



AVG Email Server Edice 2011

Uživatelský manuál

Verze dokumentace 2011.04 (21.4.2011)

Copyright AVG Technologies CZ, s.r.o. Všechna práva vyhrazena.
Všechny ostatní obchodní značky jsou majetkem jejich registrovaných vlastníků.

Tento produkt používá RSA Data Security, Inc. MD5 Message-Digest Algorithm, Copyright (C) 1991-2, RSA Data Security, Inc. Created 1991.

Tento produkt obsahuje kód knihovny C-SaCzech, Copyright (c) 1996-2001 Jaromír Doleček (dolecek@ics.muni.cz).

Tento produkt používá kompresní knihovnu zlib Copyright (C) 1995-1998 Jean-loup Gailly and Mark Adler.



Obsah

1. Úvod	4
2. Podmínky instalace	5
2.1 Podporované operační systémy	5
2.2 Podporované e-mail servery	5
2.3 Hardwarové požadavky	5
2.4 Odinstalujte předchozí verze	5
2.5 Servisní balíčky pro MS Exchange	6
3. Instalační proces AVG	7
3.1 Spuštění instalace	7
3.2 Aktivujte vaši licenci	8
3.3 Zvolte typ instalace	9
3.4 Uživatelská instalace - uživatelské volby	9
3.5 Dokončení instalace	11
4. Kontrola pošty pro MS Exchange Server 2007/2010	13
4.1 Přehled	13
4.2 Kontrola pošty pro MS Exchange (směrovací TA)	16
4.3 Kontrola pošty pro MS Exchange (SMTP TA)	17
4.4 Kontrola pošty pro MS Exchange (VSAPI)	18
4.5 Technické upozornění	20
4.6 Akce nad nálezy	21
4.7 Filtrování e-mailů	22
5. Kontrola pošty pro MS Exchange Server 2003	24
5.1 Přehled	24
5.2 Kontrola pošty pro MS Exchange (VSAPI)	27
5.3 Akce nad nálezy	30
5.4 Filtrování e-mailů	31
6. AVG pro Kerio MailServer	32
6.1 Konfigurace	32
6.1.1 Antivirus	32
6.1.2 Filtrování příloh	32
7. Nastavení komponenty Anti-Spam	36



7.1 Anti-Spam princip	36
7.2 Anti-Spam rozhraní	36
7.3 Anti-Spam nastavení	38
7.3.1 Průvodce trénováním Anti-Spam databáze	38
7.3.2 Výběr složky se zprávami	38
7.3.3 Způsob filtrování zpráv	38
7.4 Výkon	43
7.5 RBL	44
7.6 Whitelist	45
7.7 Blacklist	46
7.8 Pokročilé nastavení	47
8. Manažer nastavení AVG	48
9. FAQ a technická podpora	51



1. Úvod

Tento uživatelský manuál je kompletní dokumentací programu **AVG Email Server 2011**.

AVG Email Server 2011 je jedním z produktů nové řady oceňovaného bezpečnostního software AVG, jež byl navržen pro klid vaší duše a stoprocentní bezpečnost vašeho serveru. Stejně jako všechny produkty nové řady AVG byl i **AVG Email Server 2011** kompletně a od základů postaven tak, aby nadále dostal své pověsti uznávaného bezpečnostního programu a současně nabídl svým uživatelům zcela nové, efektivnější a uživatelsky přívětivé rozhraní.

Nový **AVG Email Server 2011** přináší moderní grafické rozhraní v kombinaci s agresivnějším a rychlejším testováním. Pro větší pohodlí přináší více procesů v plně automatickém režimu a nabízí nové 'inteligentní' uživatelské možnosti, které se přizpůsobí vašim potřebám.

Poznámka: Tato dokumentace obsahuje pouze popis specifických vlastností edice AVG Email Server 2011. Ostatní nastavení a vlastnosti aplikace AVG naleznete popsány v dokumentaci k Internet Security Edici, která je dostupná skrze <http://www.avg.cz>.



2. Podmínky instalace

2.1. Podporované operační systémy

AVG Email Server 2011 je určen k ochraně e-mail serverů s těmito operačními systémy:

- Windows 2008 Server (x64 a x86)
- Windows 2003 Server (x86, x64) SP1

2.2. Podporované e-mail servery

Podporovány jsou následující e-mail servery:

- MS Exchange Server 2003
- MS Exchange Server 2007
- MS Exchange Server 2010
- AVG pro Kerio MailServer – verze 6.7.2 a vyšší

2.3. Hardwarové požadavky

Minimální hardwarové požadavky pro **AVG Email Server 2011** jsou tyto:

- Intel Pentium CPU 1,5 GHz
- 500 MB volného místa na pevném disku (z instalací dříve)
- 512 MB RAM paměti

Doporučené hardwarové požadavky pro **AVG Email Server 2011** jsou tyto:

- Intel Pentium CPU 1,8 GHz
- 600 MB volného místa na pevném disku (z instalací dříve)
- 512 MB RAM paměti

2.4. Odinstalujte předchozí verze

Máte-li nainstalovanou starší verzi **AVG Email Serveru**, je nutné ji před zahájením instalace **AVG Email Server 2011** odinstalovat. Odinstalaci je třeba provést ručně pomocí standardních funkcí Windows:

- V nabídce **Start/Nastavení/Ovládací panel/Přidat nebo odebrat programy** zvolte příslušný program.



Poznámka: Vždyjte zvýšenou pozornost volbě správného AVG programu ze seznamu instalovaných programů! Nejprve musíte odinstalovat AVG Email Server Edici a teprve poté AVG File Server Edici.

- Po odinstalaci **AVG Email Server Edice** přistoupíte k odinstalaci předchozí verze **AVG File Server Edice**. Tuto akci provedete snadno z nabídky **Start/Programy/AVG/Odinstalovat AVG**.
- Pokud jste dříve používali verzi AVG 8.x či starší, nezapomenejte odinstalovat také jednotlivé serverové doplňky.

Poznámka: Při procesu odinstalace bude restartován proces store.

Doplňky pro Exchange - spusíte setupes.exe s parametrem /uninstall ze složky, kde je doplněk nainstalován:

např. C:\AVG4ES2K\setupes.exe /uninstall

Doplňky pro Lotus Domino/Notes - spusíte setupln.exe s parametrem /uninstall ze složky, kde je doplněk nainstalován:

např. C:\AVG4LN\setupln.exe /uninstall

2.5. Servisní balíčky pro MS Exchange

Pro instalaci **MS Exchange 2003 Serveru** není nutná instalace žádných dodatečných balíčků, ale v každém případě doporučujeme, abyste se snažili udržovat svůj systém v co možná nejaktuálnějším stavu a pravidelně instalovali nové servisní balíčky a záplaty, aby bylo dosaženo nejvyšší možné úrovně bezpečnosti.

Servisní balíček pro MS Exchange 2003 Server (instalace je volitelná) najdete na adrese:

<http://www.microsoft.com/exchange/evaluation/sp2/overview.mspx>

Při zahájení instalace budou prověřeny všechny verze systémových knihoven. Bude-li nutné doinstalovat novější knihovny, instalátor označí zastaralé knihovny koncovkou *.delete*. Takto označené knihovny pak budou odstraněny při restartu systému.

Servisní balíček pro MS Exchange 2007 Server (instalace je volitelná)

<http://www.microsoft.com/downloads/details.aspx?FamilyID=44c66ad6-f185-4a1d-a9ab-473c1188954c&displaylang=en>



3. Instalační proces AVG

Pro instalaci AVG na váš počítač budete aktuální instalační soubor. Instalační soubor najdete na CD, které bylo součástí zakoupeného balení AVG, ale tento soubor může již být zastaralý.

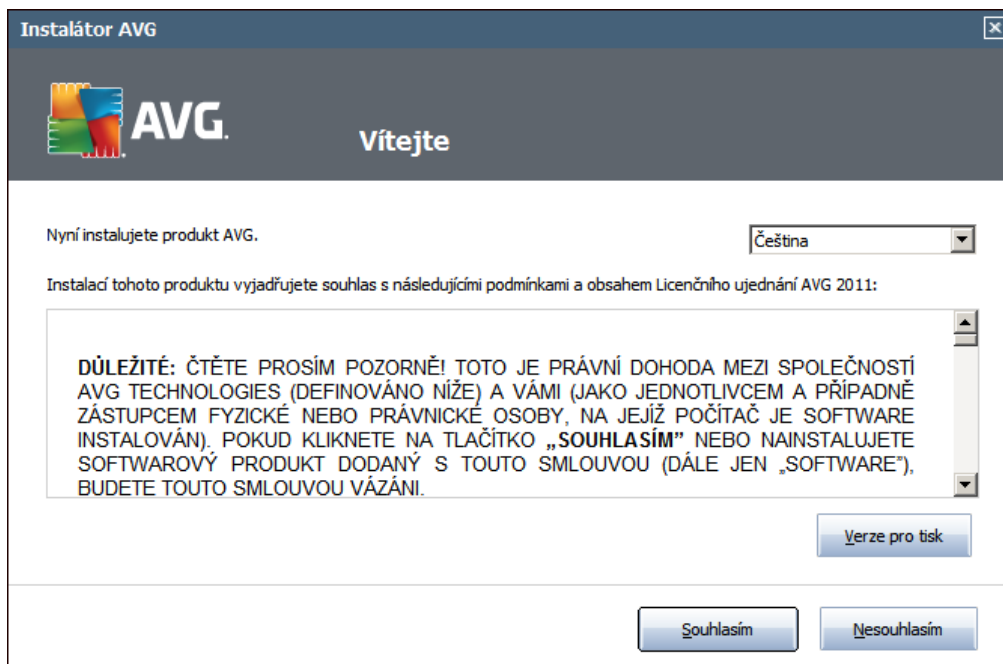
Doporučujeme vám proto navštívit [web AVG: http://www.avg.cz/stahnout?prd=msw](http://www.avg.cz/stahnout?prd=msw) a nejnovější instalační soubor si odtud stáhnout.

Poznámka: K dispozici jsou dva instalační balíčky - jeden pro 32bitové operační systémy (s označením x86) a jeden pro 64bitové operační systémy (s označením x64). Při instalaci je tedy třeba použít instalační balíček odpovídající vašemu operačnímu systému.

Během instalace budete požádáni o své licenční číslo. Ujistěte se proto prosím, že jej máte k dispozici. Pokud jste AVG zakoupili on-line, vaše licenční číslo vám bylo doručeno e-mailem.

Instalace probíhá ve sledu dialogových oken, z nichž každé vysvětluje, co je třeba v konkrétním kroku provést. Popis jednotlivých oken nyní nabízíme:

3.1. Spuštění instalace



Instalační proces je zahájen otevřením úvodního dialogu. V tomto dialogu máte možnost zvolit jazyk, v němž bude instalační proces probíhat. V horní části okna zvolte z rozbalovacího menu jazyk, v němž chcete komunikovat.

V dialogu se dále nachází Licenční ujednání - tedy plné znění závazné licenční smlouvy AVG. Text si přečtete a svůj souhlas s licenčním ujednáním potvrdíte stiskem tlačítka **Souhlasím**.

