat nový zaměstnanec. Dosavadní postup byl následující:

1. Vytvořit uživatelský účet v *Active Directory*.
2. Importovat uživatele do *Kerio MailServeru* (nebo zde založit účet stejného jména a nastavit ověřování pomocí systému Kerberos).

Při použití LDAP databáze stačí provést pouze krok *1*. Po instalaci *Kerio Active Directory Extensions* je dialog pro přidání uživatelského účtu rozšířen o záložku, ve které lze doplnit specifické informace pro *Kerio MailServer* (e-mailové adresy, přeposílání, kvótu atd.).

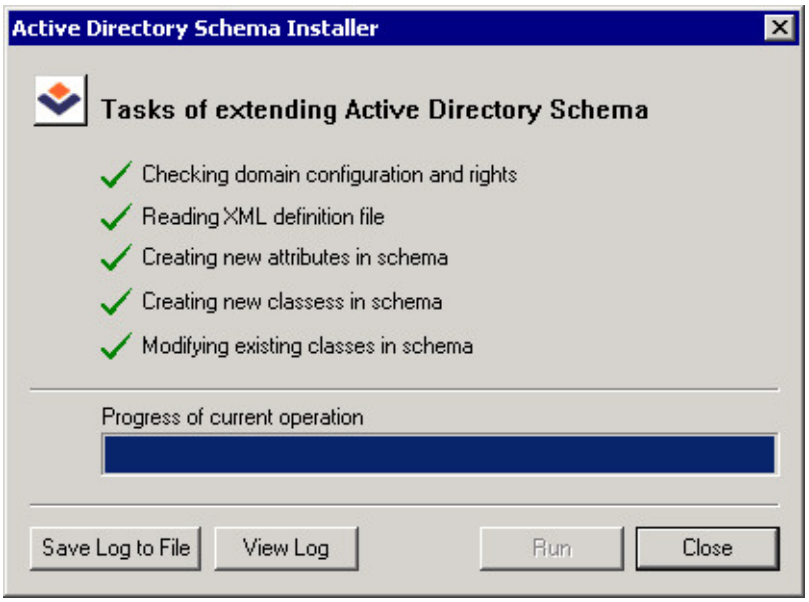
Účet tedy vytvoříte pouze jednou — v databázi *Active Directory*. *Kerio MailServer* a *Microsoft Active Directory* spolupracují online, účet v *Kerio MailServeru* již není třeba vytvářet.

Upozornění:

- Pokud účet vytvoříte v programu *Kerio Administration Console*, zobrazí se upozornění, že účet bude vytvořen pouze lokálně — nebude tedy duplikován do databáze *Active Directory*.
- V případě nedostupnosti *Active Directory* serveru nebude možné se k aplikaci *Kerio MailServer* přihlásit. Pro tento případ doporučujeme vytvořit alespoň jeden lokální administrativní účet s právy pro čtení i zápis.
- Při zakládání uživatelského účtu je nutno uživatelské jméno zapsat v ASCII. Pokud bude uživatelské jméno obsahovat národní znaky, může se stát, že se uživatel nebude moci přihlásit ke svému účtu.

29.1 Instalace Active Directory Extensions

Instalace *Active Directory Extensions* je standardně prováděna pomocí průvodce. Po odsouhlasení licenčních podmínek je možno vybrat cílový adresář. V dalším kroku se objeví okno zobrazující průběh instalace. V levém dolním rohu okna jsou umístěna tlačítka pro zobrazení záznamu o instalaci (*View Log*) a jeho uložení do souboru (*Save Log to File*).



Obrázek 29.1 Průběh instalace

Poznámky:

1. V závislosti na instalované verzi prohlížeče *Microsoft Internet Explorer* můžete být ještě vyzváni k instalaci komponenty *Microsoft XML Parser*. Pokud se tato výzva objeví, je třeba *Microsoft XML Parser* nainstalovat, jinak nemůže být instalace *Kerio Active Directory Extensions* dokončena!

2. *Kerio Active Directory Extensions* je k dispozici pouze v anglickém jazyce.

Systémové požadavky

Active Directory Extensions podporuje ve *Windows 2000 Server* typy *Active Directory NT compatible* i *2000 native*. Ve *Windows 2003* typy *Active Directory 2000 native* a *Active Directory 2003*.

29.2 Active Directory

Active Directory je adresářová služba, která uchovává informace o objektech v síti *Microsoft Network* (uživatelích, skupinách, počítačích atd.). Aplikace podporující *Active Directory* si pomocí této adresářové služby zjišťují parametry a práva objektů. Základem *Active Directory* je strukturovaná databáze.

Uživatele a skupiny v doméně jsou provázány s LDAP databází *Active Directory*. Výhodou použití LDAP je, že jsou uživatelské účty udržovány na jednom místě, čímž se výrazně snižuje administrativní náročnost a pravděpodobnost vzniku chyb (viz kapitolu 7.6). Uživatelé i skupiny je nutno přidávat pomocí *MMC* (*Microsoft Management Console*). Nový uživatel či skupina přidaná do domény provázané s *Active Directory* pomocí *Kerio Administration Console* se uloží pouze do lokální databáze *Kerio MailServeru*.

MMC spustíme z menu *Start* → *Nastavení* → *Ovládací panely* → *Nástroje pro správu* → *Uživatelé a počítačové služby Active Directory* (*Start* → *Settings* → *Control Panel* → *Administrative tools* → *Active Directory Users And Computers*).

29.3 Definice uživatelského účtu

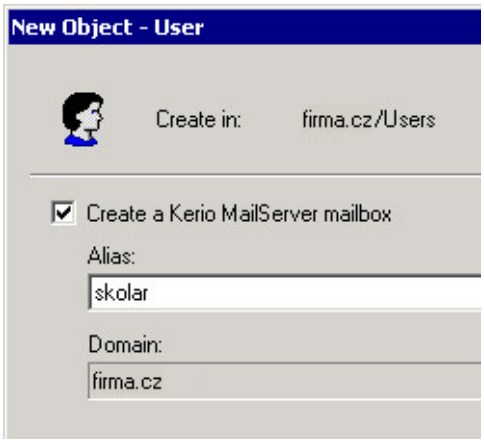
V konzoli *Uživatelé a počítačové služby Active Directory* zvolíme sekci *Uživatelé* (*Users*). Volbou *Nový* → *Uživatel* (*New* → *User*) spustíme průvodce pro vytvoření nového uživatelského účtu.

Upozornění: Při zakládání uživatelského účtu je nutno uživatelské jméno zapsat v ASCII. Pokud bude uživatelské jméno obsahovat národní znaky, může se stát, že se uživatel nebude moci přihlásit ke svému účtu.

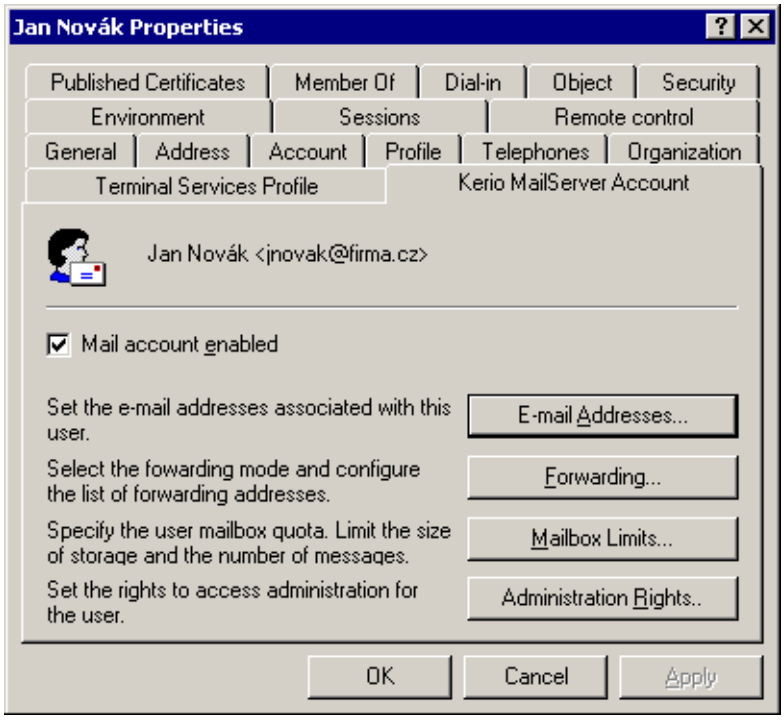
Standardní průvodce je rozšířen o novou záložku pro vytvoření *Kerio MailServer* účtu.

Nyní je třeba zaškrtnout volbu *Create a Kerio MailServer mailbox*, aby byly vytvořeny položky databáze, s nimiž bude *Kerio MailServer* pracovat. Položka *Alias* slouží k nastavení základní e-mailové adresy uživatele (do této položky je automaticky dosazováno přihlašovací jméno uživatele zadané v prvním kroku průvodce).

Další parametry účtu je možno nastavit v jeho vlastnostech. Na vytvořený uživatelský účet klikneme pravým tlačítkem myši a v kontextovém menu zvolíme *Vlastnosti* (*Properties*). V dialogu vybereme záložku *Kerio MailServer Account*, která nabízí následující volby:



Obrázek 29.2 Nastavení Kerio MailServer účtu



Obrázek 29.3 Záložka Kerio MailServer Account

Mail Account Enabled

Zapnutí volby povoluje e-mailový účet v *Kerio MailServeru*. Bude-li volba vypnuta, *Kerio MailServer* bude tento uživatelský účet ignorovat.

E-mail Addresses

Nastavení e-mailových adres (aliasů) pro daného uživatele. Ve výchozím nastavení má uživatel přiřazenu jednu e-mailovou adresu tvořenou jeho uživatelským jménem a doménou, v níž je účet definován.

Forwarding

Nastavení přesměrování pošty na zadané e-mailové adresy. Volba *Forward to:* způsobí přeposílání zpráv pro daného uživatele na všechny adresy uvedené v tomto poli.

Volba *Deliver messages to both* způsobí, že pošta bude nejen přesměrována, ale zároveň také ukládána do lokální schránky (tzn. zasílání kopií zpráv na zadané adresy).

Mailbox Limits

Nastavení omezení schránky dle velikosti místa na disku serveru (*Storage size*) a počtu zpráv ve schránce (*Number of messages*). Každý z těchto limitů je možno vypnout (volba *Do not limit...*) — pak se na schránku příslušné omezení nevztahuje.

Obrázek 29.4 Nastavení omezení schránky

Administration Rights

Nastavení přístupových práv uživatele ke správě *Kerio MailServeru*. Možnosti jsou následující:

- *No access to administration* — bez přístupu ke správě. Tato volba je výchozí a vyhovuje ve většině případů (běžní uživatelé by neměli mít přístup ke správě serveru). Pro správu *Kerio MailServeru* doporučujeme vytvořit lokální účet (viz kapitola 13), aby bylo možno *Kerio MailServer* spravovat i v případě výpadku sítě či *Active Directory* serveru.
- *Read only access to administration* — přístup pouze pro čtení. Uživatel se může k serveru přihlásit pomocí *Kerio Administration Console* a prohlížet si nastavení, nemůže ale provádět žádné změny.
- *Read/write access to administration* — plný přístup ke správě. Uživatel může provádět veškeré administrační úkony. Toto právo by mělo být uděleno jen velmi omezenému počtu osob.

29.4 Definice skupiny

Z hlediska *Kerio Active Directory Extensions* je definice skupiny téměř identická s definicí uživatelského účtu. Průvodce vytvořením skupiny je rovněž rozšířen o jeden krok, v němž je možno skupině přiřadit primární e-mailovou adresu.

Záložka *Kerio MailServer Account* umožňuje pouze definici e-mailových adres skupiny (tlačítko *E-Mail Addresses*) a nastavení přístupových práv ke správě *Kerio MailServeru* (tlačítko *Administration Rights*.).

Podrobné informace najdete v kapitole 29.3.

Kapitola 30

Kerio Open Directory Extensions

Kerio Open Directory Extensions je rozšíření adresářové služby *Apple Open Directory* o možnost mapování účtů do *Kerio MailServeru* (rozšiřuje schéma LDAP databáze o položky *Kerio MailServeru*). V praxi to znamená, že při vytváření, změnách nebo rušení uživatelských účtů a skupin v databázi *Apple Open Directory* se změny okamžitě promítnou do *Kerio MailServeru*.

Upozornění:

- Pokud účet vytvoříte v programu *Kerio Administration Console*, zobrazí se upozornění, že účet bude vytvořen pouze lokálně — nebude tedy duplikován do databáze *Open Directory*.
- V případě nedostupnosti *Open Directory* serveru nebude možné se k aplikaci *Kerio MailServer* přihlásit. Pro tento případ doporučujeme vytvořit alespoň jeden lokální administrativní účet s právy pro čtení i zápis.
- Při zakládání uživatelského účtu v *Apple Open Directory* je nutno uživatelské jméno zapsat v ASCII. Pokud bude uživatelské jméno obsahovat národní znaky, může se stát, že se uživatel nebude moci přihlásit ke svému účtu.

30.1 Instalace Kerio Open Directory Extensions

Instalační balík s *Kerio Open Directory Extensions* je možno získat zdarma na produktových stránkách společnosti *Kerio Technologies*.

Instalace *Kerio Open Directory Extensions* probíhá standardně pomocí průvodce.

Při použití konfigurace Mac OS X serverů typu *Master/Replica* je nutné *Kerio Open Directory Extensions* nainstalovat jak na *master* server, tak na všechny jeho *replica* servery. V opačném případě nebude mapování účtů funkční.

Systémové požadavky

Kerio Open Directory Extensions lze od verze 6.1 nainstalovat na operační systém *Mac OS X 10.3 (Panther)* a vyšší.

30.2 Apple Open Directory

Apple Open Directory je adresářová služba standardně dodávaná se systémy *Mac OS X Server*. Tato adresářová služba je obdobou *Active Directory* firmy *Microsoft*. Stejně jako *Active Directory* umožňuje uchovávat informace o objektech v síti (uživatelích, skupinách, počítačích atd.), ověřovat uživatele, atd.

Informace o uživatelích a skupinách v *Apple Open Directory* jsou uloženy v LDAP databázi *Open LDAP*. Výhodou mapování účtů do *Kerio MailServeru* je, že jsou uživatelské účty a skupiny udržovány na jednom místě a nemusí být importovány a spravovány v *Apple Open Directory* a *Kerio MailServeru* zároveň. Pouze v případě, že je potřeba definovat konfiguraci specifickou pro poštovní schránky (např. kvótu schránky nebo přeposílání pošty), musí být provedena v *Kerio MailServeru* (kapitola 13).

Upozornění: Při zakládání uživatelského účtu v *Apple Open Directory* je nutno uživatelské jméno zapsat v ASCII. Pokud bude uživatelské jméno obsahovat národní znaky, může se stát, že se uživatel nebude moci přihlásit ke svému účtu.

30.3 Nastavení mapování uživatelů do Kerio MailServeru

Na *Mac OS X Serveru* obvykle nejsou kromě instalace *Kerio Open Directory Extensions* nutná žádná další nastavení. Jediným omezením je nutnost uložení uživatelských jmen v ASCII. Pokud bude uživatelské jméno obsahovat národní znaky, může se stát, že se uživatel nebude moci přihlásit ke svému účtu.

V *Kerio MailServeru* je třeba provést následující:

1. V nastavení domény musí být povoleno a nastaveno mapování uživatelských účtů z adresářové služby *Apple Open Directory* (více viz kapitolu 7.6).

2. V nastavení domény musí být nastaveno ověřování uživatelů přes *Kerberos* (více viz kapitolu 7.7).

3. V nastavení uživatele musí být nastaveno ověřování uživatelů přes *Kerberos* (více viz kapitolu 13.2).

Kapitola 31

KMS Web Administration

KMS Web Administration je webové rozhraní pro přístup ke správě domény, respektive uživatelských účtů, skupin a aliasů v ní obsažených. Toto rozhraní umožňuje rozložení správy uživatelů na více osob, aniž by tyto osoby měly právo přistupovat k celé správě *Kerio MailServeru*.

KMS Web Administration byla vyvinuta zejména pro poskytovatele Internetu a jejich zákazníky, aby tito zákazníci mohli sami přistupovat k nastavení uživatelských schránek, skupin a aliasů ve svých doménách a podle aktuální potřeby je přidávat, měnit nebo odstraňovat.

Upozornění: Účty mapované do *Kerio MailServeru* z LDAP databáze nelze pomocí webového rozhraní editovat. Tyto účty se budou v *KMS Web Administration* zobrazovat pouze pro čtení.

31.1 WWW prohlížeče

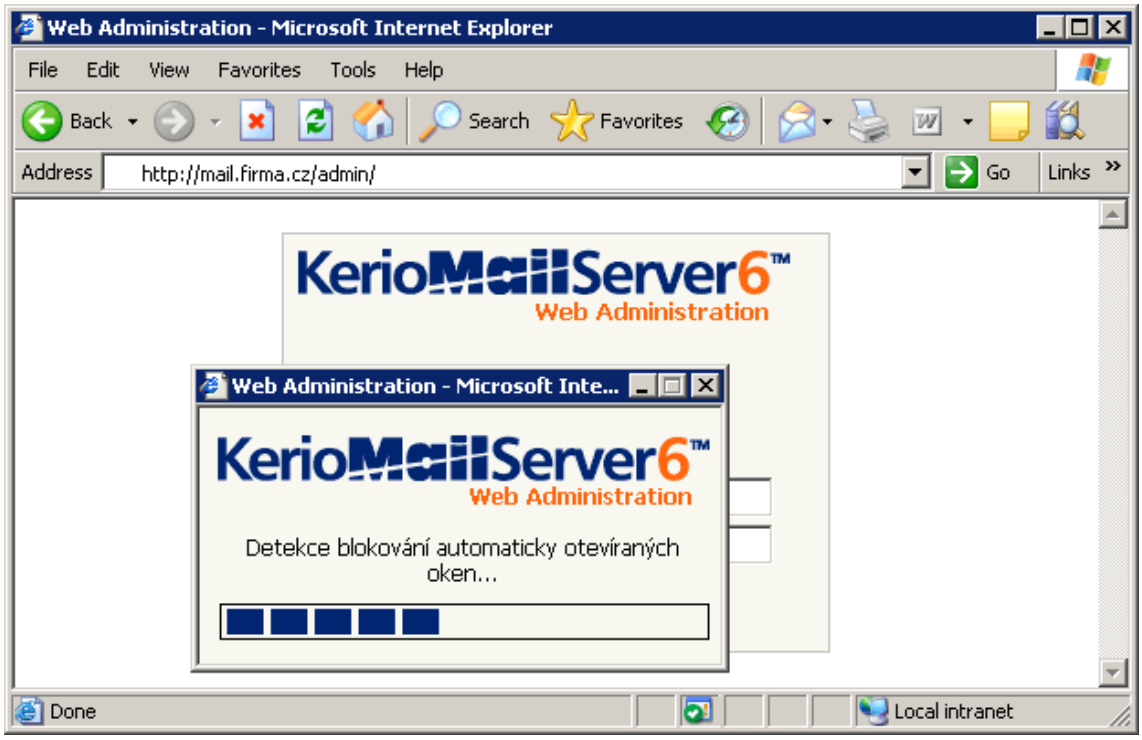
Pro přístup k rozhraní *KMS Web Administration* lze použít nové verze všech běžných prohlížečů podporující JavaScript a kaskádové styly (CSS). Podporované jsou prohlížeče:

- *Microsoft Internet Explorer* verze 6 a 7
- *Firefox* verze 1.5 a 2
- *Safari* verze 1.3, 2 a 3 na Mac OS X 10.5 Leopard

Chcete-li využívat zabezpečený přístup k rozhraní *KMS Web Administration* (protokolem HTTPS), musí prohlížeč podporovat zabezpečení SSL. Je-li možno jej konfigurovat (např. v prohlížeči *Microsoft Internet Explorer*), doporučuje se povolit podporu verzí SSL 3.0 a TLS 1.0.

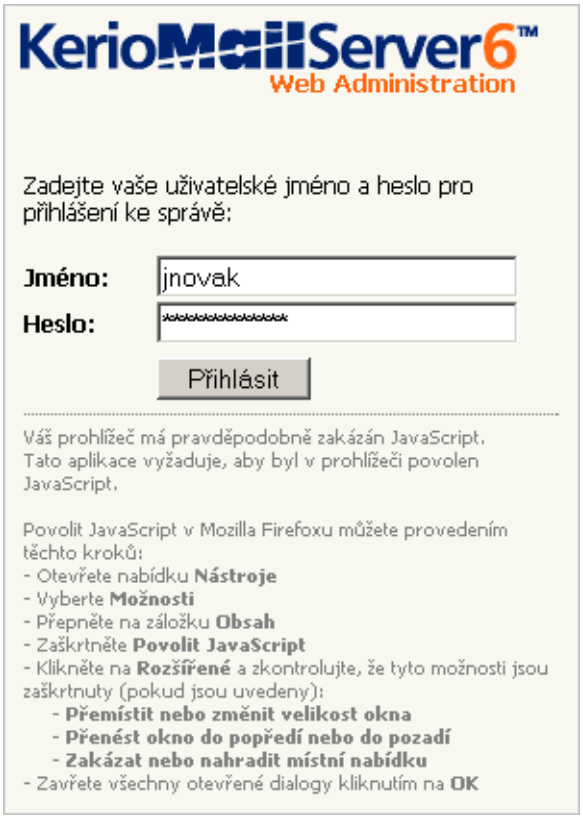
Blokování Pop-up oken a JavaScriptu

Pokud máte nainstalovanou a spuštěnou jakoukoli aplikaci, která blokuje *Pop-up* okna (pop-up killery) a/nebo JavaScript, je nutné nastavit pro *KMS Web Administration* výjimku.



Obrázek 31.1 Detekce pop-up blockerů

KMS Web Administration obsahuje utilitu pro detekci *Pop-up* blockerů/killerů a zákazu JavaScriptu. Před prvním spuštěním přihlašovací stránky k rozhraní *KMS Web Administration* tato utilita zkontroluje, zda je výjimka pro adresu *Kerio MailServeru* nastavena (viz obrázek 31.1). Pokud ne, objeví se na úvodní stránce pod přihlašovacím dialogem text s varováním a postupem, jak výjimku nastavit (viz obrázek 31.2).



Obrázek 31.2 Přihlašovací stránka s postupem, jak nastavit výjimku pro Kerio Web Administration

31.2 Přístupová práva k webovému rozhraní

Přístup do *KMS Web Administration* je ošetřen speciálními přístupovými právy, která lze nastavit v administrační konzoli *Kerio MailServeru*. Uživatelům s těmito právy je umožněn přístup do *KMS Web Administration*, kde mohou spravovat všechny účty a skupiny dané domény. Kromě uživatelů se speciálně nastavenými přístupovými právy má do *KMS Web Administration* automaticky přístup také každý uživatel s právy pro čtení a zápis do *Kerio MailServeru*.

Upozornění: Uživatelé a skupiny s plnými právy pro administraci *Kerio MailServeru* se v rozhraní nezobrazují, nelze je tedy žádným způsobem editovat.

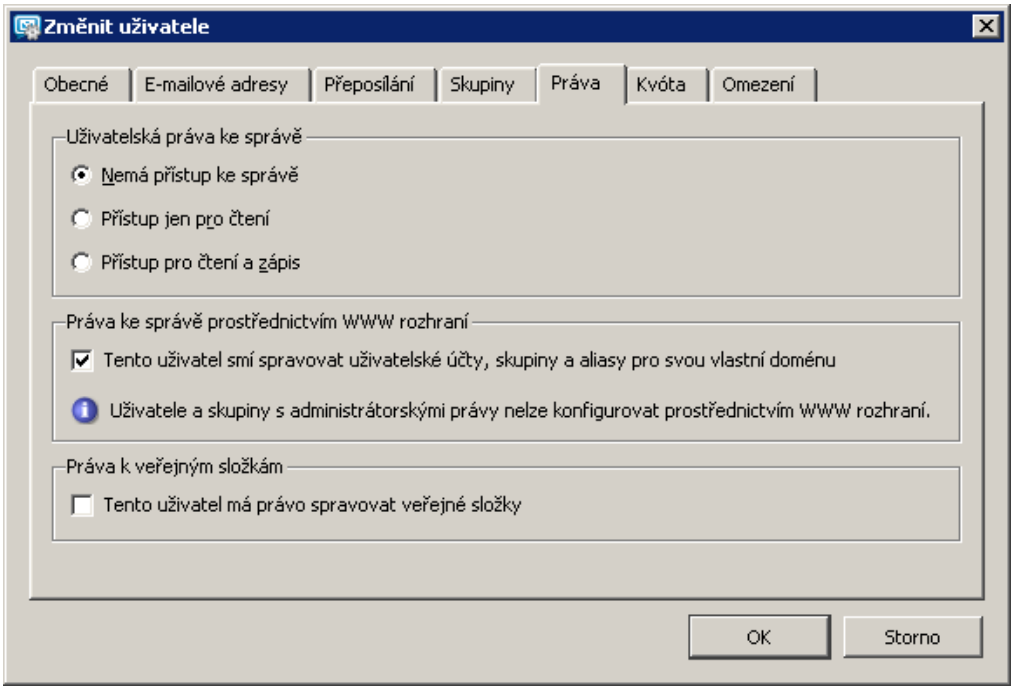
Nastavení

Přístupová práva pro přístup ke *KMS Web Administration* lze nastavit takto:

1. V administrační konzoli se přepneme do sekce *Nastavení domény →Uživatelské účty*.

2. Vybereme a myší označíme uživatele, kterému chceme práva přidělit.

3. Stiskneme tlačítko *Změnit*. Otevře se dialog *Změnit uživatele*, kde se přepneme do záložky *Práva*.



Obrázek 31.3 Nastavení přístupových práv ke KMS Web Administration

4. V záložce zaškrtneme položku *Tento uživatel smí spravovat uživatelské účty, skupiny a aliasy pro svou vlastní doménu* (viz obrázek 31.3).

5. Nastavení odsouhlasíme tlačítkem *OK*.

31.3 Nastavení potřebná pro webovou správu

Aby byla správa přes webové rozhraní plně funkční, je nutno provést některá nastavení v *Kerio Administration Console*:

1. V *Kerio MailServeru* musí být spuštěna služba HTTP, případně její zabezpečená verze HTTPS (kapitola 6).

2. V administrační konzoli je nutno povolit v sekci *Konfigurace* → *Vzdálená správa* správu přes WWW rozhraní, případně kvůli větší bezpečnosti omezit toto povolení na určitou skupinu IP adres (kapitola 12.3).

3. Vybranému uživateli musí být nastavena přístupová práva pro webovou administraci. Tato práva lze nastavit v sekci *Nastavení domény* → *Uživatelské účty*. V editačním dialogu vybraného uživatele v záložce *Práva* je nutno zaškrtnout volbu *Tento*

uživatel smí spravovat aliasy a uživatelské účty/skupiny ve své vlastní doméně (kapitola 31.2).

Stejné oprávnění lze nastavit také celé skupině uživatelů (*Nastavení domény* → *Skupiny*).

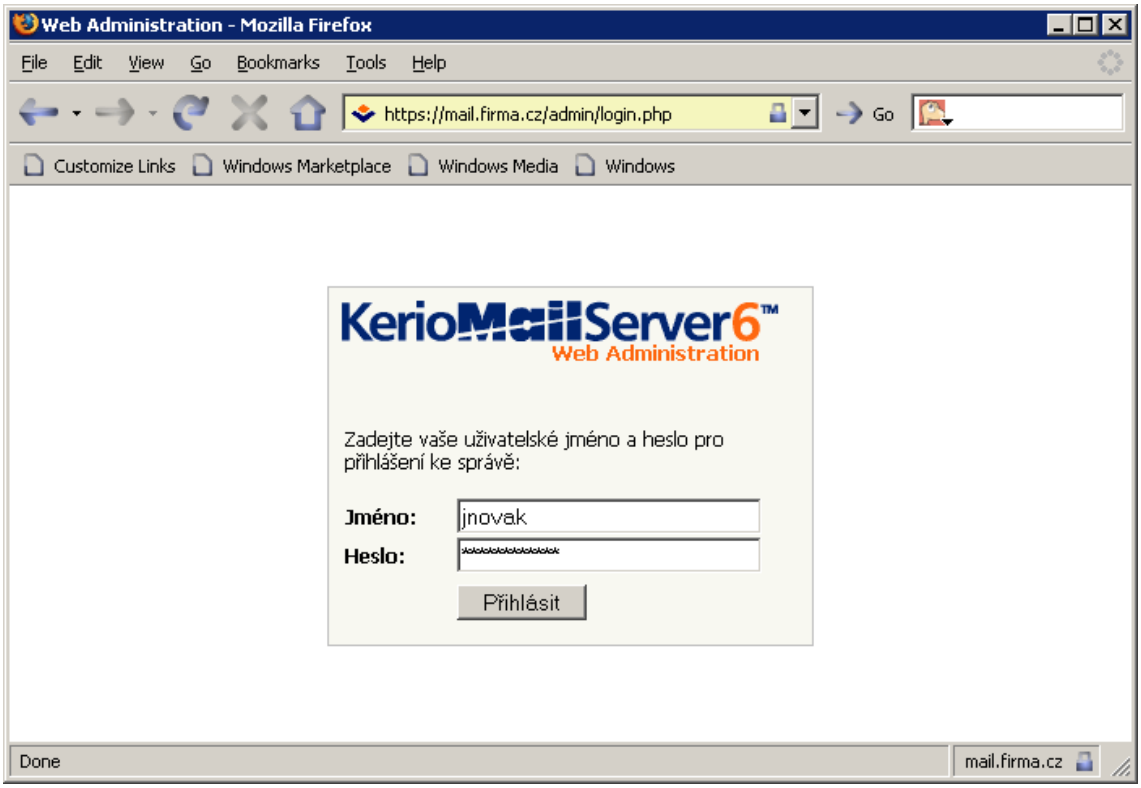
4. *Kerio MailServer* poskytuje nastavení omezení počtu uživatelů pro danou doménu. Po nastavení limitu nemůže uživatel s právy pro správu uživatelských účtů ve své doméně tento limit překročit. Nastavení limitu pro počet uživatelů v doméně se provádí v sekci *Konfigurace* → *Domény*. V editačním okně domény v záložce obecné je nutno nastavit položku *Limit počtu uživatelů v doméně* (kapitola 7.2).

