

ALWIL Software

avast32

Exchange® Server Edition

Obsah

1	Úvod	5
2	Instalace	7
2.1	Požadavky na vybavení počítače	7
2.2	Instalujeme	7
2.3	Problémy s instalací	12
3	První kroky	15
3.1	Rezidentní ochrana	15
3.2	Testování na vyžádání	15
4	Konfigurace rezidentní úlohy	17
4.1	Stránka „Úloha“	17
4.2	Stránka „Typ“	18
4.3	Stránka „Rezidentní“	18
4.4	Stránka „Exchange Server“	19
4.5	Stránka „Oblasti“	19
4.6	Stránka „Výjimky“	21
4.7	Stránka „Signatury“	22
4.8	Stránka „Notifikace“	23
4.9	Stránka „Obnovování“	24
4.10	Stránka „Plánování“	25
5	AVAPI a blokování příloh podle jména	27
5.1	Dokonalejší detekce virů	27
5.2	Blokování příloh podle jmen	28
5.3	Vypnutí používání AVAPI	30
6	Signatury	31
6.1	Co jsou to signatury?	31
6.2	Pravidla pro používání signatur	31
6.3	Nevýhody signování zpráv	32
7	Zprávy a protokoly	33
7.1	Základní charakteristika posílaných zpráv	33
7.2	Formát posílaných zpráv	33
7.3	Logovací složka Avastu	35
8	Pro administrátory	37
8.1	Systémové požadavky podruhé	37
8.2	Více o obnovování seznamu schránek	38
8.3	Používání Internet Newsgroups společně s Avastem	39
8.4	Problém se systémovým event logem	39
8.5	Služba Avastu	40
8.6	Přesouvání testovaných zpráv	43

Seznam obrázků

2.1	Zvolte Jazyk	9
2.2	Obrazovka instalačního programu	9
2.3	Licenční ujednání mezi Vámi a firmou ALWIL Software	10
2.4	Okno pro zadání aktivačního klíče	11
2.5	Zvolení typu instalace	11
2.6	Stránka pro vložení hesla	12
2.7	Volba restartu počítače	13
4.1	Stránka „Úloha“	17
4.2	Stránka „Typ“	18
4.3	Stránka „Rezidentní“	18
4.4	Stránka „Exchange Server“	19
4.5	Stránka „Oblasti“	20
4.6	Oblasti-detaily	20
4.7	Dialog pro výběr oblastí na Exchange serveru	21
4.8	Stránka „Výjimky“	22
4.9	Stránka „Signatury“	22
4.10	Stránka „Notifikace“	23
4.11	Výběr Exchange adresy	24
4.12	Formát zprávy	24
4.13	Stránka „Obnovování“	25
4.14	Stránka „Plánování“	25
7.1	Příklad nastavení vzhledu logovací složky Avastu ve standardním microsoftském klientu	35
8.1	Zahlcení procesoru aktualizací seznamu poštovních schránek	38
8.2	Uživatelské právo „Ladit programy“	40
8.3	Aplikace „Služby“ v Ovládacích panelech	40
8.4	Program Optimizer zastaví i službu Avastu	41
8.5	Služba není ještě natažena - poskytovatel čeká	42
8.6	Pohled na Správce úloh	43

1 Úvod

Vážený zákazníku, blahopřejeme Vám k zakoupení antivirového prostředku AVAST32 3.0 Exchange Server Edition, jednoho z nejlepších programů ve své třídě. Doufáme, že budete s našim produktem spokojeni a že se Vám s ním bude příjemně pracovat.

AVAST32 3.0 Exchange Server Edition představuje úplnou antivirovou ochranu Microsoft Exchange Serveru. Pracuje jako přídatný modul systému AVAST32 3.0 Network Edition. Umožňuje kontrolovat všechny, nebo jen zvolené poštovní schránky a veřejně přístupné oblasti na serveru. Je schopen oznámit nalezení infikované zprávy jejímu odesílateli, příjemci i dalším osobám. Systém signatur zaručuje optimální vyhledávání virů pro Váš server.

V případě jakýchkoli problémů s programem či nejasností kontaktujte svého prodejce nebo firmu ALWIL Trade. Jejich pracovníci Vám rádi a ochotně poradí.

Příjemnou a viry nerušenou práci na Vašem počítači Vám přejí pracovníci firmy ALWIL Software.

2 Instalace

AVAST32 3.0 Exchange Server Edition je nová verze antivirového systému AVAST vytvořeného výhradně pro MS Exchange Server. Jádro programu je určeno pro počítač s Windows NT Serverem a Exchange Serverem. Konfiguraci ale můžete provádět z jakékoli síťové stanice s Windows 9x/Me nebo Windows NT/2000/XP. Program se skládá ze dvou částí:

- první je serverová, která provádí samotnou akci a která je nainstalována přímo na počítač, na kterém běží Exchange Server,
- druhá je klientská, což je vlastně jenom přídatný modul do běžné instalace programu AVAST32 verze 3.0, který Vám umožní vzdálenou administraci

AVAST32, Exchange Server Edition vyžaduje, abyste již měli nainstalován AVAST32 verze 3.0. Před započítím instalace se ujistěte, že je AVAST32 verze 3.0 instalován, a to jak na serveru, tak na klientské stanici, ze které budete provádět správu.

2.1 Požadavky na vybavení počítače

K tomu, aby mohl být AVAST32 úspěšně nainstalován na Váš počítač a poté i bezchybně pracovat, je nutné, aby Váš počítačový systém splňoval několik základních požadavků.

Pro instalaci na server:

- procesor 486 nebo vyšší
- 64 MB paměti RAM
- Windows NT 4.0 Server
- Exchange Server 5.x
- Pokud máte Exchange 5.5 SP3, pak musí být instalován i hotfix (IS Patch) z 10.5.2000 (verze 5.5.2652.42) nebo novější (více informací viz <http://support.microsoft.com/support/kb/articles/>

Pro instalaci jako klient

- počítač splňující požadavky na běh programu AVAST32 verze 3.0

2.2 Instalujeme

Ještě před započítím instalace na server je třeba, abyste provedli určitá opatření na Vašem MS Exchange Serveru. Postupujte podle následujícího návodu:

- Spustte administrátorský program serveru (program *Microsoft Exchange Administrator*), a to v „raw“ režimu, tj. s parametrem *-raw* na příkazové řádce. Jednou z metod, jak toto udělat, je např. z příkazové řádky zadat příkaz

```
<Ex_Cesta> \bin \admin -raw
```

kde <ExCesta> je úplná cesta k adresáři, kde je MS Exchange Server nainstalován.

- Ve stromečku v levé části okna administrátorského programu přejděte do složky <Organization> \<Site> \Configuration \Servers \<Server>, kde za položky <Organization>, <Site> a <Server> pochopitelně doplňujeme jejich skutečná jména.
- V pravé části okna zvolte *System Attendant* a z menu *File* vyberte *Raw properties* (můžete též použít klávesovou zkratku Shift+Enter).
- V kombinovaném poli *List attributes of type* v dolní části okna zvolte *All*. To Vám umožní provést vyžadované změny.
- Měnit budeme celkem dva atributy. Nejprve zvolte v seznamu *Object Attributes* položku *Display Name*. Vpravo napište jméno schránky, kterou bude System Attendant používat. Toto jméno může být libovolné, ale tradičně se volí přirozeným způsobem prostě jako „System Attendant“. Dále změňte atribut *Hide from AB*, a to konkrétně na hodnotu 0 (nula). **Pozor**, nové hodnoty nestačí do pole *Edit value* pouze zapsat, musíte je vždy potvrdit stiskem tlačítka *Set*.

Touto procedurou jste zpřístupnili poštovní schránku komponenty System Attendant pro Vaši globální knihu adres. To je podstatné, protože právě pod tímto účtem Avast pracuje.

V následující druhé části přípravné fázi instalace Avastu ještě nastavíme určitá práva pro účet System Attendant. Tato práva Avast ke své práci vyžaduje. Nastavení provedete následujícím postupem:

- V administrátorském programu Exchange Serveru ve stromečku v levé části okna přejděte do složky *Organization \Site \Configuration*. V pravé části okna se objeví obsah této složky.
 - Pокlepejte na položku *Information Store Site Configuration*. Tím se Vám otevře okno s několika kartami, prostřednictvím kterých můžete konfigurovat různé věci týkající se veřejných složek na Exchange Serverech ve vaší organizaci.
 - Zvolte kartu *Top Level Folder Creation*. Na této kartě se specifikují účty, které jsou oprávněny vytvářet veřejné složky v kořenovém adresáři veřejných složek. Avast potřebuje pro svou práci takovou složku vytvořit, takže je třeba mu to nějakým způsobem umožnit. Nyní mohou nastat dva případy:
Pokud je v okénku *Allowed to create top level folders* zvolen přepínač *All*, není třeba nic dalšího nastavovat. Vytvářet složky v kořenovém adresáři mohou v tomto případě všichni, tj. i Avast, bez omezení.
Je-li však nastaveno *List*, je třeba zajistit, aby v seznamu pod tímto přepínačem byl uveden právě i účet *System Attendant*. Pokud v seznamu tento účet uveden není, stiskněte tlačítko *Modify...* a účet do seznamu přidejte. Toto nastavení by z hlediska bezpečnostní politiky Vašeho podniku nemělo představovat žádnou hrozbu, protože System Attendant je nedílnou součástí Microsoft Exchange Serveru a jako takovému by mu mělo být umožněno bez omezení na serveru pracovat (a to bez ohledu na Avast).
- Stiskněte OK pro uložení změn a ukončete administrátorský program.

Po provedení těchto úprav již můžete přistoupit k samotné instalaci.

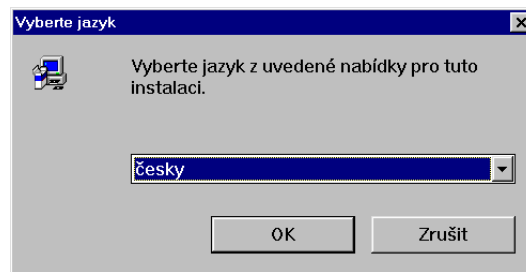
Upozornění: instalaci serverové části je nutno provádět pod administrátorským účtem MS Exchange Serveru. Jinými slovy, pro instalaci Avastu se musíte do počítače přihlásit pod administrátorským účtem (služby) MS Exchange Serveru. Bez splnění tohoto požadavku instalace neproběhne správně! Instalaci klientské části lze provádět pod jakýmkoli účtem s dostatečnými právy.

Instalace se spouští souborem SETUP.EXE z adresáře AVAST32.EXC, který se nachází na instalačním CD.

Instalace programu AVAST32 probíhá formou dialogu mezi uživatelem a instalačním programem. V následujícím textu si podrobně popíšeme jednotlivá okna, která budou v průběhu instalace zobrazena.

Instalaci je možné kdykoli přerušit - u jednotlivých oken instalace je popsáno, jakým způsobem to lze provést. Před vlastním ukončením bude uživatel dotázán, zda to s ukončením instalace myslí opravdu vážně. Po potvrzení přerušit instalace bude vše, co bylo doposud nainstalováno, odstraněno a systém bude uveden do původního stavu.

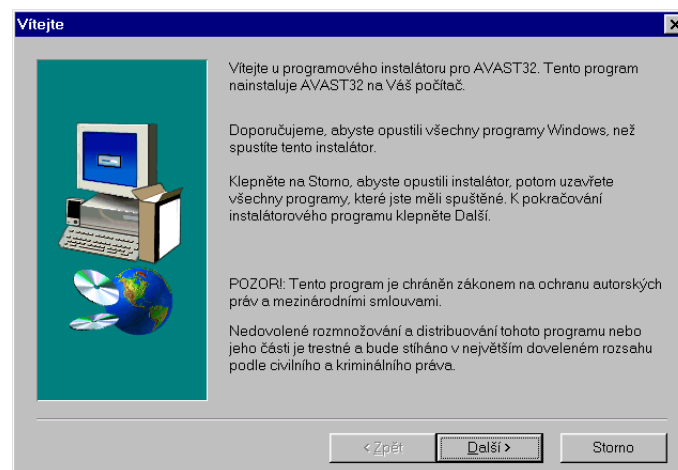
Po spuštění instalačního programu budete vyzváni, abyste zvolili jazyk (obr. 2.1), kterým chcete s programem komunikovat. Volbu provedete výběrem příslušného jazyka ze seznamu, jenž se objeví po klepnutí na šipku vpravo od aktuálního jazyka.



2.1 Zvolte Jazyk

Po zvolení jazyka budete požádáni o chvíli strpení, zatímco bude program pracovat na přípravě instalace.

Jakmile je příprava instalace dokončena, objeví se obrazovka (obr. 2.2) vlastního instalačního programu. Uprostřed je okno tzv. průvodce, který Vám pomůže s celým procesem instalace. V jeho spodní části se nachází tři tlačítka, sloužící ke sdělení Vašich pokynů průvodci.