Tlačítkem **Verze pro tisk** můžete v novém okně zobrazit verzi určenou pro tisk.



Upozornění: Později v průběhu instalace si budete také moci zvolit další jazyky pro rozhraní aplikace.

3.2. Aktivujte vaši licenci

V dialogu **Aktivujte vaši licenci** je třeba vyplnit vaše licenční číslo. Toto číslo najdete buďto na registrační kartě v krabicovém balení AVG, anebo v potvrzovacím emailu, který jste obdrželi při zakoupení AVG on-line. Licenční číslo musí být zadáno naprosto přesně ve tvaru, jak je uvedeno, proto prosím věnujte velkou pozornost jeho písemu. Pokud máte číslo k dispozici v digitální formě, doporučujeme jej do příslušného pole zkopírovat (metodou kopírovat a vložit).

Instalátor AVG

Aktivujte vaši licenci

Licenční číslo:

Příklad: 9FULL-NSDRS-KUL4L-UKSFR-L96M9-B2ALT-XWMX3

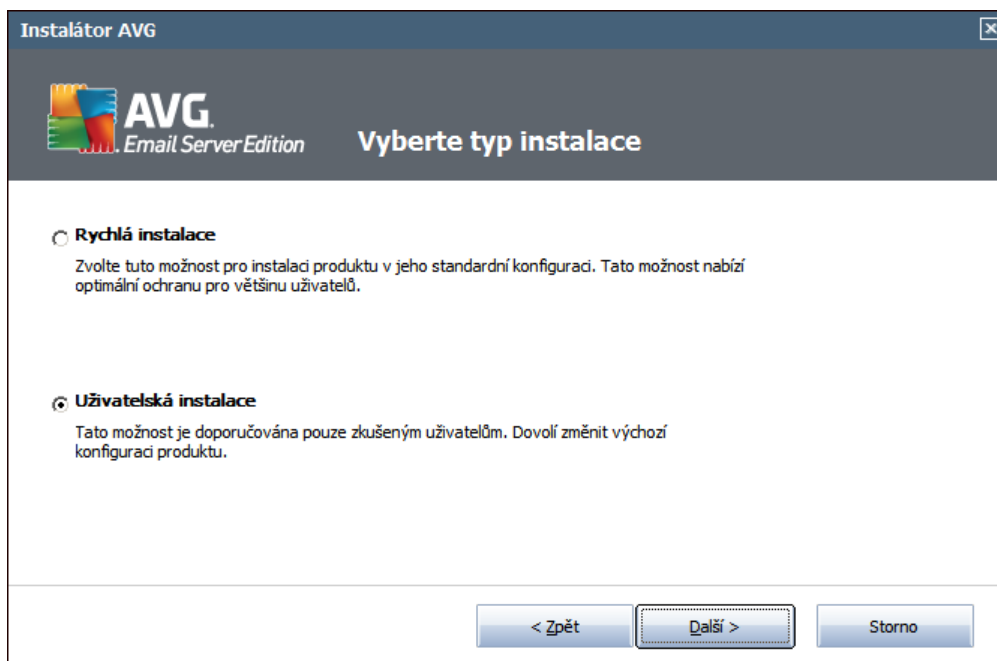
Pokud jste zakoupili produkt AVG 2011 on-line, bylo vám licenční číslo zasláno e-mailem. Abyste se vyhnuli chybám při jeho opisování, doporučujeme licenční číslo zkopírovat z e-mailu a vložit je sem.

Pokud jste zakoupili produkt v kamenné prodejně, naleznete licenční číslo v balení produktu na registrační kartě. Ujistěte se prosím, že číslo opišete z registrační karty správně.

< Zpět Další > Storno

V instalaci pokračujte stiskem tlačítka **Další**.

3.3. Zvolte typ instalace



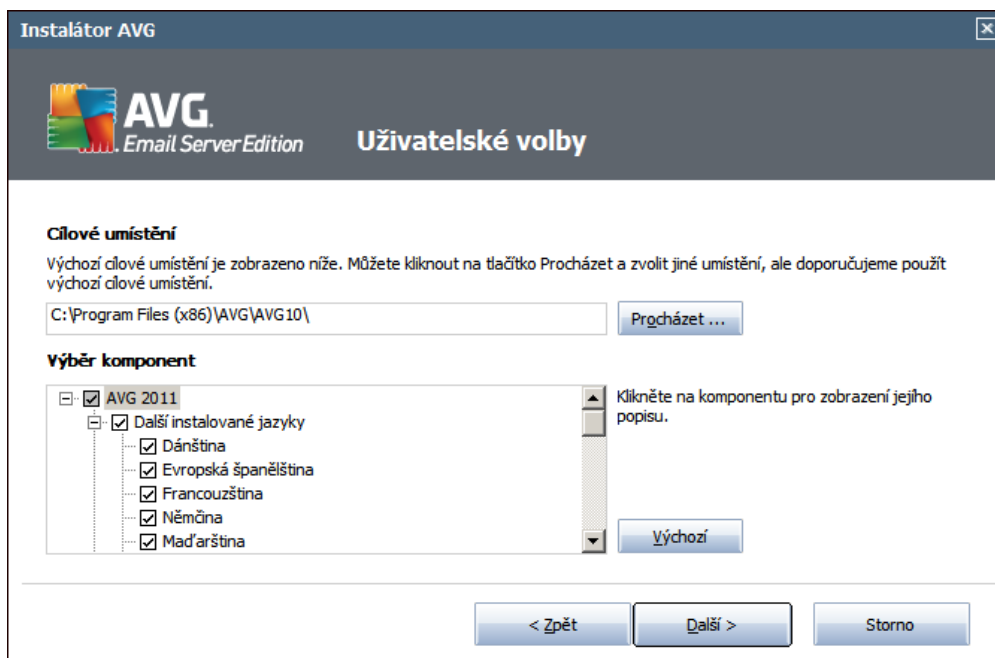
Dialog **Vyberte typ instalace** vám dává na výběr mezi **Rychlou** a **Uživatelskou** instalací.

Většinu uživatelů doporučujeme použít **rychlou instalaci**, kdy bude AVG nainstalován zcela automaticky s nastavením definovaným výrobcem. Toho nastavení zaručuje maximální úroveň bezpečnosti a optimální využití zdrojů. Pokud se v budoucnu vyskytnou potřeby, které konkrétní nastavení změní, budete mít vždy možnost editovat konfiguraci AVG přímo v aplikaci.

Uživatelská instalace je vhodná pouze pro pokročilé a znalé uživatele. Doporučujeme ji pouze v případě, že máte skutečnou potřebu instalovat AVG s nestandardním nastavením tak, aby vyhovovalo specifickým požadavkům vašeho systému.

3.4. Uživatelská instalace - uživatelské volby

V dialogu **Uživatelské volby** nejprve vyberte v sekci **Cílové umístění** kam má být program AVG nainstalován. Ve výchozím nastavení bude program instalován do adresáře programových souborů umístěném typicky na disku C:. Pokud si přejete toto umístění změnit, pomocí tlačítka **Procházet** zobrazíte strukturu vašeho disku a zvolíte adresář, kam má být AVG instalován.



V sekci **Výběr komponenty** je zobrazen přehled komponent AVG, které můžete nainstalovat. Pokud vám výchozí nastavení nevyhovuje, máte možnost jednotlivé komponenty odebrat/přidat.

Volit můžete pouze z těch komponent, které jsou zahrnuty ve vaší zakoupené licenci AVG. Pouze tyto komponenty vám také budou v dialogu nabídnuty!

- **Klient Vzdálené správy AVG** - pokud budete chtít tuto instalaci spravovat vzdáleně, zaškrtněte tuto volbu.
Poznámka: Pouze serverové komponenty z tohoto seznamu lze spravovat prostřednictvím Vzdálené správy!
- **Manažer nastavení** - nástroj určený zejména správcům sítí sloužící ke kopírování, úpravě a distribuci konfigurace AVG, kterou lze následně uložit například na přenosné médium a aplikovat znovu i jiným způsobem na vybrané stanice.
- **Další instalované jazyky** - zvolte si jazyky uživatelského rozhraní, které chcete nainstalovat.

Základní přehled jednotlivých serverových komponent (serverové doplňky):

- **Anti-Spam server pro MS Exchange**
Kontroluje všechny příchozí e-mailové zprávy a označuje nevyžádanou poštu jako SPAM. K analýze každé zprávy využívá několik metod, což zajišťuje maximální možnou ochranu proti nežádoucím zprávám.
- **Kontrola pošty pro MS Exchange (směrovací TA)**
Kontroluje všechny příchozí, odcházející a interní e-mailové zprávy procházející skrze HUB roli MS Exchange.



Dostupné pouze pro MS Exchange 2007/2010 a lze nainstalovat pouze na HUB roli.

- **Kontrola pošty pro MS Exchange (SMTP TA)**

Kontroluje e-mailové zprávy procházející skrze SMTP rozhraní MS Exchange.

Dostupné pouze pro MS Exchange 2007/2010 a lze nainstalovat na EDGE i HUB roli.

- **Kontrola pošty pro MS Exchange (VSAPI)**

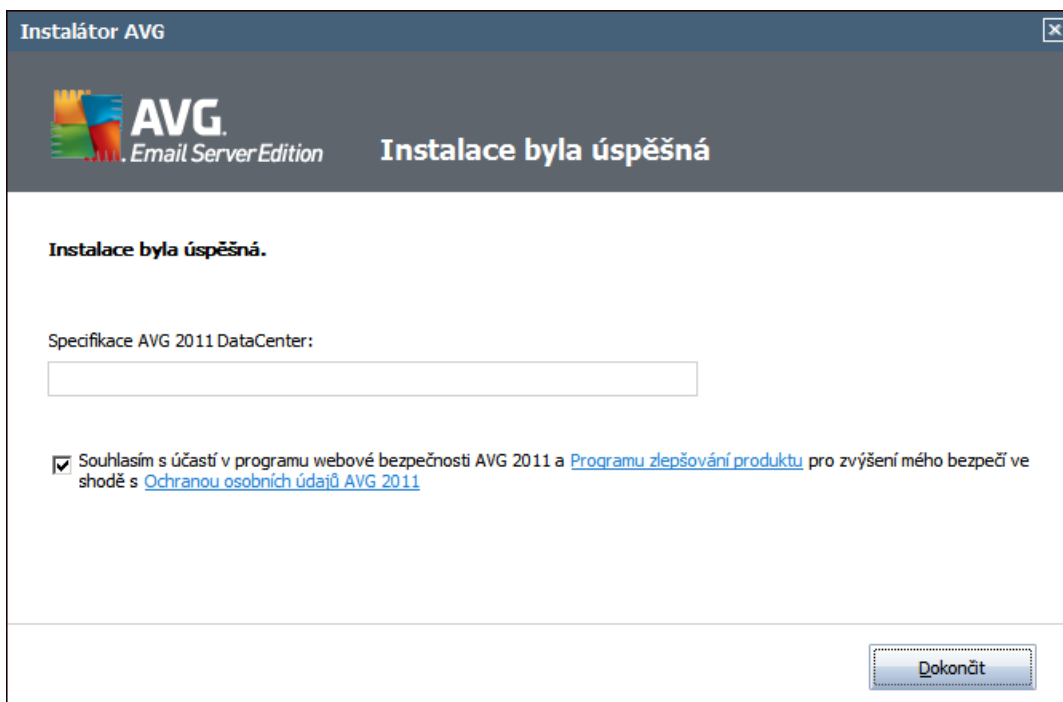
Kontroluje e-mailové zprávy uložené v uživatelských schránkách. Při nalezení viru dojde k přesunu do virového trezoru nebo kompletnímu odstranění.