31.4 Přihlášení uživatele

Pro přístup ke službě HTTP je třeba do WWW prohlížeče jako URL zadat adresu počítače, na němž *Kerio MailServer* běží, nebo jeho jméno, je-li zaneseno v DNS. V URL musí být rovněž specifikován protokol, a to buď HTTP pro nezabezpečený přístup, nebo HTTPS pro přístup zabezpečený SSL. URL tedy bude mít tvar např.: `http://192.168.1.1/admin` nebo `https://mail.firma.cz/admin`.

Při přístupu odjinud než z lokální sítě je doporučeno používat bezpečný protokol HTTPS (při použití protokolu HTTP lze velmi snadno odposlechnout a zneužít přihlašovací údaje uživatele). Při výchozím nastavení běží služby *HTTP* a *HTTPS* na standardních portech (80 a 443). Budou-li tyto porty změněny, je třeba při přístupu k dané službě uvést v URL také port, tedy např.: `http://192.168.1.1:8000/admin` nebo `https://mail.firma.cz:8080/admin`.

Je-li URL zadáno správně, zobrazí se v prohlížeči přihlašovací stránka. Zde je třeba zadat uživatelské jméno (pokud uživatel nepatří do primární domény, musí zadat celou elektronickou adresu) a heslo.



Obrázek 31.4 Přihlášení k webové správě

Odhlášení uživatele

Po ukončení práce ve *Web Administration* doporučujeme odhlásit se. K odhlášení slouží tlačítko *Odhlásit* umístěný v pravém horním rohu okna. Odhlášení zvyšuje bezpečnost dat uložených na serveru, protože přerušuje spojení s *Kerio MailServerem*. Toto opatření snižuje možnost zneužití spojení.

31.5 Záhlaví stránky

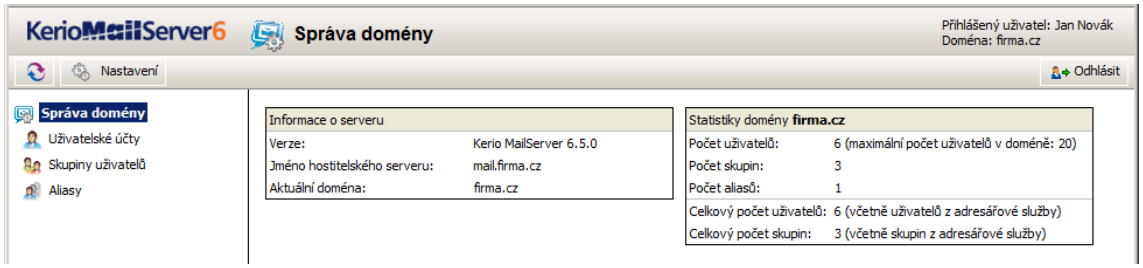
V záhlaví *KMS Web Administration* se zobrazuje název a logo společnosti. Po kliknutí na logo se otevřou produktové stránky společnosti *Kerio Technologies*.

Standardně se zobrazuje logo společnosti *Kerio Technologies*. Toto logo lze změnit za libovolné jiné v administrační konzoli *Kerio MailServeru*.

V pravém horním rohu záhlaví jsou umístěny informace o přihlášeném uživateli a doméně, kterou může spravovat (uživatel, který smí spravovat doménu, musí mít v této doméně založen účet).

31.6 Úvodní stránka

Po úspěšném přihlášení do *KMS Web Administration* se zobrazí úvodní stránka pro správu *Kerio MailServeru*. Tato stránka je rozdělena na dvě části:



Obrázek 31.5 Hlavní stránka

- Levá část okna se nikdy nemění a obsahuje seznam sekcí v podobě stromové struktury. Hlavní sekce, která se zobrazuje vždy po přihlášení, se nazývá *Správa domény* a zobrazuje obecné informace o doméně. Tato sekce obsahuje tři podsekce, a to *Uživatelské účty*, *Skupiny uživatelů* a *Aliasy*.
- Pravá část okna vždy zobrazuje obsah sekce zvolené v levé části okna.

Správa domény

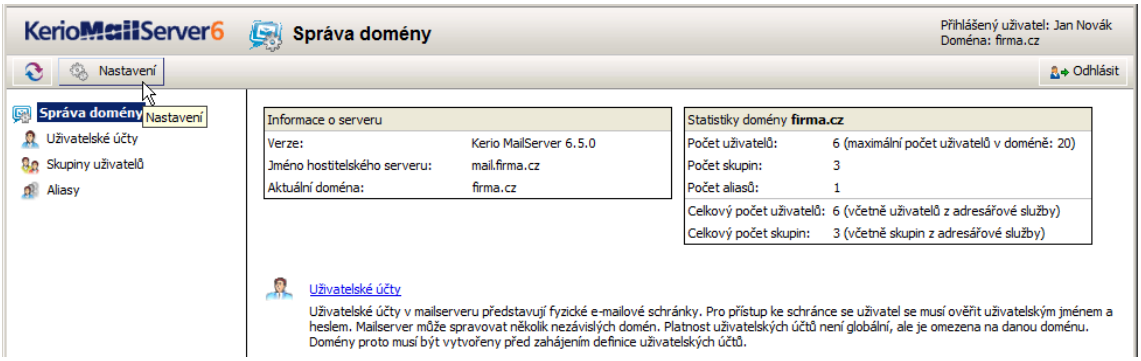
Úvodní sekce *Správa domény* obsahuje dvě tabulky informativního charakteru:

- Informace o serveru
  Verze
  Verze *Kerio MailServeru*. Podrobnější informace o produktu lze otevřít tlačítkem *About* umístěným vlevo na panelu nástrojů.
  Jméno hostitelského serveru
  Název počítače, kde je *Kerio MailServer* spuštěn.
  Aktuální doména
  Název aktuální domény. Uživatel může spravovat pouze doménu, v níž má založen uživatelský účet a nastavena příslušná práva.
- Statistiky domény
  Tabulka zobrazuje počty uživatelů, skupin a nastavených aliasů (v úvahu jsou brány pouze aliasy nastavené přímo v sekci *Aliases*).

Pod zmíněnými tabulkami lze najít jednoduché vysvětlivky k dalším podsekcím v *KMS Web Administration*.

Lokalizace KMS Web Administration

KMS Web Administration nabízí pro práci s webovým rozhraním několik lokalizací. Jazyk lze vybrat pomocí tlačítka *Nastavení*, které je umístěno na panelu nástrojů *KMS Web Administration* (viz obrázek 31.6).

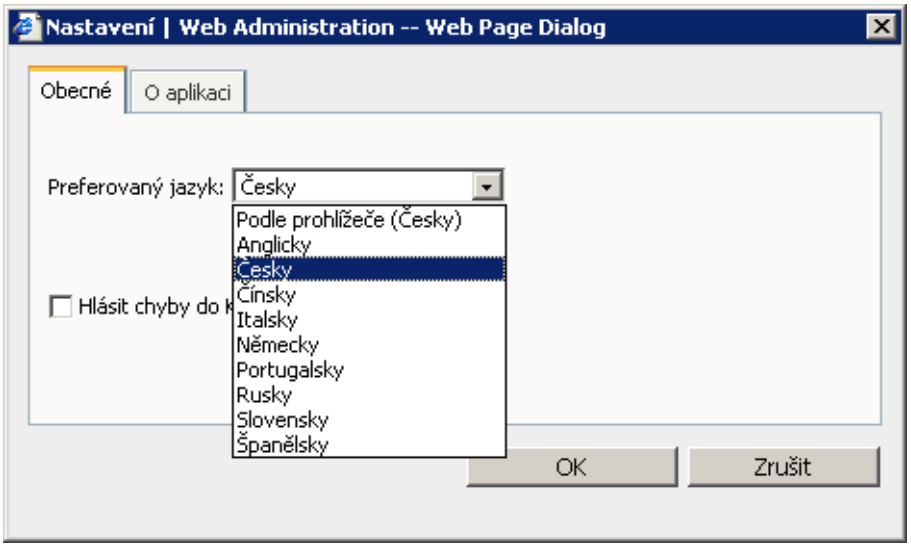


Obrázek 31.6 Tlačítko Nastavení

Po kliknutí na tlačítko se otevře dialog *Nastavení* (viz obrázek 31.7), kde je možné vybrat jednu z následujících lokalizací:

- Angličtina
- Čeština
- Čínština
- Italština
- Japonština
- Němčina
- Portugalština
- Ruština
- Slovenština
- Španělština
- Holandština
- Francouzština

Po výběru příslušné lokalizace stačí nastavení uložit tlačítkem *OK*.



Obrázek 31.7 Dialog Nastavení

31.7 Uživatelské účty

Uživatelský účet je obecný název pro jméno a heslo pro přístup ke službám serveru. V případě *Kerio MailServeru* představuje uživatelský účet navíc fyzickou e-mailovou schránku. Jméno a heslo uživatelského účtu slouží jako ověření přístupu k této schránce.

Definice uživatelského účtu

Definice nových uživatelských účtů se provádí v sekci *Uživatelské účty* tlačítkem *Nový uživatel* umístěným na panelu nástrojů. Otevře se dialog, kde jsou správci nabídnuty šablony pro vytvoření uživatelských účtů, pokud nějaká šablona byla v *Kerio MailServeru* vytvořena.

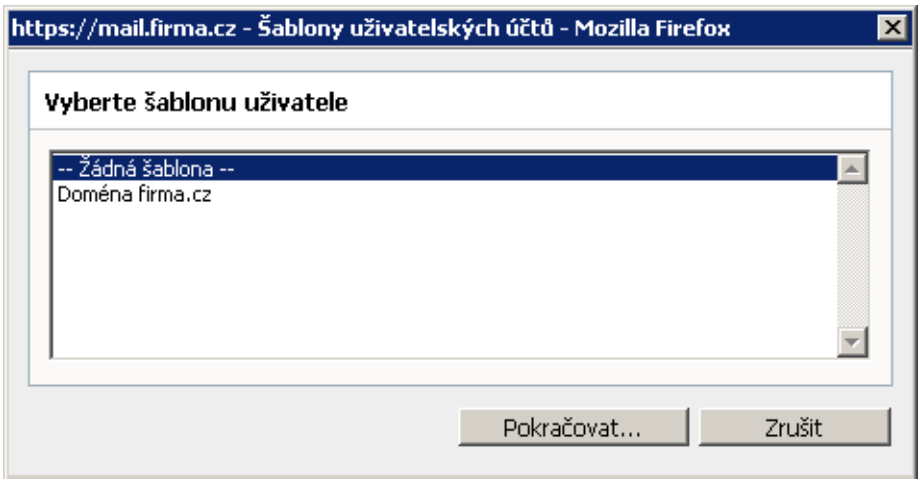
Šablony slouží v *Kerio MailServeru* k tomu, aby napomáhaly rychlejšímu zakládání uživatelských účtů s podobnými nebo stejnými parametry. Například pokud má být všem novým uživatelům nastavena stejná kvóta a typ ověřování, může správce *Kerio MailServeru* vytvořit šablonu, která tato nastavení bude obsahovat. Při jejím použití budou údaje o kvótě a typu ověřování předvyplněny.

Poznámka: Šablonu nelze vytvořit v *KMS Web Administration*. Musíte kontaktovat vašeho poskytovatele, který má nastavená plná přístupová práva ke *Kerio MailServeru*, a který tudíž může příslušnou šablonu založit.

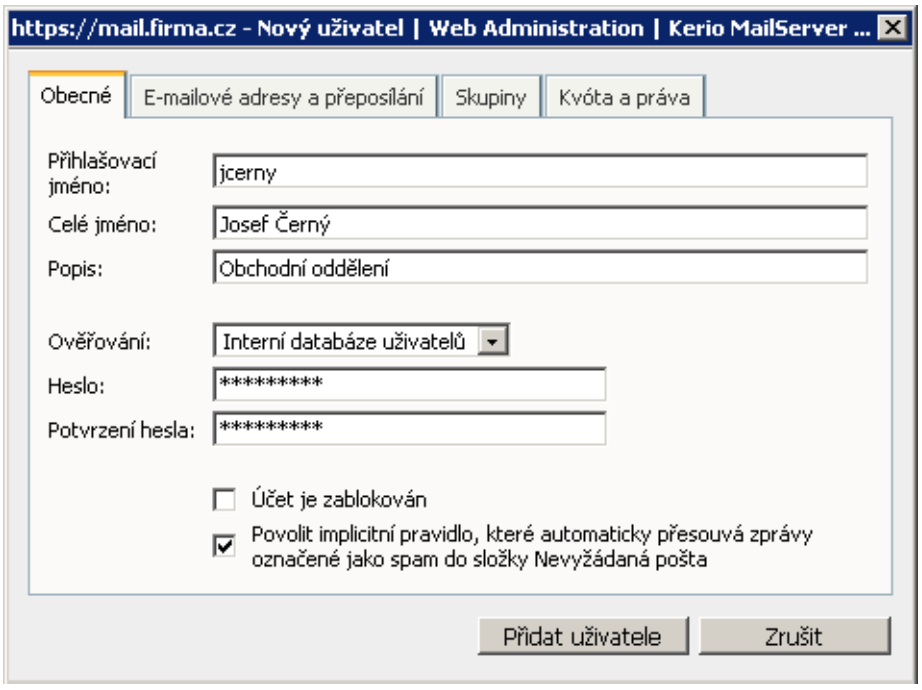
Po výběru šablony se otevře okno s několika záložkami:

Obecné

První záložka umožňuje zadání obecných informací o uživateli, jako je jeho uživatelské jméno a heslo:



Obrázek 31.8 Výběr šablony



Obrázek 31.9 Správa uživatelů — záložka Obecné

Přihlašovací jméno

Přihlašovací jméno (pozor: nejedná-li se o lokální primární doménu, pak se uživatel musí přihlašovat celou svou e-mailovou adresou, tedy např. `uzivatel@jinafirma.cz`, nikoliv pouze `uzivatel`).

Ve jménu uživatele se nerozlišují malá a velká písmena.

Celé jméno
Plné jméno (typicky jméno a příjmení daného uživatele). Položku je nutné vyplnit v případě, že uživatelské údaje z tohoto účtu budou exportovány do veřejné složky s kontakty.

Popis
Textový popis uživatele (např. funkce). Položka *Popis* má pouze informativní charakter. Může obsahovat libovolné informace nebo nemusí být vyplněna vůbec.

Ověřování
Způsob ověřování uživatele. Tuto informaci se dozvíte od svého poskytovatele.

Heslo, Potvrzení hesla
Heslo uživatele lze zadat nebo změnit pouze lokálním uživatelům. Každý uživatel by měl bezprostředně po založení účtu heslo změnit.
Bude-li heslo obsahovat speciální (národní) znaky, uživatelé se nebudou moci z některých poštovních klientů připojit ke *Kerio MailServeru*. Pro zadávání hesel uživatelů proto doporučujeme používat pouze ASCII znaky.

Účet je zablokován
Dočasné zrušení („vypnutí“) účtu bez nutnosti jej odstraňovat.

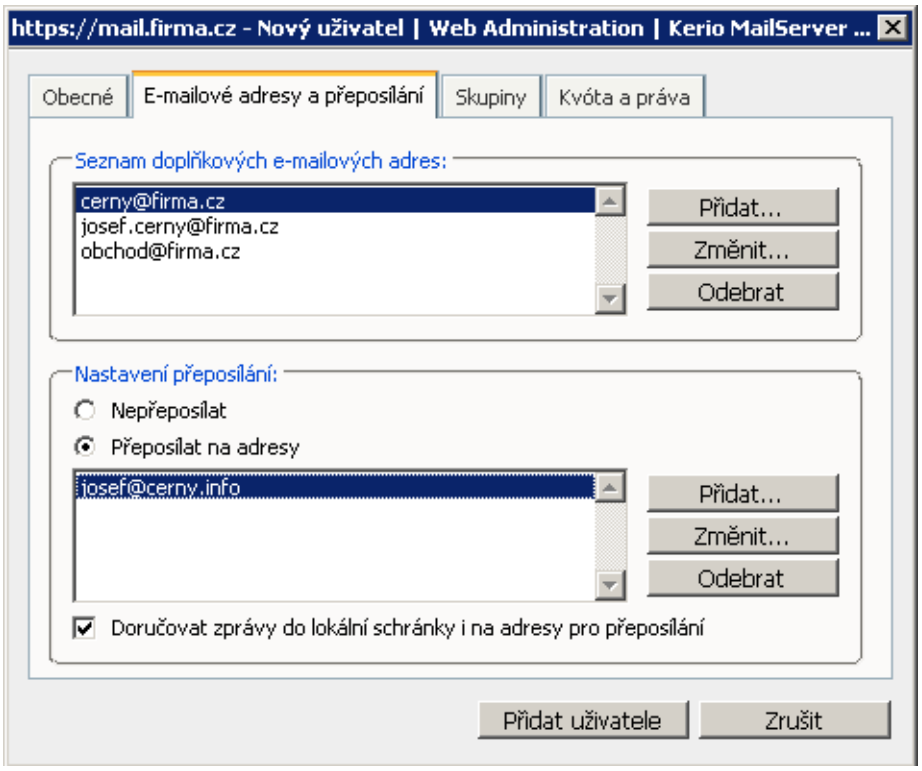
Povolit implicitní pravidlo, ...
Zaškrtnutím pravidla se při zakládání uživatelského účtu vytvoří sieve pravidlo pro nevyžádanou poštu. Všechny příchozí zprávy, které byly antispamovou kontrolou označeny jako nevyžádané, budou automaticky přesunuty do složky *Nevyžádaná pošta*. Pravidlo je možno v nastavení účtu vytvořit pouze při jeho zakládání.

E-mailové adresy a přeposílání

Seznam doplňkových e-mailových adres
Každé uživatelské schránce je možné nastavit více e-mailových adres. Do seznamu se zadávají všechny požadované e-mailové adresy daného uživatele (viz obrázek 31.10). Primární adresa uživatele (kterou nelze zrušit) je tvořena jeho uživatelským jménem a doménou, v níž se účet nachází. Ostatní adresy jsou tzv. aliasy. Aliasy lze zadávat přímo v definici uživatele nebo v sekci *Aliases*. Doporučujeme však zadávat aliasy přímo v definici uživatele — je to jednodušší a přehlednější. Co jsou aliasy a k čemu je možné je využít popisuje samostatná kapitola 31.9.

Nastavení přeposílání
Záložka *E-mailové adresy a přeposílání* umožňuje přeposílání zpráv na další e-mailové adresy. Tlačítkem *Přidat* je možno přidat adresu, na kterou se mají zprávy z této schránky přeposílat.

Volba *Doručovat zprávy do lokální schránky i na adresy pro přeposílání* zajistí, že zpráva bude uložena do lokální schránky a zároveň přeposlána na uvedené adresy (jinak bude pouze přeposlána a do lokální schránky se neuloží).



Obrázek 31.10 Správa uživatelů — záložka E-mailové adresy a přeposílání

Skupiny

V záložce *Skupiny* je možno (tlačítky *Přidat* a *Odstranit vybrané*) přidat nebo odebrat skupinu, do níž má být uživatel zařazen. Skupiny je nutno nejprve vytvořit v sekci *Skupiny uživatelů* (kapitola 31.8). Při definici skupin je ale možné stejným způsobem do skupin přidávat uživatele, a proto nezáleží na tom, zda budou nejprve vytvořeny skupiny nebo uživatelé.

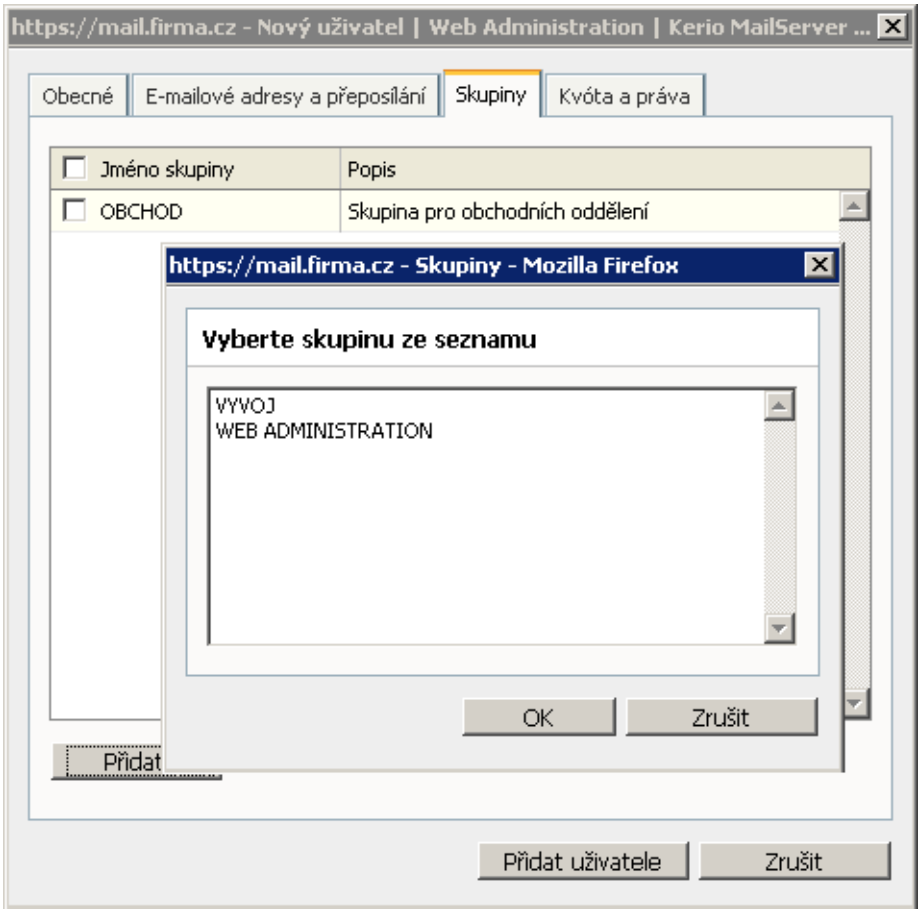
Kvóta a práva

Pro každou uživatelskou schránku lze nastavit určitá omezení nebo naopak práva:

Kvóta

Uživatelská kvóta slouží především k ochraně serveru proti zaplnění diskového prostoru. Bude-li splněna alespoň jedna z těchto podmínek, budou další zprávy adresované tomuto uživateli serverem odmítány.

Uživateli bude po naplnění kvóty zaslána varovná zpráva s doporučením na snížení počtu zpráv ve schránce.



Obrázek 31.11 Správa uživatelů — záložka Skupiny

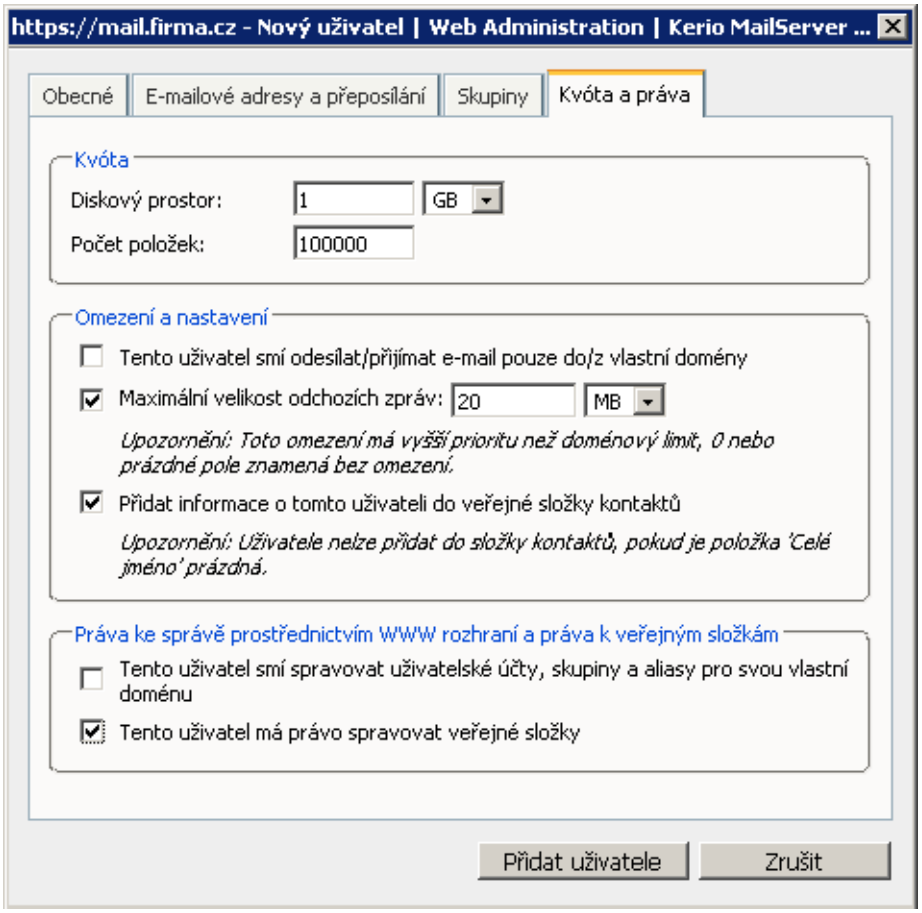
Diskový prostor
: Nastavení maximálního prostoru ve schránce. Pro pohodlné zadání číselného údaje je možno přepínat jednotky: kilobyty (*KB*), megabyty (*MB*) a gigabyty (*GB*).

Počet položek
: Maximální počet zpráv ve schránce. Další zprávy budou již serverem odmítány a zahazovány (nejsou udržovány ve frontě zpráv).

Každou z těchto položek lze nastavit na hodnotu *0* (nula), což znamená, že se na schránku nevztahuje příslušné omezení.

Omezení a nastavení

Tento uživatel smí odesílat/přijímat ...
: Volba umožňuje správci *Kerio MailServeru* omezit komunikaci pouze na lokální úroveň. To může být užitečné například při řešení bezpečnosti ve vnitrofiremní komunikaci. Žádný z uživatelů nebude moci z dané schránky odeslat zprávu ani do žádné jiné domény ani do Internetu.



Obrázek 31.12 Správa uživatelů — záložka Kvóta a práva

Maximální velikost odchozích zpráv

Nastavení limitu pro maximální velikost odchozích zpráv. Tuto volbu doporučujeme nastavit z toho důvodu, že zadáním limitu lze zabránit uživatelům, aby zahltili internetovou linku odesíláním zpráv s příliš velkými přílohami.

Je-li limit nastaven na 0, chová se *Kerio MailServer* stejně, jako by žádný limit nastaven nebyl.

Upozornění: Limit pro velikost zprávy může nastavit váš poskytovatel v *Kerio MailServeru* pro celou doménu. Po nastavení obou limitů nastávají dva případy chování:

1. Je-li uživateli nastaven vyšší limit, než je nastaven pro doménu, platí doménový limit.
2. Je-li uživateli nastaven nižší limit, než je nastaven pro doménu, platí limit nastavený uživateli.

Přidat informace o tomto uživateli do veřejné složky kontaktů
: Po zaškrtnutí volby bude do složky s veřejnými kontakty přidán kontakt uživatele. Kontakt lze do veřejné složky přidat pouze v případě, že byla v první záložce vyplněna položka *Celé jméno*.

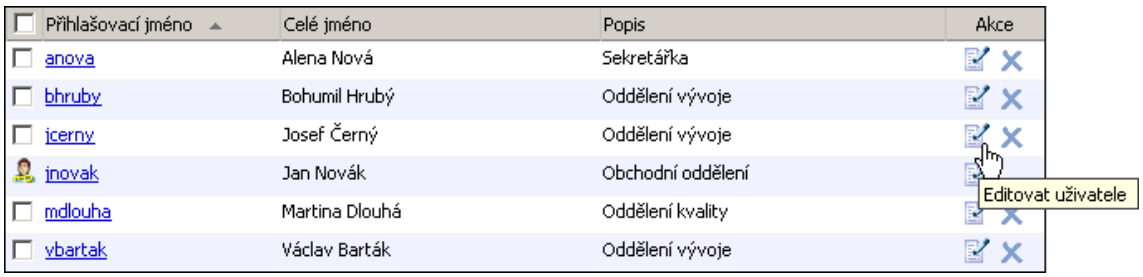
Práva ke správě prostřednictvím WWW rozhraní a práva k veřejným složkám

Tento uživatel smí spravovat ....
: Speciální právo pro přístup do *KMS Web Administration*. Toto oprávnění je nezávislé na nastavení přístupových práv do *Kerio Administration Console*.

Tento uživatel má právo spravovat veřejné složky
: Speciální právo pro administraci veřejných složek.

Editace uživatelského účtu

Změnit údaje uživatelského účtu je možné ve stejném dialogu, kde se účet zakládá. Pro jeho otevření klikneme v seznamu uživatelů buď na uživatelské jméno nebo na ikonku *Editovat uživatele* ve sloupci *Akce*.