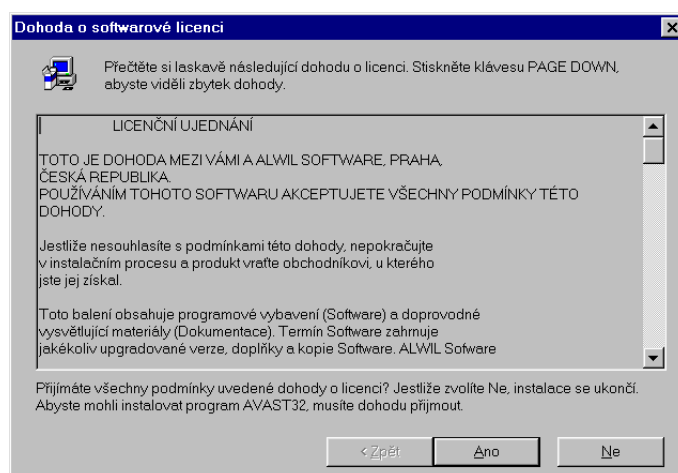


2.2 Obrazovka instalačního programu

Tlačítko „< Zpět“ slouží k návratu k předchozímu oknu průvodce. Pokud jej není možné použít (např. pokud jste u prvního kroku instalace), pak je tlačítko zšedlé. Tlačítko „Další >“ slouží naopak k přechodu na následující krok průvodce. Dříve než jej však použijete, doporučujeme Vám si důkladně přečíst obsah okna průvodce. Tlačítkem „Storno“ můžete proces instalace kdykoli přerušit.

První okno průvodce informuje uživatele o majiteli autorských práv a varuje před neoprávněnou manipulací s programem nebo jeho částí. Po jeho přečtení klepnutím na tlačítko „Další >“ přejdete k následujícímu oknu průvodce.

Další okno instalačního programu obsahuje licenční ujednání (obr. 2.3) mezi Vámi a firmou ALWIL Software. Licenční ujednání obsahuje podmínky, které musíte jako uživatel AVAST32 dodržet, a práva, která jako uživatel programu máte. Jestliže s licenčním ujednáním a se všemi jeho částmi souhlasíte, pak klepněte na tlačítko „Ano“. Průvodce Vás poté pustí k dalšímu kroku instalace. Pokud s licenčním ujednáním nesouhlasíte, klepnutím na tlačítko „Ne“ ukončíte instalační program. AVAST32 pak nebude nainstalován.



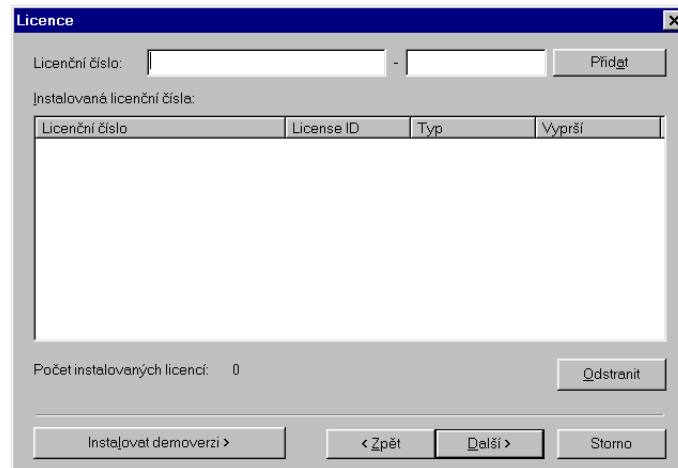
2.3 Licenční ujednání mezi Vámi a firmou ALWIL Software

Protože je licenční ujednání větší než okno průvodce, nelze jej zobrazit celé. Po pravé straně okna se nachází posuvná lišta, pomocí níž je možné se v licenčním ujednání pohybovat. Její jezdec zároveň zobrazuje pozici, ve které se právě nacházíte. Pro zobrazení zbývajících částí licenčního ujednání je možné též použít kláves pro posun kurzoru nahoru a dolů, popř. kláves označených „PgUp“ a „PgDn“ pro přesun na předcházející nebo následující stránku licenčního ujednání.

Okno, následující za oknem s licenčním ujednáním, zobrazuje soubor README.TXT. Ten obsahuje důležité informace, které jsme již nestihli zařadit do této dokumentace. Informace se mohou týkat vlastního programu, ale také např. instalace a může obsahovat i návody jak postupovat, nastanou-li nějaké problémy. Rozhodně byste si měli soubor README.TXT důkladně přečíst - ušetříte si tak možné komplikace.

V zobrazeném textu je možné se pohybovat stejným způsobem jako v případě licenčního ujednání v předchozím okně průvodce. I ovládání okna je velmi podobné. Máte-li soubor README.TXT přečtený, klepnutím na tlačítko „Ano“ přejdete na další okno průvodce. Tlačítko „< Zpět“ Vás vrátí na předchozí okno s licenčním ujednáním a tlačítkem „Ne“ instalaci programu AVAST32 ukončíte.

Další okno průvodce obsahuje dialog, do kterého je třeba zapsat aktivační klíč (obr. 2.4) Vaší kopie programu. Zapsat nebo změnit údaje v jednotlivých textových polích Vám bude umožněno po klepnutí levým tlačítkem myši na příslušné pole. Přesunout se na dané textové pole je také možné opakovaným stiskem klávesy „Tab“.

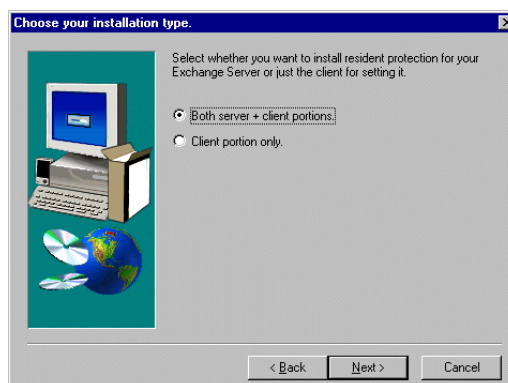


2.4 Okno pro zadání aktivačního klíče

Po zapsání aktivačního klíče jej pro jistotu ještě jednou zkontrolujte. Bez jeho správného zadání nebude program nainstalován!

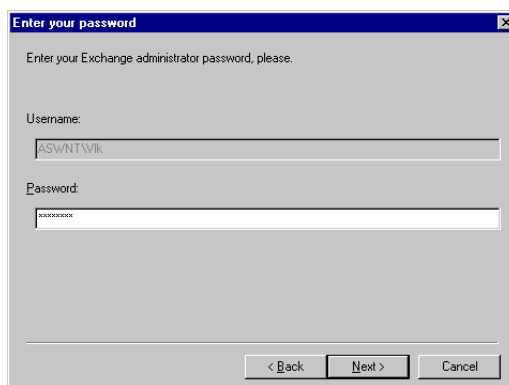
Tlačítkem „Další >“ potvrdíte zadaný aktivační klíč a jestliže byl zadán správně, pak Vás průvodce pustí k dalšímu oknu. V opačném případě obdržíte chybové hlášení a aktivační klíč budete muset opravit. Tlačítkem „< Zpět“ se vrátíte k oknu se zobrazeným souborem README.TXT.

Další okno umožňuje zvolit typ instalace (obr. 2.5). Pokud je instalace spuštěna na počítači s nainstalovaným Exchange serverem je možné zvolit instalaci buď „Server+klient“ nebo „pouze klient“. Jestliže není na počítači detekována přítomnost Exchange serveru, je nabízena pouze možnost instalace „pouze klient“. Pomocí přepínače zvolte vybraný způsob instalace. Tlačítkem „Další >“ potvrdíte vaši volbu, a průvodce Vás pustí k dalšímu oknu. Tlačítkem „< Zpět“ se vrátíte k oknu, které umožňuje zadání aktivačního klíče.



2.5 Zvolení typu instalace

Další okno se zobrazí pouze v případě, že byla zvolena „Server+klient“ instalace. Na této stránce (obr. 2.6) je třeba zadat heslo administrátorského účtu Exchange serveru. Pouze bude-li zadané heslo správné, bude možné v instalaci pokračovat. Tlačítkem „Další >“ potvrdíte zadané heslo, a průvodce Vás pustí k dalšímu oknu. Tlačítkem „< Zpět“ se vrátíte k oknu, které umožňuje zvolit typ instalace.



2.6 Stránka pro vložení hesla

Následující okno zobrazuje všechny informace, které jste průvodci zadali. Prosíme, zkontrolujte uvedené údaje a pokud Vám nevyhovují nebo neodpovídají skutečnosti, můžete se pomocí tlačítka „< Zpět“ vrátit k předchozím oknům průvodce a příslušné údaje v nich opravit. Jestliže je vše podle Vašich představ, můžete klepnutím na tlačítko „Další >“ přikročit k vlastní instalaci souborů programu AVAST32 na Váš pevný disk. Tlačítkem „Storno“ můžete instalaci přerušit.

O množství zkopírovaných souborů Vás informuje indikátor na obrazovce instalačního programu. Jakmile budou nainstalovány všechny soubory, průvodce automaticky přejde na následující okno.

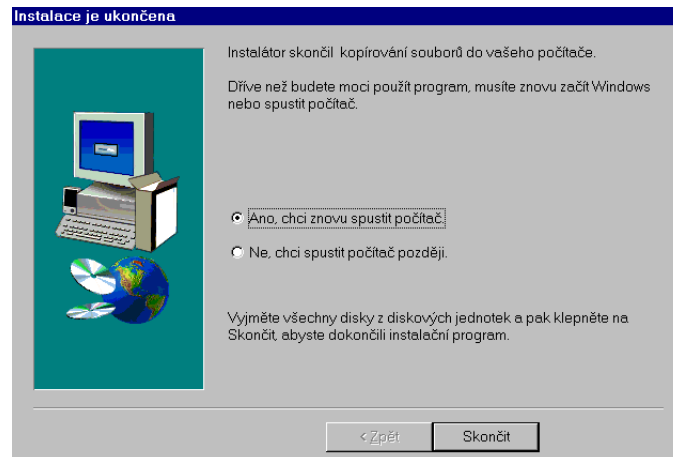
Poslední okno průvodce ukazuje tento obrázek (obr. 2.7). Obsahuje přepínače, pomocí kterých můžete určit, jestli má být počítač znovu spuštěn nebo jestli má být instalační program ukončen bez spuštění počítače. Doporučujeme Vám nechat zvolený přednastavený přepínač. Klepnutím na tlačítko „Skončit“ ukončíte instalační program a v závislosti na zvoleném přepínači bude znovu spuštěn i Váš počítač.

Po instalaci programu AVAST32 a před jeho prvním spuštěním je zapotřebí počítač znovu spustit. Pokud jste tak neučinili za pomoci průvodce na jeho posledním okně, musíte to provést později sami. V nabídce tlačítka Start zvolíte položku „Vypnout“. V zobrazeném okně potom zaškrtnete položku „Restartovat počítač“ a stiskem tlačítka „Ano“ provedete nové spuštění počítače.

2.3 Problémy s instalací

Nejnámější problémy s instalací programu AVAST32 jsou popsány zde:

- nelze nainstalovat kvůli chybě aktivačního klíče. Zadali jste špatně aktivační klíč. Ujistěte se, zda jste jej skutečně opsali správně. Pokud jste si stoprocentně jisti, že ano, písmeno „O“ si nepletete s je nejvyšší čas kontaktovat firmu ALWIL Trade s.r.o. a požadovat kontrolu aktivačního klíče.



2.7 Volba restartu počítače

- program nelze nainstalovat pro nedostatečná práva. Jak již bylo řečeno, pro instalaci tohoto programu je třeba být přihlášen pod administrátorským účtem MS Exchange Serveru. Odhlašte se, a přihlašte se jako administrátor nebo kontaktujte administrátora Vaší sítě.

Pokud dojde k nějaké jiné chybě instalace, je zapotřebí přesvědčit se, zda se nejedná o Vaši chybu či chybu Vašeho systému. Pokud zcela vyloučíte problémy na Vaší straně, kontaktujte technickou podporu. Opište si však doslovně veškerá chybová hlášení.

3 První kroky

Po úspěšně dokončené instalaci a restartu Windows můžete ihned nové funkce programu AVAST32 začít používat.

Veškeré funkce AVAST32 3.0 Exchange Server Edition jsou ovládány prostřednictvím úlohy, vytvořené v rozšířeném ovládní programu AVAST32 3.0.

Pro spuštění programu AVAST32 klikněte na tlačítko „Start“, pak zvolte složku „Programy“, dále nalistujte složku „AVAST32 Antivirus“ a v této složce klikněte na ikonu „AVAST32“.

Po spuštění programu se ujistěte, zda pracujete v rozšířeném ovládní. Pokud pracujete v jednoduchém ovládní klikněte levým tlačítkem myši na ikonu v levém horním rohu programu a vyberte rozšířené ovládní ze zobrazeného menu.

Úlohy na MS Exchange Serveru lze rozdělit do dvou skupin: rezidentní (tzv. on-access) a na vyžádání (tzv. on-demand). Klíčovou roli hraje zejména rezidentní ochrana, neboť ta jako jediná může efektivně zamezit nekontrolovanému šíření virů v reálném čase.

Podrobný popis vytváření úloh pro ochranu Exchange Serveru se nachází v následujících kapitolách.

3.1 Rezidentní ochrana

Rezidentní ochrana Exchange serveru spočívá v neustálém monitorování poštovních schránek a veřejných složek. V Avastu je tato ochrana implementována prostřednictvím nového poskytovatele, pojmenovaného Exchange Server, kterého lze zahrnout do libovolné rezidentní úlohy.