Poznámka: Nabídka komponent se liší podle verze MS Exchange, který používáte.

Pokračujte stiskem tlačítka **Další**.

3.5. Dokončení instalace

Pokud jste v předchozí volby komponent vybrali **Komponentu vzdálené správy**, můžete v tomto dialogu zadat připojovací adresy pro spojení s vaším AVG DataCenter.



Ve výchozím nastavení je zaškrtnuta také volba **Souhlasím s účastí v programu webové bezpečnosti AVG 2011 a Programu zlepšování produktu ...**. Označením této volby dáváte najevo svůj souhlas s účastí v Programu zlepšování produktu (a umožníte tak reportování informací o detekovaných hrozbách týmu expertů společnosti AVG). V rámci tohoto programu probíhá sběr anonymních informací o detekovaných hrozbách s cílem zvýšit celkovou úroveň bezpečnosti na Internetu.



Své volby potvrďte stiskem tlačítka ***Dokončit***.

Program AVG je nyní nainstalován na vašem počítači/serveru a plně funkční. Program běží ve výchozím nastavení na pozadí a nevyžaduje vaši pozornost.

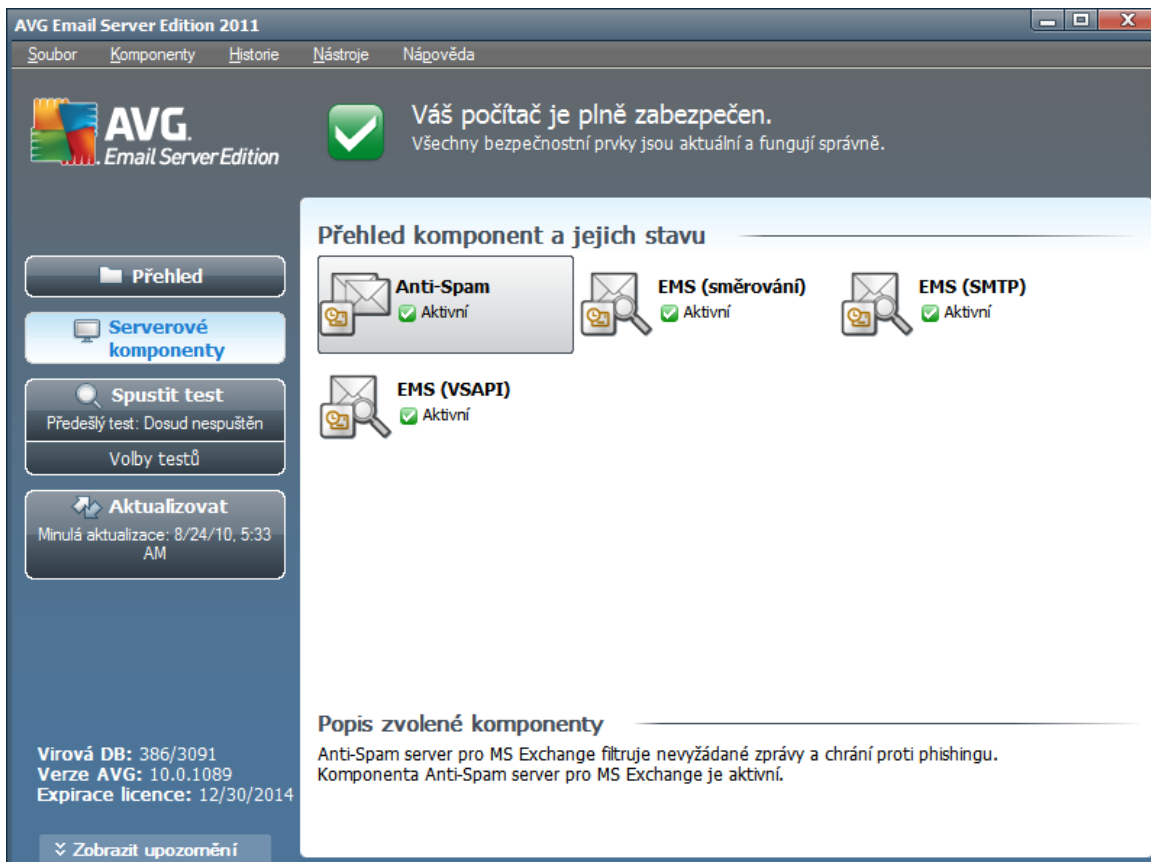
Pro nastavení ochrany pro váš e-mail server zvolte odpovídající kapitolu:

- [*Kontrola pošty pro MS Exchange Server 2007/2010*](#)
- [*Kontrola pošty pro MS Exchange Server 2003*](#)
- [*AVG pro Kerio MailServer*](#)

4. Kontrola pošty pro MS Exchange Server 2007/2010

4.1. Přehled

Konfigurace Kontroly pošty pro MS Exchange Server 2007/2010 je plně integrována v rámci aplikace AVG Email Server 2011 jako serverová komponenta.



The screenshot displays the AVG Email Server Edition 2011 management console. At the top, a status message indicates the computer is fully secured. The main area, titled 'Přehled komponent a jejich stavu', shows four active components: Anti-Spam, EMS (směrování), EMS (SMTP), and EMS (VSAPI). A left sidebar contains navigation buttons for 'Přehled', 'Serverové komponenty', 'Spustit test', and 'Aktualizovat'. The bottom left corner shows system information like 'Virová DB: 386/3091' and 'Verze AVG: 10.0.1089'. A 'Popis zvolené komponenty' section at the bottom right provides details for the Anti-Spam component.

Základní přehled jednotlivých serverových komponent:

- [**Anti-Spam - Anti-Spam server pro MS Exchange**](#)

Kontroluje všechny přichodící e-mailové zprávy a označuje nevyžádanou poštu jako SPAM. K analýze každé zprávy využívá několik metod, což zajišťuje maximální možnou ochranu proti nechtěným zprávám.

- [**EMS \(směrování\) - Kontrola pošty pro MS Exchange \(směrovací transportní Agent\)**](#)

Kontroluje všechny přicházející, odcházející a interní e-mailové zprávy procházející skrze HUB roli MS Exchange.

Dostupné pouze pro MS Exchange 2007/2010 a lze nainstalovat pouze na HUB roli.



- [EMS \(SMTP\) - Kontrola pošty pro MS Exchange \(SMTP transportní agent\)](#)

Kontroluje e-mailové zprávy procházející skrze SMTP rozhraní MS Exchange.

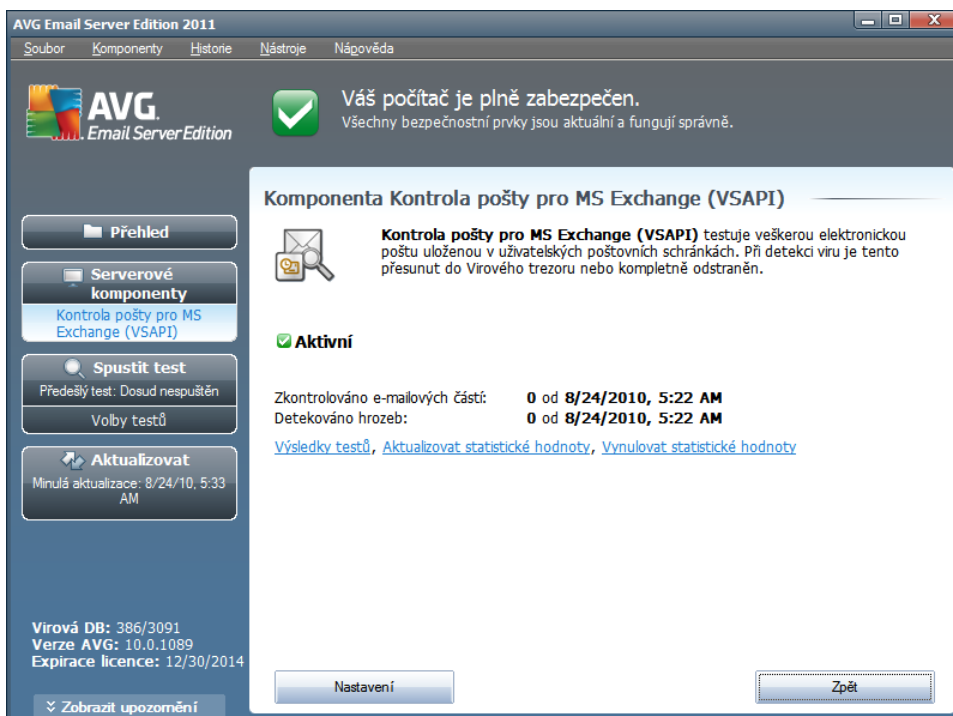
Dostupné pouze pro MS Exchange 2007/2010 a lze nainstalovat na EDGE i HUB roli.

- [EMS \(VSAPI\) - Kontrola pošty pro MS Exchange \(VSAPI\)](#)

Kontroluje e-mailové zprávy uložené v uživatelských schránkách. Při nalezení viru dojde k přesunu do virového trezoru nebo kompletnímu odstranění.

D ležitá poznámka: Pokud jste se rozhodli nainstalovat a použít VSAPI v kombinaci se sm rovacím transportním agentem na Hub Exchange roli, vaše e-mailové zprávy budou kontrolovány dvakrát. Pro změnu tohoto chování konzultujte kapitolu [Technické upozornění](#).

Klikněte dvakrát na požadovanou komponentu pro zobrazení jejího rozhraní. S výjimkou komponenty Anti-Spam sdílejí všechny komponenty společné ovládací prvky:



- **Výsledky test**

Otevře nový dialog s přehledem výsledků testů :

Výsledky testů

Zobrazit poslední 2 dny 0 hodiny
 Zobrazit výběr
 Od 8/26/2010 7:51:26 AM
 Do 8/27/2010 7:51:26 AM
 Zobrazit vše

Obnovit

Vše Infekce Spyware Varování Informace

Od	Komu	Předmět	Čas	Ty

Zavřít

Zde můžete zkontrolovat zprávy rozdlené do několika záložek podle jejich závažnosti. Více informací o konkrétní závažnosti a jejím nastavení naleznete v popisu nastavení jednotlivých serverových komponent.