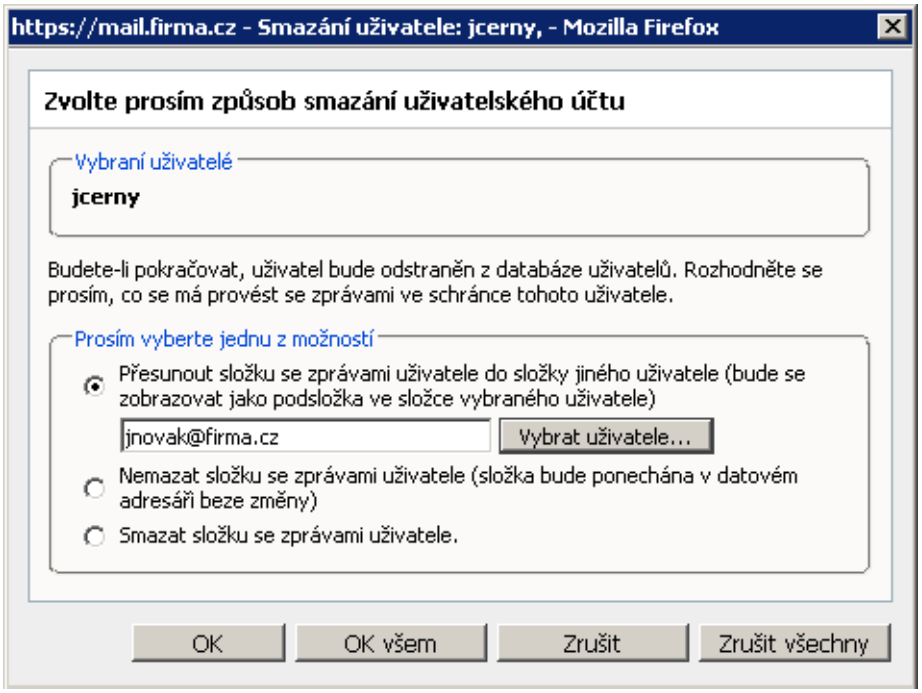


Obrázek 31.13 Změna uživatelského účtu

Zrušení uživatelského účtu

Odstranit uživatelský účet lze pomocí tlačítka *Smazat*. *Kerio MailServer* umožňuje provádět různé akce s původní schránkou uživatele. K tomuto účelu slouží dialog, který se otevře bezprostředně po stisknutí tlačítka *Odebrat*. Dialog umožňuje nastavit, zda má být schránka vymazána nebo přesunuta jinému uživateli, nebo zda má prostě zůstat v adresáři `store`.

Přesunout složku se zprávami uživatele ...
: Tato volba je užitečná zejména v případě, že jiný uživatel potřebuje se zprávami, událostmi a úkoly z této složky dále pracovat.
Celá uživatelská složka bude přesunuta jako podsložka kořenové složky vybraného uživatelského účtu. Název složky bude ve tvaru *Deleted mailbox — uzivatelske_jmeno@domena*. Tato složka bude obsahovat všechny původní složky smazané schránky.



Obrázek 31.14 Dialog pro zrušení uživatele

Poznámka: Nastane-li při přesunu uživatelské schránky problém, potom se podrobnosti o něm zaznamenají do *Warning* logu v *Kerio MailServeru*.

Nemazat složku se zprávami uživatele ...
Uživatelská složka zůstane v úložišti, aby byla v případě potřeby k dispozici.

Smazat složku se zprávami uživatele
Volbu lze využít hlavně v případě, že uživatelská složka neobsahuje žádné, nebo žádné důležité položky (zprávy, události, úkoly, atd.).

Vyhledávání uživatelů

Na panelu nástrojů je umístěno také pole pro vyhledávání, které je užitečné především v případě, že doména obsahuje velké množství uživatelů. Vyhledávání se provádí ve všech položkách uživatele — *Přihlašovací jméno*, *Celé jméno* a *Popis*.

Kromě systému vyhledávání je možno usnadnit si orientaci v uživatelích řazením podle sloupců kliknutím na jejich záhlaví.

Uživatelé mapovaní z adresářové služby

Pokud jsou v této doméně obsaženi uživatelé mapovaní z adresářové služby, zobrazí se také v *KMS Web Administration*. Data k mapovaným účtům ovšem není možné nijak měnit. Z toho důvodu existuje pod seznamem zpráv volba *Zobrazit pouze uživatele z interní databáze (skrýt uživatele z adresářové služby)*, která umožňuje všechny mapované uživatele skrýt.

31.8 Skupiny

Uživatelské účty v rámci každé domény je možno řadit do skupin. Hlavní důvody vytváření skupin uživatelů jsou následující:

- Pro skupiny uživatelů mohou být pomocí aliasů (viz kapitolu 31.9) vytvořeny tzv. skupinové adresy — e-mail poslaný na tuto adresu bude doručen všem členům skupiny.
- Skupině uživatelů mohou být nastavena specifická přístupová práva. Tato práva doplňují práva jednotlivých uživatelů.

Definice skupin uživatelů se provádí v sekci *Skupiny uživatelů*.

Definice skupiny

Novou skupinu uživatelů lze vytvořit tlačítkem *Nová skupina* v sekci *Skupiny uživatelů*. Po jeho stisknutí se zobrazí dialog s několika záložkami:

Obecné

Do záložky s názvem *Obecné* je možno doplnit jméno a popis skupiny:

Jméno skupiny
: Název skupiny (jednoznačně identifikuje skupinu).

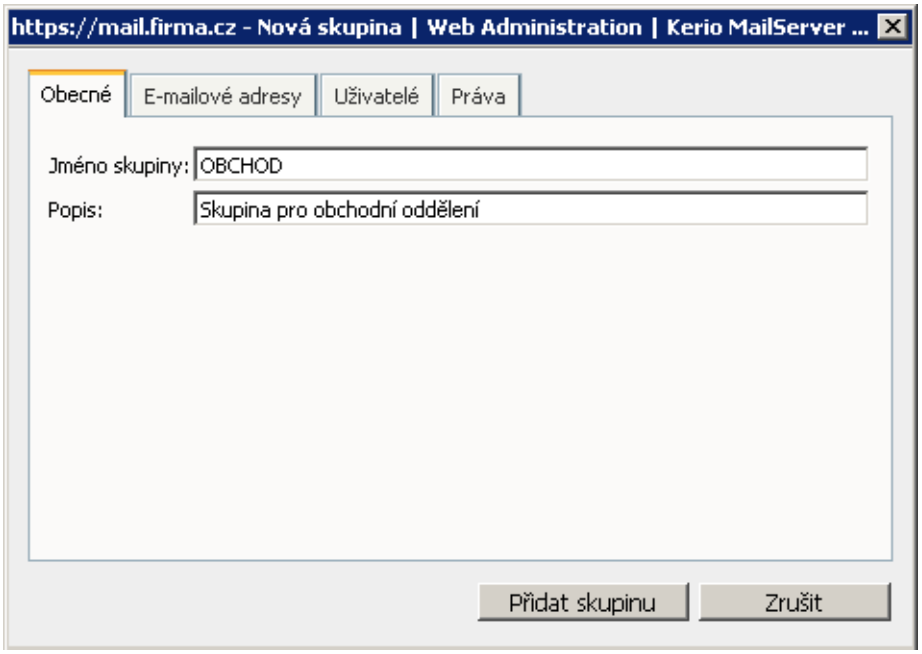
Popis
: Textový popis skupiny (má pouze informativní charakter, může obsahovat libovolné informace nebo zůstat prázdný).

E-mailové adresy

V této záložce je možno zadat všechny požadované e-mailové adresy (aliasy) dané skupiny. Skupina nemusí mít přiřazenu žádnou adresu (na rozdíl od uživatelského účtu není automaticky vytvářena adresa ze jména skupiny a domény, v níž je skupina definována).

Příklad použití skupinových adres:

Firma má obchodní oddělení, ve kterém pracují tři obchodníci. Všichni obchodníci mají založen účet v *Kerio MailServeru*. Každý z těchto třech obchodníků požaduje, aby mu byly doručovány všechny objednávky, které zákazníci odešlou do firmy přes e-mail.



Obrázek 31.15 Správa skupin — záložka Obecné

Řešením je založit skupinu s názvem `OBCHOD` a v záložce *E-mailové adresy* nadefinovat společné e-mailové adresy `sales@firma.cz` a `obchod@firma.cz` (viz obrázek 31.16). Posledním krokem je v záložce *Uživatelé* doplnit ony tři obchodníky (viz obrázek 31.17).

Ihned po založení této skupiny se budou všechny e-maily, které byly zákazníky odesílány na adresy `sales@firma.cz` nebo `obchod@firma.cz`, doručovat všem třem obchodníkům.

Skupina nemusí mít přiřazenu žádnou adresu (na rozdíl od uživatelského účtu není automaticky vytvářena adresa ze jména skupiny a domény, v níž je skupina definována).

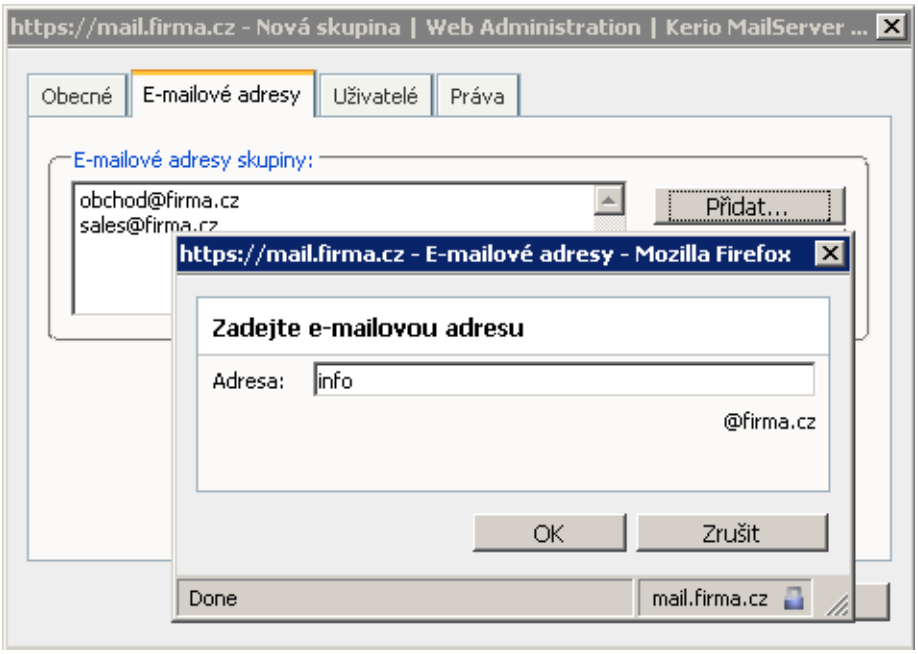
Adresy skupiny lze zadávat přímo v definici skupiny, nebo v sekci *Aliasy*. Doporučujeme však zadávat aliasy přímo v definici skupiny — je to jednodušší a přehlednější.

Uživatelé

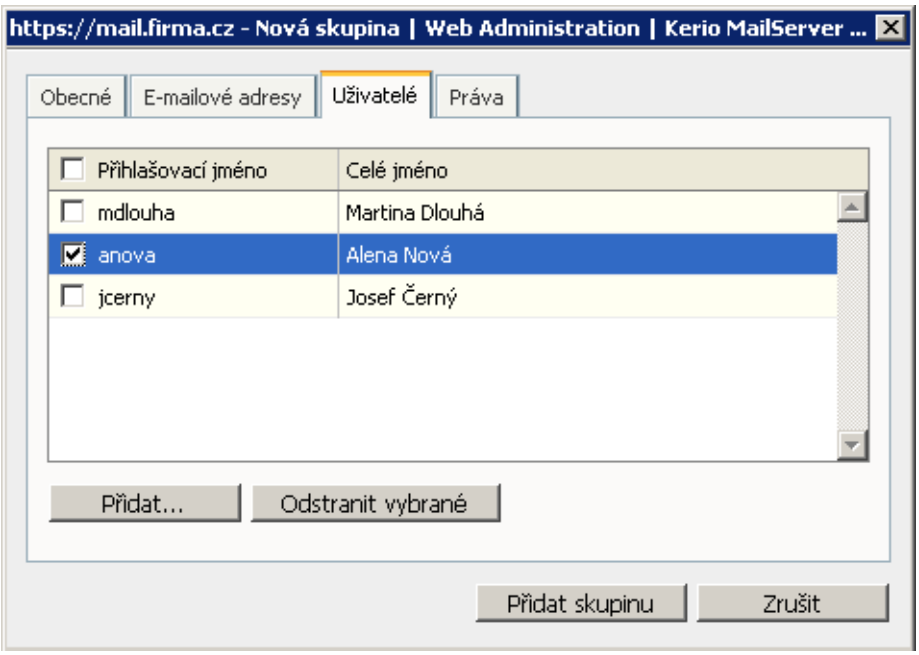
Tlačítky *Přidat* a *Odstranit vybrané* lze přidat či odebrat uživatele do/z této skupiny. Nejsou-li uživatelské účty dosud vytvořeny, může skupina zůstat prázdná a uživatelé do ní mohou být zařazeni při definici účtů (viz kapitolu 31.7).

Práva

Záložka *Práva* správci umožňuje nastavit skupině následující druhy oprávnění:



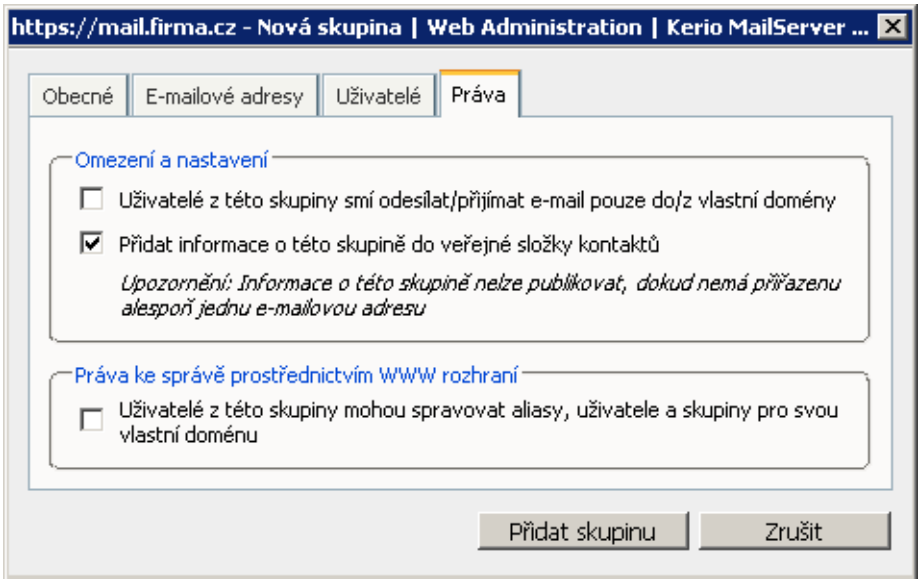
Obrázek 31.16 Správa skupin — záložka E-mailové adresy



Obrázek 31.17 Správa skupin — záložka Uživatelé

Uživatelé z této skupiny smí odesílat/přijímat ...

Volba umožňuje správci *Kerio MailServeru* omezit komunikaci pouze na lokální úroveň. To může být užitečné například při řešení bezpečnosti ve vnitro firemní



Obrázek 31.18 Správa skupin — záložka Práva

komunikaci. Žádný z uživatelů nebude moci z dané schránky odeslat zprávu ani do žádné jiné domény ani do Internetu.

Přidat informace o této skupině do veřejné složky kontaktů
Po zaškrtnutí volby bude do složky s veřejnými kontakty přidáno jméno a e-mailová adresa skupiny. Skupinu lze do veřejné složky přidat pouze v případě, že byla v druhé záložce vyplněna alespoň jedna e-mailová adresa.

Uživatelé z této skupiny mohou spravovat ...
Speciální právo pro přístup skupiny do *KMS Web Administration*. Toto oprávnění je nezávislé na nastavení přístupových práv do *Kerio Administration Console*.

Editace skupiny

Změnit údaje skupiny je možné ve stejném dialogu, kde se skupina zakládá. Pro jeho otevření klikneme v seznamu skupin buď na jméno skupiny nebo na ikonku *Editovat skupinu* ve sloupci *Akce*.

Zrušení skupiny

Tlačítkem *Smazat* na panelu nástrojů lze smazat kteroukoliv skupinu označenou zaškrtnutím levého políčka v seznamu skupin.

Vyhledávání skupin

Na panelu nástrojů je umístěno také pole pro vyhledávání, které je užitečné především v případě, že doména obsahuje velké množství skupin. Vyhledávání se provádí v položkách skupiny — *Jméno skupiny* a *Popis*.

Kromě systému vyhledávání je možno usnadnit si orientaci ve skupinách řazením podle sloupců kliknutím na jejich záhlaví.

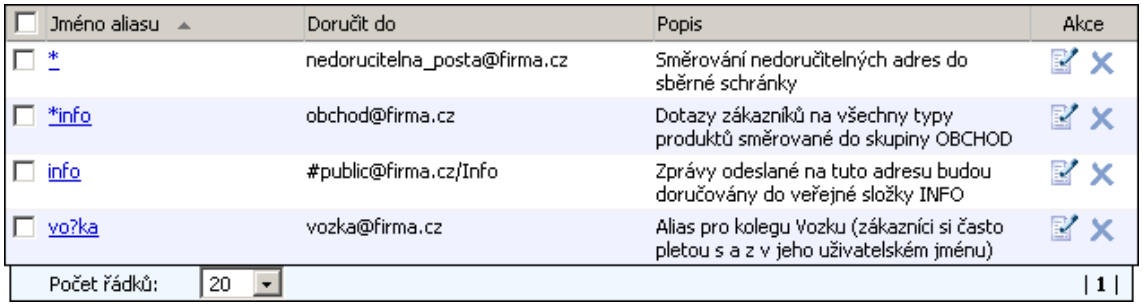
Skupiny mapované z adresářové služby

Pokud jsou v doméně obsaženy skupiny mapované z adresářové služby, zobrazí se také v *KMS Web Administration*. Data k těmto skupinám ovšem není možné nijak měnit. Z toho důvodu existuje pod seznamem zpráv volba *Zobrazit pouze skupiny z interní databáze (skrýt skupiny z adresářové služby)*, která umožňuje všechny mapované skupiny skrýt.

31.9 Aliasy

Alias je přezdívka (jiné jméno) pro uživatele, respektive pro jeho e-mailovou adresu. Jeden alias může být nadefinován jednomu nebo více různým uživatelům. To záleží na účelu, kterému bude sloužit.

U každého aliasu je nutné určit, kam mají být zprávy odeslané na tento alias doručeny. Aliasy mohou směřovat buď do jedné nebo více uživatelských schránek najednou (skupina nebo veřejná poštovní složka).



Obrázek 31.19 Aliasy

K čemu se aliasy konkrétně využívají si popíšeme na několika příkladech:

1. Firma potřebuje přes e-mail zveřejňovat různá interní sdělení. Jednou z možností jak toto provést je vytvořit veřejnou poštovní složku v rozhraní *Kerio WebMail* a přes alias do ní směřovat zprávy.

Řešením výše popsaného případu je, že všechny zprávy poslané na adresu `info@firma.cz` budou ukládány do veřejné složky `Info`. Kýžený alias definujeme takto:

`info` → `#public@firma.cz/Info`

2. Zprávy poslané na neplatné adresy (tj. adresy, kde část před znakem `@` neodpovídá žádnému uživatelskému účtu ani aliasu) mohou být doručovány vybranému uživateli nebo skupině (viz obrázek 31.20). Toto zajistí alias:

   `*` → `Admins`

   Nebude-li tento (nebo následující) alias definován, pak bude *Kerio MailServer* takové zprávy vracet odesílatelům jako nedoručitelné.

3. Pro doplnění libovolného počtu znaků v aliasu lze použít znak `*` (např.: `*sms*`, `a*00*` apod.). Alias pak bude fungovat pro všechny e-mailové adresy, které vyhoví této masce.

4. Pro doplnění právě jednoho znaku v aliasu (používá se zejména v případě, že si odesílatelé často pletou e-mailovou adresu uživatele) lze použít znak `?` (např.: `vo?ka` pokryje adresy `vozka` i `voska`).

Poznámka: Aliasy lze rovněž použít pro přiřazení další adresy uživateli nebo skupině, případně přeposílání pošty pro uživatele či skupinu na jiné adresy. Toto však doporučujeme provádět přímo v definici uživatele (viz kapitolu 31.7), resp. skupiny (viz kapitolu 31.8).

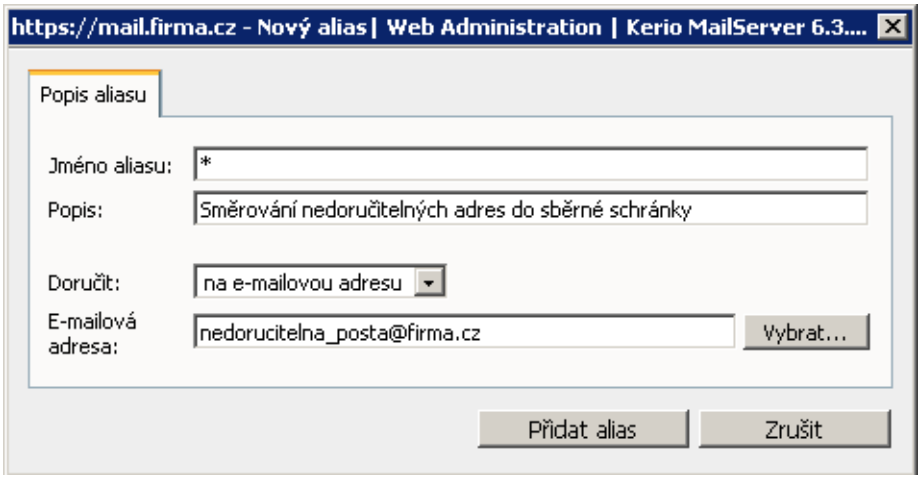
Správa aliasů

Definice aliasů se provádí v sekci *Aliasy*.

Dialog pro vytvoření nového aliasu lze otevřít tlačítkem *Nový alias*:

Jméno aliasu
: Virtuální adresa (např. `obchod` nebo `jan.novak`).
Aliasy se vždy vztahují ke spravované doméně, proto stačí do záhlaví aliasu zapsat pouze lokální část adresy (tj. část před znakem `@`).

Popis
: Textový popis aliasu. Slouží pouze pro potřebu správce, může obsahovat libovolné informace nebo zůstat nevyplněn.



Obrázek 31.20 Dialog pro vytvoření aliasu

Doručit

Položka umožňuje zadání místa, kam mají být zprávy poslané na tuto adresu doručovány. V položce lze vybrat, kam má být zpráva uložena:

- *na e-mailovou adresu* — libovolná (uživatelská nebo skupinová) e-mailová adresa. Tlačítkem *Vybrat* lze vybrat uživatele nebo skupinu ze seznamu.
  Poznámka: Nemá-li skupina doplněnou žádnou e-mailovou adresu, bude automaticky nastavena adresa ve tvaru:

  `nazev_skupiny@domena`

- *do veřejné složky* — název veřejné poštovní složky ve tvaru `#public/Slozka`.

Tlačítkem *Smazat* lze smazat kterýkoliv alias označený zaškrtnutím levého políčka v seznamu aliasů.

Na panelu nástrojů je umístěno také pole pro vyhledávání, které je užitečné především v případě, že doména obsahuje velké množství aliasů. Vyhledávání se provádí ve všech položkách aliasu — *Jméno aliasu*, *Doručit* a *Popis* .

Kapitola 32

Kerio Outlook Connector

Kerio Outlook Connector je speciální modul pro *MS Outlook*, který rozšiřuje spolupráci mezi *Kerio MailServerem* a *MS Outlookem*. Tento modul umožňuje, aby data, která uživatelé potřebují ke své práci, zůstávala uložena na serveru. Těmito daty jsou myšleny poštovní složky, kalendáře, úkoly, kontakty, poznámky a samozřejmě také veřejné složky.

Společnost *Kerio Technologies* vydala v rámci verze *Kerio MailServer 6.5.0* kromě standardního *Kerio Outlook Connectoru* nový *Kerio Outlook Connector (Offline Edition)*. *Kerio Outlook Connector (Offline Edition)* má proti *Kerio Outlook Connectoru* mnoho výhod. Hlavní z nich asi nejvíce využijí uživatelé s notebooky, protože jak napovídá název produktu, *Kerio Outlook Connector (Offline Edition)* umožňuje v *MS Outlooku* pracovat offline. K dalším výhodám bezesporu patří možnost vyhledávání v tělech zpráv nebo takzvané seskupování. O *Kerio Outlook Connectoru (Offline Edition)* se dozvíte více v sekci 32.1.

Standardní verzi *Kerio Outlook Connectoru* doporučujeme používat zejména v případě, že používáte *MS Outlook 2000*, protože *Kerio Outlook Connector (Offline Edition)* vyžaduje *MS Outlook XP* a vyšší. O *Kerio Outlook Connectoru* se dozvíte více v sekci 32.2.

32.1 Kerio Outlook Connector (Offline Edition)

Kerio Outlook Connector (Offline Edition) nabízí následující možnosti:

- Pošta, události, poznámky, kontakty a úkoly jsou ukládány v *Kerio MailServeru*, a proto jsou dostupné odkudkoliv, kde máme k dispozici internetové připojení. Připojit se můžeme nejen pomocí *MS Outlooku*, ale také přes rozhraní *Kerio WebMail* nebo jiným poštovním klientem.
- *MS Outlook* lze přepnout do režimu offline. To znamená, že můžeme poštu vyřizovat i z domova nebo třeba z autobusu. Tedy z míst, kde nemáme k dispozici internetové připojení nebo kde je příliš pomalé. Po opětovném připojení do režimu online *Kerio Outlook Connector (Offline Edition)* synchronizuje s poštovním serverem všechny změny a odešle poštu z *Outboxu*. Z popisu je patrné, že tuto vlastnost pravděpodobně využijí zejména uživatelé vlastnící notebook, protože svou poštu mohou vyřizovat odkudkoliv. Stačí otevřít *MS Outlook* a začít pracovat.
- *Kerio Outlook Connector (Offline Edition)* podporuje práci se složkami. V *MS Outlooku* můžeme tvořit hierarchicky uspořádané stromy složek s libovolnou hloubkou. Dále je podporováno sdílení složek, zobrazení veřejných složek, atd.

- V kalendářích je podporována vlastnost plánování schůzek a ve složkách s úkoly přiřazování úkolů dalším osobám.
- *Kerio Outlook Connector* umožňuje nastavení pravidel pro příchozí poštu, která jsou umístěna na serveru, a proto jsou platná globálně — pošta se bude třídit stejně v rozhraní *Kerio WebMail* i v jiných poštovních klientech.
- *Kerio Outlook Connector* nabízí vlastní antispamovou strategii.
- *Kerio Outlook Connector* umožňuje vyhledávání v tělech zpráv.
- *Kerio Outlook Connector* podporuje seskupování zpráv.

Poznámka: Kapitola popisuje nastavení v *MS Outlooku 2007*. Na starších verzích *MS Outlooku* se nastavení může mírně lišit.

Pro správnou funkci modulu musí být v *Kerio MailServeru* spuštěna služba *HTTP(S)* — přes tento protokol probíhá veškerá komunikace s *Kerio MailServerem*.

Kerio Outlook Connector je lokalizován do následujících jazyků:

- Angličtina
- Čeština
- Čínština
- Francouzština
- Holandština
- Chorvatština
- Italština
- Japonština
- Maďarština
- Němčina
- Polština
- Portugalština
- Ruština
- Slovenština
- Španělština
- Švédština

Lokalizace *Kerio Outlook Connectoru* se nastavuje automaticky podle lokalizace aplikace *MS Outlook*. V případě, že je *MS Outlook* v lokalizaci, kterou *Kerio Outlook Connector* nemá k dispozici, bude automaticky lokalizován do anglického jazyka.

Konkrétní možnosti a nastavení v *MS Outlooku* jsou popsána ve speciálním manuálu — *Kerio MailServer, Příručka uživatele*. Tento manuál je k dispozici na stránkách společnosti *Kerio Technologies* (`http://www.kerio.cz/kms-manual`).

32.1.1 Instalace

Instalaci *Kerio Outlook Connectoru* je možno spustit na těchto verzích operačního systému:

- Windows XP
- Windows Vista (32 a 64 bitů) s poslední nainstalovanou aktualizací Service Pack

Instalaci *Kerio Outlook Connectoru* je možno spustit s těmito verzemi *MS Outlooku*:

- MS Outlook XP + aktualizace Service Pack 3 (verze *Outlook XP* musí mít následující tvar: `10.0.6515.xyz`).
- MS Outlook 2003 + aktualizace Service Pack 2 (nebude-li instalace opatřena příslušnou aktualizací, *Kerio Outlook Connector* se odmítne nainstalovat).
- MS Outlook 2007 + aktualizace Service Pack 1

Kerio Outlook Connector (Offline Edition) vyžaduje Internet Explorer 6.0 a vyšší.

Upozornění: Kerio Outlook Connector (Offline edition) komunikuje se serverem přes rozhraní MAPI, které je založeno na protokolu HTTP(S). Z toho důvodu je třeba na serveru spustit službu HTTP(S) a namapovat příslušný port nebo porty na firewallu, kterým je server chráněn.

Instalace *Kerio Outlook Connectoru* probíhá standardně pomocí instalačního průvodce. Po instalaci je zapotřebí explicitně nastavit profil a poštovní účet.

Upozornění:

- Na počítači nejprve musí být nainstalován *MS Outlook*, a teprve poté *Kerio Outlook Connector (Offline Edition)*. V opačném případě nebude aplikace funkční.
- Při změně verze aplikace *MS Outlook* je nutné *Kerio Outlook Connector* ručně přeinstalovat.

Instalace na stanice kde byl nainstalován Kerio Outlook Connector

Upgrade *Kerio Outlook Connectoru* na *Kerio Outlook Connector (Offline Edition)* je ve většině případů bezproblémový. Po spuštění instalace se automaticky spustí konvertor, který převede všechny Kerio profily přihlášeného uživatele na profily pro *Kerio Outlook Connector (Offline Edition)*. Je-li stanice online připojena do Internetu, automaticky se vytvoří a aktualizuje lokální databáze *Kerio Outlook Connector (Offline Edition)*.

Speciální případy:

Jednu uživatelskou stanici využívá více uživatelů
: Využívá-li uživatelskou stanici více uživatelů, provedeme instalaci jednou a pod každým z ostatních uživatelů spustíme pouze konvertor, který je umístěn v menu *Start* → *Programy* → *Kerio* → *Outlook Profile Conversion Utility*.

Kerio Outlook Connector je instalován bez přístupu ke Kerio MailServeru

V takovém případě jsou profily změněny, avšak je třeba je po připojení k serveru dokončit:

1. V dialogu pro obsluhu profilů (*Start* → *Nastavení* → *Ovládací panely* → *Pošta* → *Zobrazit profily*) vybereme Kerio profil a stiskneme tlačítko *Vlastnosti*.
2. V průvodci klikneme na tlačítko *Uživatelské účty*.
3. V dalším kroku poklepeme na Kerio účet a jeho údaje potvrdíme tlačítkem *OK*. Dále se automaticky provede dokončení konverze na profil *Kerio Outlook Connector (Offline Edition)*.