Poskytovatel Exchange Server zajišťuje uniformní ochranu příchozích a editovaných zpráv a umožňuje poměrně bohaté možnosti konfigurace. Tyto možnosti jsou podrobně rozebrány v následující kapitole

Od prosince 2000 využívá Avast ke své činnosti kromě standardního MAPI též nové rozhraní Exchange 5.5 SP3, tzv. AVAPI, které přináší vylepšené testování zpráv (včetně odchozích), a též možnost blokování příloh podle jména. Více informací viz kapitola 5.

3.2 Testování na vyžádání

Nedílnou součástí Avastu pro MS Exchange Server je i modul pro hledání virů na vyžádání. Ten slouží k manuálnímu testování jak poštovních schránek, tak i veřejných složek na serveru.

Tento modul funguje tak, že v Avastu lze zvolit jako jednu z předdefinovaných oblastí (kromě např. lokálních pevných disků nebo CD-ROM) i oblast na Exchange Serveru.

Hledání virů na vyžádání je užitečné provést zejména brzy po instalaci Avastu, kdy ještě nemáte přehled o stupni zavirování jednotlivých schránek a potřebujete docílit počátečního stavu kompletního odvírování. Modul však může být pochopitelně užitečný i později pro rutinní ověření tohoto stavu. Lze doporučit např. použití plánovače (kupř. systémového programu „AT“) pro jeho periodické spouštění.

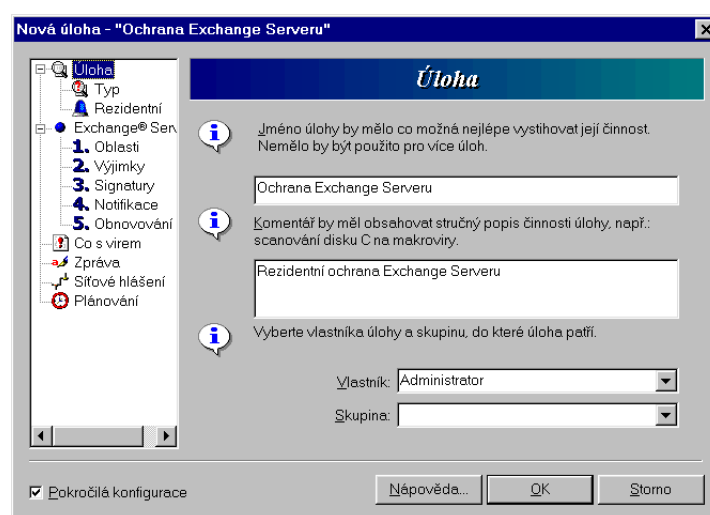
4 Konfigurace rezidentní úlohy

V následujícím textu budou popsány jednotlivé stránky s ovládacími prvky, které se týkají nastavení úlohy na rezidentní ochranu MS Exchange serveru. Obrázky zobrazené u jednotlivých stránek ukazují stránky při použití stromu při konfiguraci úlohy. Při použití průvodce nebo záložkového seznamu je podoba okna jiná, ale ovládací prvky a jejich význam jsou však tytéž.

Pro rezidentní ochranu můžete použít jak standardní úlohu „Rezidentní ochrana“ (po příslušné modifikaci, popsané níže - konkrétně zahrnutí poskytovatele Exchange Server), tak i zcela novou, vámi definovanou úlohu. Tu vytvoříte následujícím postupem: na stránce „Úlohy“ rozšířeného ovládání klikněte pravým tlačítkem myši na seznamu úloh nebo klikněte na nabídku „Úloha“ v hlavním menu programu, a ze zobrazeného menu vyberte položku „Vytvořit novou ...“. Zobrazí se dialog pro vytvoření nové úlohy.

4.1 Stránka „Úloha“

Na stránce „Úloha“ (obr. 4.1) je programem požadováno vložení jména vytvářené úlohy. To by mělo být co možná nejvýstižnější a nemělo by být kvůli přehlednosti shodné s některým jménem již existující úlohy. Jestliže nezadáte žádné jméno, nebude nová úloha vytvořena. Implicitně textové pole obsahuje „(nespecifikováno)“.



4.1 Stránka „Úloha“

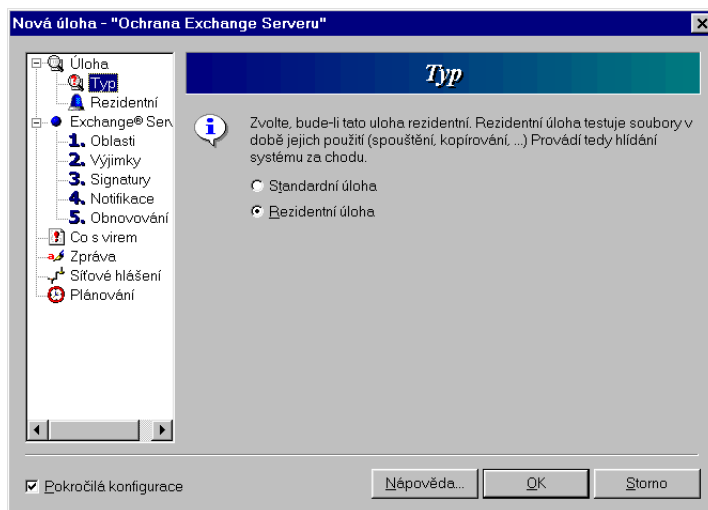
Do dalšího textového pole je možné napsat komentář úlohy stručně popisující činnost úlohy. Tato položka může zůstat prázdná.

Pomocí kombinovaného pole „Skupina“ nastavte skupinu, do které úloha patří.

Pomocí kombinovaného pole „Vlastník“ nastavte vlastníka, kterému úloha patří.

4.2 Stránka „Typ“

Na stránce „Typ“ (obr. 4.2) zvolte pomocí přepínače „Rezidentní“ vytváření rezidentní úlohy

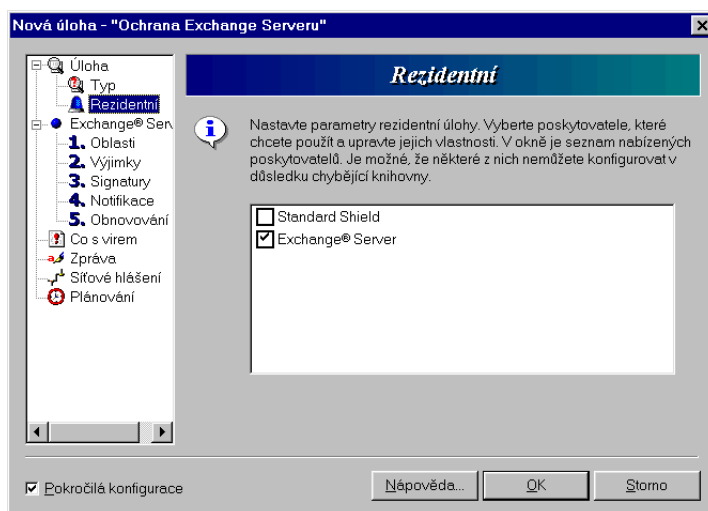


4.2 Stránka „Typ“

Po zvolení přepínače se automaticky změní možnosti dalšího nastavení úlohy.

4.3 Stránka „Rezidentní“

Stránka „Rezidentní“ (obr. 4.3) obsahuje seznam dostupných poskytovatelů rezidentní ochrany.



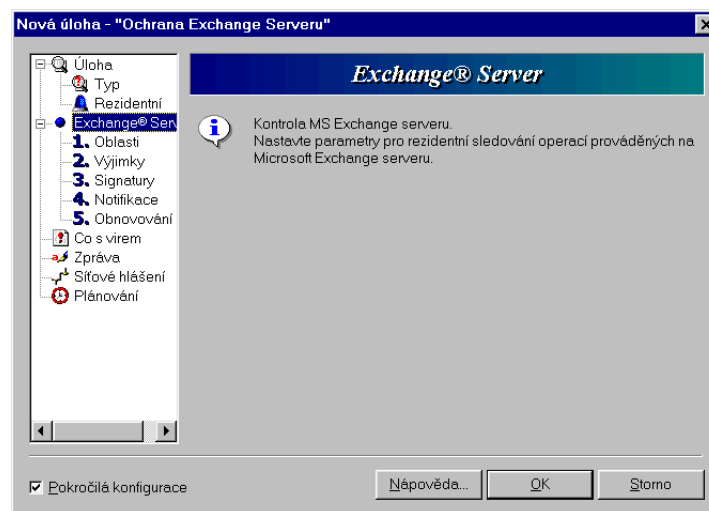
4.3 Stránka „Rezidentní“

Počet položek uvedených v seznamu je závislý na verzi programu, kterou používáte. Na této stránce zaškrtněte zaškrťovací pole „Exchange Server“. U ostatních položek seznamu můžete (ovšem nemusíte) zaškrtnutí zrušit, pokud nechcete dané poskytovatele používat. Například plně podporovaná konfigurace je i ta, kde na stejném počítači používáte jak poskytovatele pro Exchange Server, tak i Standardní štít.

Jedinou výjimkou z tohoto pravidla je poskytovatel Internet Mail - jeho používání na Exchange Serveru (nebo i jiném poštovním serveru) se nedoporučuje, neboť tento poskytovatel pro svou činnost používá též jednoduchý SMTP/POP3 server. Protože pro tyto služby jsou přiděleny pevná čísla TCP portů (u SMTP jde o 25, v případě POP3 je to 110), je možné na jednom počítači provozovat nejvýše jeden takový server (tzn. buďto server v poskytovateli Internet Mail, nebo Internet Mail Connector z Microsoft Exchange).

4.4 Stránka „Exchange Server“

Tato stránka zobrazuje pouze informace o zvoleném poskytovateli rezidentní ochrany.



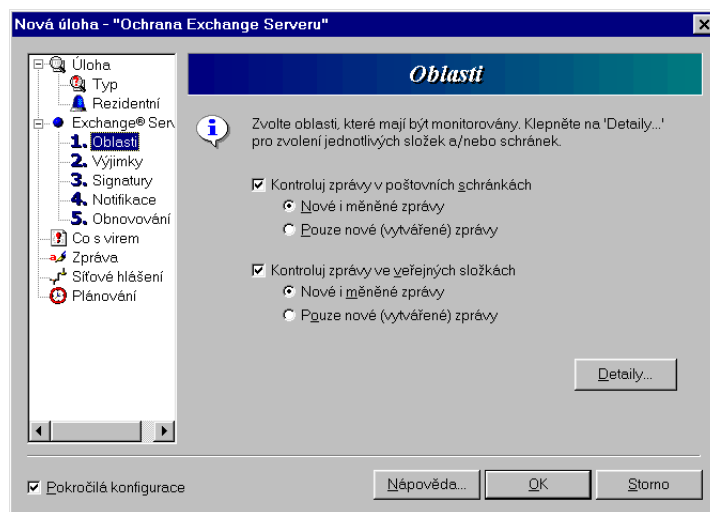
4.4 Stránka „Exchange Server“

4.5 Stránka „Oblasti“

Stránka „Oblasti“ (obr. 4.5) umožňuje uživateli nastavit oblasti, které má nově vytvářená úloha kontrolovat.

Pomocí zaškrťovacího pole „Kontroluj zprávy v poštovních schránkách“ určíte zda budou testovány zprávy v poštovních schránkách umístěných na serveru. Toto pole je standardně zaškrtnuto.

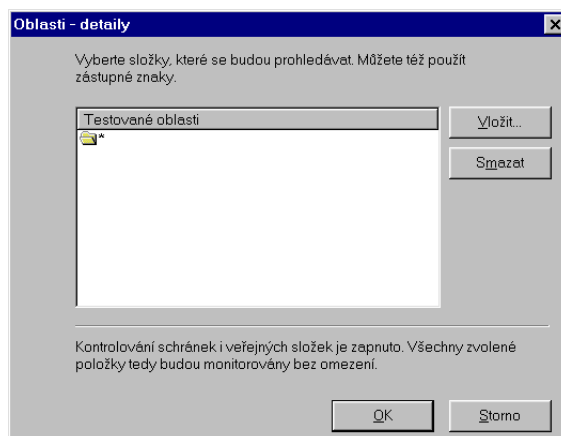
Zaškrtnutím zaškrťovacího pole „Kontroluj zprávy ve veřejných složkách“ zajistíte testování zpráv ve veřejných složkách.



4.5 Stránka „Oblasti“

Přepínače „Nové i měněné zprávy“ a „Pouze nové (vytvářené) zprávy“ slouží k určení, zda se mají testovat pouze nové zprávy nebo zároveň i zprávy měněné. Standardně je nastavena kontrola všech zpráv.

Klepnutím na tlačítko „Detaily“ se zobrazí dialog (obr. 4.6), ve kterém můžete přesně zvolit jaké schránky či složky budou kontrolovány. Zde jsou v seznamu uvedené testované oblasti. Standardně seznam obsahuje zástupný znak „*“, kterým je zajištěno testování veškerých oblastí zvolených v hlavním okně stránky „Oblasti“.



4.6 Oblasti-detaily

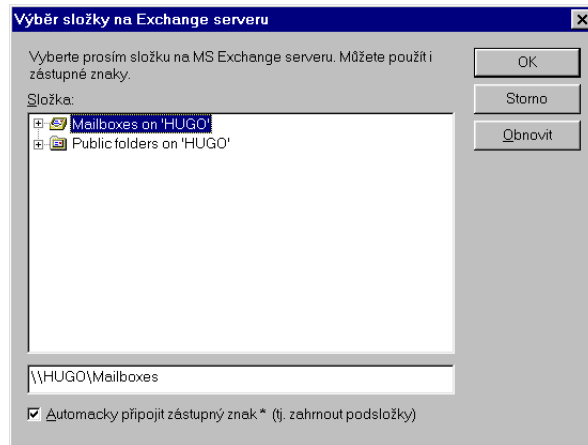
Program bude kontrolovat pouze oblasti, které jsou uvedeny v tomto seznamu. Bude-li seznam prázdný, program nebude kontrolovat žádné oblasti!