Ve výchozím nastavení jsou zobrazeny pouze výsledky za poslední dva dny. Interval pro zobrazení můžete změnit pomocí volby:

- **Zobrazit poslední** - vložte preferovaný počet dní a hodin.
- **Zobrazit výběr** - zvolte libovolný časový a datumový rozsah.
- **Zobrazit vše** - zobrazí výsledky za celé období.

Tlačítkem **Obnovit** znovu načítáte výsledky testů.

- **Aktualizovat statistické hodnoty** - aktualizuje statistiky uvedené v dialogu.
- **Vynulovat statistické hodnoty** - vynuluje všechny statistiky.

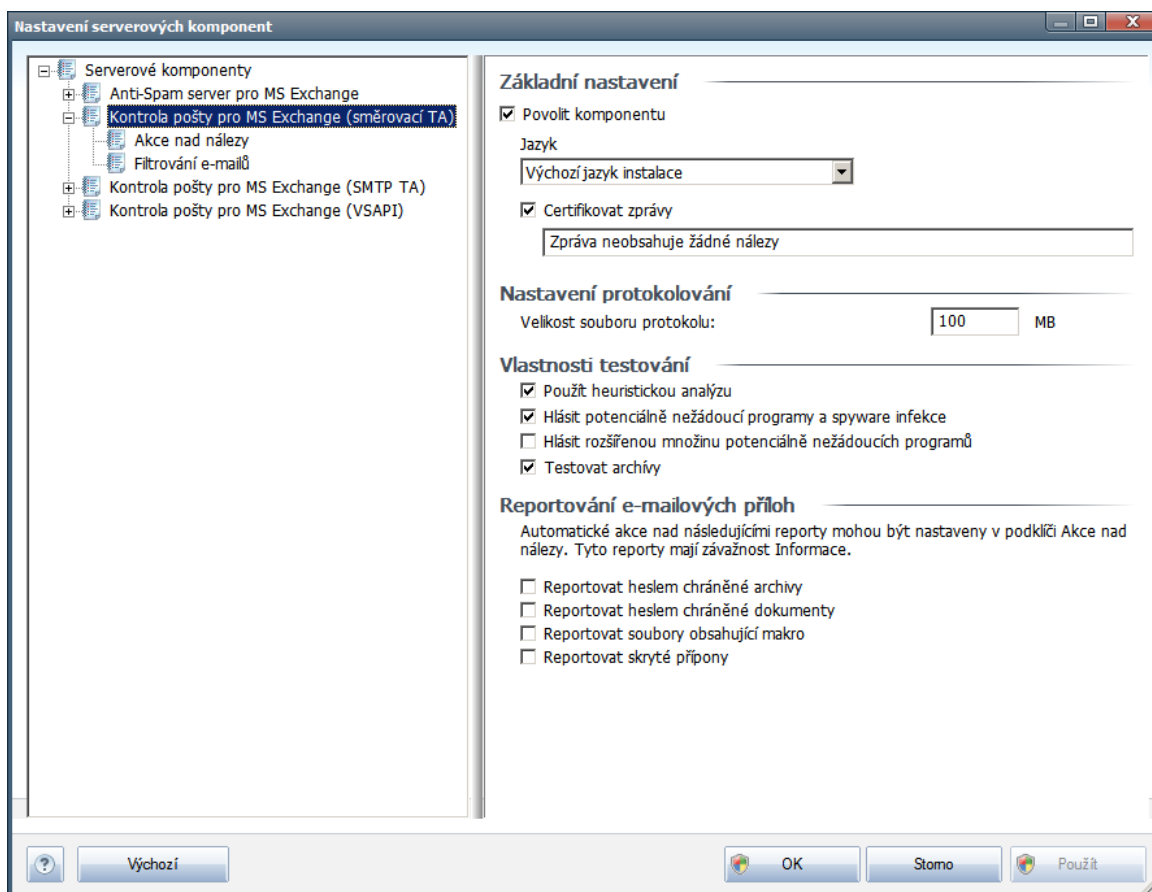
Funkční tlačítka v dialogu jsou tato:

- **Nastavení** - tímto tlačítkem otevřete nastavení dané komponenty.
- **Zpět** - tímto tlačítkem se vrátíte zpět na seznam komponent.

Bližší nastavení jednotlivých komponent naleznete v kapitolách níže.

4.2. Kontrola pošty pro MS Exchange (směrovací TA)

Tato položka obsahuje možnosti nastavení **Kontroly pošty pro MS Exchange (směrovací transportní agent)**.



V sekci **Základní nastavení** naleznete následující možnosti:

- **Povolit komponentu** - odškrtn te pro vypnutí celé komponenty.
- **Jazyk** - zvolte preferovaný jazyk komponenty.
- **Certifikovat zprávy** - zaškrtn te, pokud si p ežete p idat certifika ní poznámku ke všem testovaným zprávám. Zprávu m žete upravit v následujícím polí ku.

Sekce **Nastavení protokolování** obsahuje tyto volby:

- **Velikost souboru protokolu** - zvolte preferovanou velikost protokolovacího souboru. Výchozí hodnota je 100 MB.

Sekce **Vlastnosti testování** obsahuje tato nastavení:



- **Použit heuristickou analýzu** - zaškrtněte pro povolení použití heuristické analýzy v průběhu testování.
- **Hlásit potenciálně nežádoucí programy a spyware infekce** - zaškrtněte pro hlášení potenciálně nežádoucích programů a spyware.
- **Hlásit rozšířenou množinu potenciálně nežádoucích programů** - zaškrtnutím tohoto políčka aktivujete detekci rozšířené sady spyware: programů, které jsou v podobě od výrobce neškodné a v pořádku, ale mohou být snadno zneužity ke škodlivým účelům, případně jde o zásadně neškodné, avšak poněkud obtížující programy (různé doplňky do prohlížeče atd.). Jde o dodatečné opatření, které zlepšuje zabezpečení vašeho počítače na další úrovni, nicméně může blokovat také některé legální programy, proto je ve výchozím nastavení tato možnost vypnuta. Tato detekce je doplněna přídavnými možnostmi, samostatně tedy není dostatečně účinná: pokud chcete ochranu před základními typy spyware, pak ponechte vždy označené přídavné políčko, a toto pak označíte volitelně k nim.
- **Testovat archívy** - zaškrtněte pro zahrnutí také testování archivních souborů (zip, rar, atp.)

Sekcí **Reportování e-mailových příloh** umožní vybrat položky, které si přejete hlásit v průběhu testování. Pokud je položka zaškrtnutá, bude každá zpráva s takovou přílohou obsahovat v předmětu text [INFORMACE] (ve výchozím nastavení). Toto výchozí nastavení lze změnit ve vztahu **Akce nad nálezy**, část **Informace** (viz níže).

K dispozici jsou následující možnosti:

- **Reportovat heslem chráněné archívy**
- **Reportovat heslem chráněné dokumenty**
- **Reportovat dokumenty obsahující makra**
- **Reportovat skryté přípony**

Součástí nastavení jsou tyto podpoložky ve stromové struktuře:

- [Akce nad nálezy](#)
- [Filtrování e-mailů](#)

4.3. Kontrola pošty pro MS Exchange (SMTP TA)

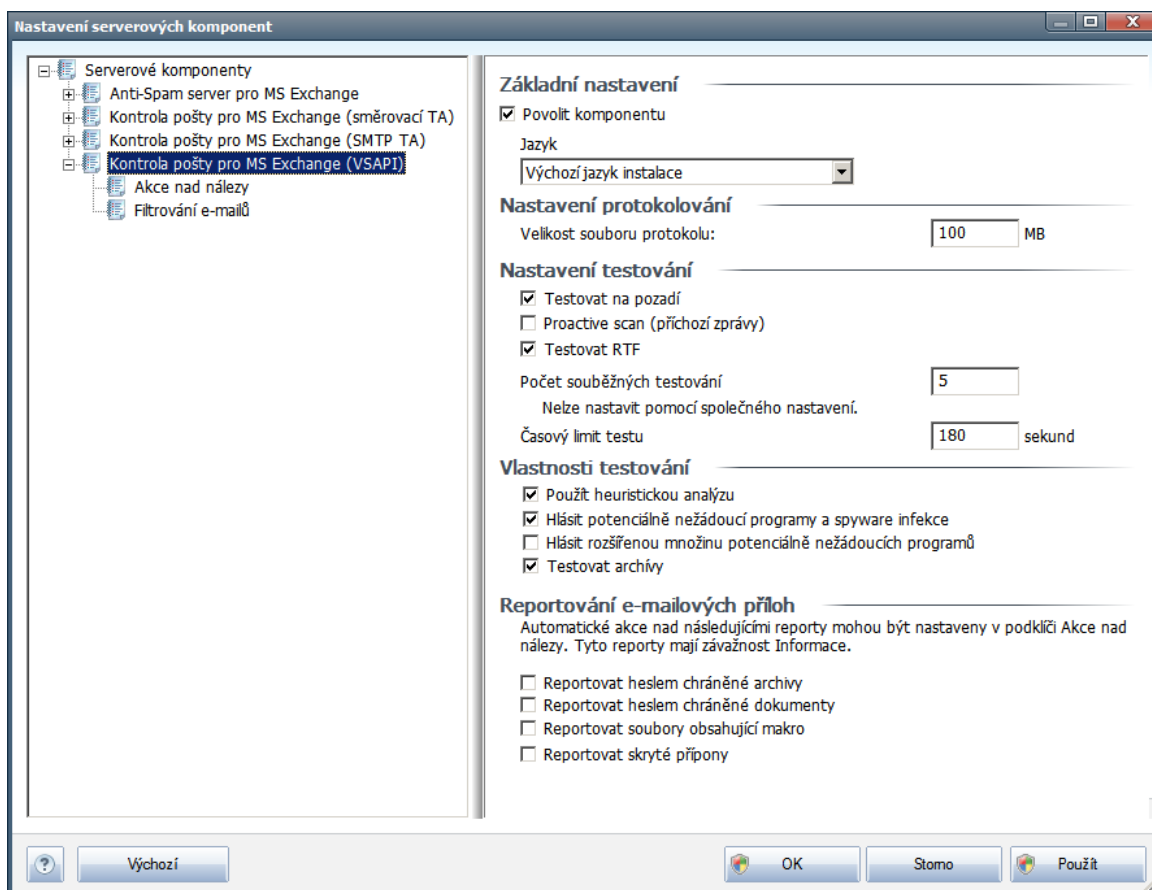
Konfigurace kontroly pošty pro MS Exchange (SMTP Transportní Agent) je stejná jako pro směrovací transportní agent. Více informací naleznete v kapitole [Kontrola pošty pro MS Exchange \(směrovací TA\)](#) výše.

Součástí nastavení jsou také tyto podpoložky ve stromové struktuře:

- [Akce nad nálezy](#)
- [Filtrování e-mailů](#)

4.4. Kontrola pošty pro MS Exchange (VSAPI)

Tato položka obsahuje možnosti nastavení **Kontroly pošty pro MS Exchange (VSAPI)**.



V sekci **Základní nastavení** naleznete následující možnosti:

- **Povolit komponentu** - odškrtn te pro vypnutí celé komponenty.
- **Jazyk** - zvolte preferovaný jazyk komponenty.