Tuto proceduru je třeba provést s každým profilem, kde je založen Kerio účet.

Nastavení profilu a poštovního účtu

Uživatelský profil je soubor, který ukládá osobní nastavení v *MS Outlook*. Uživatel si pro *MS Outlook* může vytvořit libovolné množství profilů. Využívání více profilů je nezbytné zejména ve dvou případech. Buď má k počítači přístup více lidí najednou a každý z nich potřebuje vlastní e-mailovou schránku a osobní nastavení aplikace, nebo uživatel používá více různých poštovních schránek a chce pro ně mít odlišná osobní nastavení. V ostatních případech stačí vytvořit pouze jeden profil pro jeden či více poštovních účtů.

Nový profil lze nastavit v menu *Start* → *Nastavení* → *Ovládací panely* → *Pošta*:

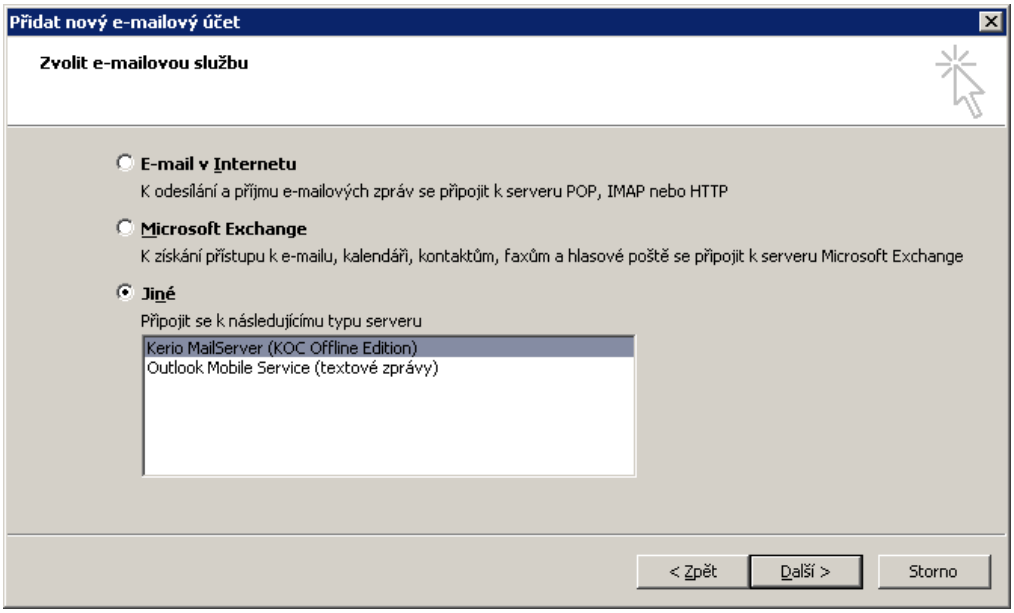
1. V dialogu *Nastavení pošty* vybereme tlačítko profily.

2. Nový profil přidáme tlačítkem *Přidat*. Jméno profilu může být libovolné.

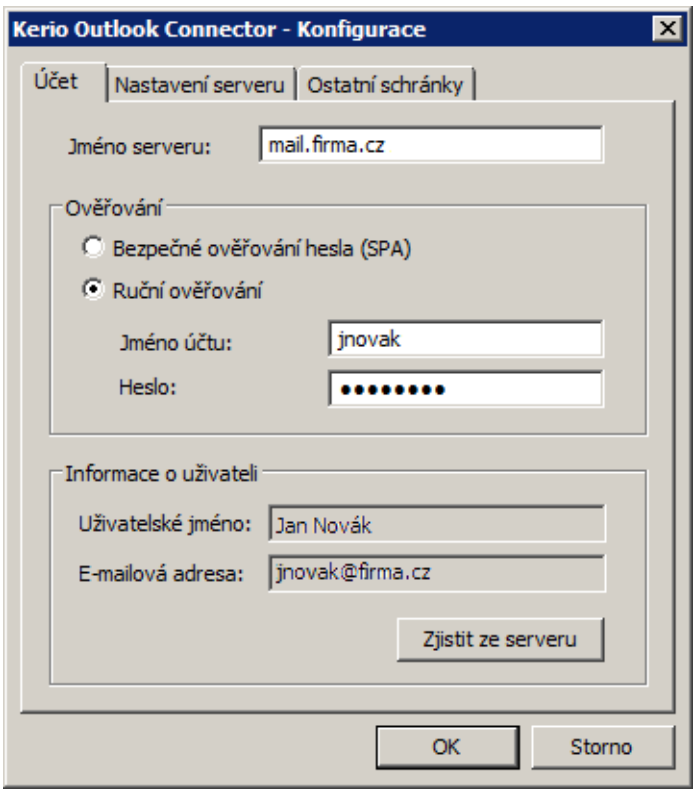
3. Otevře se průvodce pro založení nového poštovního účtu. Do dialogu není třeba nic zapisovat, stačí jen zaškrtnout volbu *Konfigurovat ručně nastavení serveru nebo další typy serverů* umístěnou vlevo dole.

4. V dialogu *Zvolit e-mailovou službu* vybereme možnost Jiné a označíme *Kerio MailServer (KOC Offline Edition)* (viz obrázek 32.1). Poté stiskneme tlačítko *Další*.

5. V dialogu v záložce *Účty* nastavíme základní parametry pro připojení k poštovnímu serveru (viz obrázek 32.2):



Obrázek 32.1 Nastavení nového účtu — výběr e-mailové služby



Obrázek 32.2 Nastavení nového účtu

Název serveru
DNS jméno nebo IP adresa poštovního serveru.

Zabezpečené ověřování hesla
Volba umožňuje využití NTLM ověřování. Po jejím zaškrtnutí uživatel nemusí nastavovat uživatelské jméno a heslo — místo jména a hesla bude použito ověřování proti *Active Directory* doméně.
Aby bylo NTLM ověřování funkční, je nutné, aby počítač i uživatelský účet byly součástí domény, proti které se uživatel ověřuje.
Upozornění: NTLM (SPA) ověřování lze využít pouze v případě, že je *Kerio MailServer* nainstalován na operačním systému Windows.

Uživatelské jméno
Uživatelské jméno používané pro přihlášení k poštovnímu serveru. Pokud uživatel není zařazen do primární domény, musí být zadána celá elektronická adresa uživatele (`jnovak@firma.cz`).

Heslo
Heslo uživatele.

Tlačítko *Test spojení* umožňuje vyzkoušet, zda byly údaje vyplněny správně, a zda je spojení s *Kerio MailServerem* v pořádku. Pokud test proběhne bez problémů, pole *Jméno* a *Elektronická adresa* budou automaticky vyplněna správnými údaji.

6. Konfigurace záložky *Nastavení serveru* je odvislá od bezpečnostní politiky, která je nastavena na serveru. Výchozí konfigurace zabezpečuje veškerou komunikaci mezi *Kerio MailServerem* a *MS Outlookem* protokolem SSL. Doporučujeme toto nastavení neměnit.

   Upozornění: Komunikace šifrovaná SSL vyžaduje instalaci SSL certifikátu vydaného důvěryhodnou certifikační autoritou.

Automatická aktualizace

Upgrade nových verzí *Kerio Outlook Connectoru* je prováděn automaticky. Je-li k dispozici nová verze, potom se bezprostředně po spuštění aplikace *MS Outlook Kerio Outlook Connector* aktualizuje.

Upozornění: Po dokončení aktualizace následuje automatický restart aplikace *MS Outlook*.

Celá aktualizace včetně restartu aplikace trvá maximálně jednu až dvě minuty.

Automatická aktualizace obsahuje kontrolu verzí *Kerio MailServeru* a *Kerio Outlook Connectoru*. To znamená, že pokud verze serveru a klienta nesouhlasí, uživatel je informován o tom, že je na serveru nainstalována jiná verze *Kerio MailServeru*, a že je třeba

klienta aktualizovat. Po odsouhlasení bude verze okamžitě aktualizována (nebo proveden downgrade — snížení verze).

Poznámka: Pokud se server od klienta liší jenom v čísle buildu (čísla verzí v upozorňujícím okně se neliší), bude klient funkční i v případě, že aktualizaci odmítnete. Pokud se server od klienta liší číslem verze (například `6.5.0` a `6.5.1`), potom se *Kerio Outlook Connector* bez příslušné aktualizace odmítne spustit.

32.1.2 Online/Offline režim

Kerio Outlook Connector (Offline Edition) podporuje režimy online a offline. Online režim je standardní režim *MS Outlooku*, který předpokládá připojení k Internetu. Offline režim umožňuje spustit *MS Outlook* a pracovat v něm bez internetového připojení. Znamená to, že je třeba mít veškerou poštu, události, úkoly, atd. uložené v lokálním úložišti na klientské stanici. Po připojení k Internetu je možné veškerá změněná data synchronizovat s poštovní schránkou umístěnou v *Kerio MailServeru*.

Režim offline lze prakticky využít zejména na notebooku, protože to umožňuje práci například v dopravních prostředcích nebo na jiných místech bez internetového připojení. Nové zprávy, události nebo úkoly se po přepojení zpět do online režimu automaticky synchronizují s úložištěm na serveru.

Standardním nastavením *MS Outlooku* je režim online. Do režimu offline se přepneme jednoduše. V menu *Soubor* na hlavním panelu klikneme na možnost *Pracovat offline*.

Zavřeme-li *MS Outlook* v režimu offline, bude při následujícím spuštění opět v režimu offline. Offline režim je třeba vypnout explicitně v menu *Soubor*.

Kerio Outlook Connector (Offline Edition) informuje o změně režimu z online do offline a o probíhající synchronizaci prostřednictvím speciální ikony, která se zobrazuje v oznamovací oblasti systému (viz obrázek 32.3). Ikona upozorňuje na následující situace:

Obrázek 32.3 Stav synchronizace

- Probíhá synchronizace — u ikony se zobrazí šipky.
- *MS Outlook* je spuštěn v režimu offline — u ikony se zobrazí šedá šipka zobrazující směr dolů.
- *MS Outlook* ztratil spojení se serverem — přes ikonu je zobrazen červený křížek.

Neprobíhá-li synchronizace a *MS Outlook* je normálně spuštěn v režimu online, ikona je skryta.

Synchronizace

Každou složku uloženou v *Kerio MailServeru* lze synchronizovat v jednom ze dvou režimů:

- Plná synchronizace položky.
- Synchronizace hlavičky a těla zprávy v prostém textu.

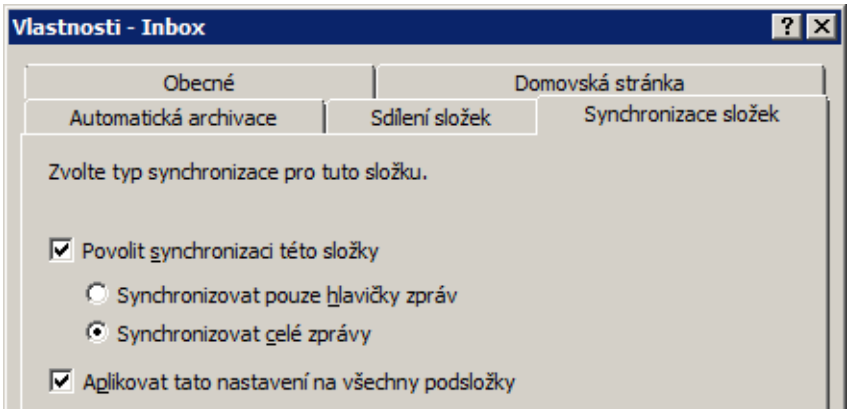
Synchronizace mezi *Kerio MailServerem* a *Kerio Outlook Connectorem* probíhá ve výchozím režimu takto:

- Doručená pošta — synchronizovány jsou celé zprávy.
- Ostatní poštovní složky — synchronizovány jsou pouze hlavičky zpráv a tělo v prostém textu.
- Události — synchronizovány jsou celé události.
- Kontakty — synchronizovány jsou celé kontakty.
- Úkoly — synchronizovány jsou celé úkoly.
- Poznámky — synchronizovány jsou celé poznámky.

Výchozí režim synchronizace lze změnit (přizpůsobit) ve vlastnostech každé složky:

1. Na vybranou složku klikneme pravým tlačítkem myši a v kontextovém menu zvolíme možnost *Vlastnosti*.

2. V okně *Vlastnosti* vybereme záložku *Synchronizace složek* (viz obrázek 32.4).



Obrázek 32.4 Nastavení synchronizace složky

Upozornění: V případě, že nechceme složku synchronizovat vůbec, stačí vypnout volbu *Povolit synchronizaci této složky*. Všechny zprávy, které daná složka již obsahuje, však budou nadále synchronizovány.

Konflikty

Konflikt synchronizace je situace, kdy je zpráva, událost nebo jakákoliv další položka změněna na serveru i v *Kerio Outlook Connectoru* v intervalu mezi synchronizacemi (synchronizace je spouštěna v určitých časových intervalech). Server v takovém případě nerozezná přesně, která ze změn dané položky je aktuální a žádoucí.

Pokud konflikt při synchronizaci nastane, vítězná položka je uložena do příslušné složky, kam měla být doručena. Verze položky, která prohrála, je umístěna do speciální složky nazvané *Konflikty*. Tato složka se zobrazuje pouze v *MS Outlooku*. V rozhraní *Kerio WebMail* ani v jiném poštovním klientovi se nezobrazí.

Obě položky, vyhrávající i prohrávající můžeme snadno porovnat a rozhodnout se, která z nich je aktuální. V případě, že je aktuální položka ze složky *Konflikty*, jednoduše ji přesuneme do správné složky a druhou verzi vymažeme.

Každý konflikt oznamuje speciální zpráva doručená do *MS Outlooku*. Obsahem předmětu zprávy je *Zpráva v konfliktu!*. Zpráva o konfliktu uvádí název zprávy, události, kontaktu nebo jiné položky, která se do konfliktu dostala a její umístění v mailboxu (ve které složce je umístěna). Lokální verze položky je přesunuta do složky *Konflikty*. Pokud je tato verze aktuální, prostě ji zaměníme za verzi v příslušné složce.

32.2 Kerio Outlook Connector

Kerio Outlook Connector nabízí následující možnosti:

- Pošta, události, poznámky, kontakty a úkoly jsou ukládány v *Kerio MailServeru*, a proto jsou dostupné odkudkoliv, kde máme k dispozici internetové připojení. Připojit se můžeme nejen pomocí *MS Outlooku*, ale také přes rozhraní *Kerio WebMail* nebo jiným poštovním klientem.
- *Kerio Outlook Connector* podporuje práci se složkami. V *MS Outlooku* můžeme tvořit hierarchicky uspořádané stromy složek s libovolnou hloubkou. Dále je podporováno sdílení složek, zobrazení veřejných složek, atd.
- V kalendářích je podporována vlastnost plánování schůzek a ve složkách s úkoly přiřazování úkolů dalším osobám.
- *Kerio Outlook Connector* umožňuje nastavení pravidel pro příchozí poštu, která jsou umístěna na serveru, a proto jsou platná globálně — pošta se bude třídit stejně v rozhraní *Kerio WebMail* i v jiných poštovních klientech.
- *Kerio Outlook Connector* nabízí vlastní antispamovou strategii.

Součástí *Kerio Outlook Connectoru* je také standardní *Nápověda* pro uživatele, která je umístěna v aplikaci *MS Outlook* na panelu nástrojů (*Nápověda → Nápověda ke Kerio Outlook Connectoru*).

Kerio Outlook Connector pro spolupráci aplikací *Kerio MailServer* a *MS Outlook* využívá otevřené rozhraní MAPI vyvinuté společností *Microsoft*. MAPI (Messaging Application Programming Interface) je univerzální rozhraní pro přenos zpráv. Je to softwarové rozhraní, které umožňuje libovolnému MAPI klientskému programu komunikovat s libovolným poštovním serverem (v našem případě *MS Outlook — Kerio MailServer*). V současné době se MAPI používá zejména pro psaní různých modulů do aplikace *MS Outlook*.

Pro správnou funkci *Kerio Outlook Connectoru* musí být v *Kerio MailServeru* spuštěny všechny příslušné služby:

- *HTTP(S)* — přes protokol probíhá automatická aktualizace verzí *Kerio Outlook Connectoru* a přes protokol HTTP také probíhá komunikace s *Free/Busy* serverem.
- *IMAP(S)* — rozhraní MAPI využívá v *Kerio MailServeru* protokol IMAP.
- *SMTP(S)* — přes protokol probíhá odesílání pošty.

Upozornění: Kromě výše zmíněných služeb je nutné namapovat příslušné porty na firewallu, kterým je server chráněn, jinak služby nebudou přístupné z Internetu (více viz sekci 2.3).

Instalaci *Kerio Outlook Connectoru* je možno spustit na těchto verzích operačního systému: Windows 2000 Professional (aktualizace Service Pack 4), XP (aktualizace Service Pack 1 nebo Service Pack 2) a Windows Vista (Home, Business, Enterprise nebo Ultimate edice).

Systém Windows musí obsahovat Internet Explorer ve verzi 6.0 a vyšší.

Kerio Outlook Connector podporuje tyto verze poštovního klienta:

- MS Outlook 2000 + aktualizace Service Pack 3 (nebude-li instalace opatřena příslušnou aktualizací, *Kerio Outlook Connector* se odmítne nainstalovat).
- MS Outlook XP + aktualizace Service Pack 3 (verze *Outlook XP* musí mít následující tvar: `10.0.6515.xyz`).
- MS Outlook 2003 + aktualizace Service Pack 2 (nebude-li instalace opatřena příslušnou aktualizací, *Kerio Outlook Connector* se odmítne nainstalovat).
- MS Outlook 2007 + aktualizace Service Pack 1

Poznámky:

- Všechna nastavení jsou popisována na *Windows XP* a *MS Outlook 2003*. Pracujete-li s *MS Outlook 2000*, nastavení se může mírně lišit (viz manuál *Kerio MailServer, Příručka uživatele*).
- *Kerio Outlook Connector* podporuje digitální podepisování zpráv. Funkce a nastavení digitálního podpisu je podrobně popsána ve standardní nápovědě pro *MS Outlook*.

Konkrétní možnosti a nastavení *Kerio Outlook Connectoru* na straně klienta jsou popsána ve speciálním manuálu — *Kerio MailServer, Příručka uživatele*. Tento manuál je k dispozici ke stažení na stránkách společnosti *Kerio Technologies* (`http://www.kerio.cz/kms-manual`).

TIP: Potřebujete-li pracovat se svou poštou také v režimu offline, pak zaměňte klasickou verzi *Kerio Outlook Connectoru* za *Kerio Outlook Connector (Offline Edition)* (viz kapitolu 32.1).

Instalaci *Kerio Outlook Connectoru* lze spustit buď samostatně nebo spolu s *Kerio MailServer Migration*.

Kerio Outlook Connector je lokalizován do následujících jazyků:

- Angličtina
- Čeština
- Čínština
- Francouzština
- Holandština
- Chorvatština
- Italština
- Japonština
- Maďarština
- Němčina
- Polština
- Portugalština
- Ruština
- Španělština
- Švédština

Lokalizace *Kerio Outlook Connectoru* se nastavuje automaticky podle lokalizace aplikace *MS Outlook*. V případě, že je *MS Outlook* v lokalizaci, kterou *Kerio Outlook Connector* nemá k dispozici, bude automaticky lokalizován do anglického jazyka.

32.2.1 Instalace a konfigurace bez použití migračního nástroje

Ruční instalace *Kerio Outlook Connectoru* pro *Kerio MailServer* probíhá standardně pomocí instalačního průvodce. Po instalaci je zapotřebí explicitně nastavit profil a poštovní účet.

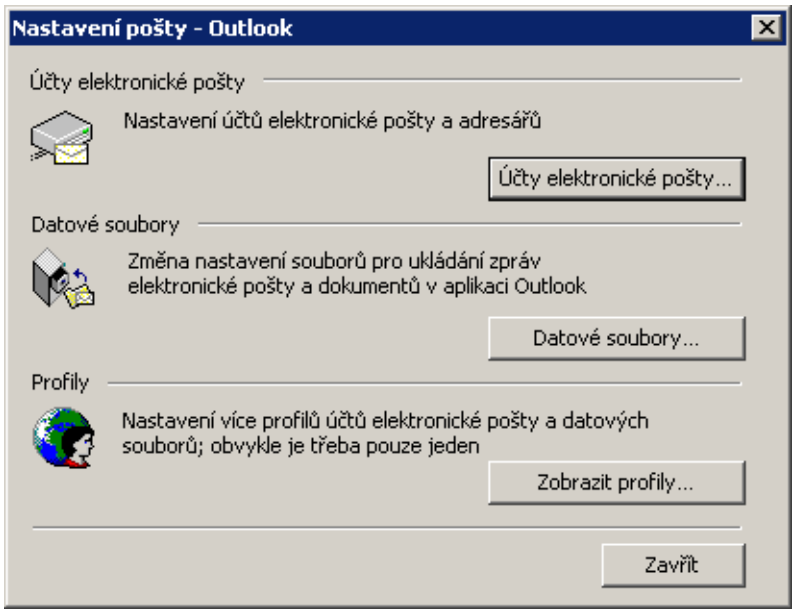
Upozornění:

- Na počítači nejprve musí být nainstalován *MS Outlook*, a teprve poté *Kerio Outlook Connector*. V opačném případě nebude aplikace funkční.
- Při změně verze aplikace *MS Outlook* je nutné *Kerio Outlook Connector* ručně přeinstalovat.

Tvorba profilu

Uživatelský profil je soubor, který ukládá osobní nastavení v *MS Outlook*. Profil je nezbytný zejména ve dvou případech. Buď má k počítači přístup více lidí najednou a každý z nich potřebuje vlastní e-mailovou schránku a osobní nastavení aplikace, nebo uživatel používá více různých poštovních schránek a chce mít pro ně odlišná osobní nastavení. Nový profil lze nastavit v menu *Start* → *Nastavení* → *Ovládací panely* → *Pošta*:

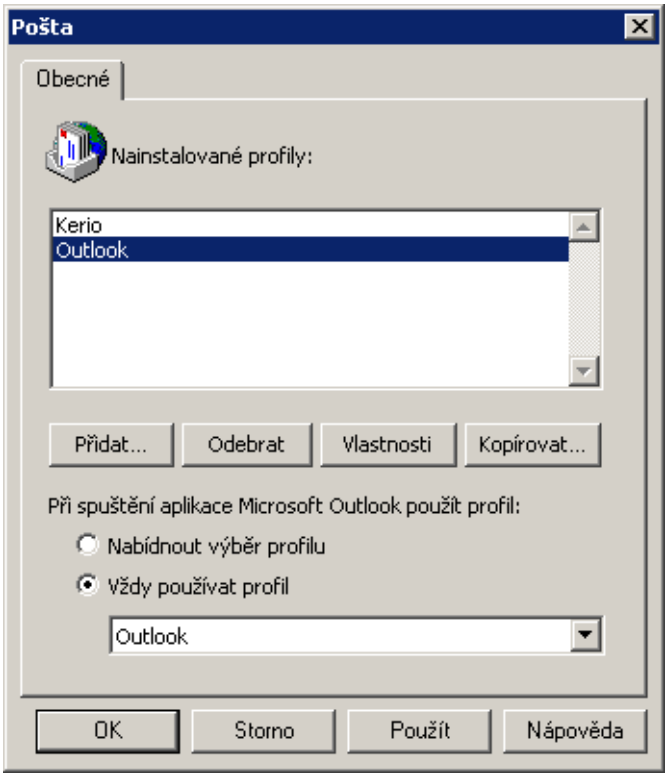
1. Otevře se dialog *Nastavení pošty — MS Outlook*, kde klikneme na tlačítko *Zobrazit profily* (viz obrázek 32.5).



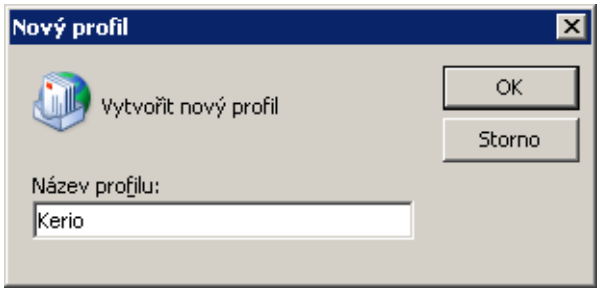
Obrázek 32.5 Nastavení profilu

2. Otevře se dialog *Pošta* (viz obrázek 32.6). Dialog slouží ke správě profilů a uživatelských účtů.

3. Klikneme na tlačítko *Přidat*. Otevře se okno s jediným volným polem pro zadání názvu nového profilu. Název profilu lze zadat zcela libovolně. Na obrázku 32.7 je zvolen název `Kerio`. Založení profilu odsouhlasíme tlačítkem *OK*.



Obrázek 32.6 Vytvoření profilu

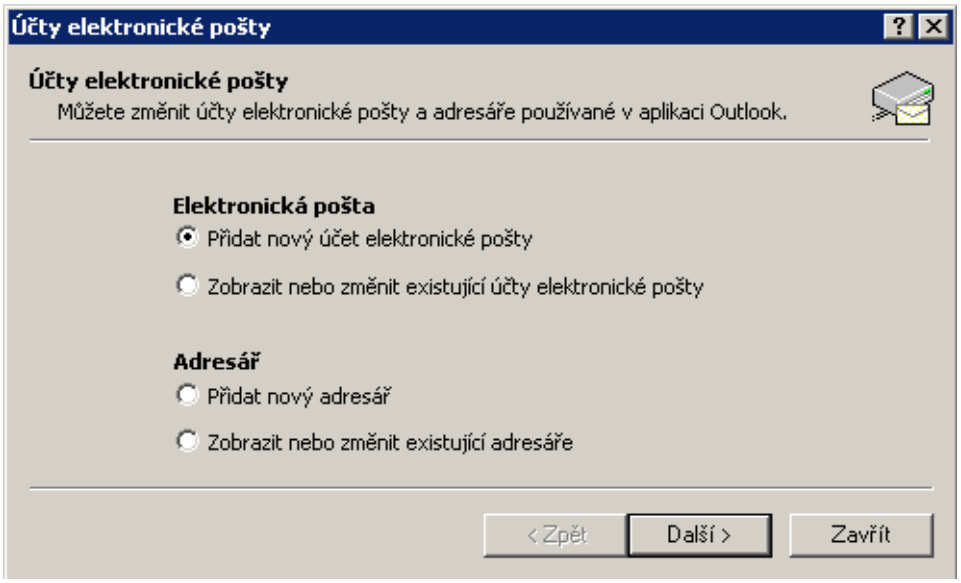


Obrázek 32.7 Nový profil

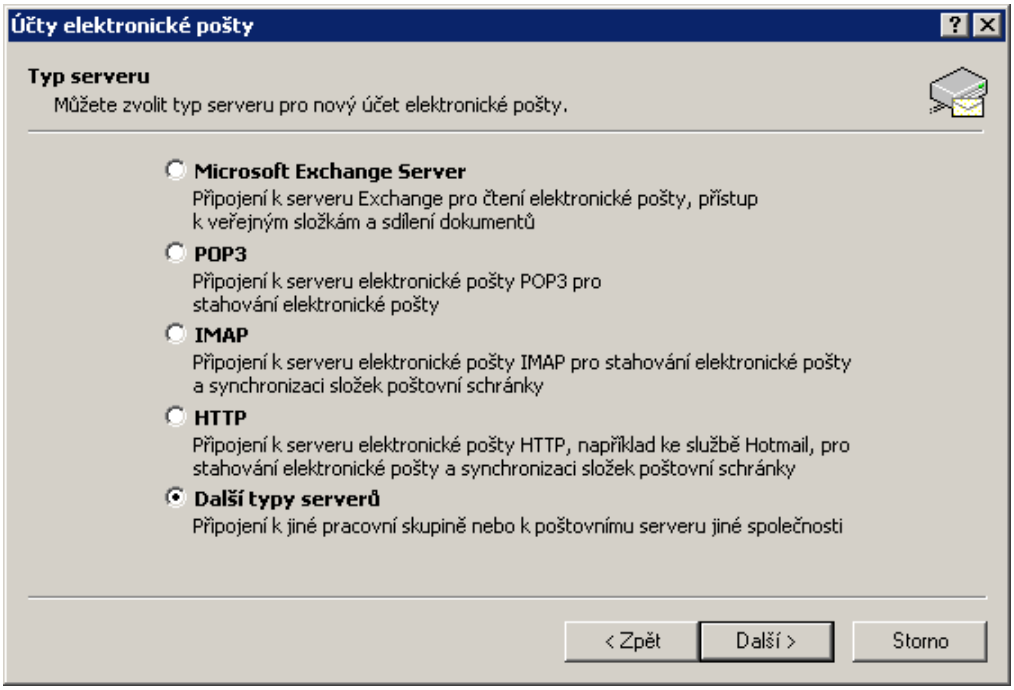
4. V novém profilu ještě není založen žádný poštovní účet. Proto se po vytvoření profilu automaticky spustí průvodce založením nového účtu.

   Standardní průvodce nabízí v prvním kroku možnost přidat nebo změnit účet elektronické pošty nebo adresář. Pro vytvoření účtu vybereme první možnost — *Přidat nový e-mailový účet* (viz obrázek 32.8).