Pomocí tlačítka „Vložit“ zobrazíte dialog (obr. 4.7) sloužící pro výběr oblastí.

Chcete-li nějakou oblast ze seznamu odstranit, pak ji nejprve vyberte levým tlačítkem myši a potom klepněte na tlačítko „Smazat“ nebo zmáčkněte klávesu „Del“.

Dialog pro výběr oblastí na Exchange serveru

V horní části dialogového okna jsou ve stromové struktuře zobrazeny dostupné oblasti. Zde nalistujete požadovanou složku a její zvolení potvrdíte stisknutím tlačítka „OK“.



4.7 Dialog pro výběr oblastí na Exchange serveru

Oblast, která má být kontrolována, můžete také zadat přímo do textové pole ve spodní části obrazovky. Ve jménu oblasti je pak možné použít i zástupné znaky „*“ (hvězdička) a „?“ (otazník) a specifikovat tak více složek najednou.

Zaškrtačací pole „Automaticky připojit zástupný znak *“ zajistí, aby u zvolené složky byly kontrolovány i její podsložky. Není-li pole zaškrtnuto, budou kontrolovány pouze zprávy ve vybrané složce, zprávy ve vnořených složkách testovány nebudou. Implicitně je testování vnořených složek povoleno.

Pomocí tlačítka „Obnovit“ můžete ze serveru získat aktualizovaný seznam dostupných položek.

Tlačítkem „Storno“ zavřete tento dialog.

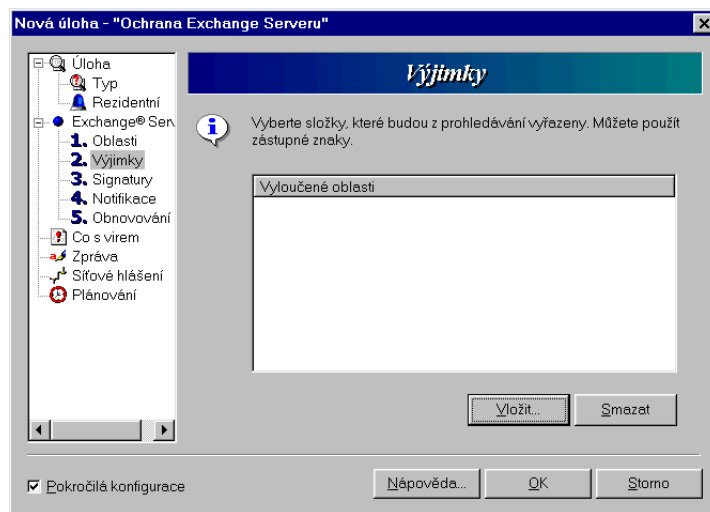
4.6 Stránka „Výjimky“

Stránka „Výjimky“ (obr. 4.8) umožňuje uživateli nastavit, které složky nemá nově vytvářená úloha kontrolovat.

Na této stránce jsou v seznamu uvedené oblasti, které jsou z testování vyřazeny. Implicitně je seznam prázdný.

Pomocí tlačítka „Vložit“ zobrazíte dialog (obr. 4.7) sloužící pro výběr oblastí, které nechcete kontrolovat.

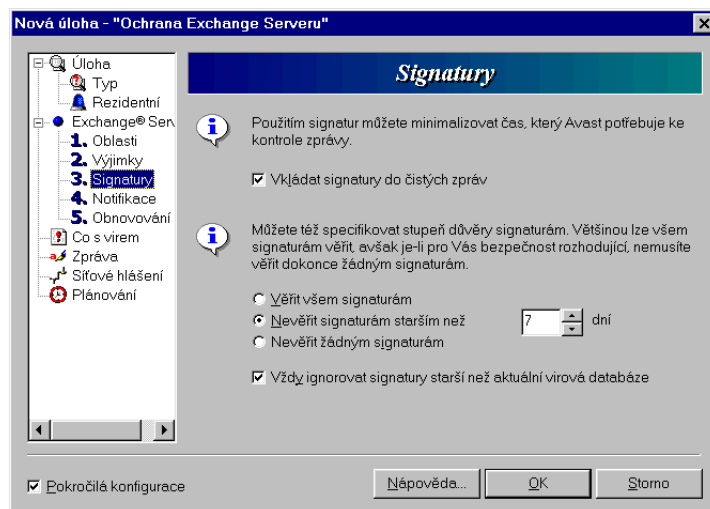
Chcete-li nějakou oblast ze seznamu odstranit, pak ji nejprve vyberte levým tlačítkem myši a potom klepněte na tlačítko „Smazat“ nebo zmáčkněte klávesu „Del“.



4.8 Stránka „Výjimky“

4.7 Stránka „Signatury“

Stránka „Signatury“ (obr. 4.9) slouží k nastavení používání signatur při kontrole zpráv.



4.9 Stránka „Signatury“

Význam a popis signatur je podrobně popsán v kapitole „Signatury“.

Zaškrtnuté pole „Vkládat signatury do čistých zpráv“ určuje, zda se budou vkládat signatury do nezavírovaných zpráv. Implicitně je vkládání signatur povoleno.

Přepínače ve spodní části obrazovky slouží k nastavení stupně důvěry signaturám.

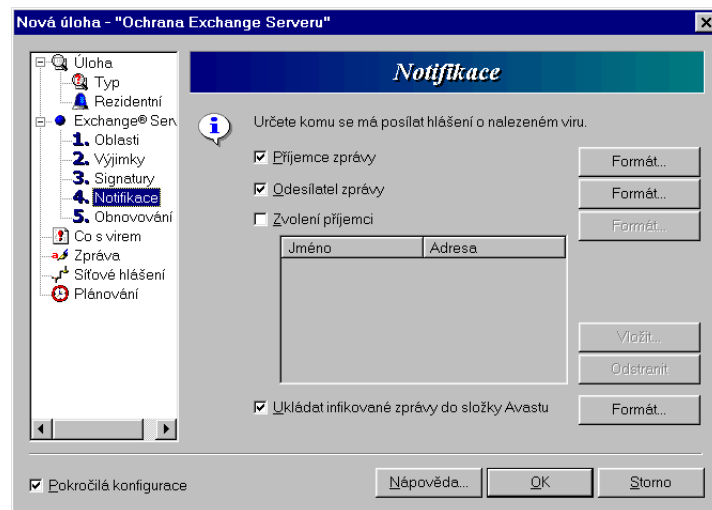
Pomocí přepínače „Věřit všem signaturám“ nebo přepínače „Nevěřit žádným signaturám“ nastavte, zda se má věřit signaturám či nikoliv.

Přepínač „Nevěřit signaturám starším než“ slouží k přesnějšímu definování důvěry signaturám. Do textového pole vedle tohoto přepínače napište číslo, kterým určíte počet dní, po jejichž uplynutí se již signaturám nebude důvěřovat.

Zaškrtnutím zaškrťovacího pole „Vždy ignorovat signatury starší než aktuální virová databáze“ zajistíte, aby byly ignorovány signatury, které jsou starší než aktuální virová databáze programu AVAST32.

4.8 Stránka „Notifikace“

Na stránce „Notifikace“ (obr. 4.10) můžete určit komu se má posílat hlášení o viru a upravit formát zasílaných zpráv.



4.10 Stránka „Notifikace“

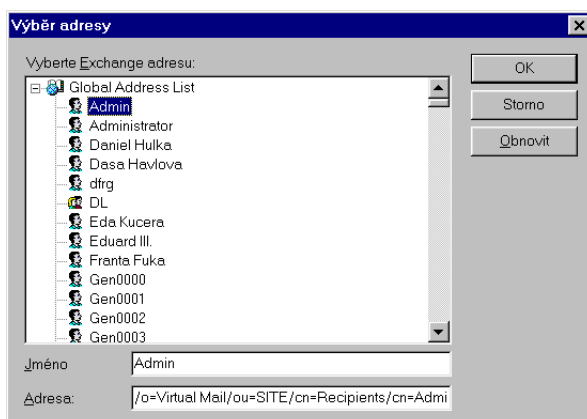
Pomocí zaškrťovacího pole „Příjemce zprávy“ určíte, že se hlášení o viru odešle příjemci zprávy

Zaškrtnutím zaškrťovacího pole „Odesílatel zprávy“ zajistíte odeslání varovné zprávy odesílateli zprávy.

Pokud chcete zvolit další příjemce zprávy, zaškrtněte zaškrťovací pole „Zvolení příjemci“. Bude Vám umožněno přidání příjemce zprávy pomocí tlačítka „Vložit“. Po stisku tohoto tlačítka se zobrazí dialog (obr. 4.11) umožňující výběr konkrétní adresy.

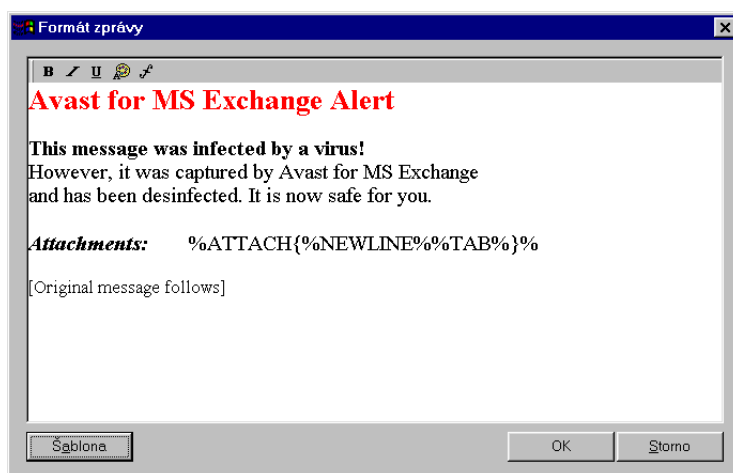
V zobrazeném dialogu nalistujte požadovanou adresu v seznamu, nebo ji můžete přímo zapsat do textového pole ve spodní části obrazovky dialogu. Jestliže jste s výběrem spokojeni klikněte na tlačítko „OK“ a adresa bude přidána do seznamu na hlavní stránce „Notifikace“.

Zaškrťovací pole „Ukládat infikované zprávy do složky Avastu“ zajistí, že infikovaná zpráva bude uložena do logovací složky Avastu ve veřejných složkách (více informací viz kapitola 7.3).



4.11 Výběr Exchange adresy

Tlačítko „Formát“ slouží k úpravě formátu zasílaných zpráv. Pokud tedy chcete změnit např. formát zprávy příjemce, klikněte na tlačítko „Formát“ vedle zakškrťacího pole „Příjemce zprávy“. Zobrazí se dialog (obr. 4.12), který Vám umožní detailně nastavit formát zprávy. Při specifikaci můžete použít bohaté formátovací možnosti standardu RTF, a též specifikovanou jistě šablony, které budou při běhu programu nahrazeny příslušnými daty. Více informací viz kapitola Zprávy a protokoly.

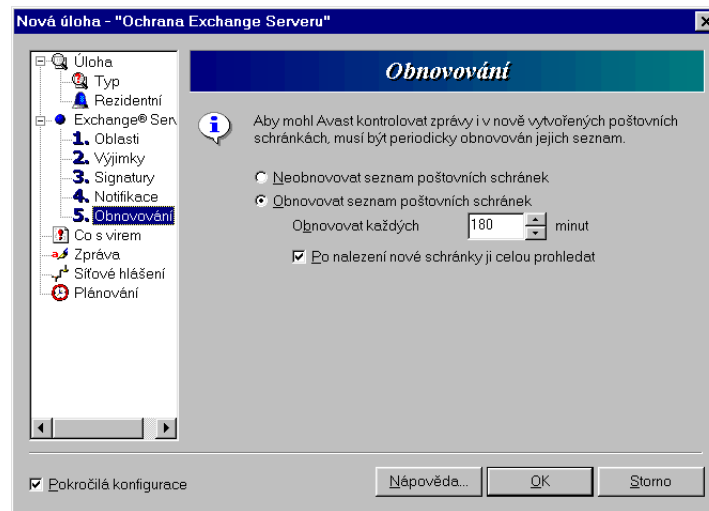


4.12 Formát zprávy

4.9 Stránka „Obnovování“

Na stránce „Obnovování“ (obr. 4.13) je možné nastavit periodu, po jejíž uplynutí má být aktualizován seznam poštovních schránek dostupných na serveru. Tato aktualizace zajistí, že budou testovány i nově vytvořené poštovní schránky.

Pomocí přepínače „Neobnovovat seznam poštovních schránek“ nebo přepínače „Obnovovat seznam poštovních schránek“ nastavte, zda se má seznam poštovních schránek obnovovat či nikoliv.