Sekce **Nastavení protokolování** obsahuje tyto volby:

- **Velikost souboru protokolu** - zvolte preferovanou velikost protokolovacího souboru. Výchozí hodnota je 100 MB.

Sekce **Nastavení testování** obsahuje tato nastavení:

- **Testovat na pozadí** - zde můžete povolit nebo zakázat proces kontroly existujícího obsahu databáze na pozadí. Kontrola uložené pošty na pozadí je jedním z prvků rozhraní VSAPI 2.0/2.5. Antivirová kontrola probíhá pro každou databázi na serveru zvlášť; vždy jsou testovány zprávy i přílohy.



Pro každou databázi je zároveň použito jedno vlákno (*thread*) s nízkou prioritou, což znamená, že ostatní úlohy, jako například ukládání e-mail zpráv do Microsoft Exchange databáze, dostanou vždy přednost. Kontrola pošty na pozadí je aplikována pro tabulku se složkami v rámci Exchange úložiště. Složka, která již byla na pozadí jednou zkontrolována, bude znovu zkontrolována až při opětovném spuštění rozhraní. Změny jednotlivých zpráv ve složkách jsou zpracovávány proaktivní kontrolou (*proactive scan*).

- **Proactive scan (příchozí zprávy)** - zde můžete povolit nebo zakázat funkci proaktivní kontroly z VSAPI 2.0/2.5. Tato funkce spočívá v dynamické správě priorit položek v testovací frontě. Jakmile jsou zprávy umístěny do úložiště serveru Exchange, jsou zařazeny také do obecné fronty k testování s nízkou prioritou (maximum 30 položek). Následně jsou testovány podle metody FIFO (First in, first out). Pokud je některé položce zaznamenán přístup zatímco je stále ve frontě, její priorita se změní na vysokou.

Poznámka: Nadbytečné zprávy jsou přesunuty do úložiště bez otestování.

Upozornění: V případě vypnutí obou voleb (**Testování na pozadí a Proactive Scan**), zůstává i nadále aktivní rezidentní test, který se spustí v momentě stahování zprávy klientem MS Outlook.

- **Testovat RTF** - zvolte, zdali si přejete testovat také RTF soubory.
- **Počet souběžných testování** - ve výchozím nastavení běží testovací proces paralelně ve více vláknech, zejména pro zvýšení obecného výkonu. Počet souběžných vláken lze změnit v tomto nastavení.
Výchozí počet vláken je vypočítán jako dvojnásobek "počet procesorů" + 1.
Minimální počet vláken je vypočítán jako ("počet procesorů" + 1) vyděleno dvěma.
Maximální počet vláken je vypočítán jako "počet procesorů" krát 5 + 1.
Pokud je nastavena hodnota nižší nebo minimální, případně maximální i vyšší, je použita hodnota výchozí.
- **Asový limit testu** - maximální souvislý interval (v sekundách), po který může jedno vlákno přistupovat k právě testovanému objektu (výchozí hodnota je 180 sekund).

Sekce **Vlastnosti testování** obsahuje tato nastavení:

- **Použít heuristickou analýzu** - zaškrtněte pro povolení použití heuristické analýzy v průběhu testování.
- **Hlásit potenciálně nežádoucí programy a spyware infekce** - zaškrtněte pro hlášení potenciálně nežádoucích programů a spyware.
- **Hlásit rozšířenou množinu potenciálně nežádoucích programů** - zaškrtnutím tohoto políčka aktivujete detekci rozšířené sady spyware: programů, které jsou v podobě od výrobce neškodné a v pořádku, ale mohou být snadno zneužity ke škodlivým účelům, případně jde o zásadně neškodné, avšak poněkud obtěžující programy (různé doplňky do prohlížeče atd.). Jde o dodatečné opatření, které zlepšuje zabezpečení vašeho počítače na další úrovni, nicméně může blokovat také některé legální programy, proto je ve výchozím nastavení tato možnost vypnuta. Tato detekce je doplněna předchozí možností, samostatně



tedy není dosta uující: pokud chcete ochranu p ed základními typy spyware, pak ponechte vždy ozna ené p edchozí polí ko, a toto pak ozna te voliteln k n mu.

- **Testovat archívy** - zaškrtn te pro zahrnutí také testování archivních soubor (zip, rar, atp.)

Secke **Reportování e-mailových p íloh** umož ũje vybrat položky, které si p ejete hlásit v pr b hu testování. Toto výchozí nastavení lze zm nit ve v tví **Akce nad nálezy**, ást **Informace** (viz níže).

K dispozici jsou následující možnosti:

- **Reportovat heslem chrán né archívy**
- **Reportovat heslem chrán né dokumenty**
- **Reportovat dokumenty obsahující makro**
- **Reportovat skryté p ípony**

N které prvky v tomto nastavení tvo í uživatelské rozší ení aplika ního rozhraní Microsoft VSAPI 2.0/2.5. Pokud se chcete blíže informovat o tomto rozhraní, následujte tyto odkazy:

- <http://support.microsoft.com/default.aspx?scid=kb;en-us:328841&Product=exch2k> – popis princip spolupráce Exchange s antivirovými programy
- <http://support.microsoft.com/default.aspx?scid=kb;en-us:823166> – informace o dopl cích ve VSAPI 2.5 v aplikaci Exchange 2003 Server

Sou ástí nastavení jsou také tyto podpoložky ve stromové struktu e:

- [Akce nad nálezy](#)
- [Filtrování e-mail](#)

4.5. Technické upozornění

Tato informace se týká situace, kdy instalujete a používáte zároveň VSAPI i sm rovací transportní agent na Hub Exchange roli. V takovém p ípad budou vaše e-mailové zprávy kontrolovány dvakrát (poprvé VSAPI rozhraním a posléze sm rovacím transportním agentem)

V d sledku zp sobu, jakým VSAPI rozhraní funguje, m že dojit k ur itým nesrovnalostem ve výsledcích testování, pop ípad ke zbyte né dvojité zát Źi p i duplicitním kontrolování. Z toho d vodu doporu ujeme užít jednoduché ešení v podob zásahu do registr (viz níže).

Poznámka: *Zm nu v registrech doporu ujeme provád t pouze zkušeným uživatel m. Zároveň p ed zm nou v registrech prove te jejich zálohu a ujist te se, že víte jakým zp sobem lze registry obnovit v p ípad problém .*

Otev ete editor registr (Windows nabídka **Start/Spustit**, vepišť výraz **regedit** a potvr te klávesou enter). Otev ete následující v tev:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchange\IS\VirusScan

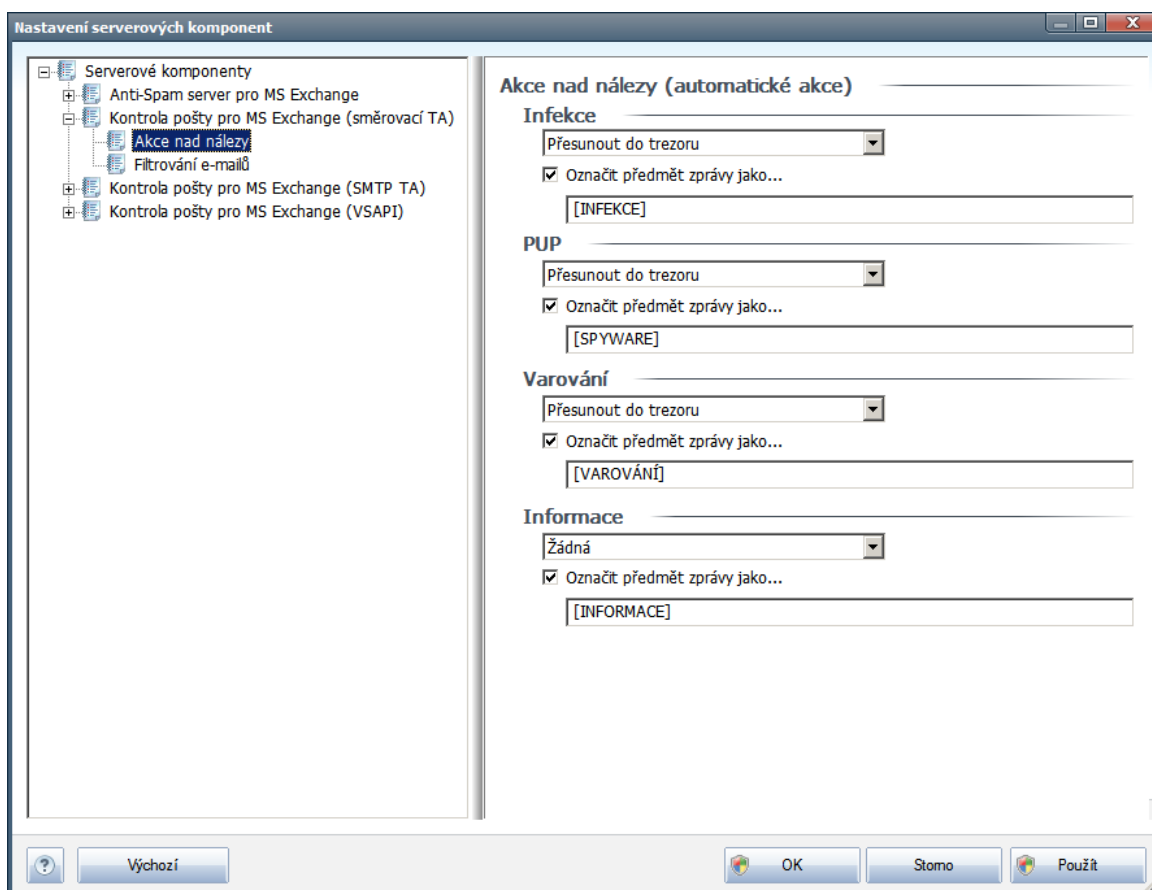


Klikn te pravým tlačítkem do pravé části dialogu a z nabídky zvolte **Nový/Hodnota DWORD (32bitová)**. Pojmenujte novou hodnotu **TransportExclusion**. Poté na ni dvakrát klikn te myší a změn te její hodnotu na **1**.

Pro informování MS Exchange serveru o dané změně je ještě potřeba změnit hodnotu **ReloadNow** na číslo 1.

Tímto způsobem vypnete testování odchozích zpráv skrze VSAPI rozhraní. Změna se projeví po několika minutách.