5. Ve druhém kroku průvodce vybereme volbu *Další typy serverů* (viz obrázek 32.9) a klikneme na tlačítko *Další*.

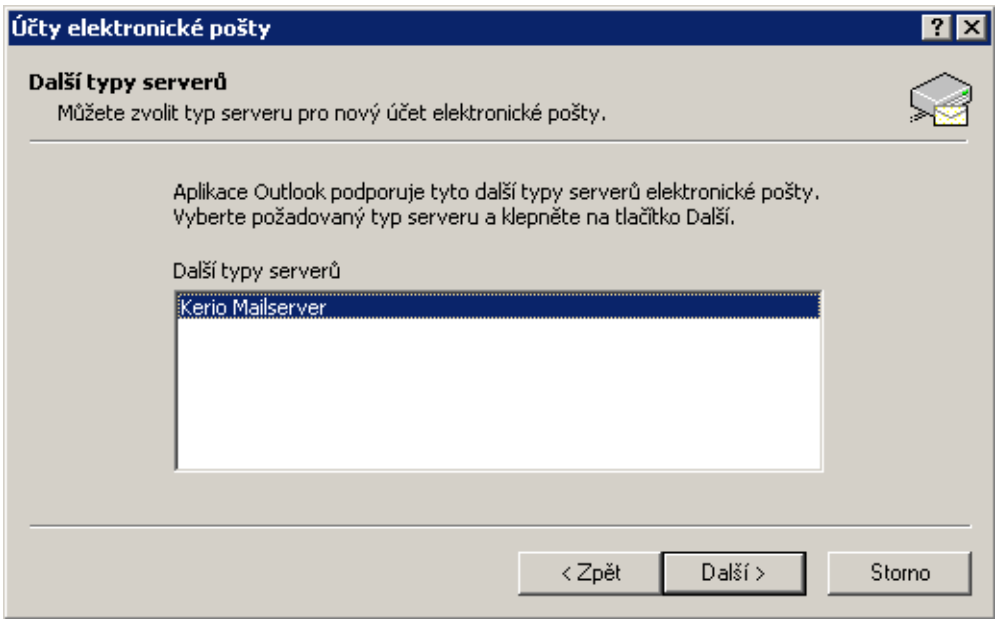


Obrázek 32.8 Nastavení účtu — přidání nového účtu



Obrázek 32.9 Nastavení účtu — zvolení typu serveru

6. Další krok průvodce umožňuje přímo zvolit typ serveru (viz obrázek 32.10). Zvolíme volbu *Kerio MailServer* (obvykle je to volba jediná).



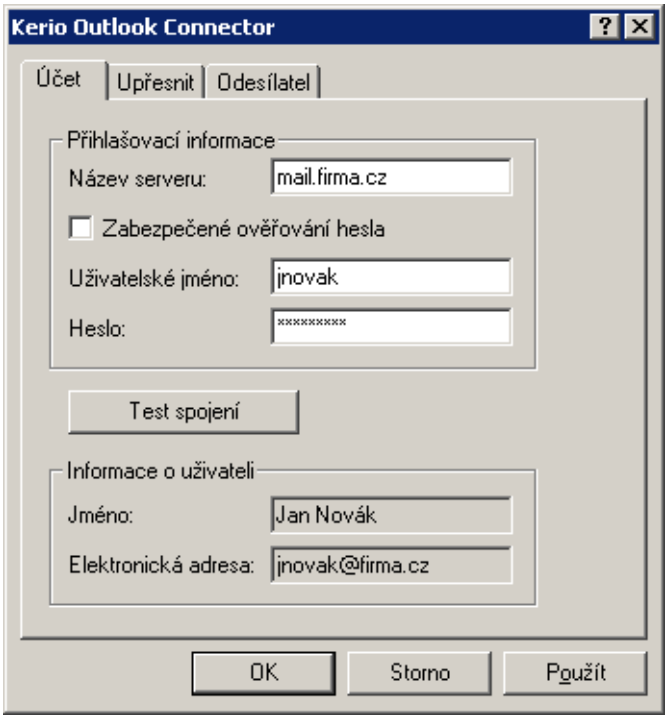
Obrázek 32.10 Nastavení účtu — zvolení Kerio MailServeru

7. Dalším krokem je nastavení *Kerio Outlook Connectoru*. Toto lze provést ve dvou záložkách okna *Kerio Outlook Connector*:

   Název serveru
   DNS jméno nebo IP adresa poštovního serveru.

   Zabezpečené ověřování hesla
   Volba umožňuje využití NTLM ověřování. Po jejím zaškrtnutí uživatel nemusí nastavovat uživatelské jméno a heslo — místo jména a hesla bude použito ověřování proti *Active Directory* doméně.
   Aby bylo NTLM ověřování funkční, je nutné, aby počítač i uživatelský účet byly součástí domény, proti které se uživatel ověřuje.
   Upozornění: NTLM (SPA) ověřování lze využít pouze v případě, že je *Kerio MailServer* nainstalován na operačním systému Windows.

   Uživatelské jméno
   Uživatelské jméno používané pro přihlášení k poštovnímu serveru. Pokud uživatel není zařazen do primární domény, musí být zadána celá elektronická adresa uživatele (`jnovak@firma.cz`).



Obrázek 32.11 Nastavení účtu — základní údaje

Heslo
: Heslo uživatele.

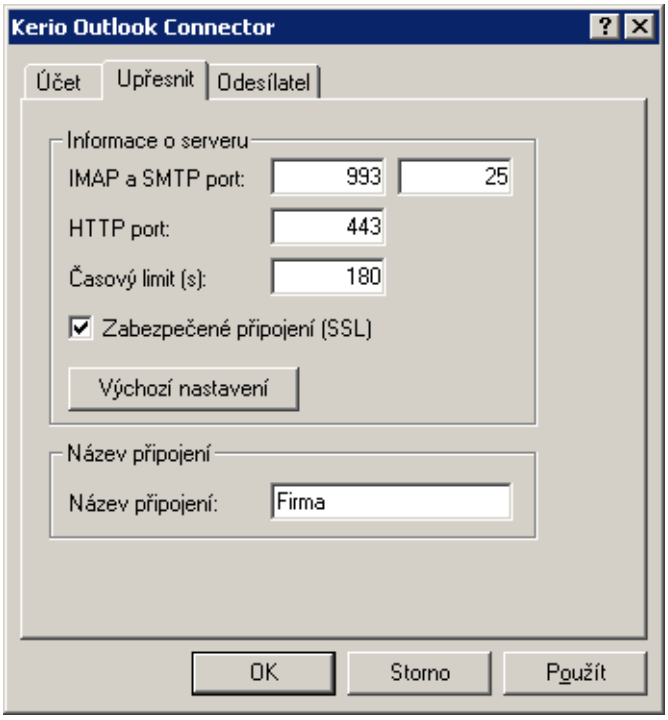
Tlačítko *Test spojení* umožňuje vyzkoušet, zda byly údaje vyplněny správně, a zda je spojení s *Kerio MailServerem* v pořádku. Pokud test proběhne bez problémů, pole *Jméno* a *Elektronická adresa* budou automaticky vyplněna správnými údaji.

Rozšířené nastavení ve druhé záložce umožňuje změnit některá nastavení týkající se komunikace.

IMAP a SMTP port
: Porty, které jsou využívány protokoly IMAP a SMTP pro komunikaci se serverem. Čísla portů musí vždy souhlasit s čísly portů nastavenými v *Kerio MailServeru*.

HTTP port
: Protokol HTTP(S) využívá *Free/Busy* kalendář a aplikace pro automatickou aktualizaci *Kerio Outlook Connectoru*. Číslo portu musí souhlasit s číslem portu pro HTTP(S) službu v *Kerio MailServeru*.

Časový limit
: Doba, po kterou aplikace čeká na odezvu *Kerio MailServeru*.



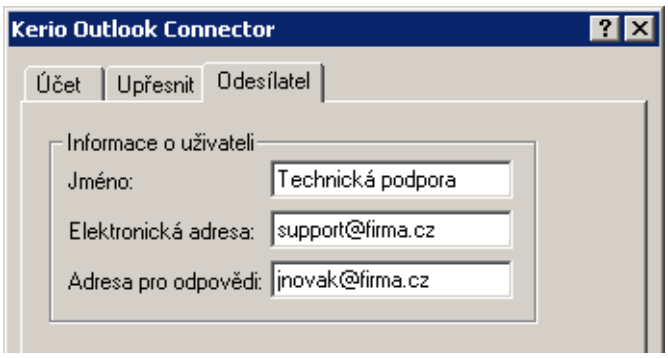
Obrázek 32.12 Nastavení účtu — porty

Zabezpečené připojení (SSL)
Volba umožňuje šifrovanou komunikaci služeb IMAP, SMTP a HTTP.

Tlačítkem *Výchozí nastavení* lze vrátit nastavené hodnoty na původní.

Název připojení
Standardním názvem připojení je *Kerio Outlook Connector Store*. Tento název lze podle libosti změnit.

Záložka *Odesílatel* obsahuje možnost konfigurace zobrazení jména, odchozí adresy a adresy pro odpovědi.



Obrázek 32.13 Nastavení účtu — nastavení informací o odesílateli

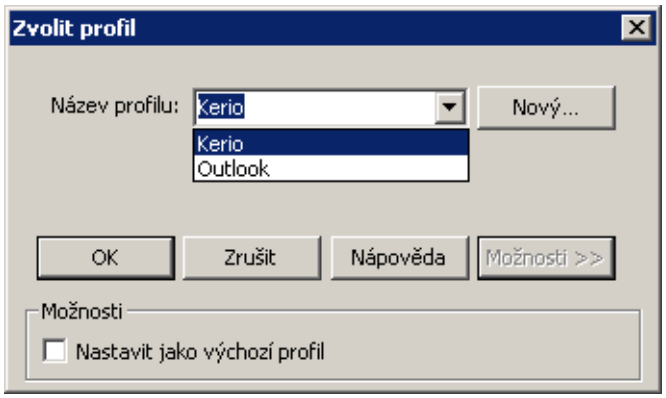
Jméno
Jméno uživatele pro odchozí poštu.

Elektronická adresa
Elektronická adresa, ze které mají být zprávy odesílány.

Adresa pro odpovědi
Adresa pro odpovědi na odeslané zprávy (položka `Reply-To:` ve zprávě).
Poznámka: Používáte-li MS Outlook 2000, potom se změny nastavené v záložce *Odesílatel* projeví až po restartu aplikace.

8. Po odsouhlasení celého nastavení tlačítkem *OK* se průvodce založením nového účtu uzavře. Nově založený profil najdeme v seznamu v dialogu *Pošta*. Nyní máme dvě možnosti nastavení práce s profily (viz obrázek 32.6):

   - *Vždy používat profil* — Náš nově vytvořený profil můžeme nastavit jako výchozí. To znamená, že při každém spuštění aplikace *MS Outlook* se automaticky otevře právě vytvořený profil s právě vytvořeným účtem.
   - *Nabídnout výběr profilu* — Dialog můžeme nastavit tak, aby se při každém spuštění aplikace *MS Outlook* zobrazilo výběrové menu se všemi profily, které jsou v něm založeny (viz obrázek 32.14).

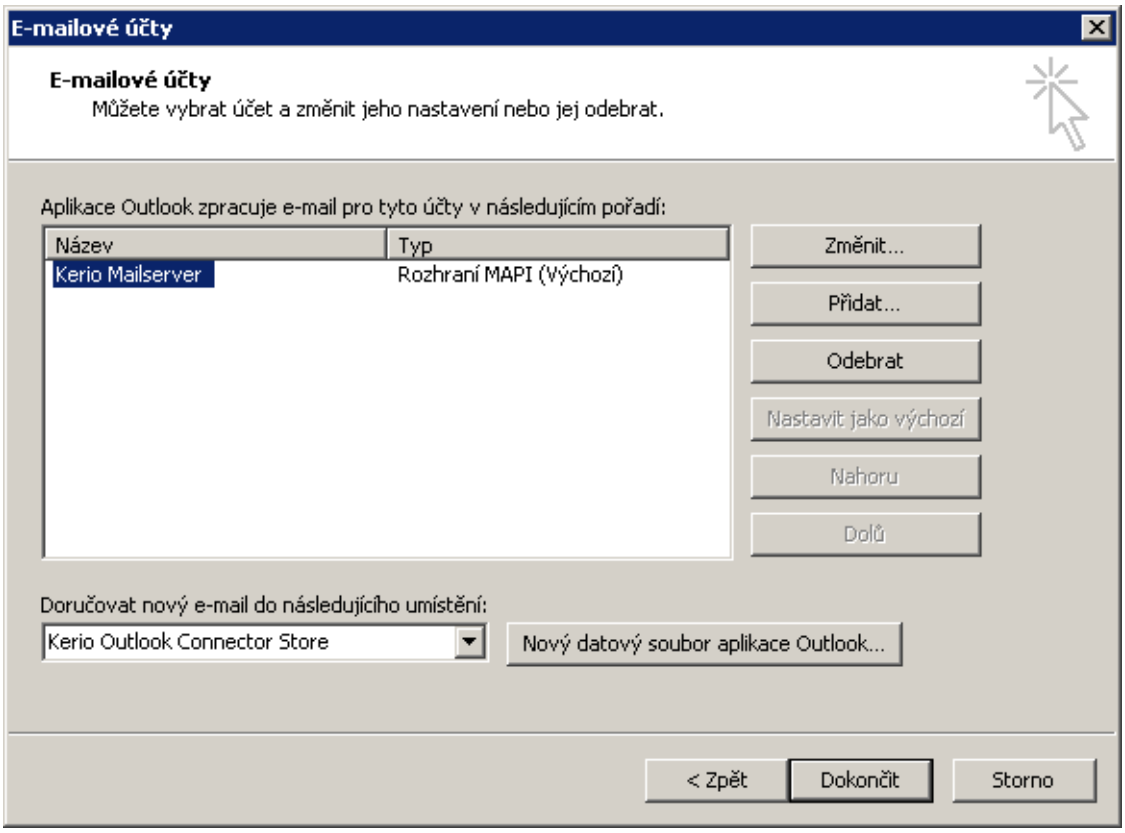


Obrázek 32.14 Výběr profilu

Upozornění: Každý profil v *MS Outlooku* může obsloužit pouze jeden účet připojený přes *Kerio Outlook Connector*. Funkci POP3 a IMAP účtů umístěných ve stejném profilu *Kerio Outlook Connector Store* neovlivní.
Poznámka: Používáte-li *MS Outlook 2000*, je nutné při konfiguraci profilu přidat položky *Kerio MailServer* a *MS Outlook Address Book*. Vyšší verze aplikace *MS Outlook* přidávají *Outlook Address Book* automaticky.

Nastavení datového souboru

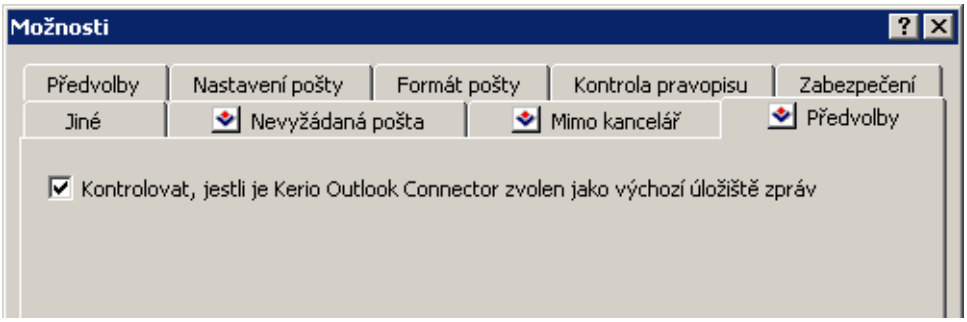
Pro správnou funkci *Kerio Outlook Connectoru* je třeba, aby výchozím datovým souborem v profilu byl *Kerio Outlook Connector Store*. Pokud tento datový soubor nebyl nastaven automaticky, lze tak učinit pomocí menu *Nástroje* → *Účty elektronické pošty* → *Zobrazit nebo změnit existující účty elektronické pošty*. Okno *Účty elektronické pošty* obsahuje menu *Doručovat nový e-mail do následujícího umístění*, kde je možné vybrat správný datový soubor (*Kerio Outlook Connector Store*).



Obrázek 32.15 Nastavení datového souboru

Kerio Outlook Connector obsahuje kontrolu, zda je *Kerio Outlook Connector Store* zvolen jako výchozí úložiště zpráv. Tato kontrola je standardně zapnuta, a v případě, že při spuštění aplikace *MS Outlook* není *Kerio Outlook Connector Store* zvolen jako výchozí úložiště, otevře se varovný dialog.

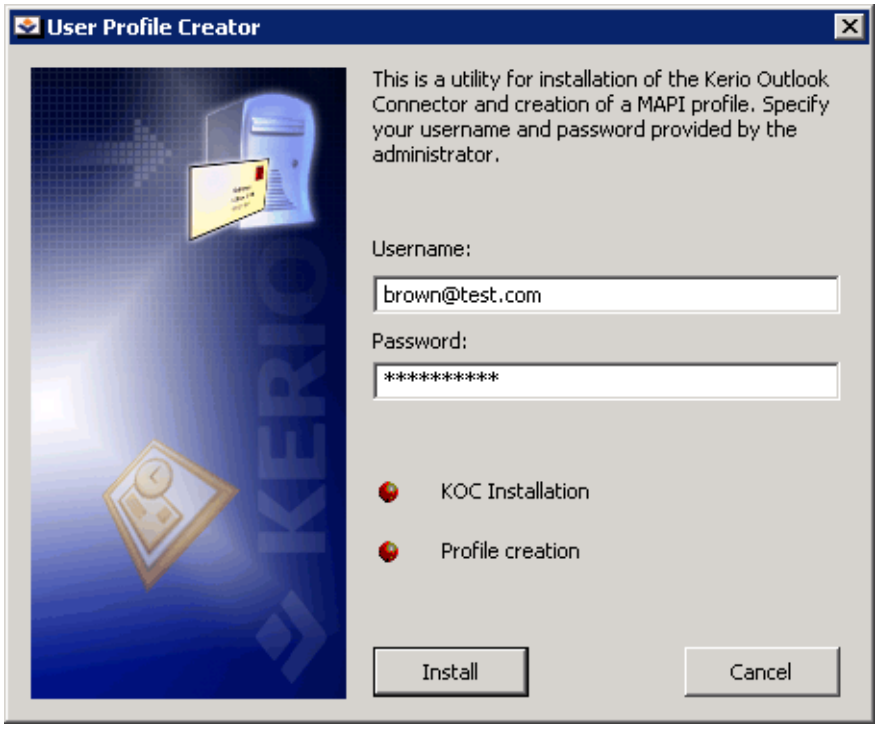
Zapnout/vypnout tuto kontrolu je možno v menu *Nástroje* → *Možnosti* → *Předvolby* (se znakem *Kerio Technologies*).



Obrázek 32.16 Kontrola úložiště

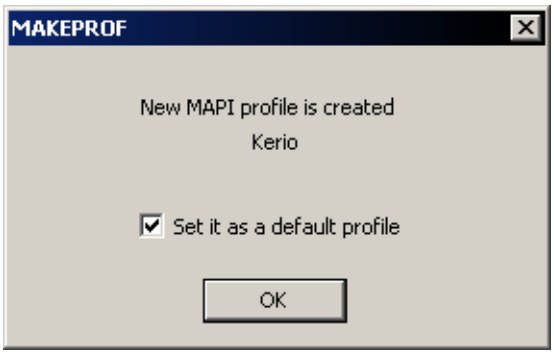
32.2.2 Instalace a vytvoření profilu pomocí migračního nástroje

Kerio Outlook Connector lze nainstalovat na klientské stanice zároveň s migrací účtů z *MS Exchange* do *Kerio MailServeru*. Migraci zprostředkovává speciální aplikace *Kerio MailServer Migration*. Zároveň s instalací je automaticky provedeno též základní nastavení profilu a účtu uživatele. Klientské počítače je možno obsloužit všechny zároveň. Každému uživateli, jehož schránka byla migrována, přijde zpráva s odkazem na automatickou instalaci *Kerio Outlook Connectoru*.



Obrázek 32.17 Průvodce vytvořením nového profilu

Jakmile uživatel klikne na odkaz, otevře se průvodce, kam je nutné zadat elektronickou adresu a heslo k e-mailové schránce. Po nastavení těchto údajů se spustí samotná instalace. Proběhla-li úspěšně, objeví se dialog s oznámením, že profil byl úspěšně vytvořen. V tomto dialogu si uživatelé mohou zaškrtnutím volby *Set it as a default profile* hned vybrat, zda chtějí nový profil používat jako výchozí. Po otevření tohoto profilu v aplikaci *MS Outlook* bude založen MAPI účet s názvem *Kerio Outlook Connector Store*, kde uživatelé najdou všechny svoje složky, poštu, události i úkoly, které předtím používali v účtu *MS Exchange*.



Obrázek 32.18 Dialog s oznámením úspěšného vytvoření profilu

Poznámka: Instalujete-li *Kerio Outlook Connector* na *MS Outlook 2000*, je nutná další konfigurace vytvořeného profilu. Do profilu musí být ručně přidána služba *Outlook Address Book*.

Upozornění: Každý profil v *MS Outlook* může obsloužit pouze jeden účet připojený přes *Kerio Outlook Connector*. Funkci POP3 a IMAP účtů umístěných ve stejném profilu *Kerio Outlook Connector Store* neovlivní.

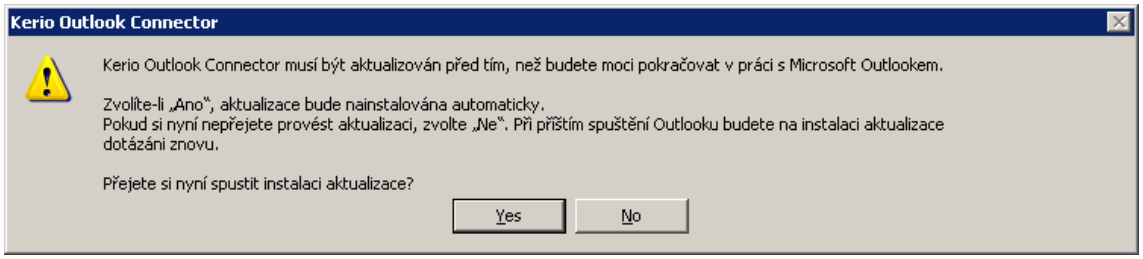
32.2.3 Aktualizace nových verzí Kerio Outlook Connectoru

Upgrade nových verzí *Kerio Outlook Connectoru* je prováděn naprosto automaticky. Je-li k dispozici nová verze *Kerio Outlook Connectoru*, potom se bezprostředně po spuštění aplikace *MS Outlook Kerio Outlook Connector* aktualizuje.

Upozornění: Po dokončení aktualizace následuje automatický restart aplikace *MS Outlook*.

Celá aktualizace včetně restartu aplikace trvá maximálně jednu až dvě minuty.

Automatická aktualizace obsahuje kontrolu verzí *Kerio MailServeru* a *Kerio Outlook Connectoru*. To znamená, že pokud verze serveru a klienta nesouhlasí, uživatel je informován o tom, že je na serveru nainstalována jiná verze *Kerio MailServeru*, a že je třeba klienta aktualizovat (viz obrázek 15.23). Po odsouhlasení tlačítkem ANO bude verze okamžitě aktualizována (nebo proveden downgrade — snížení verze).



Obrázek 32.19 Upozornění na nutnost aktualizace

Poznámka: Pokud se server od klienta liší jenom v čísle buildu (čísla verzí v upozorňujícím okně se neliší), bude klient funkční i v případě, že aktualizaci odmítnete. Pokud se server od klienta liší číslem verze (například `6.4.0` a `6.4.1`), potom se *Kerio Outlook Connector* bez příslušné aktualizace odmítne spustit.

Kapitola 33

Kerio Synchronization Plug-in

Kerio Synchronization Plug-in je rozšíření do aplikace *MS Outlook*, které umožňuje využívat základní groupwarové funkce (Kalendář, Kontakty a Poznámky) v osobních složkách. *Kerio Synchronization Plug-in* byl vytvořen pro často cestující uživatele, kteří potřebují pracovat se svou poštou, kalendářem a kontakty lokálně. Výhodou plug-inu, kromě možnosti využití groupwarových funkcí, je práce v režimu offline s možností po přepnutí do režimu online se připojit ke *Kerio MailServeru* a změněná data synchronizovat.

Poznámka: Pracovat offline v *MS Outlooku* lze také pomocí *Kerio Outlook Connectoru (Offline edition)* (více viz sekci 32.1).

Kerio Synchronization Plug-in k synchronizaci využívá protokol SyncML. SyncML je univerzální protokol pro synchronizaci dat z různých typů zařízení, přes jakoukoliv síť a s jakýmkoli úložištěm. V *Kerio Synchronization Plug-inu* je postaven nad službou HTTP.

Součástí *Kerio Synchronization Plug-inu* je také standardní *Nápověda*, která je umístěna v menu *Kerio Synchronization Plug-inu* na panelu nástrojů aplikace *MS Outlook*. Tuto nápovědu lze najít také v menu *Start* → *Programy* → *Kerio* → *Synchronization Plug-in*.

Upozornění: Kerio MailServer podporuje synchronizaci přes SyncML protokol pouze pro klientské rozšíření *Kerio Synchronization Plug-in*.

Instalaci *Kerio Synchronization Plug-inu* je možno spustit na těchto verzích operačního systému: Windows 2000 Professional (aktualizace Service Pack 4), XP (aktualizace Service Pack 1 nebo Service Pack 2) a Windows Vista (Home, Business, Enterprise nebo Ultimate edice).

Systém Windows musí obsahovat Internet Explorer ve verzi 6.0 a vyšší.

Pro správnou funkci *Kerio Synchronization Plug-inu* musí být v *Kerio MailServeru* spuštěny všechny příslušné služby:

- *HTTP(S)* — přes protokol probíhá samotná synchronizace a také automatická aktualizace nových verzí plug-inu.
- *IMAP(S)* — pro IMAP účty, pokud jsou uživateli využívány.
- *POP3(S)* — pro POP3 účty, pokud jsou uživateli využívány.
- *SMTP(S)* — přes protokol probíhá odesílání pošty.
- *LDAP(S)* — pokud budou chtít uživatelé využívat vyhledávání pomocí adresářové služby LDAP (více viz kapitolu 19).

Upozornění: Kromě výše zmíněných služeb je nutné namapovat příslušné porty na firewallu, kterým je server chráněn, jinak služby nebudou přístupné z Internetu (více viz sekci 2.3).

Kerio Synchronization Plug-in lze nainstalovat na následující verze *MS Outlooku*:

- MS Outlook 2000 + aktualizace Service Pack 3
- MS Outlook XP + aktualizace Service Pack 3
- MS Outlook 2003 + aktualizace Service Pack 2 (pro instalaci je třeba alespoň aktualizace Service Pack 1)
- MS Outlook 2007 + aktualizace Service Pack 1

Upozornění: Nelze využívat najednou *Kerio Outlook Connector* a *Kerio Synchronization Plug-in*. Obě aplikace mohou být nainstalovány a používány v jedné aplikaci *MS Outlook*, ale nemohou být využívány v jednom profilu nebo dokonce jedním účtem. *Kerio Synchronization Plug-in* může synchronizovat kalendářové a kontaktní složky pouze v osobních složkách aplikace *MS Outlook*. Ty lze kombinovat pouze s klasickým IMAP nebo POP3 účtem. MAPI účet synchronizovat nelze.

Konkrétní možnosti a nastavení *Kerio Synchronization Plug-inu* jsou popsána ve speciálním manuálu — *Kerio MailServer, Příručka uživatele*, který je k dispozici ke stažení na stránkách společnosti *Kerio Technologies* (`http://www.kerio.cz/kms-manual`).

Pokud se v synchronizaci objeví nějaký problém, zapněte v záznamu *Debug* volbu *Sync ML Synchronization* (jak a kde volbu zapnout je popsáno v kapitole 22.8). Záznam průběhu synchronizace vám může napomoci s přesnější identifikací a následným vyřešením problému.

Kerio Synchronization Plug-in je lokalizován do následujících jazyků:

- Angličtina
- Čeština
- Čínština
- Francouzština
- Holandština
- Chorvatština
- Italština
- Japonština
- Maďarština
- Němčina
- Polština
- Portugalština
- Ruština
- Španělština
- Švédština

Lokalizace *Kerio Synchronization Plug-in* se nastavuje automaticky podle lokalizace aplikace *MS Outlook*. V případě, že je *MS Outlook* v lokalizaci, kterou *Kerio Synchronization Plug-in* nemá k dispozici, bude automaticky lokalizován do anglického jazyka.

33.1 Instalace

Instalaci *Kerio Synchronization Plug-inu* je obvykle potřeba provést jenom jednou. Aktualizace na nové verze probíhá automaticky a uživatele nebude nijak zatěžovat (viz níže).

Instalace probíhá pomocí standardního průvodce. Aby proběhla úspěšně, je třeba provést následující kroky:

1. Ukončíme *MS Outlook*, pokud je spuštěn.
2. Provedeme instalaci *Kerio Synchronization Plug-inu*.
3. V aplikaci *MS Outlook* vytvoříme nový profil (jak se vytváří nový profil najdete v kapitole 32.2.1).
4. V průběhu vytváření profilu nastavíme příslušný POP3 nebo IMAP účet.
5. Spustíme *MS Outlook* a nastavíme synchronizaci podle návodu v uživatelské příručce ke *Kerio Synchronization Plug-inu*.

Využívá-li více uživatelů jeden *MS Outlook* a chtějí-li tito uživatelé ve svých účtech využít *Kerio Synchronization Plug-in*, potom je třeba:

1. aby každý z uživatelů využíval jiný profil (v každém profilu bude fungovat synchronizace jen na jednom účtu),
2. aby každý uživatel provedl instalaci *Kerio Synchronization Plug-inu* zvlášť,
3. aby byla první instalace provedena pod lokálním administrátorem,
4. aby měl každý z uživatelů nastavena práva „Power User“ nebo aby měl uděleno právo zápisu do adresáře, kam je *Kerio Synchronization Plug-in* nainstalován.

Upozornění:

- Na počítači nejprve musí být nainstalován *MS Outlook*, a teprve poté *Kerio Synchronization Plug-in*. V opačném případě nebude aplikace funkční.
- Při změně verze aplikace *MS Outlook* je nutné *Kerio Synchronization Plug-in* ručně přeinstalovat.

Automatická aktualizace

Aktualizace nových verzí *Kerio Synchronization Plug-inu* je prováděna naprosto automaticky a nezávisle na uživatelích. Aktuální verze *Kerio Synchronization Plug-inu* monitoruje *Kerio MailServer Engine*. Možnost stažení nové verze se zobrazuje v administrační konzoli (sekce *Další volby*, záložka *Aktualizace* — kapitola 15.6).