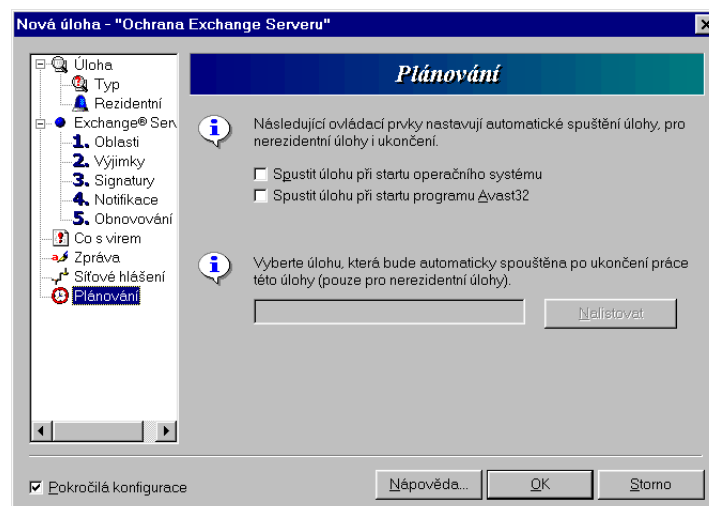
4.13 Stránka „Obnovování“

Pokud zvolíte „Obnovovat seznam poštovních schránek“, bude moci periodu obnovy blíže specifikovat pomocí textového pole „Obnovovat každých“.

Zaškrtnuté pole „Po nalezení nové schránky ji celou prohledat“ určuje, zda se má nově nalezená poštovní schránka prohledat na přítomnost známých virů.

4.10 Stránka „Plánování“

Stránka „Plánování“ (obr. 4.14) obsahuje nastavení automatického spuštění a ukončování úloh.



4.14 Stránka „Plánování“

Zaškrtnutím pole „Spustit úlohu s operačním systémem“ uživatel sdělí programu, že vytvářená úloha má být spuštěna ihned po přihlášení uživatele. Implicitně není pole zaškrtnuto.

Zaškrťovací pole „Spustit úlohu při startu programu AVAST32“ zapíná spouštění úlohy automaticky po startu programu AVAST32. Spouštění úlohy zároveň s programem AVAST32 je implicitně vypnuto.

5 AVAPI a blokování příloh podle jména

Jako novinka byla do Avastu pro MS Exchange Server v prosinci 2000 (build 304) přidána podpora nového antivirového rozhraní, tzv. AVAPI. Toto rozhraní je k dispozici pouze v MS Exchange 5.5 SP3 nebo vyšší, a pro jeho správnou funkčnost je nezbytně nutné mít při použití SP3 též nainstalován hotfix, který odstraňuje chybu, která byla obsažena v původní verzi a způsobovala občasný pád serveru. Více informací o tomto hotfixu viz systémové požadavky v kapitole 2.1.

Provozujete-li na serveru Exchange 5.5 SP2 nebo nižší, nebude AVAPI Avastem používáno (jelikož není k dispozici) a žádná z dále popsanych funkcí nebude pochopitelně fungovat. Máte-li tedy Exchange 5.5 se starším service packem, velice vám doporučujeme, abyste zvážili upgrade na poslední SP.

Nové AVAPI Avast používá ke dvěma účelům. Za prvé jde o dokonalejší detekci virů, za druhé o blokování určitých příloh zpráv podle jejich jmen.

5.1 Dokonalejší detekce virů

Implicitní rozhraní, které Avast pro Exchange používá ve všech svých verzích (tzv. MAPI), má tři zásadní nevýhody.

Jednak je to skutečnost, že je-li server velmi vytížen, není garantováno, že antivirový program bude pro určitou zprávu volán (tzn. je možné, že (potenciálně zavirovaná) zpráva projde přes server neotestovaná). Tato vlastnost je dosti zásadního charakteru, protože hovoří o tom, že za jistých okolností antivirový program na Exchange serveru může opravdu propouštět viry.

Dále potom je značnou nevýhodou rozhraní MAPI fakt, že je-li jedna zpráva adresována více příjemcům, dostane k ní Avast přístup až poté, co je rozkopírována do jednotlivých poštovních schránek. Tj. pokud např. přijde infikovaná zpráva, která je adresována 300 uživatelům na daném serveru, musí Avast ze zprávy virus odstraňovat celkem 300 krát, což je samozřejmě velmi zdlouhavá práce. Některé viry ovšem přesně takto fungují - rozesílají zprávy s velkým počtem adresátů. Příkladem je např. nechvalně známý virus *I Love You*.

Třetím problémem s MAPI je nemožnost kontroly odchozí pošty. Opravdu, antivirové programy používající MAPI jsou omezeny na testování zpráv ukládaných do informační databáze MS Exchange, tj. přijímaných a editovaných zpráv. K odesílaným zprávám nemají přístup.

Tyto nevýhody si zjevně uvědomili i programátoři Microsoftu, a proto bylo do Exchange 5.5 SP3 zavedeno nové rozhraní, tzv. AVAPI, které mělo všechny tyto problémy efektivně řešit. Hned z kraje je však nutno poznamenat, že stávající verze AVAPI má své (a to dost dost značné) nedostatky. Je to rozhraní velmi jednoduché, které, zhruba řečeno, dává antivirovému programu možnost přístupu k přílohám zpráv ještě před jejich doručením do poštovní schránky. Neumožňuje přístup k těle zprávy; nedává možnost zjišťovat či měnit ani další atributy zprávy, např. adresu příjemce nebo odesílatele, apod. Proto pro implementaci robustního antivirového systému je třeba použít kombinaci obou rozhraní, která by v ideálním případě měla zaručit skutečně velmi vysoký stupeň bezpečí.

Poznamenejme, že do Exchange 2000 SP1 je plánováno zahrnutí nového rozhraní, tzv. AVAPI 2.0, které by již mělo být dostatečně bohaté na to, aby antivirový program mohl zcela zanevřít na onen hybridní MAPI/AVAPI model a přitom efektivně pracovat.

AVAPI: Testování příchozích zpráv

Testování příchozích zpráv by nyní mělo fungovat podobně, jako tomu bylo při použití samotného MAPI ve starších verzích Avastu pro Exchange (tzn. virus je ze zprávy smazán, resp. je ve zprávě vyléčen, do zprávy je vloženo upozornění pro příjemce, odesílateli je poslána výtka, v logovací složce Avastu je vytvořen záznam atd.), avšak nyní spolehlivěji.

Toho je docíleno tím, že v první fázi je zpráva předpřipravena procesem na úrovni AVAPI, který provede test jednotlivých příloh a najde-li v nich virus, přílohy přejmenuje a změní jejich obsah, aby byl pro příjemce bezpečný. V druhé fázi se pak dostane ke zprávě proces pracující na úrovni MAPI (k tomu dojde pouze v případě, že server není zcela vytížen) a ten provede dodatečné zpracování, jako léčení, posílání poplašných zpráv apod.

Z toho vyplývá, že i když je ke zprávě přiložen virus a server je zcela vytížen, uživatel je mimo nebezpečí, neboť krok 2 sice nebude proveden, krok 1 však ano.

AVAPI: Testování odchozích zpráv

Pro odchozí poštu je situace trochu jiná, neboť tam se proces na úrovni MAPI k testování zprávy nikdy nedostane. Tam se tedy vždy provede pouze krok 1 (testování na úrovni AVAPI) a zpráva je ponechána v „polohotovém“ stavu. Konkrétně to vypadá zpravidla tak, že místo zavirovaného souboru je odeslán soubor s dočasným názvem typu „___Avast disinfected file__PLEASE IGNORE!.dat“, který ovšem již virus neobsahuje - jeho otevření je pro příjemce bezpečné (obsahuje pouze jistá binární data). Podstatné je, že uživatel se nemůže nakazit.

V případě odesílané infikované pošty též nejsou rozesílány poplašné zprávy (ty zajišťuje výhradně proces na úrovni MAPI). Ve skutečnosti však toto tvrzení neplatí zcela absolutně, neboť po odeslání se obvykle kopie zprávy ukládá do složky „Odeslaná pošta“, kde ji zachytí/odviruje jak proces AVAPI, tak i MAPI. Poplachy tedy vlastně rozeslány budou, ale nebudou se týkat samotné odeslané zprávy, nýbrž její kopie, která se ukládá do poštovní schránky uživatele pro archivní účely.

5.2 Blokování příloh podle jmen

Jako nová vlastnost byla v souvislosti s používáním AVAPI do Avastu pro MS Exchange přidána možnost blokování (=odstraňování) příloh ze zpráv podle jejich jmen. Tato vlastnost může být užitečná při propuknutí rozsáhlé virové infekce, kdy je potřeba opravdu účinně a co nejdříve zasáhnout. K nezaplacení pak může tato volba být v případě rychlého rozšíření nového viru, který zatím není obsažen ve virové databázi.

Filozofie této vlastnosti vychází z toho, že e-mailem šířené viry a červy jsou zpravidla přikládány ke zprávám jako přílohy se známými, pevnými jmény. Tak např. první verze viru *I Love You* byla šířena jako příloha se jménem *Love letter for you.txt.vbs*. Přestože většina antivirových firem reagovala na tento virus relativně svižně, závratná rychlost jeho šíření stejně způsobila, že aktualizovaná virová databáze se v mnoha případech nedostala k zákazníkovi včas. Přitom by vlastně bývalo stačilo, kdyby se všechny doručené přílohy se jménem *Love letter for you.txt.vbs* prostě ze zpráv odstraňovaly, a virus by se do organizace vůbec nedostal.

Jde tedy o to, že v případech bezprostředního ohrožení můžeme připustit odstraňování souborů nikoliv podle jejich *obsahu*, nýbrž podle pouhého *jména*.

Jelikož však jde o poměrně triviální způsob „detekce“ virů, doporučujeme možnosti blokování užívat buďto pouze v případě akutního nebezpečí, nebo jen pro soubory s notoricky známými jmény (jako např. zmiňovaný Love Letter).

Jak nastavit blokování příloh zpráv podle jmen

Nastavení blokování příloh podle jmen se v Avastu provádí pomocí voleb v systémovém registru. Pro editaci důrazně doporučujeme použít program RegEdt32.exe namísto implicitního RegEdit.exe, protože umožňuje korektní práci s hodnotami typu REG_MULTI_SZ (pole textových řetězců), které Avast používá.

Všechny hodnoty v registrech, týkající se blokování, jsou ve složce

`HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\AvExSvc\Parameters.`

Konkrétně jsou definovány následující hodnoty:

- *BlockEnable* (typ REG_DWORD) - přepínač zapnutí/vypnutí blokování. Hodnota 1 znamená, že blokování je zapnuto, 0 vypnuto.
- *BlockFileNames* (typ REG_MULTI_SZ) - pole textových řetězců, z nichž každý specifikuje jednu masku jména přílohy, která se má ze zpráv odstraňovat. Při specifikaci můžete plně využívat zástupné znaky ? (náhrada jednoho znaku) a * (náhrada libovolného počtu znaků). Hodnota je efektivní pouze v případě, že *BlockEnable*=1.
- *BlockReplaceFileName* (typ REG_SZ) - udává jméno souboru, kterým bude původní (blokovaný) soubor (tj. ten, který vyhovuje alespoň jedné masce v poli *BlockFileNames*) nahrazen. Ve specifikaci můžete použít též symbol „%s“ (bez uvozovek), který bude Avastem za běhu nahrazen jménem původního souboru (např. při specifikaci `_Deleted_%s.txt` a původním jménu souboru `Happy99.exe` bude jméno náhrady `_Deleted_Happy99.exe.txt`).
- *BlockReplaceFileContents* (typ REG_MULTI_SZ) - určuje obsah souboru, kterým budou blokované soubory nahrazeny. Každý řetězec v *BlockReplaceFileContents* bude do souboru zapsán jako jedna řádka. Jako obsah je např. vhodné uvést upozornění, že původní soubor byl odstraněn, protože bezpečnostní politika serveru neumožňuje jeho doručení.

Poznámka: Změny v registrech budou uvedeny v platnost okamžitě po jejich uložení. Není potřeba restartovat žádný program nebo službu. Dále, funkčnost blokování je nezávislá na aktuálním stavu služby Avast for MS Exchange nebo poskytovatele Exchange Server. Měla by pracovat vždy, je-li nastaveno *BlockEnable*=1 (jedinou podmínkou je samozřejmě přítomnost Exchange Serveru 5.5 SP3 nebo vyšší, jinak není AVAPI vůbec k dispozici).

Poznámka: Protože pro administrátora je poměrně obtížné udržovat seznam jmen nebezpečných příloh, bude ALWIL Software v případě bezprostředních nebezpečí poskytovat .reg soubor, pomocí nějž můžete nastavit hodnotu *BlockFileNames* tak, aby byl Avast schopen infiltrovat i ty nejnovější viry.

5.3 Vypnutí používání AVAPI

Pokud potřebujete používání AVAPI vypnout, můžete tak učinit. K tomu slouží hodnota *Enabled* ve složce

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MSEExchangeIS\VirusScan

v systémovém registru. Nastavení této hodnoty na nulu znamená, že rozhraní AVAPI se nebude používat (Avast se tedy bude chovat jako v případě nasazení na Exchange 5.5 SP2 nebo nižší).

Přestože tato složka obsahuje i řadu dalších hodnot, nedoporučuje se je měnit, neboť jejich nesprávné nastavení může vést k chybné funkčnosti systému.

Změna v nastavení by se měla projevit zhruba do jedné minuty.

Upozornění: Vypnutí používání rozhraní se AVAPI se obecně příliš nedoporučuje, neboť Avast tím ztrácí jak možnost dokonalejšího testování příchozí i odchozí pošty, tak i schopnost blokování příloh podle jmen, užitečného při útoku nového, neznámého viru.