4.6. Akce nad nálezy



V části **Akce nad nálezy** lze zaškrtnout a vybrat automatické akce, které mají být provedeny v průběhu testování. Akce jsou k dispozici pro následující položky:

- **Infekce**
- **PUP (Potenciálně nežádoucí programy)**
- **Varování**

- **Informace**

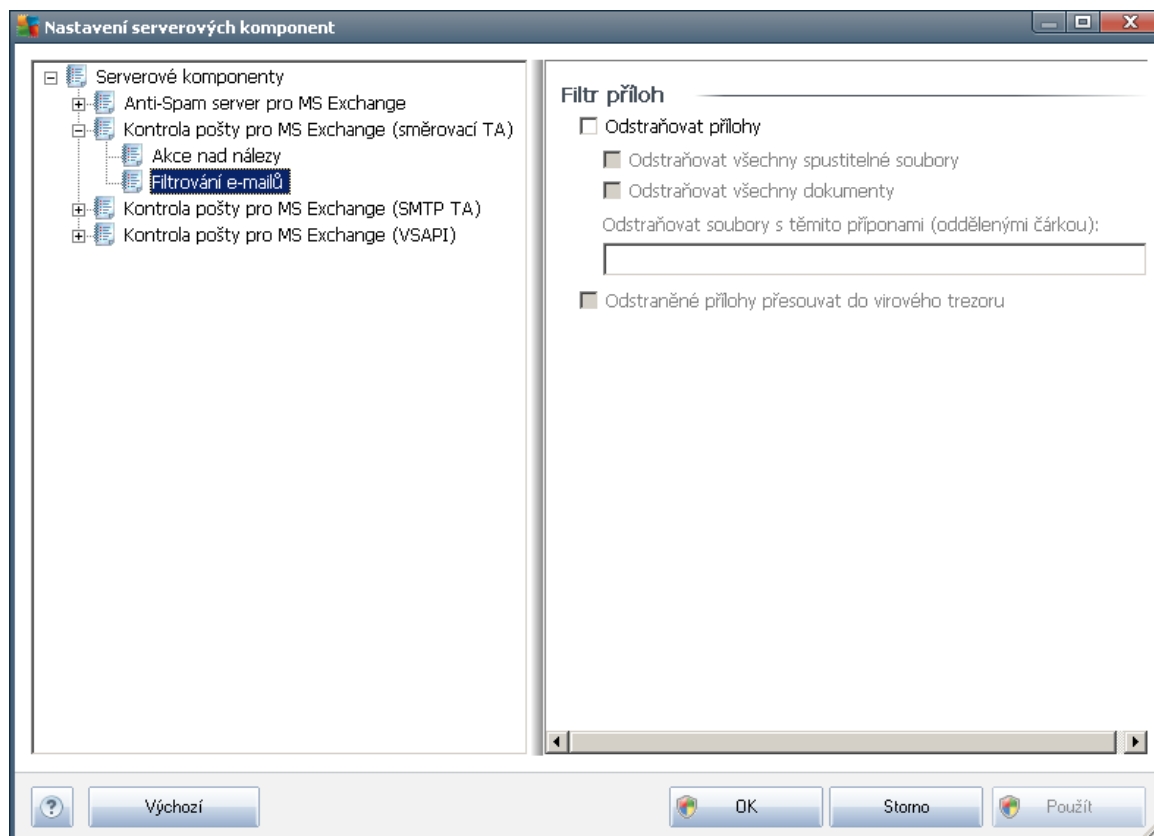
Z rolovací nabídky zvolte pro každou položku vždy jednu akci:

- **Žádná** - nebude provedena žádná akce.
- **Posunout do trezoru** - dané nebezpečí bude posunuto do Virového trezoru.
- **Odstranit** - dané nebezpečí bude odstraněno.

Pokud si přejete přidat do přední zprávy zpracované určitou akci textovou informaci pro lepší identifikaci a přehled, zaškrtněte příslušné políčko **Označit zprávy jako** a vložte požadovanou hodnotu.

Poznámka: Poslední zmíněnou vlastnost nelze aplikovat v případě nastavení Kontroly pošty pro MS Exchange (VSAPI).

4.7. Filtrování e-mailů



V části **Filtr příloh** můžete zvolit přílohy, které mají být automaticky odstraněny. K dispozici jsou následující možnosti:

- **Odstraňovat přílohy** - zaškrtněte pro povolení této funkce.



- **Odstranit všechny spustitelné soubory** - odstraní všechny spustitelné přílohy.
- **Odstranit všechny dokumenty** - odstraní všechny dokumenty v příloze.
- **Odstranit soubory s tímto příponami (oddělenými čárkou)** - vložte přípony, které si přejete automaticky odstranit. Hodnoty oddělte čárkou.
- **Odstranit přílohy přesouvání do virového trezoru** - zaškrtněte, pokud nechcete, aby byly filtrované přílohy odstráněny rovnou. Je-li toto políčko zaškrtnuté, budou všechny přílohy zvolené prostřednictvím tohoto dialogu automaticky přesouvány do karanténního prostředí Virového trezoru. Jedná se o bezpečné místo pro ukládání potenciálně škodlivých souborů - můžete k nim přistupovat a zkoumat je, aniž by mohly ohrozit váš systém. Do Virového trezoru se dostanete z hlavní obrazovky aplikace **AVG Email Server 2011**. V horní nabídce klikněte levým tlačítkem myši na položku **Historie** a následně z kontextového menu zvolte **Virový trezor**.



5. Kontrola pošty pro MS Exchange Server 2003

5.1. Přehled

Konfigurace Kontroly pošty pro MS Exchange Server 2003 je plně integrována v rámci aplikace AVG Email Server 2011 jako serverová komponenta.

The screenshot shows the AVG Email Server Edition 2011 interface. At the top, there is a menu bar with options: Soubor, Komponenty, Historie, Nástroje, Nágověda, Beta, and Odešlat připomínku. Below the menu, the AVG logo and 'Email Server Edition' are displayed. A green checkmark icon indicates that the computer is fully secured: 'Váš počítač je plně zabezpečen. Všechny bezpečnostní prvky jsou aktuální a fungují správně.' The main area is titled 'Přehled komponent a jejich stavu' and shows two active components: 'Anti-Spam' and 'EMS (VSAPI)', both marked as 'Aktivní'. On the left side, there are several buttons: 'Přehled', 'Serverové komponenty', 'Spustit test' (with a sub-message 'Předěšlý test: Dosud nespuštěn' and 'Volby testů'), and 'Aktualizovat' (with a sub-message 'Minulá aktualizace: 8/31/10, 5:41 AM'). At the bottom left, system information is shown: 'Virová DB: 395/3103', 'Verze AVG: 10.0.1095', and 'Expirace licence: 10/30/2010'. A 'Zobrazit upozornění' button is at the bottom left. Below the component overview, there is a section 'Popis zvolené komponenty' with a description for the Anti-Spam component: 'Anti-Spam server pro MS Exchange filtruje nevyžádané zprávy a chrání proti phishingu. Komponenta Anti-Spam server pro MS Exchange je aktivní.'

Základní přehled jednotlivých serverových komponent:

- [Anti-Spam - Anti-Spam server pro MS Exchange](#)

Kontroluje všechny příchozí e-mailové zprávy a označuje nevyžádanou poštu jako SPAM. K analýze každé zprávy využívá několik metod, což zajišťuje maximální možnou ochranu proti nechtěným zprávám.

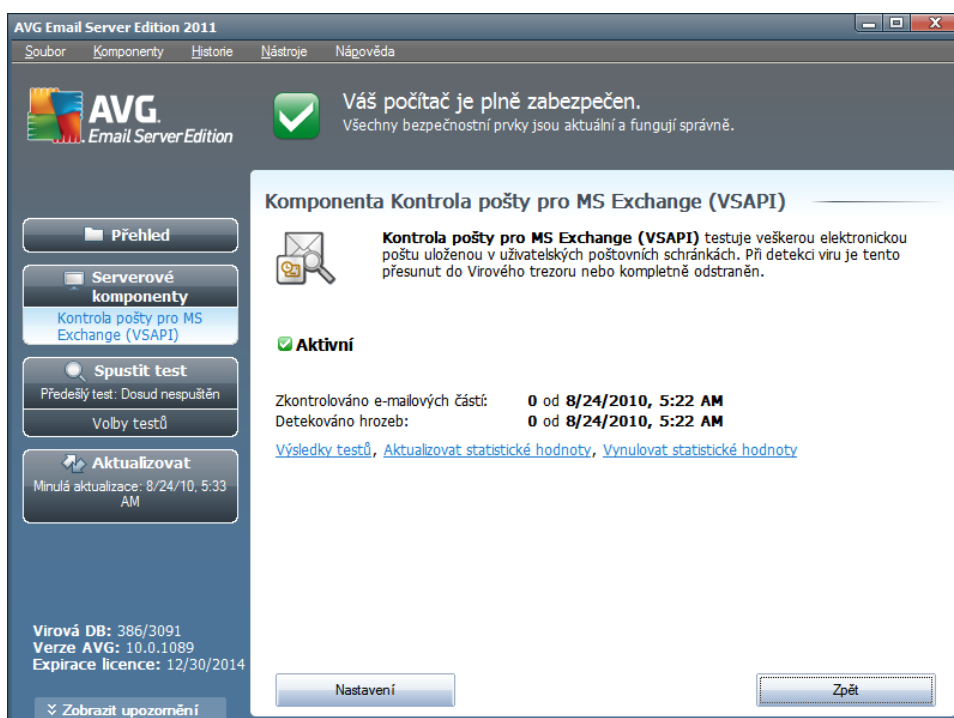
- [EMS \(VSAPI\) - Kontrola pošty pro MS Exchange \(VSAPI\)](#)

Kontroluje e-mailové zprávy uložené v uživatelských schránkách. Při nalezení viru dojde k přesunu do virového trezoru nebo kompletnímu odstranění.

Klikněte dvakrát na požadovanou komponentu pro zobrazení jejího rozhraní. V případě **komponenty**

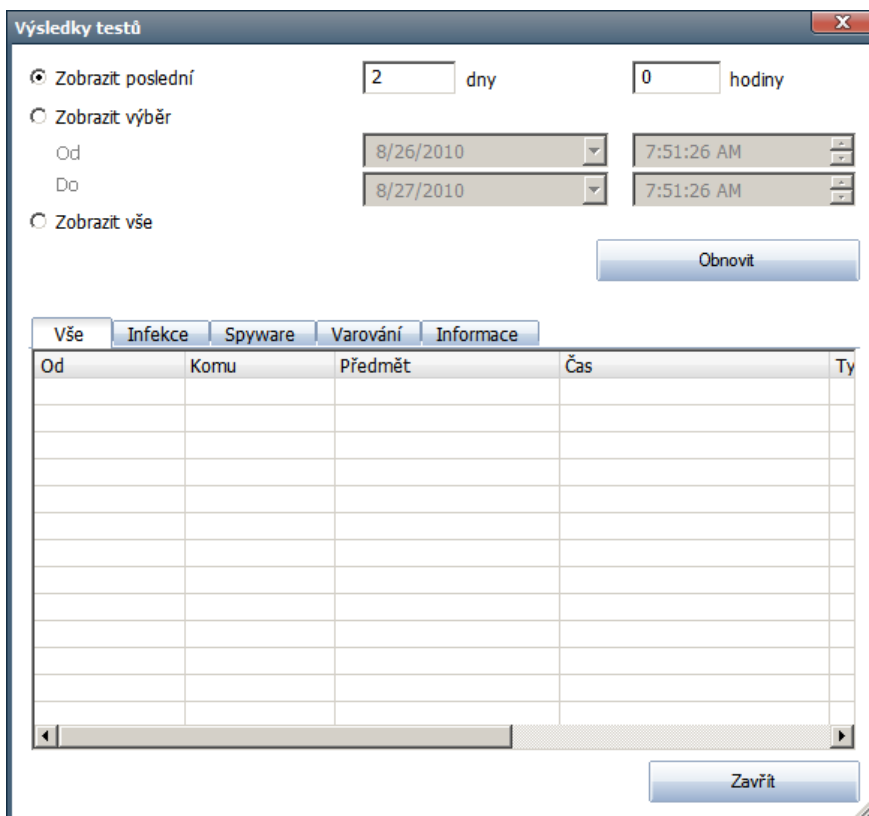


Anti-Spam se otevírá její vlastní unikátní dialog, popsáný v [samostatné kapitole](#). V případě komponenty **Kontrola pošty pro MS Exchange (VSAPI)** jsou ovládací prvky v jejím hlavním rozhraní následující:



- **Výsledky test**

Otevírá nový dialog s přehledem výsledků testů :



Od	Komu	Předmět	Čas	Ty

Zde můžete zkontrolovat zprávy rozdlené do několika záložek podle jejich závažnosti. Více informací o konkrétní závažnosti a jejím nastavení naleznete v popisu nastavení jednotlivých serverových komponent.