Nové verze *Kerio Synchronization Plug-inu* jsou ukládány v adresáři

```
Kerio\MailServer\webmail\download
```

Upozornění: Je-li v *Kerio MailServeru* povolena pouze komunikace přes HTTPS (například z důvodu bezpečnostní politiky serveru), potom je třeba, aby byl v *Internet Exploreru* klientské stanice nainstalován důvěryhodný certifikát *Kerio MailServeru* (může to být i self-signed certifikát). V opačném případě nebudou nové verze automaticky aktualizovány.

Poznámka: Kerio Synchronization Plug-in je aktualizován bezprostředně po spuštění *MS Outlooku* (ještě před výběrem profilu). Z toho důvodu se bude *Kerio Synchronization Plug-in* aktualizovat i v případě, že chcete pracovat v profilu který *Kerio Synchronization Plug-in* nevyužívá.

Kapitola 34

Podpora standardu iCalendar

Podpora formátu *iCalendar* ze strany *Kerio MailServeru* umožňuje různým aplikacím, které formát *iCalendar* podporují (například *MS Outlook 2007*, *Apple iCal*, *Windows Calendar*, *Mozilla Calendar*, *Lotus Notes* nebo *Ximian Evolution*) publikovat a přihlašovat kalendáře přes *Kerio MailServer*.

Kerio MailServer explicitně podporuje kalendáře v *MS Outlook 2007*, *Windows Calendar* ve Windows Vista a aplikaci *Apple iCal* na systémech Apple Mac OS X.

34.1 Internetové kalendáře v MS Outlooku 2007

MS Outlook 2007 umožňuje sdílení kalendářů přes Internet. Kalendáře je možné poskytnout pomocí přihlášení a publikace:

- *Přihlášení kalendáře* — přihlášení kalendáře znamená stažení kalendáře z webového úložiště do lokálního.
- *Publikace kalendáře* — publikace kalendáře znamená poskytnutí kalendáře do webového úložiště.

K manipulaci s kalendáři využívá *MS Outlook 2007* standard pro výměnu kalendářových dat iCalendar (dále iCal).

Kerio MailServer podporuje formát iCal, a proto je možné přihlašovat si do *MS Outlooku* kalendáře uložené v *Kerio MailServeru* a stejně tak je možné kalendáře do schránek *Kerio MailServeru* publikovat. Uživatelé si mohou přihlašovat nejen vlastní kalendáře, ale také kalendáře nasdílené jinými uživateli.

Upozornění: Přihlášené kalendáře jsou v *MS Outlooku* k dispozici pouze pro čtení. Publikované kalendáře jsou k dispozici pouze pro čtení na serveru (například při přístupu ke kalendářům pomocí rozhraní *Kerio WebMail* nebude možné publikované kalendáře měnit).

Komunikace při přihlášení probíhá pomocí protokolu HTTP. Z toho vyplývá, že je třeba spustit tuto službu v *Kerio MailServeru*. Kromě toho je nutné namapovat příslušný port na firewallu, kterým je server chráněn, jinak služba nebude přístupná z Internetu (více viz sekci 2.3).

Používání přihlašování a publikování kalendářů může být výhodná zejména v těch případech, kdy uživatelé chtějí zobrazit kalendář osoby, která nemá založen účet v *Kerio*

MailServeru nebo v případě, kdy chce naopak svůj kalendář poskytnout kalendář veřejně na Internetu.

Konkrétní možnosti a nastavení v *MS Outlooku* jsou popsána ve speciálním manuálu — *Kerio MailServer, Příručka uživatele*. Tento manuál je k dispozici na stránkách společnosti *Kerio Technologies* (`http://www.kerio.cz/kms-manual`).

34.2 Windows Calendar

Windows Calendar je aplikace pro správu kalendářů vyvinutá firmou *Microsoft Corporation* pro operační systém *Windows Vista*. Tato aplikace umožňuje promítnutí událostí z více kalendářů do jednoho rozvrhu a identifikovat tak rychle konflikty v časovém plánu. Kalendáře mohou být umístěny buď přímo na disku, nebo je možno přihlásit si kalendáře umístěné na webovém serveru. Kalendáře je možné na webový server také publikovat.

Podpora ze strany *Kerio MailServeru* spočívá v možnosti publikovat kalendáře do své poštovní schránky na serveru nebo si do *Windows Calendar* kalendáře z poštovní schránky přihlašovat. Uživatelé si mohou přihlašovat nejen vlastní kalendáře, ale také kalendáře nasdílené jinými uživateli.

Upozornění: Přihlášené kalendáře jsou ve *Windows Calendar* k dispozici pouze pro čtení. Publikované kalendáře jsou k dispozici pouze pro čtení na serveru (například při přístupu ke kalendářům pomocí rozhraní *Kerio WebMail* nebude možné publikované kalendáře měnit).

Komunikace při přihlášení (subskripce) probíhá pomocí protokolu HTTP nebo HTTPS. Publikace kalendářů probíhá pouze přes HTTPS. Z toho vyplývá, že je třeba spustit tuto službu v *Kerio MailServeru* a na počítač s *Windows Calendar* nainstalovat validní SSL certifikát *Kerio MailServeru*. Kromě toho je nutné namapovat příslušný port na firewallu, kterým je server chráněn, jinak služba nebude přístupná z Internetu (více viz sekci 2.3).

Aplikace *Windows Calendar* podporuje formát *iCalendar*. *iCalendar* je standard pro výměnu kalendářových dat. Zabudováním podpory standardu *iCalendar* do *Kerio MailServeru* vznikla možnost spolupráce *Kerio MailServeru* a *Windows Calendar*.

Poznámka: Budou-li kalendáře publikované jako podsložky hlavního kalendáře *Calendar*, budou se všechny události zobrazovat také ve *Free/Busy* kalendáři.

Konkrétní možnosti a nastavení v *Windows Calendar* jsou popsána ve speciálním manuálu — *Kerio MailServer, Příručka uživatele*. Tento manuál je k dispozici ke stažení na stránkách společnosti *Kerio Technologies* (`http://www.kerio.cz/kms-manual`).

34.3 Apple iCal

Apple iCal je aplikace vyvinutá firmou *Apple Computer* pro operační systémy řady *Mac OS X*. Aplikace umožňuje správu libovolného množství kalendářů a také promítnutí událostí z více kalendářů do jednoho rozvrhu a identifikovat tak rychle konflikty v časovém plánu.

Kalendáře mohou být umístěny buď přímo na disku, nebo je možno přihlásit si s právy pro čtení kalendáře umístěné na webovém serveru. Dále je možné kalendáře na webový server publikovat.

Podpora ze strany *Kerio MailServeru* spočívá v možnosti publikovat kalendáře do své poštovní schránky na serveru nebo si do *Apple iCal* kalendáře z poštovní schránky přihlašovat. Uživatelé si mohou přihlašovat nejen vlastní kalendáře, ale také kalendáře nasdílené jinými uživateli.

Upozornění: Přihlášené kalendáře jsou v *Apple iCal* k dispozici pouze pro čtení. Publikované kalendáře jsou k dispozici pouze pro čtení na serveru (například při přístupu ke kalendářům pomocí rozhraní *Kerio WebMail* nebude možné publikované kalendáře měnit).

Poznámka: Od verze *Apple iCal* pro Mac OS X Tiger je možné synchronizovat lokálně uložené kalendáře s kalendáři umístěnými v *Kerio MailServeru*. K tomu je potřeba nainstalovat aplikaci *Kerio Sync Connector* (více viz kapitolu 40).

Přihlášení (subskripce) i publikace kalendářů jsou prováděny pomocí protokolu HTTP (použití HTTPS není v tomto případě možné). Z toho vyplývá, že je třeba v *Kerio MailServeru* spustit službu HTTP. Kromě toho je nutné namapovat příslušný port na firewallu, kterým je server chráněn, jinak služba nebude přístupná z Internetu (více viz sekci 2.3).

Ke správě kalendářů využívá *Apple iCal*, jak ostatně vyplývá již z názvu, formát *iCalendar* (vyskytuje se také pod názvem *iCal*). *iCalendar* je standard pro výměnu kalendářových dat. Zabudováním podpory standardu *iCalendar* do *Kerio MailServeru* vznikla možnost spolupráce *Kerio MailServeru* a *Apple iCal*.

Poznámka: Budou-li kalendáře publikované jako podsložky hlavního kalendáře *Calendar*, budou se všechny události zobrazovat také ve *Free/Busy* kalendáři.

Konkrétní možnosti a nastavení v *Apple iCal* jsou popsána v manuálu *Kerio MailServer, Příručka uživatele*. Tento manuál je k dispozici ke stažení na stránkách společnosti *Kerio Technologies* (`http://www.kerio.cz/kms-manual`).

Kapitola 35

Podpora protokolu CalDAV

Kerio MailServer obsahuje od verze 6.5.0 podporu protokolu CalDAV, což je rozšíření rozhraní WebDAV, které bylo navrženo speciálně pro výměnu kalendářových dat. Více se o tomto protokolu dozvíte na stránkách `http://www.caldav.org/`. CalDAV standard je definován v RFC 4791.

CalDAV je protokol založený na protokolu HTTP, proto pokud jej budete chtít používat, je třeba provozovat v *Kerio MailServeru* službu HTTP(S).

Pomocí protokolu lze synchronizovat kalendáře, plánovat schůzky za pomoci Free/Busy serveru nebo delegovat kalendáře dalším uživatelům *Kerio MailServeru*.

35.1 Apple iCal

Oficiálně podporovaným CalDAV klientem je aplikace *Apple iCal*, což je specializovaný program pro správu kalendářů v systémech Mac OS X. *Apple iCal* podporuje protokol CalDAV od verze Mac OS X 10.5 Leopard. Podpora ze strany *Kerio MailServeru* v současné době umožňuje:

- synchronizaci kalendářů,
- synchronizace To Do se složkou Úkoly,
- plánování schůzek,
- přihlášení delegovaných kalendářů,
- poskytování Free/Busy informací o uživatelích, kteří mají založen účet v *Kerio MailServeru*.

Upozornění: Po spuštění synchronizace přes CalDAV v *Apple iCal* se automaticky vypne synchronizace kalendářů přes *Kerio Sync Connector*. Synchronizace kontaktů, pokud je nakonfigurována, zůstane spuštěna.

35.2 Nastavení

Aby se klient mohl připojit ke *Kerio MailServeru*, je nutné nastavit správnou URL adresu pro připojení.

Apple iCal

```
http(s)://<servername>/caldav
```

například:

`http(s)://mail.firma.cz/caldav`

Ostatní klienti (například Mozilla Sunbird)

`http(s)://<servername>/calendars/<domain>/<user>/<calendarname>`

například:

`http(s)://mail.firma.cz/calendars/firma.cz/jnovak/Calendar`

Kapitola 36

Podpora pro ActiveSync

Podpora protokolu *ActiveSync* umožňuje uživatelům synchronizovat jejich e-maily, kalendář, kontakty a případně také úkoly a poznámky s mobilními zařízeními založenými na systémech *Windows Mobile*, *Palm OS* a *Symbian* (aktuální seznam podporovaných mobilních zařízení obsahuje sekce 36.2). *ActiveSync* protokol je založen na protokolu HTTP(S). Pro síťové připojení využívá technologie WiFi, GPRS, UMTS, a další.

Kerio MailServer podporuje protokol přímo, takže pokud podporu *ActiveSync* obsahuje také zařízení, není třeba do zařízení instalovat žádnou utilitu. Pokud zařízení protokol nepodporuje, potom je třeba do něj nainstalovat aplikaci, která synchronizaci umožní. Popis nastavení všech konkrétních zařízení obsahuje příručka k danému zařízení, ale také manuál *Kerio MailServer, Příručka uživatele* (`http://www.kerio.cz/kms-manual`), který v kapitole `Synchronizace dat s mobilními zařízeními` soustřeďuje jednoduché návody nastavení synchronizace všech podporovaných zařízení.

Podpora protokolu nevyžaduje žádná nastavení ani na straně *Kerio MailServeru*. Jedinou podmínkou je spuštění služby HTTP(S) na standardním portu (v případě HTTP je to port 80 a v případě verze šifrované SSL je to port 443). Porty ve většině podporovaných mobilních zařízeních nelze měnit na nestandardní.

Upozornění: Kromě spuštění služeb na serveru je také nutné namapovat příslušný port nebo porty pro HTTP a HTTPS na firewallu, kterým je server chráněn, jinak služba nebude přístupná z Internetu (více viz sekci 2.3).

36.1 Typy synchronizace

Synchronizovat data *Kerio MailServeru* s mobilním zařízením lze dvěma různými způsoby:

1. Přímá synchronizace se serverem.
2. Synchronizace pomocí desktopové aplikace, kterou nainstalujeme na svou pracovní stanici.

Poznámka: Oba způsoby synchronizace je obvykle možné kombinovat.

Přímá synchronizace s Kerio MailServerem

Tímto typem synchronizace, jejím nastavením, možnostmi a praktickým využitím se budeme věnovat v celé kapitole *Podpora pro ActiveSync*.

Při přímé synchronizaci odpadá nutnost připojit se zařízením ke svému osobnímu počítači. Technologie umožňuje připojit se přes HTTP(S) protokolem *ActiveSync* přímo k poštovnímu serveru a synchronizovat složky v poštovní schránce se složkami v mobilním zařízení. Pokud má zařízení nastaveno také přístup na Internet, může si uživatel data synchronizovat kdykoliv, v novějších typech zařízení díky takzvané *DirectPush* technologii dokonce online.

Tento typ synchronizace umožňuje synchronizovat následující typy složek:

- poštovní složky,
- kontakty (kromě Palm Treo 650),
- kalendář,
- úkoly — synchronizaci úkolů umožňují pouze zařízení se systémem *Windows Mobile 5.0* a vyšší.

Poznámka: Implementace protokolu *ActiveSync* v *Kerio MailServeru* umožňuje také synchronizaci veřejných a sdílených poštovních složek (platí pouze pro zařízení s *Windows Mobile*).

K přímé synchronizaci se serverem je potřeba nastavit následující:

- V *Kerio MailServeru* musí být spuštěna služba HTTP(S). Pokud se uživatel bude chtít připojit k serveru z Internetu, potom bude třeba také povolit příslušný port (obvykle pouze pro službu HTTPS) na firewallu, za kterým je *Kerio MailServer* spuštěn.
- V zařízení musí být správně nastaveno síťové připojení.
- Bude-li se uživatel připojovat přes protokol HTTPS (doporučeno z bezpečnostních důvodů), pak je třeba mít v zařízení nainstalován důvěryhodný certifikát (více viz kapitolu 36.4).
- Zařízení musí být nastaveno tak, aby se mohlo připojit ke *Kerio MailServeru*. To závisí na typu zařízení:

  Windows Mobile

  V systémech Windows Mobile je třeba nastavit aplikaci *ActiveSync* tak, aby se mohla připojit k serveru. Toto nastavení je pro různé verze Windows Mobile odlišné. V zásadě ale otevřeme v zařízení aplikaci *ActiveSync*, v *Menu* vyhledáme položku *Add Server Source* (Windows Mobile 2005) nebo v menu *Tools* vyhledáme záložku *Server* (Windows Mobile 2003) a zde doplníme internetové jméno *Kerio MailServeru* a uživatelské jméno a heslo pro připojení ke schránce. Podrobně tato nastavení popisuje manuál *Kerio MailServer, Příručka uživatele* (`http://www.kerio.cz/kms-manual`). Zde lze najít jednoduché návody nastavení aplikace *ActiveSync* pro všechny podporované verze Windows Mobile.

Palm Treo 650, 680 a 700p
: Synchronizace přes *ActiveSync* s poštovním serverem se v *Palm Treo 650* nastavuje v poštovním klientovi *Versa Mail*. V konfiguraci účtu je třeba nastavit volbu *Mail Service* na *Exchange ActiveSync* a doplnit do účtu internetové jméno *Kerio MailServeru* a přihlašovací jméno a heslo pro připojení ke schránce.
Podrobněji je toto nastavení popsáno v manuálu *Kerio MailServer, Příručka uživatele* (`http://www.kerio.cz/kms-manual`).

Nokia E-series
: Mobilní zařízení řady *Nokia Eseries* podporují protokol *ActiveSync*, pokud do zařízení nainstalujeme aplikaci *Email For Exchange* vyvinutou společností *Nokia*. Instalaci a nastavení popisuje manuál *Kerio MailServer, Příručka uživatele* (`http://www.kerio.cz/kms-manual`).

Mobilní zařízení s RoadSync
: Aplikace RoadSync společnosti *DataViz* umožňuje synchronizaci pošty, kalendáře a kontaktů přes *ActiveSync* protokol. O aplikaci a nastavení mobilních zařízení lze najít příslušné informace na `http://www.dataviz.com/`.

Synchronizace pomocí desktopové aplikace ActiveSync

Tuto možnost synchronizace pouze zmiňujeme, protože synchronizace probíhá nezávisle na *Kerio MailServeru* a její nastavení lze najít v uživatelských příručkách k desktopové aplikaci *ActiveSync*, případně v manuálu k danému zařízení.

Upozornění: Zde uvedená nastavení platí pouze pro *Windows Mobile*.

Pro úspěšnou synchronizaci dat pomocí desktopové aplikace *ActiveSync* je potřeba následující:

- Mobilní zařízení musí obsahovat některou verzi aplikace *ActiveSync* (všechny podporované verze systémů *Windows Mobile* ji mají ve standardní výbavě).
- Osobní počítač uživatele musí být vybaven aplikací *MS Outlook*. V *MS Outlooku* musí být založen účet připojený ke *Kerio MailServeru* (doporučujeme nastavit Kerio účet doplněný o *Kerio Outlook Connector*, protože pak je možné synchronizovat také složky typu *Poznámky*).
- Osobní počítač uživatele musí obsahovat desktopovou aplikaci *ActiveSync*.

Synchronizace se serverem přes desktopovou aplikaci probíhá tak, že data ze serveru má díky přihlášenému poštovnímu účtu k dispozici *MS Outlook*. *MS Outlook* se synchronizuje s desktopovou aplikací *ActiveSync* a desktopová aplikace se po připojení k zařízení může synchronizovat se zařízením. Celý proces funguje samozřejmě i obráceně. Po připojení zařízení se nová data synchronizují přes desktopovou aplikaci *ActiveSync* s aplikací *MS Outlook* a ta data promítne i do složek v *Kerio MailServeru*.

Nespornou výhodou synchronizace přes *MS Outlook* a desktopovou aplikaci je možnost synchronizace všech typů složek, které se na serveru nacházejí (tedy i úkoly a poznámky ve všech verzích zařízení).

36.2 Podporované verze ActiveSync a mobilních zařízení

Kerio MailServer podporuje tyto verze protokolu *ActiveSync*:

- ActiveSync 1.0 (Windows Mobile 2002, Palm OS — Palm Treo 650)
- ActiveSync 2.0 (Windows Mobile 2003, Palm OS — Palm Treo 680, 700p)
- ActiveSync 2.1 (Windows Mobile 2003 SE)
- ActiveSync 2.5 (Windows Mobile 5.0, Windows Mobile 5.0 AKU2)

Poznámka: Číslo verze *ActiveSync* je v tomto případě číslo verze protokolu, ne číslo verze desktopové aplikace.

Kerio MailServer podporuje celou řadu mobilních zařízení. Tabulka 36.1 obsahuje přehled podporovaných zařízení založených na systému *Windows Mobile*.

Verze	Založeno na	Datum vydání
Windows Mobile 2002 (Pocket PC 3.0)	Windows CE 3.0	Leden 2002
Windows Mobile 2003 (Pocket PC 4.2)	Windows CE 4.20	Červen 2003
Windows Mobile 2003 Second Edition (SE)	Windows CE 4.21	Březen 2004
Windows Mobile 5.0	Windows CE 5.0	Květen 2005
Windows Mobile 5.0 AKU2	Windows CE 5.1	Únor 2006
Windows Mobile 6.0	Windows CE 5.2	Únor 2007

Tabulka 36.1 Přehled podporovaných systémů založených na systému MS Windows Mobile

Poznámka: Kerio MailServer podporuje jak *Windows Mobile* pro Pocket PC, tak edici pro Smartphone (systém pro zařízení bez dotykového displeje).

Další podporovaná zařízení obsahuje tabulka 36.2.

Podrobnosti o jednotlivých funkcích zařízení a jeho nastavení lze získat z originálního manuálu k danému zařízení. Nastavení aplikace *ActiveSync* v zařízení, tak aby se toto zařízení mohlo připojit ke *Kerio MailServeru* a úspěšně synchronizovat data, popisuje samostatná kapitola `Synchronizace dat s mobilními zařízeními` v manuálu *Kerio MailServer, Příručka uživatele* (`http://www.kerio.cz/kms-manual`).

Různé verze systémů poskytují různé možnosti spolupráce. Starší verze *Windows Mobile* neumožňují využití všech možností *Kerio MailServeru*. Vlastnosti využitelné na jednotlivých verzích podporovaných operačních systémů znázorňuje tabulka 36.3.

Následující vlastnosti *Kerio MailServer* nepodporuje:

Typ zařízení	Systém
Palm Treo 650, 680 a 700p	Palm OS
Palm Treo 700w a 750v	Windows Mobile 5.0 AKU2
Nokia Eseries[a]	Symbian OS 9.1
Nokia N73 a N95[b]	Symbian S60 3rd edition
Sony Ericsson M600, P990i[c]	Symbian UIQ

[a] Zařízení Nokia Eseries jsou podporována po instalaci externí aplikace Mail for Exchange 1.3.0 a vyšší.
[b] Obě zařízení Nokia Nseries jsou podporována po instalaci externí aplikace Mail for Exchange 1.6.1 a vyšší.
[c] Sony Ericsson M600 a P990i jsou podporovány po instalaci externí aplikace Exchange ActiveSync 2.10 a vyšší.

Tabulka 36.2 Přehled ostatních podporovaných zařízení

Typ zařízení	Pošta	Kalendář	Kontakty	Úkoly	Direct Push	Global Address Lookup	Kerio Smart Wipe
WM 2002	ANO	ANO	ANO				ANO
WM 2003 a WM 2003 SE	ANO	ANO	ANO				ANO
WM 5.0	ANO	ANO	ANO	ANO			ANO
WM 5.0 AKU2	ANO	ANO	ANO	ANO	ANO	ANO	ANO
WM 6.0	ANO	ANO	ANO	ANO	ANO	ANO	ANO
Palm Treo 700w a 750v	ANO	ANO	ANO	ANO	ANO	ANO	ANO
Palm Treo 650	ANO	ANO			ANO[a]	ANO[a]	ANO
Palm Treo 680 a 700p	ANO	ANO	ANO		ANO[b]	ANO[b]	ANO
Nokia Eseries[c]	ANO	ANO	ANO		ANO	ANO	ANO
Nokia N73 a N95[d]	ANO	ANO	ANO		ANO	ANO	ANO
Sony Ericsson M600 a P990i[e]	ANO	ANO	ANO		ANO	ANO	ANO

[a] Vyžaduje upgrade na VersaMail 3.5 a instalaci Exchange ActiveSync Update for Treo 650 smartphone. Bližší informace lze najít na `http://software.palm.com/`.
[b] Vyžaduje instalaci EAS SP 2 update (`http://www.palm.com/us/support/downloads/treo/easupdate.html`).
[c] Zařízení Nokia Eseries jsou podporována po instalaci externí aplikace Mail for Exchange 1.3.0 a vyšší.
[d] Obě zařízení Nokia Nseries jsou podporována po instalaci externí aplikace Mail for Exchange 1.6.1 a vyšší.
[e] Sony Ericsson M600 a P990i jsou podporovány po instalaci externí aplikace Exchange ActiveSync 2.10 a vyšší.

Tabulka 36.3 Podpora vlastností mobilních zařízení

- Nastavení bezpečnostní politiky ze serveru (Enforce Security Policy)
- SMS-based Always Up-To-Date (AUTD)

36.3 RoadSync

Kerio MailServer podporuje aplikaci *RoadSync 2.0* vyvinutou společností *DataViz*. *RoadSync* umožňuje synchronizaci dat mezi *Kerio MailServerem* a mobilními zařízeními. Synchronizace probíhá pomocí protokolu *ActiveSync*.

RoadSync podporuje synchronizaci následujících typů složek:

- Pošta,
- Kalendář,
- Kontakty.

Aplikaci *RoadSync* lze nainstalovat na následující typy mobilních zařízení:

- Symbian UIQ,
- Symbian S80,
- Symbian S60 3rd Edition,
- Palm OS (synchronizace je omezena pouze na e-maily),
- Java MIDP 2.0 (synchronizace je omezena pouze na e-maily).

Více informací o produktu *RoadSync* a konkrétně podporovaných zařízeních lze najít na stránkách společnosti *DataViz* `http://www.dataviz.com/`.

36.4 SSL šifrování

ActiveSync může pro komunikaci využívat protokol HTTP nebo jeho šifrovanou verzi HTTPS.

Upozornění: Z bezpečnostních důvodů důrazně doporučujeme používat pro synchronizaci výhradně protokol HTTPS, protože *ActiveSync* používá k ověření na serveru pouze nešifrované přihlašovací údaje uživatele.

Princip šifrování služeb spuštěných v *Kerio MailServeru* popisuje kapitola 10. Tento princip mimo jiné předpokládá instalaci validního SSL certifikátu do zařízení.

Validní certifikát musí obsahovat tyto náležitosti:

- Certifikát musí být vydán důvěryhodnou certifikační autoritou. To znamená, že mobilní zařízení musí znát kořenový certifikát serveru. *Windows Mobile* standardně obsahuje kořenové certifikáty několika certifikačních autorit. Jejich seznam lze najít na stránkách společnosti Microsoft Corporation.
- Musí být platné datum certifikátu, a zároveň je třeba mít nastavené správné datum a čas v zařízení.
- Certifikát musí obsahovat platný název poštovní domény, kterou *Kerio MailServer* obsluhuje.

Jako validní certifikát lze pro šifrovanou komunikaci využít buď certifikát vydaný důvěryhodnou certifikační autoritou (ten je sice poměrně drahý, ale na druhou stranu s ním

nejsou žádné problémy při instalaci), nebo certifikát vydaný interní certifikační autoritou, a nebo lze využít takzvaný self-signed certifikát vytvořený přímo v *Kerio MailServeru* (více viz kapitolu 10).

V případě certifikátu od certifikační autority, kterou zařízení podporuje, není potřeba nic nastavovat ani instalovat. V případě interních nebo self-signed certifikátů je třeba do zařízení kořenový certifikát nainstalovat.

Windows Mobile potřebuje certifikát kódovaný v DER X.509 formátu. Soubor musí mít příponu `.cer`. Nejsnadnějším způsobem, jak certifikát do zařízení nainstalovat, je stáhnout ho pomocí prohlížeče v zařízení.

Kerio MailServer svůj certifikát ve zmiňovaném formátu poskytuje na URL adrese `http://nazev_serveru/server.cer`

V zařízeních s *Windows Mobile 2002* lze pro komunikaci použít pouze protokol HTTPS. Nešifrovaná verze není vůbec podporována. Navíc je třeba, aby *Kerio MailServer* používal k ověření certifikát ověřený certifikační autoritou. K tomu lze použít buď certifikát ověřený podporovanou komerční certifikační autoritou (podporovány jsou certifikáty od certifikačních autorit VeriSign, CyberTrust, Thawte a Entrust) nebo je třeba do zařízení nainstalovat kořenový certifikát autority, která vydala certifikát pro *Kerio MailServer* (více viz sekci *Povolení instalace kořenového certifikátu ve WM 2002*).

Upozornění: Do *Windows Mobile 2002* nelze nainstalovat self-signed certifikát *Kerio MailServeru*. Musí to být certifikát kořenový, ověřený alespoň interní certifikační autoritou.

Od verze *Windows Mobile 2003* nastavení aplikace *ActiveSync* obsahuje volbu pro zapnutí/vypnutí SSL šifrování. Použití SSL šifrování však důrazně doporučujeme, protože synchronizace pro ověřování uživatelů používá pouze metodu basic authentication (přihlašovací údaje jsou přenášeny nešifrovaně a je možné je odchytit a přečíst).

Od verze *Windows Mobile 2003* je instalace self-signed certifikátu do zařízení poměrně jednoduchá. Postup obsahuje sekce *Instalace kořenového self-signed certifikátu Kerio MailServeru*.

Upozornění: Bezpečnostní pravidla v zařízeních typu Smartphone s *Windows Mobile 2005* zakazují instalaci nových kořenových certifikátů. V takových případech je nutné nejprve povolit instalaci kořenových certifikátů v registru zařízení (postup viz níže).

Instalace self-signed certifikátu Kerio MailServeru

Instalaci self-signed certifikátu *Kerio MailServeru* lze provést následovně:

1. V případě, že chceme certifikát nainstalovat do zařízení *Windows Mobile 2002* nebo do *Windows Mobile 5.0 Smartphone Edition*, je třeba se nejprve řídit návody v dalších

sekcích *Povolení instalace kořenového certifikátu ve WM 2002* a *Povolení instalace kořenového certifikátu ve WM 5.0 Smartphone Edition*. V ostatních případech začneme instalaci certifikátu bodem 2 tohoto návodu.

2. V mobilním zařízení spustíme internetový prohlížeč.

3. Do adresního řádku zadáme adresu serveru ve tvaru

   `http://nazev_serveru/server.cer`

   (například `http://mail.firma.cz/server.cer`)

   nebo

   `https://nazev_serveru/server.cer`

   (například `https://mail.firma.cz/server.cer`)

4. Prohlížeč se zeptá, zda chceme certifikát stáhnout do zařízení. Tlačítkem *OK* stažení certifikátu potvrdíme.

5. Dále se zařízení zeptá, zda chceme certifikát nainstalovat a používat jej. I toto okno potvrdíme tlačítkem *OK*.

Nyní je certifikát nainstalován.

Povolení instalace kořenového certifikátu ve WM 2002

Pro přidání kořenového certifikátu vydaného certifikační autoritou, kterou zařízení standardně nepodporuje je potřeba provést následující:

1. Stáhneme aplikaci `AddRootCert` [409KB] a rozbalíme ji.

2. Soubor `addrootcert.exe` nakopírujeme do zařízení.

3. Do zařízení zkopírujeme certifikát serveru (certifikát musí být kódovaný v DER X.509 formátu a musí mít koncovku `.cer`).