6 Signatury

Přestože proces hledání virů je poměrně rychlý (samozřejmě v závislosti na daném souboru), zátěž, která může být antivirovým programem na server naložena, nemusí být obecně nijak malá. Je-li na serveru běžný velký provoz, může časová náročnost na testování virů dokonce značně přesáhnout možnosti serveru, což nevěstí nic dobrého.

Avast32, Exchange Server Edition se snaží v největší možné míře takovým konfliktním situacím předcházet. Jednak jeho chování je spíše defenzivní, tj. nikdy se nesnaží pro sebe získat nějaký strojový čas „navíc“ na úkor samotného MS Exchange Serveru (více o tom viz administrátorská kapitola Systémové požadavky podruhé), jednak implementuje tzv. signatury.

6.1 Co jsou to signatury?

Signatury si lze představit jako malé nálepky, které Avast lepí (je-li to konfigurací úlohy umožněno) na jednotlivé nezavirované zprávy v poštovních schránkách a veřejných složkách na serveru. Na těchto nálepkách jsou podrobné údaje o jednotlivých souborech, které jsou ve zprávě přiloženy, včetně jejich velikosti, jména, stavu atp.

Najde-li tedy Avast při své práci zprávu, která obsahuje signaturu, jejíž obsah přesně odpovídá údajům sestaveným ze souborů přiložených ke zprávě samotné, je vysoce pravděpodobné, že zpráva (respektivně soubory k ní přiložené) nebyla od poslední kontroly Avastem změněna, a není tedy nutno tuto zprávu znovu prohlížet.

Tímto způsobem je tedy teoreticky možno předejít značnému množství „zbytečného“ testování.

6.2 Pravidla pro používání signatur

Z výše uvedeného plyne, že signatury mohou být mocným nástrojem pro minimalizaci zátěže na server. Zvláště v prostředích, kde je server využíván primárně pro práci na vývěskách (zprávách umístěných ve veřejných složkách) může používání signatur radikálním způsobem zkrátit dobu, kterou bude virová kontrola vyžadovat.

Naproti tomu v prostředí, kde server slouží v podstatě pouze jako odesílatel/příjemce elektronické pošty z/do firemní sítě, nebude efektivita používání signatur příliš vysoká, protože zprávy pochopitelně přicházejí nesignované a je tedy stejně nutné, aby je Avast prohlížel po jejich příchodu vždy celé.

Následuje výčet některých vlastností signatur.

- Jednotlivé signatury jsou šifrovány. Tím je do značné míry zamezeno tomu, aby nějaký pirát propašoval do vaší sítě zavirovanou zprávu již obohacenou platnou signaturou.
- Velikost signatury je opravdu malá - u většiny zpráv nepřesahuje 100 bajtů. To znamená, že i v případě značného množství signovaných zpráv (řekněme desítky až stovky tisíc) se celková velikost příliš nezvýší.

- Signatury jsou vkládány pouze do zpráv, které obsahují alespoň jeden příložený soubor; zprávy bez příloh totiž nemohou obsahovat žádné viry a jsou tedy Avastem obecně ignorovány.
- Práce se signaturami je velice rychlá - nemusíte se obávat, že by Avast zbytečně zaměstnávala, na úkor „užitečnější“ práce.
- Používání signatur se nedoporučuje pouze v případě, že si nemůžete dovolit podstupovat jakákoli rizika. Přestože je to velice nepravděpodobné (ze statistického hlediska téměř vyloučené), může se přece jenom stát, že Avast sice shledá signaturu za platnou, ale ve skutečnosti ve zprávě bude virus (který je Avast normálně schopen detekovat). Tato možnost je však, jak už bylo několikrát řečeno, spíše teoretická.
- Samotná akce signování zprávy je Avastem prováděna v momentě, kdy by za normálních okolností mělo dojít (nebo skutečně došlo) k testování souborů příložených k této zprávě. To je zpravidla v čase ukládání zprávy na serverový disk (do informační databáze). To souvisí s jednou nevýhodou používání signatur, která je uvedena v následující kapitole.

6.3 Nevýhody signování zpráv

Dosud jsme se zmínili hlavně o výhodách signatur. Jaké jsou však jejich nevýhody?

Kromě mírného vzrůstu potřebného prostoru (což v naprosté většině případů nevádí) je zde jeden závažnější problém, který poněkud hlouběji souvisí se způsobem, jakým klienti MS Exchange Serveru otevírají zprávy.

Představte si, že editujete zprávu umístěnou někde ve veřejné složce na serveru. Protože jste důkladní a máte špatné zkušenosti s výpadky proudu, zprávu ukládáte, i když na ní ještě nepřestáváte pracovat (tj. nezavíráte ji). Co se však stane při ukládání: zpráva se uloží, a kontrolu převezme Avast. Ten zprávu shledá čistou, a protože to má nastaveno, pokusí se přiložit k ní signaturu. Tím ji však mírně pozmění (chápeme-li jednu zprávu jako celek, nedělitelnou entitu), což se samozřejmě v té chvíli nedozví Váš klient, který má zprávu stále otevřenou. Při příštím ukládání však klient zjistí, že zpráva byla mezitím „pozměněna“ (právě tím, že k ní přibyla ona signatura), což zpravidla interpretuje tak, že došlo ke konfliktnímu editování dvěma klienty najednou a nahlásí příslušnou chybu uživateli (a zpravidla ještě původní zprávu přibalí k nové verzi, a obě zprávy okamžitě zavře).

Toto chování je samozřejmě nepřijatelné. Proto bylo nutno zajistit, aby k němu nedocházelo. Proto byli tvůrci programu nuceni sáhnout po řešení (alespoň částečném): signatury ve *veřejných složkách* jsou lepeny pouze na vytvářené (tj. nové) zprávy, narozdíl od editovaných (tj. jen měněných) zpráv. Toto chování se může změnit v budoucích verzích systému *Avast32, Exchange Server Edition*, kde již bude, doufejme, tento problém řešen bez újmy na funkčnosti.

7 Zprávy a protokoly

V této kapitole si povíme něco o zprávách, které *Avast32, Exchange Server Edition* posílá při případné infekci, a také o speciálním logu, kam se ukládají nejen záznamy o nalezených virech, ale též samotné infikované soubory. Tyto poplašné zprávy jsou velmi podstatné, protože dávají srozumitelnou formou najevo, že byla nalezena infikovaná pošta, a umožňují tak efektivně podchytit nebezpečí v jeho raném stádiu a předejít většině nepříjemností spjatých se zamořením podnikové sítě počítačovými viry.

Protože *Avast32, Exchange Server Edition* je vlastně pouze klientem systému *Avast32 3.0*, je samozřejmě automaticky možné zvolit široké spektrum poplašných událostí, které se mají Avastem při detekované infekci provést; více o tom viz manuál nebo nápověda běžného Avastu.

Akce, o kterých pojednává tato kapitola, jsou však nad rámcem těchto implicitních akcí, poskytovaných každému klientu systému *Avast32 3.0* automaticky. Tyto nové akce jsou k dispozici pouze ve vydání pro Exchange Server, a to zejména proto, že tato verze je určena na servery, kde je důkladné posílání poplašných zpráv a správné zapisování do logů nadmíru důležité.

7.1 Základní charakteristika posílaných zpráv

Pokud Avast nalezne virus v poštovní zprávě, může rozeslat poplašnou zprávu třem skupinám lidí:

- **Původnímu příjemci.** Je logické, že je-li nalezen virus, je o této skutečnosti notifikován její příjemce. Do této poplašné zprávy, posílané Avastem, je zároveň automaticky vloženo i tělo zprávy původní, tj. příjemce má možnost přechíst všechny elementy původní zprávy, které byly Avastem shledány bezpečnými. Co se týče zavirovaných elementů, zde připadají v úvahu dvě možnosti: buďto je Avast schopen virus odstranit (a v tom případě infikovaný soubor nahradí vyčištěným), nebo ne (a potom je zavirovaný soubor ze zprávy jednoduše odstraněn).
- **Odesílateli zprávy.** Avast může rovněž posílat notifikaci odesílateli zprávy (tj. tomu, od koho virus pochází). Ten virus buďto poslal neúmyslně, a v tom případě jistě ocení, že jej Avast na tuto skutečnost upozorní, nebo úmyslně, a potom si může být tento záškodník alespoň jist, že jeho zlý úmysl nedošel zdárného konce.
- **Administrátorovi nebo komukoli jinému.** Kromě zmiňovaných dvou skupin lidí je Avast schopen ještě rozesílat poplašné zprávy na jakoukoli jinou adresu. Je plně v rukou správce, aby určil a nastavil, komu všemu se budou tyto zprávy v případě detekovaného viru zasílat.

7.2 Formát posílaných zpráv

Jak bylo již uvedeno v kapitole o nastavování konfigurace, formát poplašných zpráv lze v Avastu měnit. To se může hodit zejména v případě, kdy standardní obsah zpráv, dodávaný s Avastem, z nějakého důvodu nevyhovuje.

Základní pravidla pro posílání poplašných zpráv jsou následující:

- Tři různé typy zpráv, o kterých bylo pojednááno v minulé kapitole, lze konfigurovat samostatně. To je rozumné, protože zpráva posílaná např. původnímu příjemci bývá zpravidla jiná než ta, která je zasílaná administrátorovi.
- Za tělo vámi konfigurované zprávy pro *příjemce* Avast automaticky připojí tělo zprávy původní. Proto bývá výhodné uvést do formátu této zprávy nějaký oddělovač.
- Ve všech zprávách lze používat rozšířené editační prostředky, jako např. změnu barev a fontů, zhruba v rozsahu standardu RTF. Mimo to lze do zprávy ukládat speciální šablony, které jsou rozvinuty (nahrazeny) až za běhu podle údajů z infikované zprávy, resp. souboru.

Následuje podrobný popis jednotlivých šablon:

Jednoduché šablony - pomocí těchto šablon se specifikují jednoduché (tj. nesložené) hodnoty.

- **%FROM%** - jméno (příp. adresa) odesílatele původní (zavirované) zprávy.
- **%TO%** - jméno (příp. adresa) příjemce (nebo příjemců, bylo-li jich víc) původní (zavirované) zprávy.
- **%SUBJECT%** - téma (neboli předmět) původní (zavirované) zprávy.
- **%SUBMITTED%** - datum a čas odeslání původní (zavirované) zprávy.
- **%LOCATION%** - Místo (poloha na serveru), kde byla zavirovaná zpráva nalezena. Byla-li tato zpráva nalezena na více místech, je uvedeno pouze první takové.
- **%NEWLINE%** - jednoduché zalomení řádku.
- **%TAB%** - jednoduchý tabelátor (posun o kousek vpravo).

Složené šablony slouží ke specifikaci složených hodnot, typicky údajů o zavirovaných souborech.

- **%ATTACH%** - Seznam zavirovaných souborů, nalezených v dané zprávě.
- **%ATTACHSeparátor%** - rozšířená forma seznamu zavirovaných souborů. Oproti prvnímu způsobu umožňuje nastavit separátor (tzn. oddělovací znak nebo znaky) mezi jednotlivými soubory. Zde lze s výhodou využít šablon **%NEWLINE%** a **%TAB%**, uvedených v paragrafu Jednoduché šablony.

Doplňkové šablony slouží k dalšímu upřesnění zapisovaných údajů. Šablona **%ATTACH%** (či její rozšířená verze **%ATTACHSeparátor%**) zapisuje informace o každém napadeném souboru ve tvaru

jméno_souboru (*jméno_viru*) [*status*]

kde *status* je akce, která byla se souborem vykonána (buďto smazán nebo odvírován). Pomocí doplňkových šablon můžete blíže specifikovat slovo, které bude doplněno za daný status při rozvíjení složených šablon. Jsou definovány tyto doplňkové šablony:

- **%DELETED= Slovo%**, kde parametr **Slovo** definuje právě slovo, které bude vloženo k zápisu o zavirovaném souboru, byl-li Avastem *odstraněn*. Není-li tato šablona uvedena, použije Avast anglické „Deleted“.
- **%CLEANED= Slovo%**, kde parametr **Slovo** definuje slovo, které bude vloženo k zápisu o zavirovaném souboru, byl-li Avastem *vyčištěn* (zbaven virů). Není-li tato šablona uvedena, použije Avast anglické „Cleaned“.

Po jejich použití jsou doplňkové šablony ze zasílané zprávy Avastem vymazány (ve výsledné, plně rozvinuté zprávě tedy nejsou nikdy obsaženy). To také znamená, že jejich umístění může být kdekoli v těle zprávy (i když zpravidla bývá zvykem je umísťovat na konec).

7.3 Logovací složka Avastu

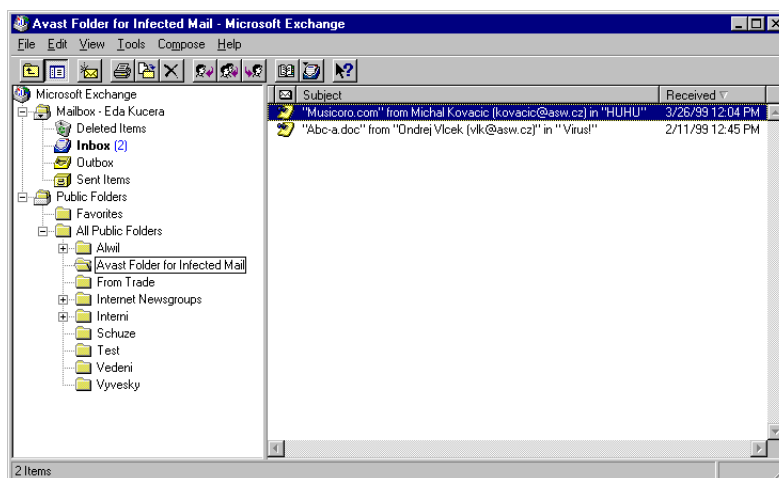
Avast32, Exchange Server Edition je v případě zavirované zprávy schopen nejen tuto zprávu vyčistit, ale zapsat o této události též speciální zprávu do svého logu. Nejde však pouze o zapsání zprávy (funkčnost samotného logování, tj. zapisování v případě, že se něco děje, je samozřejmá a je mimo jiné automaticky přístupná každému klientu jádra Avast32).