Ve výchozím nastavení jsou zobrazeny pouze výsledky za poslední dva dny. Interval pro zobrazení můžete změnit pomocí volby:

- **Zobrazit poslední** - vložte preferovaný počet dní a hodin.
- **Zobrazit výběr** - zvolte libovolný časový a datumový rozsah.
- **Zobrazit vše** - zobrazí výsledky za celé období.

Titulkem **Obnovit** znovu načítete výsledky testů.

- **Aktualizovat statistické hodnoty** - aktualizuje statistiky uvedené v dialogu.
- **Vynulovat statistické hodnoty** - vynuluje všechny statistiky.

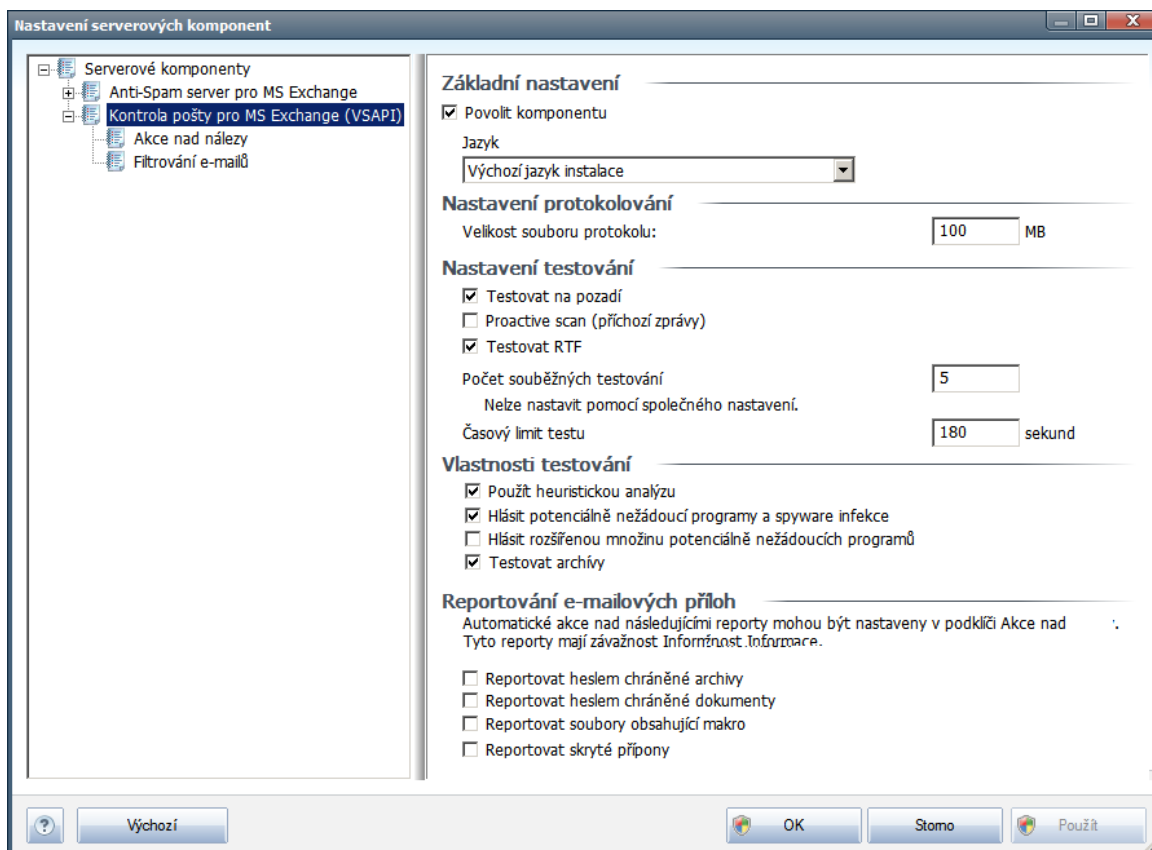
Funkční tlačítka v dialogu jsou tato:

- **Nastavení** - tímto tlačítkem otevřete nastavení dané komponenty.
- **Zpět** - tímto tlačítkem se vrátíte zpět na seznam komponent.

Bližší nastavení jednotlivých komponent naleznete v kapitolách níže.

5.2. Kontrola pošty pro MS Exchange (VSAPI)

Tato položka obsahuje možnosti nastavení **Kontroly pošty pro MS Exchange (VSAPI)**.



V sekci **Základní nastavení** naleznete následující možnosti:

- **Povolit komponentu** - odškrtnete pro vypnutí celé komponenty.
- **Jazyk** - zvolte preferovaný jazyk komponenty.

Sekce **Nastavení protokolování** obsahuje tyto volby:

- **Velikost souboru protokolu** - zvolte preferovanou velikost protokolovacího souboru. Výchozí hodnota je 100 MB.

Sekce **Nastavení testování** obsahuje tato nastavení:

- **Testovat na pozadí** - zde můžete povolit nebo zakázat proces kontroly existujícího obsahu databáze na pozadí. Kontrola uložené pošty na pozadí je jedním z prvků rozhraní VSAPI 2.0/2.5. Antivirová kontrola probíhá pro každou databázi na serveru zvlášť; vždy jsou testovány zprávy i přílohy.



Pro každou databázi je zároveň použito jedno vlákno (*thread*) s nízkou prioritou, což znamená, že ostatní úlohy, jako například ukládání e-mail zpráv do Microsoft Exchange databáze dostane vždy přednost. Kontrola pošty na pozadí je aplikována pro tabulku se složkami v rámci Exchange úložiště. Složka, která již byla na pozadí jednou zkontrolována, bude znovu zkontrolována až při opětovném spuštění rozhraní. Změny jednotlivých zpráv ve složkách jsou zpracovávány proaktivní kontrolou (*proactive scan*).

- **Proactive scan (příchozí zprávy)** - zde můžete povolit nebo zakázat funkci proaktivní kontroly z VSAPI 2.0/2.5. Tato funkce spočívá v dynamické správě priorit položek v testovací frontě. Jakmile jsou zprávy umístěny do úložiště serveru Exchange, jsou zařazeny také do obecné fronty k testování s nízkou prioritou (maximum 30 položek). Následně jsou testovány podle metody FIFO (First in, first out). Pokud je některé položce zaznamenán přístup zatímco je stále ve frontě, její priorita se změní na vysokou.

Poznámka: Nadbytečné zprávy jsou přesunuty do úložiště bez otestování.

Upozornění: I v případě vypnutí obou voleb (**Testování na pozadí a Proactive Scan**), zůstává i nadále aktivní rezidentní test, který se spustí v momentě stahování zprávy klientem MS Outlook.

- **Testovat RTF** - zvolte, zdali si přejete testovat také RTF soubory.
- **Počet souběžných testování** - ve výchozím nastavení běží testovací proces paralelně ve více vláknech, zejména pro zvýšení obecného výkonu. Počet souběžných vláken lze změnit v tomto nastavení.
Výchozí počet vláken je vypočítán jako dvojnásobek "počet procesorů" + 1.
Minimální počet vláken je vypočítán jako ("počet procesorů" + 1) vyděleno dvěma.
Maximální počet vláken je vypočítán jako "počet procesorů" krát 5 + 1.
Pokud je nastavena hodnota nižší nebo minimální, případně maximální i vyšší, je použita hodnota výchozí.
- **Asový limit testu** - maximální souvislý interval (v sekundách), po který může jedno vlákno přistupovat k právě testovanému objektu (výchozí hodnota je 180 sekund).

Sekce **Vlastnosti testování** obsahuje tato nastavení:

- **Použít heuristickou analýzu** - zaškrtněte pro povolení použití heuristické analýzy v průběhu testování.
- **Hlásit potenciálně nežádoucí programy a spyware infekce** - zaškrtněte pro hlášení potenciálně nežádoucích programů a spyware.
- **Hlásit rozšířenou množinu potenciálně nežádoucích programů** - zaškrtnutím tohoto políčka aktivujete detekci rozšířené sady spyware: programů, které jsou v podobě od výrobce neškodné a v pořádku, ale mohou být snadno zneužity ke škodlivým účelům, případně jde o zásadně neškodné, avšak poněkud obtížící programy (různé doplňky do prohlížeče atd.). Jde o dodatečné opatření, které zlepšuje zabezpečení vašeho počítače na další úrovni, nicméně může blokovat také některé legální programy, proto je ve výchozím nastavení tato možnost vypnuta. Tato detekce je doplněna původní možností, samostatně



tedy není dosta uující: pokud chcete ochranu p ed základními typy spyware, pak ponechte vždy ozna ené p edchozí polí ko, a toto pak ozna te voliteln k n mu.

- **Testovat archívy** - zaškrtn te pro zahrnutí také testování archivních soubor (zip, rar, atp.)

Sekce **Reportování e-mailových p íloh** umož ňuje vybrat položky, které si p ejete hlásit v pr b hu testování. Toto výchozí nastavení lze zm nit ve v tv **Akce nad nálezy**, ást **Informace** (viz níže).