4. V zařízení klikneme na soubor `addrootcert.exe` a spustíme ho.

5. Otevře se aplikace, ve které certifikát nainstalujeme.

6. Zařízení restartujeme.

Povolení instalace kořenového certifikátu ve WM 5.0 Smartphone Edition

Zařízení typu Smartphone s operačním systémem *Windows Mobile 5.0* a *Windows Mobile 5.0 AKU2* mají jako součást své bezpečnostní politiky zakázáno instalovat kořenové certifikáty, které nebyly vydány důvěryhodnými certifikačními autoritami.

Abychom mohli do zařízení nainstalovat kořenový certifikát od autority, kterou dané zařízení nepodporuje (certifikát vydaný interní certifikační autoritou nebo self-signed certifikát *Kerio MailServeru*), je potřeba do mobilního zařízení nainstalovat některý z editorů registrů mobilních zařízení a pomocí tohoto editoru instalaci kořenového certifikátu povolit. Jednou z možností může být například aplikace `regeditSTG.zip` (24.01 KB), kterou lze získat zdarma na stránkách `http://www.htceurope.com/`.

Pomocí tohoto editoru registrů provedeme následující změnu:

1. Z výše uvedených stránek stáhneme aplikaci `regeditSTG.zip` a rozbalíme ji.
2. Přesuneme editor do mobilního telefonu (například pomocí desktopové aplikace *MS ActiveSync*).

   Upozornění: Soubor je třeba přesunout skutečně do telefonu a ne na paměťovou kartu.
3. Na soubor v telefonu klikneme a spustíme ho.
4. Spustíme `regeditSTG.exe` a najdeme uzel `HKLM\Security\Policies\Policies`
5. Změníme tři následující položky registru:
   - 00001001 na ze 2 na 1
   - 00001005 ze 16 na 40
   - 00001017 ze 128 na 144
6. Nyní bude možné certifikát bez problémů stáhnout ze serveru a nainstalovat jej podle návodu v sekci 36.4.

   Upozornění: Takzvaný „tvrdý reset“ zařízení změnu registru vymaže a je potřeba ji provést znovu.

SSL šifrování v zařízeních Sony Ericsson

Instalace self-signed certifikátu *Kerio MailServeru* způsobí, že zařízení bude vyžadovat souhlas s každou synchronizací se serverem:

```
[Security Information       ?]
The certificate could not be
verified.
```

```
Select 'Certificate details' to get
more information about the
certificate.
Do you want to accept the
certificate and proceed?
[ Yes ]  [  No  ]  [ Details ]
```

Z tohoto důvodu doporučujeme instalovat do zařízení certifikát podepsaný důvěryhodnou certifikační autoritou.

36.5 Vzdálené vymazání obsahu zařízení

Vzdálené vymazání obsahu zařízení umožňuje správci *Kerio MailServeru* pomocí jednoho kliknutí v administrační konzoli odstranit obsah synchronizovaných složek nebo dokonce obsah celého mobilního zařízení (takzvaný „tvrdý“ restart zařízení). Tato vlastnost může být velmi užitečná v případě, že uživatel mobilní zařízení ztratil nebo pokud mu bylo odcizeno. Data na zařízení jsou takto více chráněna a nemohou se dostat do rukou nepovolaným osobám. Kromě vymazání dat tento úkon zamezí také dalšímu připojení zařízení ke *Kerio MailServeru*, protože kromě vymazání synchronizovaných dat v zařízení *Kerio MailServer* zakáže přístup tohoto zařízení původními přihlašovacími údaji uživatele.

Zda bude možné provést restart zařízení nebo pouze odstranění složek podléhajících synchronizaci záleží na typu zařízení a hlavně systému. Tvrdý restart po síti totiž podporuje pouze systém *Windows Mobile 5.0 AKU2*. Nižší verze *Windows Mobile* tuto vlastnost nepodporují, a proto lze pouze vzdáleně odstranit všechna data podléhající synchronizaci aplikací *ActiveSync*.

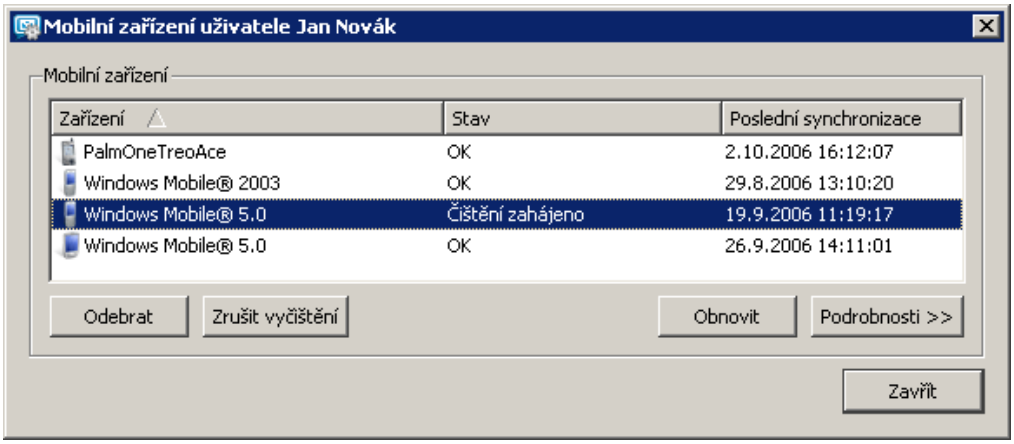
Poznámka: Vzdálené vymazání zařízení neumožňuje vymazání paměťových karet. Na paměťovou kartu se však standardně nahrávají přílohy e-mailových zpráv. *ActiveSync* umožňuje vymazání veškerých synchronizovaných dat, včetně zmíněných příloh. Takže po vzdáleném vymazání obsahu zařízení budou vymazána všechna data v zařízení a zároveň přílohy e-mailových zpráv uložené v paměťové kartě.

Vzdálené vymazání obsahu zařízení můžeme provést v administrační konzoli v sekci *Nastavení domény* → *Uživatelské účty*:

1. Označíme uživatele, který potřebuje vymazat obsah zařízení.

2. Pravým tlačítkem myši otevřeme kontextové menu a vybereme v něm položku *Stav* → *Mobilní zařízení*.

3. Otevře se okno pro správu mobilních zařízení daného uživatele (viz obrázek 36.1).



Obrázek 36.1 Dialog pro správu mobilních zařízení

4. Označíme zařízení, kterému chceme vymazat obsah a stiskneme tlačítko *Vyčistit*.

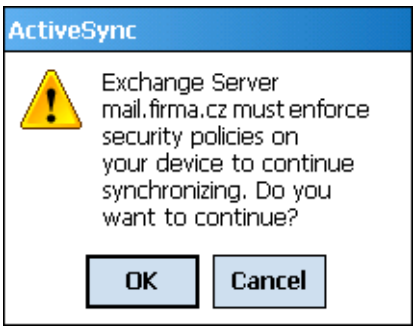
Upozornění: K vymazání obsahu dojde při následujícím připojení zařízení ke *Kerio MailServeru*. Takže pokud uživatel zařízení ztratil, informujte ho o tom, že při případném nalezení zařízení nesmí spustit synchronizaci a zároveň se musí ihned obrátit na správce, aby vymazání obsahu před použitím zařízení nejprve zrušil. Ke zrušení slouží tlačítko *Zrušit čištění*, které se objeví po použití tlačítka *Vyčistit*.

Informace o průběhu vyčištění zařízení se vypisují do záznamu *Security* (popisem záznamu *Security* se podrobně zabývá sekce 22.4).

Souhlas uživatele s možností vzdáleného vymazání obsahu zařízení

V operačních systémech Windows Mobile vyžaduje vzdálené vymazání obsahu zařízení explicitní souhlas uživatele s bezpečnostními pravidly synchronizace. Jinými slovy, uživatel musí odsouhlasit, že správce serveru může vzdálené vymazání provést. Z toho důvodu se během první synchronizace, která mezi zařízením a *Kerio MailServerem* proběhne (obvykle po nastavení přihlašovacích údajů *Kerio MailServeru* do aplikace *ActiveSync*), zobrazí v zařízení dialog (viz obrázek 36.2), který uživatel musí odsouhlasit. Bez tohoto odsouhlasení nebude možné synchronizaci dokončit.

Kerio MailServer tento souhlas na uživateli vyžaduje při první synchronizaci zařízení se serverem proto, aby se souhlas nezobrazil až ve chvíli, kdy zařízení může držet nepovolaná osoba.



Obrázek 36.2 Souhlas s vymazáním obsahu zařízení

36.6 Odstranění zařízení ze správce mobilních zařízení

Uživatelé mohou svá mobilní zařízení v průběhu času měnit za novější typy. Ty starší jsou ovšem i nadále připojeny ke *Kerio MailServeru*. Toto není žádný velký problém. Ovšem už z důvodu přehlednosti a orientace v zařízeních doporučujeme vymazat zařízení, která již nejsou používána.

Nepoužívaná mobilní zařízení lze vymazat následujícím způsobem:

1. V sekci *Nastavení domény* → *Uživatelské účty* vybereme uživatele, který už nepoužívá dané zařízení.
2. Klikneme na schránce pravým tlačítkem myši a otevřeme kontextové menu, kde vybereme položku *Mobilní zařízení*.
3. Otevře se okno pro správu mobilních zařízení uživatele (viz obrázek 36.1).
4. Označíme zařízení, kterému chceme vymazat obsah a stiskneme tlačítko *Smazat*.

36.7 Záznamy synchronizace

Celý proces synchronizace lze sledovat pomocí nástrojů k zaznamenávání komunikace. Tyto nástroje jsou umístěny jak v administrační konzoli *Kerio MailServeru*, tak přímo v mobilním zařízení. Tato sekce obsahuje popis a nastavení těchto nástrojů:

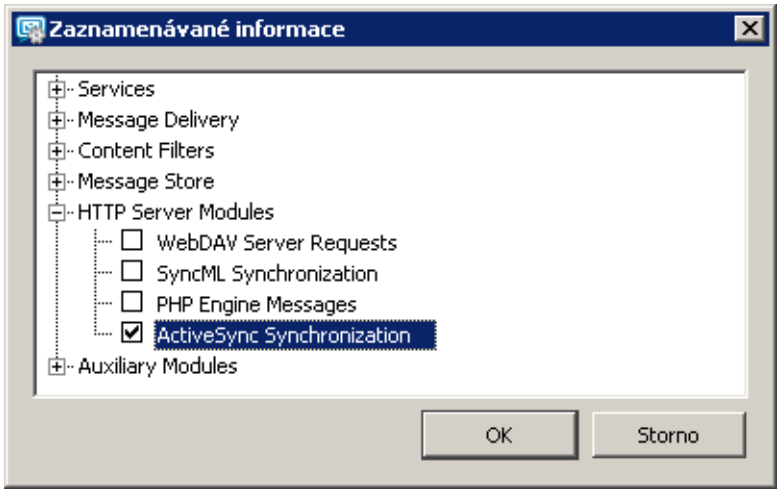
Záznam synchronizace v Kerio MailServeru

Kerio Administration Console obsahuje pro záznam komunikace speciální volbu v záznamu *Debug* (záznam *Debug* a jeho volby popisuje sekce 22.8). Záznam komunikace lze spustit následovně:

1. V administrační konzoli *Kerio MailServeru* se přepneme do sekce *Záznamy* → *Debug*.
2. Klikneme pravým tlačítkem myši v okně záznamu a vyvoláme kontextové menu.

3. V kontextovém menu klikneme na volbu *Zprávy*.

4. Otevře se dialog *Zaznamenávané informace*, kde zaškrtneme volbu *ActiveSync Synchronization*.



Obrázek 36.3 Dialog pro nastavení záznamu Debug

5. Nastavení uložíme tlačítkem *OK*.

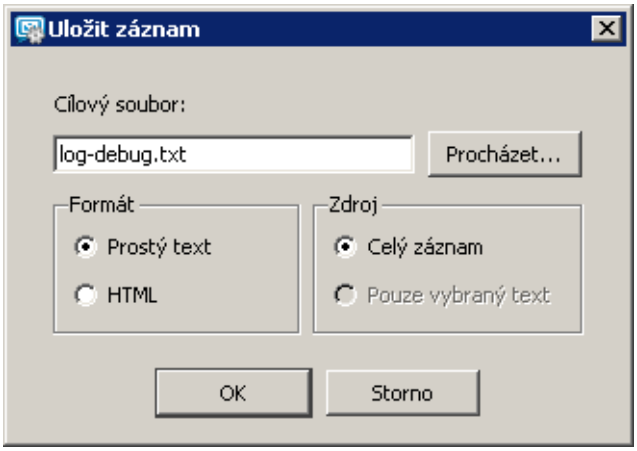
Po nastavení záznamu je třeba spustit synchronizaci mezi zařízením a serverem, aby se mohl vytvořit záznam.

V případě potřeby lze záznam synchronizace také uložit:

1. Záznam lze do souboru uložit v sekci *Záznamy* → *Debug*.

2. Na vytvořeném záznamu klikneme pravým tlačítkem myši a v kontextovém menu vybereme volbu *Uložit záznam*.

3. V dialogu *Uložit záznam* zvolíme místo uložení souboru, vybereme formát souboru (na výběr máme mezi formáty TXT a HTML) a dialog odsouhlasíme (viz obrázek 36.4).



Obrázek 36.4 Dialog pro uložení záznamu

Záznam synchronizace v mobilních zařízeních

Aplikace *ActiveSync* v systémech *Windows Mobile* obsahuje vlastní záznamy každé synchronizace, které mohou napomoci při řešení problémů s komunikací. Záznamy lze zapnout v *Advanced* dialogu aplikace *ActiveSync*.

Windows Mobile záznamy ukládá do adresáře `\Windows\Activesync`. Každá synchronizace je uložena v samostatném souboru, přičemž se ve zmíněném adresáři nacházejí vždy poslední tři záznamy. Soubory se záznamy se nazývají:

`Exchange Server0.txt`

`Exchange Server1.txt`

`Exchange Server2.txt`

Tyto záznamy mohou být potřeba například při řešení problémů s technickou podporou společnosti *Kerio Technologies*.

36.8 Řešení případných problémů

Problémy se synchronizací jedné složky ve Windows Mobile

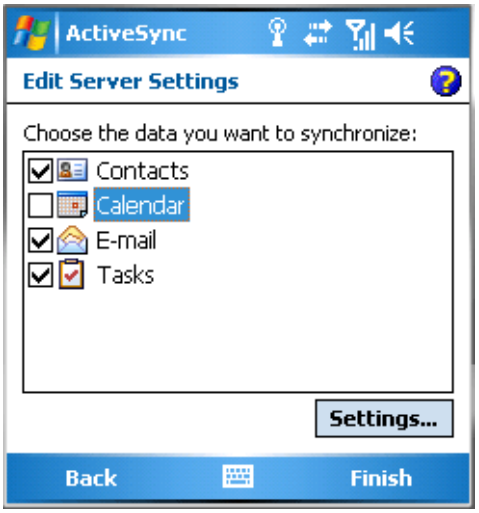
Problém

Uživateli se může stát, že se mu nebude dařit synchronizovat některou ze složek, kterou má k synchronizaci přihlášenu.

Řešení

V nastavení aplikace *ActiveSync* provedeme následující:

1. V nastavení aplikace *ActiveSync* odebereme složku ze seznamu synchronizovaných složek.



Obrázek 36.5 Odebrání poškozené složky ze seznamu synchronizovaných složek

2. Provedeme takzvaný „Soft reset“ zařízení.
3. Provedeme synchronizaci zařízení se serverem bez oné poškozené složky.
4. Pokud nyní proběhla synchronizace bez problémů, složku opět do seznamu synchronizovaných složek přidáme a zkusíme synchronizovat.
5. V případě neúspěchu kontaktujeme technickou podporu společnosti *Kerio Technologies*.

Problémy se synchronizací všech složek ve Windows Mobile

Problém

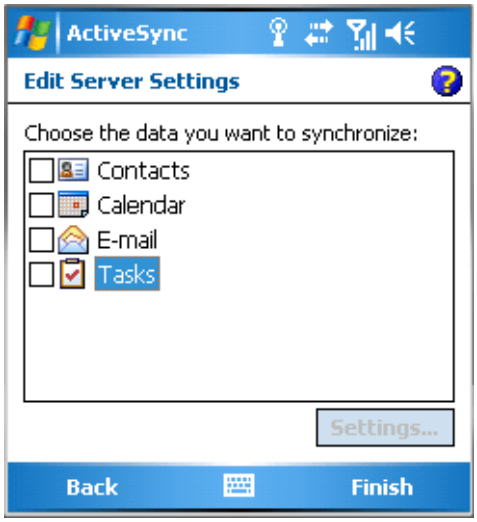
Uživateli se nedaří synchronizovat složky přihlášené k synchronizaci.

Řešení

V nastavení aplikace *ActiveSync* provedeme následující:

1. V nastavení aplikace *ActiveSync* odebereme (odškrtneme) všechny složky ze seznamu synchronizovaných složek (viz obrázek 36.6) a nastavení uložíme.
2. Provedeme takzvaný „Soft reset“ zařízení.
3. Složky do seznamu synchronizovaných složek opět přidáme a zkusíme synchronizovat.
4. V případě neúspěchu kontaktujeme technickou podporu společnosti *Kerio Technologies*.

Poznámka: Kromě tohoto postupu je možné také zrušit v *ActiveSync* účet celý a po restartu zařízení ho znovu nastavit. Data podléhající synchronizaci se ze zaří-



Obrázek 36.6 Odebrání složek ze seznamu synchronizovaných složek

zení vymažou. Po založení nového účtu se všechna data načtou znovu, obvykle již správně.

Zařízení se nemůže připojit k serveru

Řešení tohoto problému může být několik. Především je třeba zkontrolovat následující:

- V zařízení musí být správně nastaven přístup k síti, aby se zařízení mohlo připojit ke *Kerio MailServeru*.
- V nastavení aplikace *ActiveSync* je třeba zjistit, zda jsou správně zadány přihlašovací údaje.
- V *Kerio MailServeru* musí být povolena služba HTTP(S) na standardních portech (na většině zařízení nelze nastavit nestandardní port pro komunikaci).
- Komunikuje-li zařízení přes protokol zabezpečený SSL, je třeba zkontrolovat, zda problém není v SSL certifikátu (více viz sekci 36.4).
- Pokud se uživatel připojuje k serveru z Internetu, je třeba mít na firewallu povoleny standardní porty protokolu HTTP(S).

Kapitola 37

Podpora pro BlackBerry přes NotifyLink

Služba *NotifyLink* provozovaná společností *Notify Technology Corporation* umožňuje spolupráci mezi mobilními zařízeními a různými servery. *Kerio MailServer* této služby využívá k synchronizaci dat mezi zařízeními *BlackBerry* a datovým úložištěm *Kerio MailServeru*.

Komunikace mezi *NotifyLink* serverem a *Kerio MailServerem* probíhá přes rozhraní WebDAV a protokol IMAP, proto je třeba spustit v *Kerio MailServeru* služby HTTP(S), IMAP(S) a LDAP pro vyhledávání kontaktů. Žádná další nastavení nejsou na straně *Kerio MailServeru* nutná.

Upozornění: Kromě nastavení služeb na serveru je nutné namapovat příslušné porty na firewallu, kterým je server chráněn, jinak služby nebudou přístupné z Internetu (více viz sekci 2.3).

Synchronizace *BlackBerry* přes *NotifyLink* umožňuje synchronizovat následující složky:

- Pošta — synchronizovány jsou všechny osobní složky včetně podsložek.
- Kalendář — synchronizován je pouze hlavní osobní kalendář.
- Kontakty — synchronizovat je možné všechny složky, které si uživatel vybere při konfiguraci.
- Úkoly — synchronizována je pouze hlavní osobní složka s úkoly.

Služba *NotifyLink* je placená a je možné si ji předplatit na stránkách `http://www.notifycorp.com/`, kde lze také najít návod k nastavení zařízení a další užitečné informace.

Kapitola 38

Podpora pro Microsoft Entourage

MS Entourage je poštovní klient pro Mac OS X podporovaný ze strany *Kerio MailServeru*. Podpora využívá rozhraní pro *MS Exchange* v *Entourage* a umožňuje:

- práci s groupwarovými daty (pošta, kalendář, kontakty a veřejné poštovní složky),
- využívání *Free/Busy* serveru,
- připojení různých LDAP databází pro vyhledávání kontaktů,
- učení bayesovského filtru pomocí přesouvání složek do Junk E-mail nebo INBOXu (více viz kapitolu 16.1).

Podpora pro spolupráci *Kerio MailServeru* a *MS Entourage* je přímá. To znamená, že na klientské stanice se nemusí instalovat žádná rozšiřující aplikace, pouze je nutné správně nastavit základní parametry účtu pro *Exchange*.

Pro správnou funkci *Microsoft Entourage* musí být v *Kerio MailServeru* spuštěny všechny potřebné služby:

- *HTTP(S)* — pomocí této služby *Kerio MailServer* komunikuje s rozhraním WebDAV a *Free/Busy* serverem.
- *LDAP(S)* — pokud je uživateli využíváno vyhledávání kontaktů v LDAP databázi *Kerio MailServeru*.
- *SMTP(S)* — pro odesílání pošty (pouze pro verzi *MS Entourage X* a IMAP a POP3 účty ve všech verzích).
- *IMAP(S)* — je nutno spustit v případě, že uživatelé využívají *MS Entourage X*.

Upozornění: Kromě nastavení služeb na serveru je nutné namapovat příslušné porty na firewallu, kterým je server chráněn, jinak služby nebudou přístupné z Internetu (více viz sekci 2.3).

Kerio MailServer podporuje tyto verze poštovního klienta:

- *MS Entourage X* pro Mac OS X
- *MS Entourage 2004* + MS Office 2004 for Mac sp2 — 11.3.3 pro Mac OS X
- *MS Entourage 2008*

MS Entourage musí být nainstalován na následujících verzích operačního systému Mac OS X:

- Mac OS X 10.3.9 Panther
- Mac OS X 10.4 Tiger
- Mac OS X 10.5 Leopard

Upozornění: Každý uživatelský profil v *MS Entourage* může obsloužit jen jeden *Exchange* účet. Každý další takový účet nebude funkční. Funkci POP3 a IMAP účtů nastavení neovlivňuje.

Pokud se v komunikaci mezi *Kerio MailServerem* a Exchange účtem v *MS Entourage* objeví nějaký problém, zapněte v záznamu *Debug* volbu *WebDAV Server Requests* (jak a kde lze volbu zapnout je popsáno v kapitole 22.8). Záznam průběhu komunikace vám může při řešení problému výrazně napomoci.

Konkrétní možnosti a nastavení na straně klienta jsou popsána ve speciálním manuálu — *Kerio MailServer, Příručka uživatele*. Tento manuál je k dispozici ke stažení na stránkách společnosti *Kerio Technologies* (`http://www.kerio.cz/kms-manual`).

Základní nastavení

Nastavení se liší podle verze *MS Entourage*. Z toho důvodu bude nastavení rozděleno do tří částí. První se bude zabývat nastavením *MS Entourage* verze X, druhá novější verzí 2004 a třetí verzí 2004 s aktualizací Service Pack 2 spolu s verzí 2008.

Základní rozdíl mezi verzí X a verzemi 2004 a 2008 spočívá v přístupu k datům na serveru. Ve verzi *MS Entourage X* jsou zprávy stahovány ze serveru přes protokol IMAP a kalendáře s kontakty jsou synchronizovány přes rozhraní WebDAV (Web Distributed Authoring and Versioning). *MS Entourage 2004* a vyšší používá rozhraní WebDAV i pro stahování a odesílání pošty.

Další rozdíly vyjadřuje tabulka 38.1.

Znak	MS Entourage X	MS Entourage 2004	MS Entourage 2008
Vyhledávání kontaktů přes LDAP	ANO	ANO	ANO
Podpora Free/Busy	ANO	ANO	ANO
Delegace složek	NE	ANO	ANO
Podpora veřejných složek s kontakty a kalendáři	NE	ANO	ANO
Podpora více kalendářových a kontaktních složek v jednom účtu	NE	ANO	ANO
Podpora Out-of-office	NE	NE	ANO

Tabulka 38.1 Podporované vlastnosti

Kapitola 39

Podpora pro Apple Address Book

Kerio MailServer umožňuje podporu standardního adresáře operačního systému Mac OS X *Apple Address Book*. Podpora spočívá v možnosti prohledávání kontaktů v LDAP databázi *Kerio MailServeru* a od verze Mac OS X 10.3 také obousměrnou synchronizaci kontaktů s uživatelskou schránkou v *Kerio MailServeru*. Podporu konkrétních možností v závislosti na verzi Mac OS X zobrazuje tabulka 39.1.

Kerio MailServer podporuje *Apple Address Book* v následujících verzích:

- *Apple Address Book pro Mac OS X 10.2 Jaguar*
- *Apple Address Book pro Mac OS X 10.3 Panther*
- *Apple Address Book pro Mac OS X 10.4 Tiger*
- *Apple Address Book pro Mac OS X 10.5 Leopard*

Verze OS	Vyhledávání v LDAP databázi Kerio MailServeru	Podpora synchronizace kontaktů pomocí Apple iSync	Synchronizace pomocí Kerio Sync Connectoru
Mac OS X 10.2	ANO	NE	NE
Mac OS X 10.3	ANO	ANO	NE
Mac OS X 10.4	ANO	ANO	ANO
Mac OS X 10.5	ANO	ANO	ANO

Tabulka 39.1 Podpora Apple Address Book na jednotlivých verzích Mac OS X

Pro komunikaci mezi *Kerio MailServerem* a aplikací *Apple Address Book* je třeba spustit v administrační konzoli *Kerio MailServeru* následující služby:

- LDAP(S) — službu je třeba spustit, pokud uživatelé chtějí využívat prohledávání v LDAP databázi *Kerio MailServeru*.
- HTTP(S) — službu je třeba spustit, pokud uživatelé chtějí využívat možnosti synchronizace kontaktů.

Upozornění: Kromě nastavení služeb na serveru je nutné namapovat příslušné porty na firewallu, kterým je server chráněn, jinak služby nebudou přístupné z Internetu (více viz sekci 2.3).

Nastavení aplikace *Apple Address Book* a případně také *Kerio Sync Connectoru* jsou popsána ve speciálním manuálu — *Kerio MailServer, Příručka uživatele*. Tento manuál je k dispozici ke stažení na stránkách společnosti *Kerio Technologies* (http://www.kerio.cz/kms-manual).

Kapitola 40

Kerio Sync Connector for Mac

Kerio Sync Connector je program pro obousměrnou synchronizaci dat mezi *Kerio MailServerem* a aplikacemi *Apple iCal* a *Apple Address Book*:

- *Apple iCal — Kerio Sync Connector* umožňuje obousměrnou synchronizaci lokálně uložených událostí a položek To Do.
- *Apple Address Book — Kerio Sync Connector* umožňuje obousměrnou synchronizaci lokálně uložených kontaktů.
  Upozornění: Kerio Sync Connector nepodporuje synchronizaci distribučních seznamů.

Hlavní výhodou *Kerio Sync Connectoru* je možnost nastavení synchronizace obou aplikací v jednom místě. Aplikaci *Apple iCal* navíc přináší obousměrnou synchronizaci vybraného lokálního kalendáře nebo kalendářů s úložištěm v *Kerio MailServeru*.

Kerio Sync Connector využívá pro synchronizaci dat protokol WebDAV. Z toho důvodu je třeba v *Kerio MailServeru* spustit služby HTTP a HTTPS.

Upozornění: Kromě nastavení služeb na serveru je nutné namapovat příslušné porty na firewallu, kterým je server chráněn, jinak služby nebudou přístupné z Internetu (více viz sekci 2.3).

Kerio Sync Connector je třeba nainstalovat na pracovní stanice uživatelů s operačními systémy Apple Mac OS X 10.4.9 a vyšší. K instalaci je zapotřebí instalační balík ve tvaru `kerio-ksc-6.5.0-1069.mac.dmg`, který lze získat zdarma na stránkách společnosti *Kerio Technologies*. Postup při instalaci je následující:

1. Dvojím kliknutím otevřeme instalační balík.
2. Otevře se *Finder*, který instalační balík otevře jako disk a nabídne spustitelný instalační soubor *Kerio MailServer Installer*.
3. Instalaci provedeme pomocí standardního instalačního průvodce.

Konkrétní možnosti a nastavení v *Kerio Sync Connectoru* jsou popsány ve speciálním manuálu — *Kerio MailServer, Příručka uživatele*. Tento manuál je k dispozici ke stažení na stránkách společnosti *Kerio Technologies* (`http://www.kerio.cz/kms-manual`).

Pokud mají uživatelé nainstalován systém Mac OS X 10.5 Leopard, doporučujeme využívat místo synchronizace kalendářů přes *Kerio Sync Connector* raději vestavěný CalDAV

účet v *Apple iCal* (více viz sekci 35). To znamená, že po instalaci *Kerio Sync Connectoru* je třeba vypnout synchronizaci kalendářů a nastavit CalDAV účet v *Apple iCal*. Nastavení nijak neovlivní synchronizaci kontaktů v *Apple Address Book*.