Log Avastu pro Exchange Server je poněkud bohatší. Při svém prvním spuštění si Avast vytvoří na Exchange Serveru vlastní složku (v kořenovém adresáři veřejných složek), implicitně pojmenovanou „Avast Infected (<jméno_serveru>)“. Do této složky pak v průběhu své práce průběžně zapisuje údaje o nalezených zavirovaných zprávách.

Formát těchto zpráv lze, stejně jako v případě poplašných zpráv, libovolně měnit z konfiguračního prostředí programu, a v těchto zprávách lze též používat všechny šablony, jak byly uvedeny dříve. Pokud není aktivní modul AVAPI, budou do logu vloženy i *původní (zavirované) soubory!*

Složka Avastu může tedy sloužit jako jakési úložiště pro nalezené viry (bohužel pouze v případě, že není aktivní testování na úrovni AVAPI, protože jinak AVAPI modul okamžitě infikované soubory ze zprávy zase odstraní). Vzhledem k tomu, že zavirované soubory lze z této složky i normálním způsobem extrahovat a dále s nimi na disku manipulovat, je jistě nutné nabádat na maximální opatrnost při takovéto, relativně nebezpečné, činnosti. Rozhodně by neměla být umožněna uživatelům - neadministrátorům. To lze zajistit např. tak, že *k danému adresáři umožníme přístup pouze úzké skupince lidí*. Rovněž nelze než doporučit, aby tento adresář byl nastaven v administračním programu Exchange Serveru jako „neviditelný“.

Zprávy v logovací složce Avastu tedy lze, pokud na to máte příslušná práva, prohlížet jako jakékoli jiné zprávy ve veřejných složkách na MS Exchange Serveru. Pro pohodlnější práci se administrátorovi doporučuje, aby si ve svém klientském programu (tj. programu, prostřednictvím kterého přistupuje ke zprávám na serveru) poněkud pozměnil standardní nastavení vzhledu pro tento adresář. Výhodné bývá nastavit široké sloupce pro *předmět* a *datum/čas*, které nejlépe prozradí povahu obsahu, a zcela vyřadit sloupce *odesílatel* a *adresát*, jež jsou pro logovací zprávy irelevantní. Příklad pro standardní microsoftský klient, který je nedílnou součástí balíku MS Exchange Server, je na obrázku.



7.1 Příklad nastavení vzhledu logovací složky Avastu ve standardním microsoftském klientu

Ačkoli je logování standardně zapnuto, lze jej samozřejmě i zcela vypnout, jak o tom hovoří kapitola o nastavování konfigurace. Vypnutí logování může sloužit zejména jako časová optimalizace, neboť při rozsáhlejší nábaze může urychlit činnost systému.

Poznámka: Jméno logovací složky Avastu lze změnit. Pokud však chcete toto učinit, nestačí složku na serveru pouze přejmenovat, protože Avast se bude dál pokoušet zapisovat zprávy do složky s původním jménem (tj. pokud nebude existovat, tak si ji vytvoří a bude zapisovat do ní). Ke korektnímu přejmenování je tedy nutné Avast o této změně informovat. To lze provést pomocí nastavení v INI souboru Avast32.ini, který je umístěn v adresáři \Avast32\Data (na serveru). V sekci [Exchange Server] se nalézá položka LogFolder=, za níž následuje právě jméno složky, do které Avast zapisuje logovací zprávy. Změna se projeví po restartu služby Avastu.

8 Pro administrátory

Tato kapitola popisuje některé pokročilejší partie používání systému *Avast32, Exchange Server Edition*. Jelikož je určena administrátorům, od čtenáře se předpokládají poněkud hlubší znalosti problematiky než u předešlých kapitol.

8.1 Systémové požadavky podruhé

Přestože hned v úvodu byly zhruba specifikovány požadavky na systém, které by měly být splněny pro úspěšné provozování Avastu, je třeba je nyní určitým způsobem rozebrat a upřesnit.

Rozhodující roli nesporně hrají dva faktory: velikost operační paměti a vytížení serveru. Podívejme se na oba podrobněji:

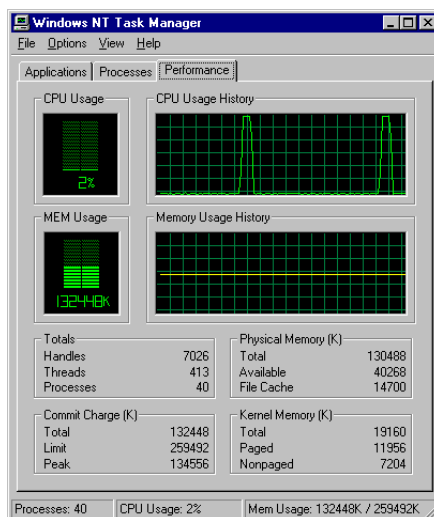
- **Velikost operační paměti.** Systém *Avast32, Exchange Server Edition*, je na paměť relativně dosti náročnou aplikací. To lze částečně ospravedlnit tím, že ceny RAM se již dlouhou dobu drží velmi nízko a nebývá výjimkou, že větší poštovní servery mívají 256, 512, nebo i více MB operační paměti, aniž by ji zpravidla nějak výrazněji využívaly. Jaké jsou tedy požadavky Avastu? Jak už to bývá, tato čísla se opět odvíjejí od kapacity serveru. Horní odhad vyžadované paměti lze získat z formule $2MB + (5KB \text{ krát počet poštovních schránek nebo veřejných složek})$. Má-li tedy Váš server například 5000 poštovních schránek, je třeba zajistit, aby Avast měl k dispozici 27MB volné operační paměti. Samozřejmě, není-li fyzická RAM k dispozici, program se pravděpodobně spustí i tak, ale paměť bude muset být alokována z odkládacího souboru na pevném disku, a tím se může rychlost činnosti celého systému dramaticky snížit.
- **Vytížení serveru.** Otázka vytížení serveru je obecně velice složitá. Existují o ní celé knihy, ve kterých se polemizuje, jaké je optimální využití serveru, aby ještě nebyl přetížen, a hledají se alternativní metody jak přetížení serveru předcházet. Stav přetížení může totiž zásadním způsobem negativně ovlivnit jeho funkčnost. Od administrátora většího serveru se předpokládá, že je s těmito věcmi dobře obeznámen a že dbá na to, aby vytížení jeho serveru bylo pod nějakou únosnou hranicí (k monitorování zátěže lze použít více programů, z nichž dva jsou dokonce ve standardní dodávce Windows NT - Performance Monitor a samozřejmě jednoduchý Správce úloh). Rozhodně nelze doporučit stav, kdy vytížení serveru konstantně přesahuje 80-90%. Jak s otázkou vytížení souvisí Avast? Faktem je, že Avast se při práci chová velice neinvazivně: jeho výkonný kód neběží s nějakou zvlášť vysokou prioritou a zjednodušeně lze říci, že „Avast svou práci dělá, až když je na ni čas“ (rozuměj až když procesor není příliš vytížen). To je velice podstatný moment, protože je třeba si uvědomit, že pakliže je server vytížen neustále, nemusí tento čas být takřka nikdy a účinnost systému rapidně klesá. Proč byl zvolen tento neinvazivní postup? Odpověď je jednoduchá - celý MS Exchange Server je ve své podstatě navržen jako asynchronní a jakékoli zanášení synchronnosti do něj by mohlo zásadním způsobem ohrozit jeho stabilitu. Všechny operace jsou tedy vykonávány asynchronně, a je tedy jen a jen na systému, kdy Avastu přidělí čas na to, aby dělal svou práci (tj. hledal ve zprávách viry).

8.2 Více o obnovování seznamu schránek

Již víme, pomocí nastavení na poslední stránce konfigurace poskytovatele „Exchange® Server“ při editaci úlohy se dá nastavit, jak často Avast aktualizuje svůj interní seznam spravovaných poštovních schránek. Vysvětleme si, co to přesně znamená a jaké důsledky má to které nastavení této hodnoty.

Pro to, aby mohl Avast hlídat obsah pošty v poštovní schránce, musí ji nejprve otevřít. K tomu, aby ji mohl otevřít, musí vědět, že existuje. Při spouštění si služba Avastu vytváří interní seznam všech schránek na serveru. Dokud tedy není žádná schránka přidána, Avast hlídá všechny (samozřejmě podle konfigurace oblastí, které se mají hlídat, ale to není podstatné; podstatné je, že *může* hlídat všechny). Problém však nastane, když někdo (zpravidla administrátor) vytvoří novou schránku. Bohužel, MS Exchange Server nedává aplikacím žádnou příležitost se tuto skutečnost dozvědět. Kdyby tomu tak bylo, bylo by vše jednoduché - Avast by při přidání nové schránky tuto jednoduše otevřel a začal monitorovat i ji. Protože tomu tak ale není, je nutné, aby Avast periodicky (v nějakých časových intervalech) obnovoval tento svůj seznam schránek, a byl tak schopen zpracovat potenciální změny, které v tomto seznamu nastaly (tj. např. nové schránky). A délka tohoto intervalu je přesně to číslo, které se nastavuje ve zmiňovaném konfiguračním okně.

Možná si říkáte: proč se takovou „prkotinou“ vůbec zabývat? Odpověď je nasnadě - vybudování seznamu schránek je operace, která na dobu několika vteřin (většinou 3-10, podle rychlosti počítače a kapacity serveru) zcela (na 100%) zahltí procesor (obr. 8.1). Bylo by samozřejmě krásné a pohodlné, kdyby Avast mohl svůj interní seznam aktualizovat každou chvíli (řekněme každých 20 sekund). Avšak v důsledku toho, že tato operace je tak náročná by bylo takové časté obnovování značně nehospodárné. Proto je umožněno, aby si administrátor sám mohl nastavit interval, který mu nejvíce vyhovuje.



8.1 Zahlcení procesoru aktualizací seznamu poštovních schránek

Je zřejmé, že na téměř stacionárních serverech, na kterých nikdy (nebo skoro nikdy) žádné schránky nepřibývají, nemá smysl specifikovat příliš nízkou hodnotu. Přesto se však doporučuje aktualizaci občas automaticky provádět. Jako rozumné v tomto případě se jeví hodnoty jako 24 nebo 48 hodin (při konfiguraci se zadávají tyto hodnoty v minutách, tj. 1440, resp. 2880 minut).

Existují však servery, na kterých se uživatelské schránky mění poměrně často, a to mnohdy

i automaticky (tj. potom není možné, aby administrátor po každém přidání schránek alespoň manuálně vynutil okamžitou aktualizaci seznamu pomocí tlačítka v konfiguračním okně). Hraje-li bezpečnost vysokou roli, je v tomto případě nutno nastavit dobu obměňování na nízkou hodnotu, typicky 10 - 20 minut.

Implicitní nastavení, 180 minut, je jakýmsi kompromisem. Mělo by dobře posloužit pro většinu průměrně velkých serverů. Přesto však, pokud se však Váš server blíží spíše k stacionárnímu stavu (jak byl definován výše), nelze než doporučit, abyste tuto hodnotu poněkud zvýšili (a předešli tak častějšímu vytížení serveru).

Poznámka: Aktualizace interního seznamu se netýká veřejných složek na serveru, a rovněž tak složek uvnitř jednotlivých poštovních schránek. Detekce nových složek se provádí zcela jiným způsobem a je zajišťováno zcela automaticky.

8.3 Používání Internet Newsgroups společně s Avastem

Avast nepodporuje práci s Internet Newsgroups (tj. rezidentně nehlídá viry ve složce s news). Odebíráte-li pomocí Vašeho Exchange Serveru news, musíte zajistit, aby Avast věděl o správném názvu složky, do kterého se tyto zprávy stahují. Po instalaci Exchange Serveru je pro tento účel vytvořena složka pojmenovaná Internet Newsgroups v kořenovém adresáři veřejných složek. Pokud jste název této složky změnili (např. počestěním), musíte Avastu umožnit se o této změně dozvědět. Konkrétně musíte toto jméno správně nastavit v souboru Avast32.ini, který je umístěn v adresáři \Avast32\Data (na serveru). V sekci [Exchange Server] se nalézá položka NewsFolder=, za níž by mělo následovat právě aktuální jméno složky, kterou používáte pro news. Implicitně se používá hodnota Internet Newsgroups (i v případě, že se položka NewsFolder= v souboru vůbec nevyskytuje). Případná změna se projeví až po restartu služby Avastu, který se doporučuje v tomto případě provést co nejdříve. Zůstalo-li jméno složky s news od instalace serveru nezměněno, není potřeba v Avastu nic nastavovat.

Všechny zprávy, které se ve složce s news objeví, budou z rezidentního skenování bezpodmínečně vyloučeny.