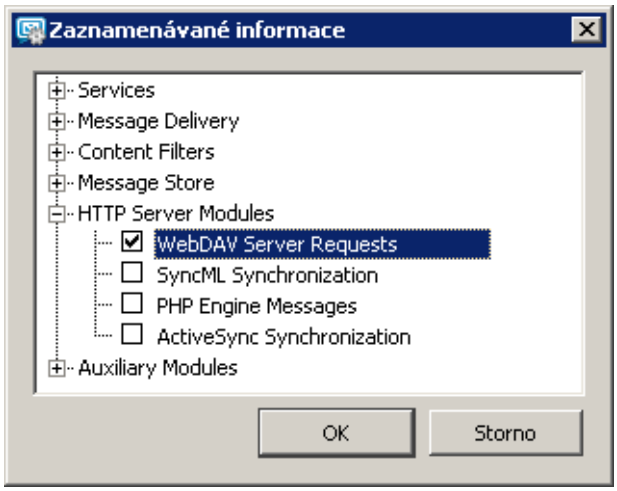
Řešení možných problémů se synchronizací

Kerio MailServer i *Kerio Sync Connector* poskytuje nástroje pro řešení případných problémů se synchronizací:

Záznamy komunikace

Komunikaci mezi *Kerio MailServerem* a *Kerio Sync Connectorem* lze zaznamenávat jak na straně *Kerio MailServeru*, tak na straně *Kerio Sync Connectoru*:

- *Kerio MailServer*
  1. Otevřeme *Kerio Administration Console* → *Záznamy* → *debug*.
  2. V okně záznamu otevřeme pravým tlačítkem myši místní nabídku a vybereme položku *Zprávy*.
  3. Otevře se okno *Zaznamenávané informace*, kde zaškrtneme volbu *WebDAV Server Requests* (viz obrázek 40.1).



Obrázek 40.1 Nastavení v záznamu debug

  Po vyřešení problému doporučujeme záznam opět vypnout.
- *Kerio Sync Connector*
  1. Otevřeme *System Preferences* → *Kerio Sync Connector* a přepneme se do záložky *Advanced*.
  2. Zaškrtneme volbu *Enable debug logging* (viz obrázek 40.2).
     Záznam najdeme v aplikaci *Console* (*Applications* → *Utilities* → *Console*).

Obrázek 40.2 Nastavení záznamu v Kerio Sync Connectoru

Oprava synchronizace

V případě problémů se synchronizovanými daty může k řešení pomoci oprava synchronizace. Při opravě bude vytvořena kopie dat buď na serveru nebo v klientovi a tato kopie přemaže stranu opačnou tak, aby obě úložiště obsahovala stejná data. Rizikem opravy může být ztráta části dat, která byla uložena od poslední synchronizace.

Postup při opravě synchronizace je následující:

1. Otevřeme *System Preferences* → *Kerio Sync Connector* a přepneme se do záložky *Advanced*.
2. Stiskneme tlačítko *Repair*.
3. Otevře se okno s dotazem, zda chceme provést synchronizaci podle dat na serveru nebo podle dat na klientovi. Po výběru stiskneme tlačítko *OK* a data se synchronizují.

Odeslání reportu do Kerio Technologies

V případě, že problém se synchronizací způsobuje chyba v aplikaci, doporučujeme odeslat záznam synchronizace do společnosti *Kerio Technologies*, kde bude podroben analýze.

Veškeré informace uložené ve výpisu budou použity pouze k odstranění problémů spojených s používáním tohoto produktu. Údaje ani vaše e-mailová adresa nebudou žádným způsobem zneužity.

Odeslat report můžeme následujícím způsobem:

1. Otevřeme *System Preferences* → *Kerio Sync Connector* a přepneme se do záložky *Advanced*.
2. Stiskneme tlačítko *Send report*.
3. Otevře se okno pro odeslání e-mailové zprávy se záznamem a doplněnou o

adresu odesílatele. Zprávu stačí pouze odeslat.

Kapitola 41

Podpora pro Apple Mail

Kerio MailServer od verze 6.1.2 podporuje některé funkce pro týmovou spolupráci IMAP a Entourage účtů v *Apple Mail 10.4* a vyšší. Podpora umožňuje zobrazení složek s událostmi, kontakty a úkoly v poštovním klientovi.

Podpora pro spolupráci *Kerio MailServeru* a *Apple Mail* je přímá. To znamená, že na klientské stanice se nemusí instalovat žádná rozšiřující aplikace, pouze je nutné podporu povolit v konfiguračním souboru *Kerio MailServeru*:

1. Zastavíme *Kerio MailServer* — před každou ruční editací konfiguračních souborů je třeba vždy nejprve zastavit *Kerio MailServer Engine*.

2. V adresáři, kam je nainstalován *Kerio MailServer*, najdeme soubor s názvem `mailserver.cfg` a otevřeme ho.

   Pokud soubor editujeme na platformách *Mac OS X* nebo *Linux*, potom se nejprve do systému přihlásíme jako root (speciální uživatel s plnými přístupovými právy do systému).

3. Pomocí vyhledávání najdeme řádek s hodnotou `IMAPFullListing` a místo číslice `0` k této hodnotě přiřadíme číslici `1`.

4. Změnu v souboru uložíme a *Kerio MailServer* opět spustíme.

Nastavení plné podpory protokolu IMAP v *Kerio MailServeru* způsobí, že všichni uživatelé využívající pro přístup ke své poště protokol IMAP budou mít k dispozici všechny typy složek i podsložek (pošta, kalendáře, kontakty a úkoly) ve svých poštovních klientech. Tyto složky však budou zobrazeny jako poštovní složky, kde všechny události, kontakty nebo úkoly budou zobrazeny ve formě e-mailových zpráv s přílohou ve formátu `.vcf` v případě kontaktu nebo `.ics` v případě události a úkolu. Z tohoto důvodu je třeba důkladně si rozmyslet, zda má spuštění plné podpory IMAP v *Kerio MailServeru* opravdu smysl, a zda přinese uživatelům očekávanou přidanou hodnotu.

Pro správnou funkci účtů v *Apple Mail* musí být v *Kerio MailServeru* spuštěny všechny příslušné služby:

- *HTTP(S)* — službu je nutno spustit pro Exchange účty, pokud jsou uživateli využívány.
- *IMAP(S)* — službu je nutno spustit jak pro IMAP, tak pro Exchange účty.
- *SMTP(S)* — přes protokol probíhá odesílání pošty.

Upozornění: Kromě nastavení služeb na serveru je nutné namapovat příslušné porty na firewallu, kterým je server chráněn, jinak služby nebudou přístupné z Internetu (více viz sekci 2.3).

Konkrétní možnosti a nastavení v *Apple Mail* jsou popsána ve speciálním manuálu — *Kerio MailServer, Příručka uživatele*. Tento manuál je k dispozici ke stažení na stránkách společnosti *Kerio Technologies* (`http://www.kerio.cz/kms-manual`).

Kapitola 42

Podpora pro Apple iPhone

Kerio MailServer podporuje od verze 6.4.1 mobilní zařízení *Apple iPhone 1.0*. Vlastností, které jsou ze strany *Kerio MailServeru* podporovány, je celá řada:

- Poštu lze odesílat a přijímat přes protokoly IMAP, POP3 a SMTP nebo synchronizovat s desktopovými aplikacemi *Apple Mail* a *Outlook Express* přes *Apple iTunes*.
- Kontakty a kalednář lze synchronizovat s desktopovými aplikacemi pomocí *Apple iTunes*. Synchronizovat kalendář a kontakty lze s aplikacemi *Apple iCal*, *Apple Address Book* a *Microsoft Outlook* (XP, 2003 a 2007).
- Na *Safari* lze spustit jak plnou verzi *Kerio WebMail* tak *Kerio WebMail Mini*.
  Upozornění: V plné verzi *Kerio WebMailu* nelze měnit existující kontakty, události, úkoly ani poznámky.

Podpora *Apple iPhone* ze strany *Kerio MailServeru* vyžaduje instalaci programu iTunes 7.3 a vyšší na stanice uživatelů. *iTunes* slouží k synchronizaci mezi desktopovým klientem a *Apple iPhone*.

Synchronizace mezi desktopovou aplikací a *Apple iPhone* vyžaduje následující operační systémy:

- Windows XP Service Pack 2 a novější,
- Mac OS X 10.4.10 a vyšší.

Z výše zmíněného vyplývá, že je třeba v Kerio MailServeru spustit následující služby:

- *HTTP(S)* — službu je nutno spustit pro přístup k rozhraní *Kerio WebMail*.
- *POP3(S)* — službu je nutno spustit pro účty typu POP3.
- *IMAP(S)* — službu je nutno spustit pro IMAP účty.
- *SMTP(S)* — přes protokol probíhá odesílání pošty.

Kromě výše zmíněných služeb je třeba namapovat na firewallu chránícím server příslušné porty, aby služby byly dostupné z Internetu (více viz sekci 2.3).

Upozornění: Pokud komunikace mezi *Kerio MailServerem* a poštovním klientem probíhá na portu 25, může nastat problém s odesíláním pošty. Veřejné WiFi sítě často nepodporují komunikaci na nešifrovaných verzích protokolů, takže SMTP na portu 25 může být blokován. Uživatelé v takovém případě nemohou ze sítě odesílat svou poštu. SMTPS na portu 465 však obvykle bývá otevřeno. Z toho důvodu doporučujeme uživatelům nastavit jejich poštovní klienty na šifrování pomocí SMTPS.

42.1 Pošta

Poštovní účet lze v *Apple iPhone* nastavit manuálně nebo je možno využít automatické konfigurace:

Automatická konfigurace

Při synchronizaci přes *iTunes* lze využít i automatické synchronizace poštovních složek v *Apple Mail* nebo na systému *Windows* v programu *Outlook Express* (nastavení účtu typu IMAP).

Ruční konfigurace

Ruční konfigurace vyžaduje pouze standardní nastavení příchozího a odchozího serveru. *Apple iPhone* nabízí tři typy účtů: IMAP, POP3 a EXCHANGE. Všemi typy účtů se lze připojit ke *Kerio MailServeru*.

Podrobnosti k nastavení obsahuje kapitola o *Apple iPhone* v manuálu `Kerio MailServer 6, Příručka uživatele`.

42.2 Synchronizace událostí a kontaktů

Přímá synchronizace *Apple iPhone* a *Kerio MailServeru* není podporována. Kalendáře i kontakty lze synchronizovat pouze přes desktopovou aplikaci *Apple iTunes* verze 7.3 a vyšší:

Kalendář

Kalendáře lze synchronizovat s aplikacemi:

- *Apple iCal* — synchronizovat lze všechny kalendáře.
- *MS Outlook* — synchronizovat lze pouze výchozí kalendář.
- *Windows Calendar* — *iTunes* synchronizaci nepodporují.

Kontakty

Kalendářová data lze synchronizovat s následujícími aplikacemi:

- *Apple Address Book* — všechny položky kontaktu jsou synchronizovány.
- *MS Outlook* — všechny podstatné položky jsou synchronizovány, synchronizuje se pouze jedna složka s kontakty, synchronizace distribučních seznamů není podporována.
- *Windows Contacts* — všechny položky kontaktu jsou synchronizovány, distribuční seznamy jsou synchronizovány jako tzv. skupina.

Kapitola 43

Technická podpora

Společnost *Kerio Technologies* poskytuje registrovaným uživatelům na produkt *Kerio MailServer* bezplatnou e-mailovou a telefonickou technickou podporu. Kontakty naleznete na konci této kapitoly. Naši technici vám rádi ochotně pomohou s jakýmkoliv problémem.

Značné množství problémů lze ale vyřešit svépomocí (zpravidla i rychleji). Než se rozhodnete kontaktovat technickou podporu *Kerio Technologies*, proveďte prosím následující:

- Pokuste se najít odpověď v tomto manuálu. Jednotlivé kapitoly obsahují velmi detailní popis funkcí aplikace *Kerio MailServer* a možnosti jejich využití pro optimální nastavení serveru.
- Nenajdete-li odpověď na vaši otázku zde, pokuste se ji najít:
  1. na stránkách produktu *Kerio MailServer* (`http://www.kerio.cz/kms`),
  2. na stránkách technické podpory (`http://www.kerio.cz/support`).
- Dalšími zdroji cenných informací může být diskusní fórum uživatelů aplikace *Kerio MailServer* na stránkách `http://forums.kerio.cz/` a znalostní databáze, kterou lze najít na stránkách `http://support.kerio.cz/`.
- Konkrétní dotazy na technickou podporu lze zadávat do speciálního webového formuláře umístěného na stránkách `http://support.kerio.cz/`.

43.1 Kontakty

USA

Kerio Technologies Inc.

2350 Mission College Blvd., Suite 400

Santa Clara, CA 95054

Tel.: +1 408 496 4500

Písemná technická podpora je dostupná na adrese http://support.kerio.com/.

http://www.kerio.com/

Velká Británie

Kerio Technologies UK Ltd.

Enterprise House

Vision Park

Histon

Cambridge CB4 9ZR

Tel.: +44 1223 202 130, Fax.: +44 1223 233 055

Písemná technická podpora je dostupná na adrese http://support.kerio.com/.

http://www.kerio.co.uk/

Česká Republika

Kerio Technologies s.r.o.

Anglické nábřeží 1/2434

301 49 Plzeň

Tel.: +420 377 338 902

Písemná technická podpora je dostupná na adrese http://support.kerio.cz/.

http://www.kerio.cz/

Příloha A

Právní doložka

Microsoft®, Windows®, Windows NT®, Internet Explorer®, Active Directory®, Outlook®, ActiveSync®, Entourage® a Windows Mobile® jsou registrované ochranné známky společnosti Microsoft Corporation.

Apple®, iCal®, Mac OS®, Safari™, Tiger™ a Panther® a Open Directory logo™ jsou registrované ochranné známky nebo ochranné známky společnosti Apple Computer, Inc.

Palm®, Treo™ a VersaMail® jsou registrované ochranné známky nebo ochranné známky společnosti Palm, Inc.

Red Hat® a Fedora™ jsou registrované ochranné známky nebo ochranné známky společnosti Red Hat, Inc.

SUSE® je registrovaná ochranná známka společnosti Novell Inc.

Mozilla® a Firefox® jsou registrované ochranné známky společnosti Mozilla Foundation.

Linux® je ochranná registrovaná známka Linuse Torvaldse.

Kerberos™ je ochranná známka Massachusetts Institute of Technology (MIT).

McAfee® a Proven Security™ jsou registrované ochranné známky nebo ochranné známky společnosti Network Associates, Inc.

avast!® je registrovaná ochranná známka společnosti ALWIL Software.

Symantec™ je ochranná známka společnosti Symantec Corporation.

eTrust™ je ochranná známka společnosti Computer Associates International, Inc.

ClamAV™ je ochranná známka společnosti Tomasz Kojm.

VisNetic® a VisNetic AntiVirus™ jsou registrované ochranné známky nebo ochranné známky společnosti Deerfield Communications Inc.

Cybertrust® je registrovaná ochranná známka společnosti Cybertrust Holdings, Inc. a/nebo jejích poboček.

Thawte® je registrovaná ochranná známka společnosti VeriSign, Inc.

Entrust® je registrovaná ochranná známka společnosti Entrust, Inc.

Sophos® je registrovaná ochranná známka společnosti Sophos Plc.

ESET® a NOD32® jsou registrované ochranné známky společnosti ESET, LLC.

Grisoft® a AVG® jsou registrované ochranné známky společnosti Grisoft Inc.

NotifyLink® je registrovaná ochranná známka společnosti Notify Technology Corporation.

BlackBerry® je registrovaná ochranná známka společnosti Research In Motion Limited.

RoadSync™ je ochranná známka společnosti DataViz Inc.

Nokia® a Mail for Exchange® jsou registrované ochranné známky společnosti Nokia Corporation.

Symbian™ je ochranná známka společnosti Symbian Software Limited.

Sony Ericsson® je registrovaná ochranná známka společnosti Sony Ericsson Mobile Communications AB.

SpamAssassin™ je ochranná známka Apache Software Foundation.

SpamHAUS® je registrovaná ochranná známka společnosti The Spamhaus Project Ltd.

Příloha B

Použité open-source knihovny

Tento produkt obsahuje následující knihovny volně šiřitelné ve formě zdrojových kódů (open-source):

Free Type 2

FreeType2 je knihovna pro zobrazovaní fontů, která byla navržena jako malá, rychlá, vysoce modulární a portovatelná, a zároveň poskytující kvalitní výstup.

The FreeType Project is copyright ©1996-2000 by David Turner, Robert Wilhelm, and Werner Lemberg.

Heimdal Kerberos

Used by KMS on Linux via libtauth.

Heimdal je implementace Kerberosu 5, psaného hlavně ve Švédsku. Je volně dostupný pod licencí podobné BSD (pozn.: balík obsahuje i části knihovny libdes, od Erica Younga, která je pod jinou licencí). Jiné další volné implementace jsou od MIT a Shishi. Také MS Windows a Sun Java mají implementaci Kerberosu.

Copyright ©1997-2000 Kungliga Tekniska Hogskolan (Royal Institute of Technology, Stockholm, Sweden). All rights reserved.

Copyright ©1995-1997 Eric Young (eay@mincom.oz.au). All rights reserved.

Copyright ©1990 by the Massachusetts Institute of Technology

Copyright ©1988, 1990, 1993 The Regents of the University of California. All rights reserved.

Copyright ©1992 Simmule Turner and Rich Salz. All rights reserved.

Copyright ©1997-2000 Kungliga Tekniska Hogskolan (Royal Institute of Technology, Stockholm, Sweden). All rights reserved.

IBPP

Copyright ©2000-2006 T.I.P. Group S.A. a IBPP Team

Permission is hereby granted, free of charge, to any person or organization („You“) obtaining a copy of this software and associated documentation files covered by this license (the „Software“) to use the Software as part of another work; to modify it for that purpose; to publish or distribute it, modified or not, for that same purpose; to permit persons to whom the other work using the Software is furnished to do so; subject to the following conditions: the above copyright notice and this complete and unmodified permission notice shall be included in all copies or substantial portions of the Software; You will not misrepresent modified versions of the Software as being the original.

The Software is provided „as is“, without warranty of any kind, express or implied, including but not limited to the warranties of merchantability, fitness for a particular purpose and noninfringement. In no event shall the authors or copyright holders be liable for any claim, damages or other liability, whether in an action of contract, tort or otherwise, arising from, out of or in connection with the software or the use of other dealings in the Software.
IBPP je rozhraní k databázi Firebird pro aplikace psané v C++.
Domovská stránka: http://www.ibpp.org/

libiconv

Copyright ©1999-2003 Free Software Foundation, Inc.
Autor: Bruno Haible
Domovská stránka: http://www.gnu.org/software/libiconv/
Knihovna *libiconv* je šířena pod licencí LGPL.
Kerio MailServer obsahuje upravenou verzi této knihovny. Kompletní zdrojové kódy upravené knihovny *libiconv* jsou k dispozici na adrese:

http://download.kerio.cz/dwn/kms-iconv.zip

libIDL

LibIDL je vnější rozhraní pro CORBA 2.2 IDL a Netscape's XPIDL.
Copyright ©1998, 1999 Andrew T. Veliath.

libjpeg

Libjpeg je knihovna pro zacházení s obrázky ve formátu JPEG (JFIF).
Copyright ©1991-1998, Thomas G. Lane.
This software is the work of Tom Lane, Philip Gladstone, Jim Boucher, Lee Crocker, Julian Minguillon, Luis Ortiz, George Phillips, Davide Rossi, Guido Vollbeding, Ge' Weijers, and other members of the Independent JPEG Group.

libpng

Libpng je oficiální referenční knihovna pro formát PNG. Podporuje téměř všechny vlastnosti PNG formátu.
Copyright ©2000-2002 Glenn Randers-Pehrson.

libspf

libspf2 implementuje Sender Policy Framework, který představuje část páru protokolů SPF/SRS. Knihovna libspf2 umožňuje poštovním serverům jako jsou Sendmail, Postfix, Exim, Zmailer a MS Exchange kontrolu SPF záznamů. Zároveň ověřuje SPF záznam a kontroluje, zda je odesílající server oprávněn odesílat poštu pro doménu, ze které byla zpráva odeslána. Toto opatření zabraňuje podvrhům běžně užívaným spammery a viry/červy (více viz http://www.libspf2.org/).
Copyright ©2005 by Shevekand Wayne Schlitt, all rights reserved.

libtiff

Libtiff je knihovna pro manipulaci s obrázky ve formátu TIFF.
Copyright ©1988-1997 Sam Leffler
Copyright ©1991-1997 Silicon Graphics, Inc.

php_mbstring

Copyright ©2001-2004 The PHP Group.
Copyright © 1998,1999,2000,2001 HappySize, Inc. All rights reserved.
Domovská stránka: http://www.php.net/downloads.php
Knihovna *php_mbstring.dll* používá knihovnu *libmbfl*, která je šířena pod licencí LGPL.
Kerio MailServer obsahuje upravenou verzi této knihovny. Kompletní zdrojové kódy upravené knihovny *php_mbstring* jsou k dispozici na adrese:

http://download.kerio.cz/dwn/kms-mbstring.zip

myspell

Knihovna pro kontrolu pravopisu.
Copyright 2002 Kevin B. Hendricks, Stratford, Ontario, Canada And Contributors. All rights reserved.

OpenLDAP

Volně šiřitelná implementace protokolu *LDAP* (*Lightweight Directory Access Protocol*).
Copyright ©1998-2004 The OpenLDAP Foundation.

OpenSSL

Implementace protokolů *Secure Sockets Layer* (SSL v2/v3) a *Transport Layer Security* (TLS v1).
Tento produkt obsahuje software vyvinutý sdružením *OpenSSL Project* pro použití v *OpenSSL Toolkit* (http://www.openssl.org/).

PHP

PHP je široce používaný obecný skriptovací jazyk, který se používá obzvláště pro vývoj web aplikací a může být vložený přímo do HTML kódu.
Copyright ©2001-2004 The PHP Group.

zlib

Všestranně použitelná knihovna pro kompresi a dekompresi dat.
Copyright ©1995-2003 Jean-Loup Gailly and Mark Adler.

Slovníček pojmů

Aplikační protokol

Aplikační protokoly jsou neseny v paketech protokolu TCP, příp. UDP, a slouží přímo k přenosu uživatelských (aplikačních) dat. Existuje mnoho standardních aplikačních protokolů (např. SMTP, POP3, HTTP, FTP apod.), programátor aplikace si však může navrhnout libovolný vlastní (nestandardní) způsob komunikace.

DoS útok

DoS (Denial of Service) je typ útoku, který spočívá v zahlcení serveru požadavky jiného počítače nebo počítačů tak, aby nestíhal plnit požadavky regulérních uživatelů nebo v horším případě útoku podlehl.

DSN

DSN (Delivery Status Notification) je zpráva o stavu doručení e-mailové zprávy, doručenka. Existuje několik druhů potvrzení o doručení zprávy. Pokud není odesílatelem určeno jinak, posílá mu mailový server pouze chybové zprávy (odložení, neúspěch).

E-mailová adresa

Určuje příjemce a odesílatele zprávy při komunikaci elektronickou poštou. Skládá se z lokální části (před znakem `@`) a domény (část za znakem `@`). Doména určuje místo (organizaci), kam bude zpráva doručena, a lokální část pak konkrétního příjemce v rámci této organizace.

ETRN

Přijímáte-li poštu protokolem SMTP a váš server není trvale připojen do Internetu, může se pošta shromažďovat na jiném SMTP serveru (typicky sekundární server pro danou doménu). V okamžiku připojení do Internetu vyšle váš SMTP server příkaz ETRN (jeden z příkazů protokolu SMTP), čímž si žádá o poslání uložených e-mailů.

Nejsou-li na daném SMTP serveru žádné zprávy uloženy, nemusí na příkaz ETRN vůbec odpovědět. Proto je třeba definovat dobu (timeout), po které SMTP server ukončí spojení, jestliže žádné e-maily nepřijal.

Firewall

Software nebo hardwarové zařízení, které chrání počítač nebo počítačovou síť před průnikem zvenčí (typicky z Internetu).

IMAP

Internet Message Access Protocol (IMAP) je protokol umožňující klientům pracovat se svými zprávami na serveru, bez nutnosti stahování na lokální počítač. Uživatel se tak může připojovat k serveru z více různých počítačů a má vždy k dispozici všechny své zprávy (pokud by byly zprávy staženy na lokální disk určitého počítače, nebyly by z ostatních počítačů dostupné).
K téže schránce lze (za určitých podmínek) přistupovat protokoly IMAP i POP3 současně.

IP

IP (Internet Protocol) je protokol, který nese ve své datové části všechny ostatní protokoly. Nejdůležitější informací v jeho hlavičce je zdrojová a cílová IP adresa, tedy kým (jakým počítačem) byl paket vyslán a komu je určen.

IP adresa

32-bitové číslo jednoznačně určující počítač v Internetu. Zapisuje v desítkové soustavě jako čtveřice bytů (`0–255`) oddělených tečkami (např. `200.152.21.5`). Každý paket obsahuje informaci, odkud byl vyslán (zdrojová IP adresa), a kam má být doručen (cílová IP adresa).

Kerberos

Protokol pro bezpečné ověřování uživatelů v síťovém prostředí. Byl navržen organizací MIT (Massachusetts Institute of Technology) v rámci projektu Athena. Protokol je založen na principu důvěryhodné třetí strany. Uživatelé se přihlašují svým heslem k centrálnímu serveru (KDC, Key Distribution Center) a od něho dostávají šifrované vstupenky (tickets) pro přihlášení k různým službám v síti.

LDAP

LDAP (Lightweight Directory Access Protocol) je internetový protokol pro přístup k adresářovým službám. V adresářích bývají uloženy informace o uživatelských účtech a jejich právech, počítačích v síti apod. Nejčastěji používají LDAP e-mailové programy pro vyhledávání e-mailových adres a řízení doručování pošty (*Microsoft Active Directory*).

MAPI

MAPI (Messaging Application Programming Interface) je programovací aplikační rozhraní (API) firmy *Microsoft*. Je to softwarové rozhraní, které umožňuje jakémukoliv programu podporujícímu MAPI pracovat s libovolným poštovním systémem (*Kerio MailServer*) a tedy posílat a zpracovávat data bez ohledu na typ a výrobce komunikačních prostředků.

Maska subsítě

Maska subsítě rozděluje IP adresu na dvě části: adresu sítě a adresu počítače v této síti. Maska se zapisuje stejně jako IP adresa (např. 255.255.255.0), ale je třeba ji vidět jako 32-bitové číslo mající zleva určitý počet jedniček a zbytek nul (maska tedy nemůže mít libovolnou hodnotu). Jednička v masce subsítě označuje bit adresy sítě a nula bit adresy počítače. Všechny počítače v jedné subsíti musejí mít stejnou masku subsítě a stejnou síťovou část IP adresy.

MX záznamy

Jeden z typů záznamů, které mohou být uloženy v DNS. Obsahuje informaci o poštovním serveru pro danou doménu (tzn. na který SMTP server má být poslán e-mail pro tuto doménu). MX záznamů pro jednu doménu může být více, pak mají různou prioritu a mohou definovat např. primární a záložní (sekundární) server.

NNTP

NNTP (Network News Transfer Protocol) je jednoduchý textový protokol, který rozšiřuje, načítá a umisťuje zprávy na Internetu.

Notifikace

Stručná zpráva (upozornění) na určitou událost — např. přijetí e-mailu. Zpravidla se posílá formou krátké textové zprávy (SMS) na mobilní telefon.

POP3

Post Office Protocol je protokol, který umožňuje uživatelům stahovat zprávy ze serveru na svůj lokální disk. Je vhodný zejména pro klienty, kteří nemají trvalé připojení do Internetu.

Na rozdíl od protokolu IMAP, POP3 neumožňuje uživatelům manipulovat se zprávami na serveru. Veškeré operace s nimi musí být prováděny na počítači klienta. POP3 umožňuje přístup pouze do uživatelovy složky *INBOX* a nepodporuje veřejné a sdílené složky.

Port

16-bitové číslo (`1–65535`) používané protokoly TCP a UDP pro identifikaci aplikací (služeb) na daném počítači. Na jednom počítači (jedné IP adrese) může běžet více aplikací současně (např. WWW server, poštovní klient, WWW klient — prohlížeč, FTP klient atd.). Každá aplikace je však jednoznačně určena číslem portu. Porty `1–1023` jsou vyhrazené a používají je standardní, příp. systémové služby (např. `80` = WWW). Porty nad `1024` (včetně) mohou být volně použity libovolnou aplikací (typicky klientem jako zdrojový port nebo nestandardní aplikací serverového typu).

Poštovní schránka

Místo, kde jsou přijaté e-maily na serveru uloženy. Poštu si klient může ze schránky vybírat (protokolem POP3), anebo pracovat se zprávami přímo na serveru (protokolem IMAP).

Fyzicky je schránka reprezentována adresářem na disku, který je vytvořen v adresáři *Kerio MailServeru* (`mail/jmeno_uzivatele`). V tomto adresáři jsou vytvářeny další podadresáře, reprezentující jednotlivé složky).
Schránky nejsou vytvořeny při definici uživatelů, konkrétní schránka je vždy vytvořena až po přijetí prvního e-mailu, který do ní má být uložen.

RFC

Request For Comments. RFC je soubor obecně a dobrovolně uznávaných standardů. Je to soubor číslovaných dokumentů, kde každý z nich se věnuje nějaké části síťové komunikace.

SMTP

Simple Mail Transfer Protocol je základní protokol, který se používá pro odesílání pošty v Internetu. Odesílatel a příjemce zprávy je určen e-mailovou adresou.

Spam

Nevyžádaný, zpravidla reklamní e-mail. Spamy bývají rozesílány hromadně, přičemž adresy příjemců získávají rozesílatelé nelegálními cestami (např. odposlouchávám síťové komunikace).

SSL

Protokol pro zabezpečení a šifrování TCP spojení. Původně byl navržen firmou Netscape pro zabezpečení přenosu WWW stránek protokolem HTTP, dnes je podporován téměř všemi standardními internetovými protokoly — SMTP, POP3, IMAP, LDAP atd.
Na začátku komunikace se nejprve asymetrickou šifrou provede výměna šifrovacího klíče, který je pak použit pro (symetrické) šifrování vlastních dat.

TLS

Transport Layer Security. Nástupce SSL, de facto SSL verze 3.1. Tato verze je standardizována organizací IETF a přijata všemi významnými firmami (např. Microsoft Corporation).

WebDAV

WebDAV (Web Distributed Authoring and Versioning) je rozhraní rozšiřující protokol HTTP o možnost skupinově editovat a spravovat soubory umístěné na serverech.

WebMail

Rozhraní *Kerio MailServeru*, které umožňuje přístup k poště pomocí WWW prohlížeče. V *Kerio WebMailu* je rovněž možno měnit některá uživatelská nastavení (např. filtrování zpráv nebo heslo).

Rejstřík

N

O

P

R

S