8.4 Problém se systémovým event logem

Microsoft Exchange Server je systém, který poměrně hojně využívání možnosti zapisovat do event logu. Přestože časté zápisy do event logu mohou leckdy pomoci administrátorům odhalit různé problémy, skýtají v sobě i potenciální problém v podobě přeplnění logu.

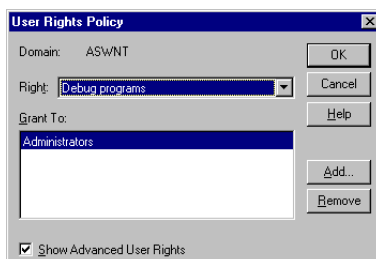
Zaplnění event logu lze předcházet více způsoby. Nejjednodušší, ale nikoli nejlepší, je prostě log nastavit tak, aby se starší zprávy přepisovaly novějšími. Tím však automaticky administrátor ztrácí schopnost logy uchovávat, protože je zde vždy nebezpečí, že některé „nečtené“ zprávy již byly přepsány novějšími.

Výhodnější metodou je rezervovat na harddisku pro log hodně místa (je-li to možné, klidně desítky megabajtů) a zprávy periodicky uchovávat a mazat ručně. Tím se zaručí, že se nikdy nesmažou nezaregistrované zprávy, avšak na úkor toho, že administrátor má více práce.

Co se týče množství zpráv, které do event logu zapisuje Avast, není třeba se za normálních okolností obávat přeplnění. Zprávy jsou zapisovány jen zřídka. Vyjimku však tvoří následující případ:

Pokud nemá uživatelský účet, pod kterým je MS Exchange Server (a tedy i Avast32, Exchange Server Edition) instalován, uděleno právo „Ladit programy“ (obr. 8.2), je

počet zpráv, zapisovaných Avastem do event logu, značný. Proto je nutné zajistit, aby zmiňovaný účet měl dané právo přiděleno! Toto přidělení je nutné provést na lokálním počítači (tj. na serveru, kde fyzicky běží MS Exchange Server) , nikoliv na doménovém kontroleru.



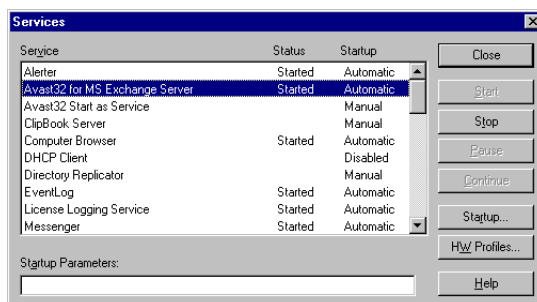
8.2 Uživatelské právo „Ladit programy“

Důvodem je skutečnost, že některé služby MS Exchange Serveru, často volané Avastem, samy zapisují do event logu. Avast má v sobě zabudovaný mechanismus, který tyto zprávy dokáže filtrovat, avšak tento mechanismus funguje právě jenom v případě, že je uděleno právo „Ladit programy“. Toto privilegium musí být přiděleno na lokálním počítači, protože Windows NT vyhodnocují bezpečnostní nastavení pro systémové služby právě z lokální (a ne z doménové) bezpečnostní databáze.

Při instalaci Windows NT je toto právo standardně přiděleno celé skupině Administrators, takže stačí zajistit, aby administrátorský účet Exchange Serveru byl obsažen v této skupině. Toto je samozřejmě zcela legitimní požadavek, který je v 99,9% případů vždy automaticky splněn (jednoduše řečeno, po administrátorském účtu pro Exchange se tedy požaduje, aby byl zároveň i administrátorským účtem pro počítač, na kterém Exchange běží).

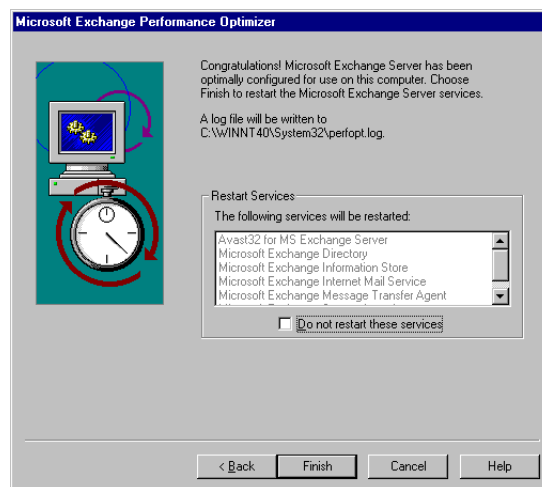
8.5 Služba Avastu

Jak již bylo několikrát zmíněno, jádro programu tvoří systémová služba. Tato služba se jmenuje „Avast32 for MS Exchange Server“ a je uložena v souboru AvExSrv.exe. Instalační program ji implicitně nastavuje tak, aby ji operační systém nahrával automaticky při každém spuštění počítače, podobně jako je tomu u služeb samotného MS Exchange Serveru.



8.3 Aplikace „Služby“ v Ovládacích panelech

Zvláštní péče je věnována tomu, aby bylo zajištěno, že služba Avastu je vždy nahrána až po službách Exchange Serveru, a naopak, pokud jsou služby Exchange Serveru vypínány, tak aby služba Avastu byla vypnuta ještě před nimi. Proto pokud se pokusíte manuálně spustit službu Avastu, budou nejprve aktivovány služby Exchange (což dává dobrý smysl, protože jinak by nemělo význam Avast startovat), a též při deaktivaci služeb Exchange se nejprve deaktivuje Avast. Např. aplikace Optimizer (obr. 8.4), která je standardní součástí balíku BackOffice, potřebuje pro svou činnost vypnout služby Exchange. Protože však služba Avastu je na nich závislá, musí Optimizer ukončit i ji, jak to ukazuje obrázek. Vše je zajištěno zcela transparentně. Po skončení své práce Optimizer (nebo jakýkoli jiný program, který manipuluje se službami Exchange Serveru) službu Avastu zase spustí.



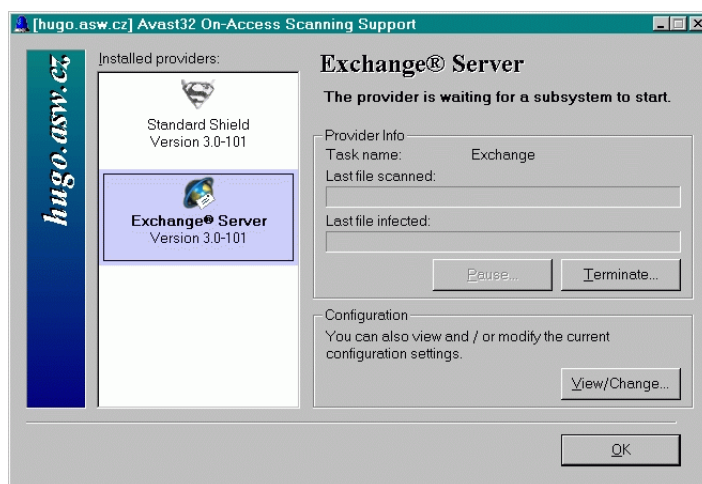
8.4 Program Optimizer zastaví i službu Avastu

Důležitou roli též hraje rychlost spuštění této služby. Hned zpočátku je třeba upozornit, že doba potřebná ke spuštění může být značná. Tato doba je přímo úměrná kapacitě serveru (tj. celkovému počtu poštovních schránek a veřejných složek, které jsou na serveru umístěny). Klíčovou roli hraje počet poštovních schránek (doba potřebná k inicializaci veřejných složek je proti ní zanedbatelná). Testy ukázaly, že na průměrném serveru (Pentium II 266 MHz, 128 MB RAM, SCSI) čas potřebný na inicializaci osciloval někde mezi 2 až 3 minutami na 500 schránek. To znamená, že uchová-li Váš server řekněme 5000 schránek, může tento čas dosahovat až půl hodiny! Tento údaj se může na první pohled zdát hrozivý, ale uvědomíte-li si, jak často server přestartováváte (v optimálním případě by k tomu nemělo docházet v podstatě nikdy), není to zase tak velký problém. V každém případě je ale nutné o této skutečnosti vědět.

Se startovacím časem úzce souvisí ještě jedna malá nepříjemnost, se kterou by měl být administrátor obeznámen. Tou je skutečnost, že status služby Avastu, který je uveden např. v ovládacích panelech v programu „Služby“, nepřiliš přesně odráží aktuální stav této služby. Důvodem je nepříjemný fakt, že systém Windows NT čeká na inicializaci každé služby maximálně 30 vteřin, a pokud tato nezmění do této doby svůj status na „běžící“, systém ji považuje za mrtvou a místo pokračování jejího natahování celý proces ukončí a nahlásí chybovou zprávu. Vzhledem k tomu, že čas potřebný k inicializaci služby Avastu může tento půlminutový interval značně přesáhnout (jak bylo uvedeno v minulém odstavci), byli její tvůrci nuceni sáhnout po alternativním řešení: po rychlé kontrole, že inicializace patrně dopadne úspěšně (tato kontrola nezabere víc než pár vteřin) je již status služby změněn na „běžící“, přestože služba v tom okamžiku ještě fakticky neběží. Pak je teprve dokončena samotná inicializace. Tím je zajištěno, že Windows NT jsou se službou

spokojeny (protože tato se rozběhla v povolené době), ale právě za cenu toho, že pole status nemusí přesně odrážet skutečnost.

Jak tedy zjistit přesný a pravdivý status služby Avastu? Je to docela jednoduché: stačí na serveru spustit libovolnou rezidentní úlohu, používající poskytovatele „Exchange® Server“ a poté zkontrolovat status tohoto poskytovatele. Kontrolu můžete učinit například vzdálenou rezidentní konzolí, kterou jednoduše vyvoláte odkudkoli ze sítě z kontextového menu počítače v rozšířeném ovládní Avastu. Pokud se objeví hláška, že poskytovatel čeká na spuštění podsystému, znamená to, že služba ještě nebyla zcela natažena (viz obr. (obr. 8.5)). Jestliže ale program nahlásí, že poskytovatel je aktivní, je to známkou toho, že inicializace služby proběhla úspěšně.

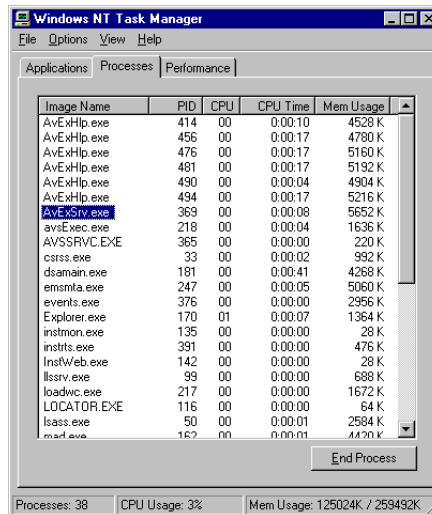


8.5 Služba není ještě natažena - poskytovatel čeká

Poslední upozornění o službě Avastu je následující: tato služba z technických důvodů při svém startu spouští další program z dodávky balíku *Avast32, Exchange Server Edition*, který se jmenuje „AvExHlp.exe“. Na tom není zase nic tak neobvyklého. Neobvyklé je, že nepouští jednu, ale často i více kopií tohoto programu. Počet těchto kopií je opět přímo úměrný kapacitě serveru. Zhruba lze říci, že je spuštěna 1 kopie programu AvExHlp.exe na každých 200 poštovních schránek nebo veřejných složek. To znamená, že pokud Váš server obsahuje řekněme 2000 schránek nebo složek, služba Avastu pustí deset kopií tohoto pomocného programu. Administrátorovi se tak např. při pohledu na systémového Správce úloh (obr. 8.6) může zdát něco podezřelého.

Služba Avastu (AvExSrv.exe) (obr. 8.6) může při své práci vyžadovat i větší množství kopií pomocného programu AvExHlp.exe. Dalšími součástmi Avastu jsou služby jeho jádra - avsSrv.exe a avsExec.exe

Znovu tedy upozorňujeme, že toto chování je zcela v pořádku a že vyplývá ze samotné architektury produktu *Avast32, Exchange Server Edition*.



8.6 Pohled na Správce úloh

8.6 Přesouvání testovaných zpráv

Protože Avast implicitně testuje zprávy až po jejich doručení do uživatelské poštovní schránky, je teoreticky možné, že si uživatel může (potenciálně zavirovanou) zprávu otevřít ještě před tím, než se Avastu podaří její testování dokončit. Aby se zamezilo těmto situacím, byla do Avastu přidána volba, že právě testované zprávy budou přesunuty do speciální (pro uživatele nepřístupné) složky, a po dokončení testování budou vráceny na své původní místo. Tím se výrazně snižuje možnost jejich otevření uživatelem ještě před otestováním.

Volba přesouvání testovaných zpráv je implicitně zapnuta. Může však způsobovat problémy s jistými klientskými programy, které spoléhají na notifikace o nových zprávách (a též s tzv. „pravidly“). V tom případě ji můžete vypnout, a to pomocí nastavení v INI souboru Avast32.ini, který je umístěn v adresáři \Avast32\Data (na serveru). V sekci [Exchange Server] se nalézá položka HidePendingMessages=, za níž by mělo následovat číslo 1 (zprávy budou přesouvány) nebo 0 (zprávy nebudou přesouvány).