K dispozici jsou následující možnosti:

- **Reportovat heslem chrán né archívy**
- **Reportovat heslem chrán né dokumenty**
- **Reportovat dokumenty obsahující makro**
- **Reportovat skryté p ípony**

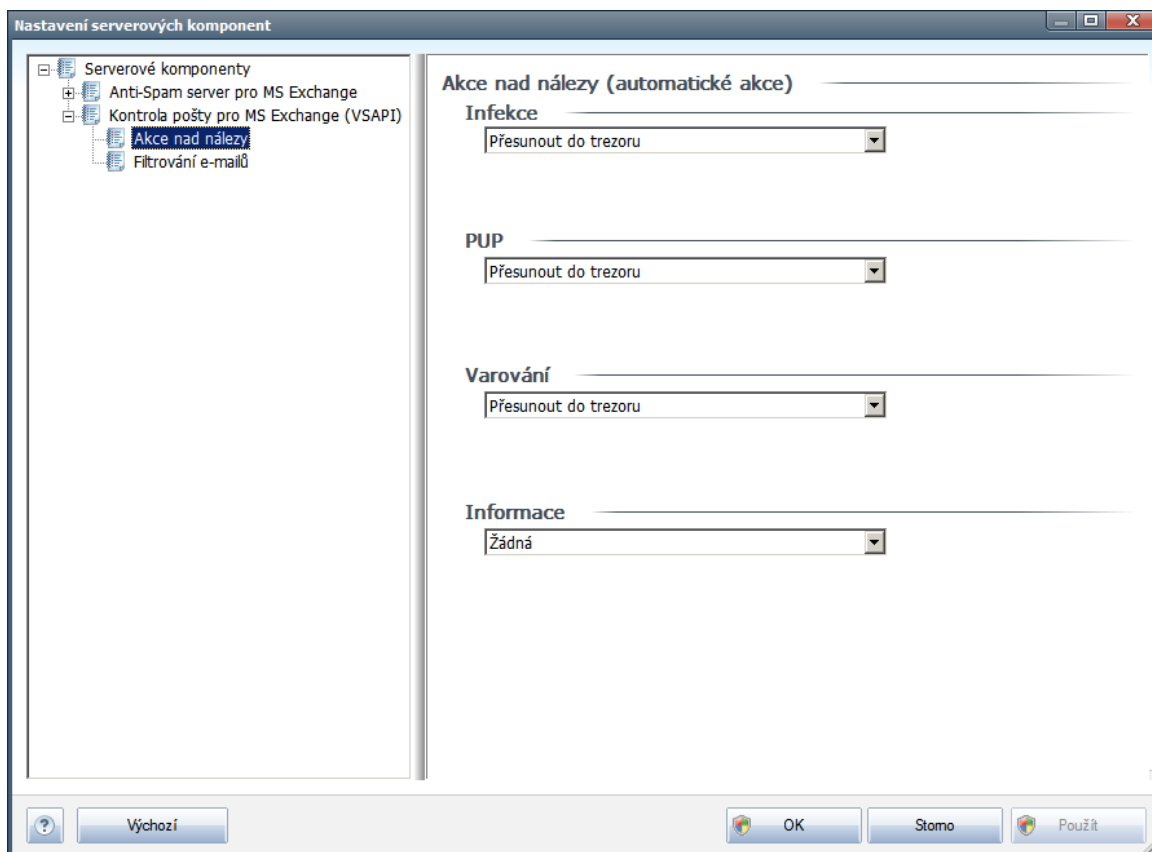
N které prvky v tomto nastavení tvo í uživatelské rozší ení aplika ního rozhraní Microsoft VSAPI 2.0/2.5. Pokud se chcete blíže informovat o tomto rozhraní, následujte tyto odkazy:

- <http://support.microsoft.com/default.aspx?scid=kb;en-us:328841&Product=exch2k> – popis princip spolupráce Exchange s antivirovými programy
- <http://support.microsoft.com/default.aspx?scid=kb;en-us:823166> – informace o dopl cích ve VSAPI 2.5 v aplikaci Exchange 2003 Server

Sou ástí nastavení jsou také tyto podpoložky ve stromové struktu e:

- [**Akce nad nálezy**](#)
- [**Filtrování e-mail**](#)

5.3. Akce nad nálezy



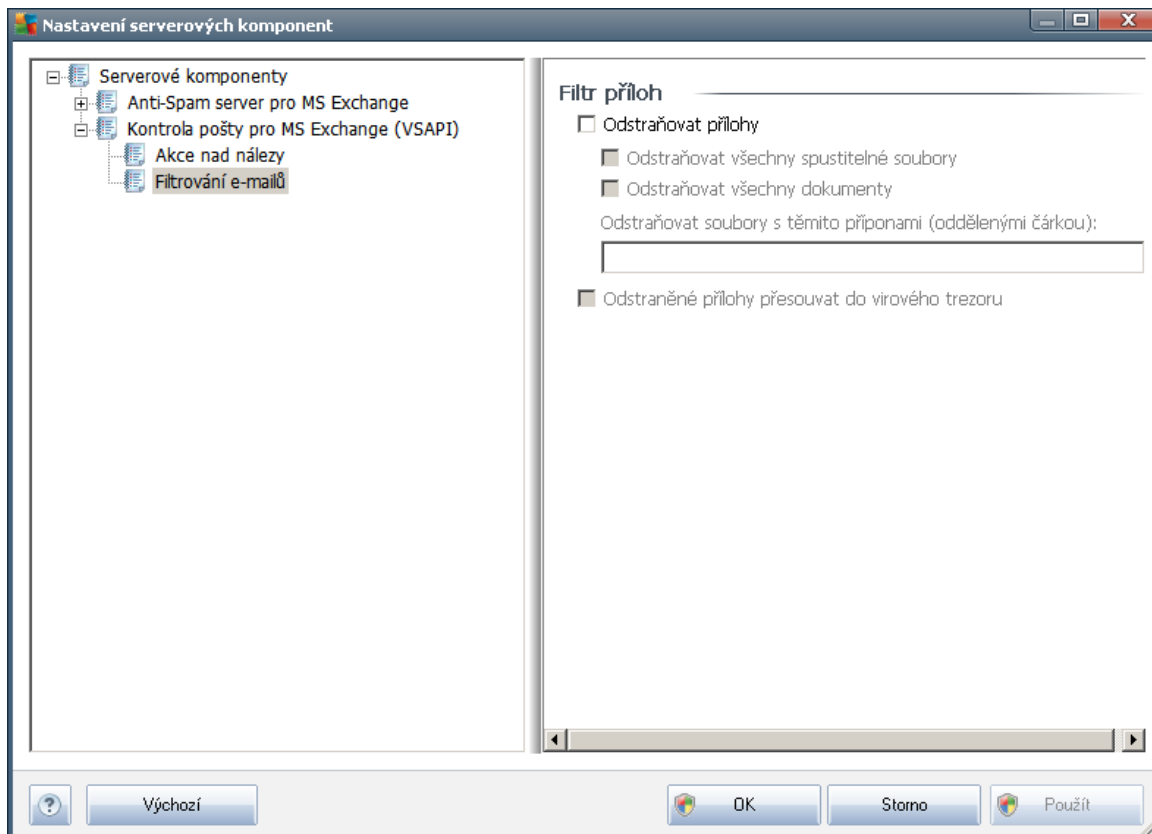
V části **Akce nad nálezy** lze zaškrtnout a vybrat automatické akce, které mají být provedeny při běhu testování. Akce jsou k dispozici pro následující položky:

- **Infekce**
- **PUP (Potenciálně nežádoucí programy)**
- **Varování**
- **Informace**

Z rolovací nabídky zvolte pro každou položku vždy jednu akci:

- **Žádná** - nebude provedena žádná akce.
- **Přesunout do trezoru** - dané nebezpečí bude přesunuto do Virového trezoru.
- **Odstranit** - dané nebezpečí bude odstraněno.

5.4. Filtrování e-mailů



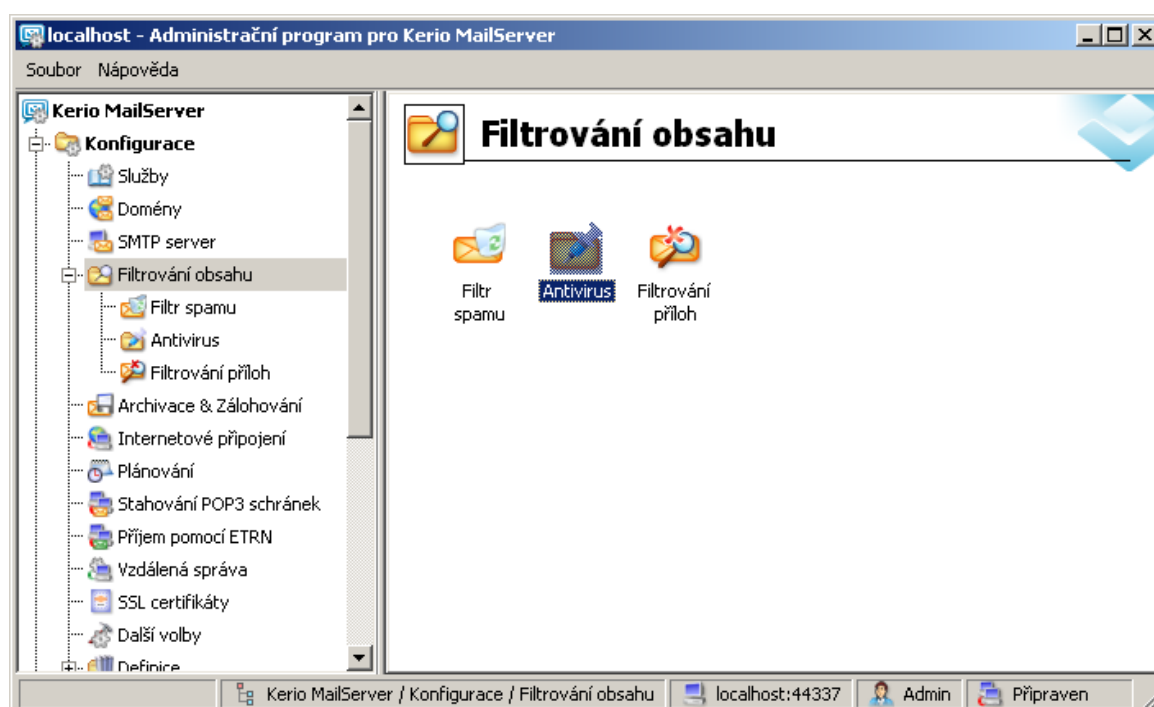
V části **Filtr příloh** můžete zvolit přílohy, které mají být automaticky odstraněny. K dispozici jsou následující možnosti:

- **Odstraňovat přílohy** - zaškrtněte pro povolení této funkce.
- **Odstraňovat všechny spustitelné soubory** - odstraní všechny spustitelné přílohy.
- **Odstraňovat všechny dokumenty** - odstraní všechny dokumenty v příloze.
- **Odstraňovat soubory s těmito příponami (oddělenými čárkou)** - můžete přípony, které si přejete automaticky odstranit. Hodnoty oddělte čárkou.
- **Odstraněné přílohy přesouvat do virového trezoru** - zaškrtněte, pokud nechcete, aby byly filtrované přílohy odstraněny rovnou. Je-li toto políčko zaškrtnuté, budou všechny přílohy zvolené prostřednictvím tohoto dialogu automaticky přesouvány do karanténního prostředí Virového trezoru. Jedná se o bezpečné místo pro ukládání potenciálně škodlivých souborů - můžete k nim přistupovat a zkoumat je, aniž by mohly ohrozit váš systém. Do Virového trezoru se dostanete z hlavní obrazovky aplikace **AVG Email Server 2011**. V horní nabídce klikněte levým tlačítkem myši na položku **Historie** a následně z kontextového menu zvolte **Virový trezor**.

6. AVG pro Kerio MailServer

6.1. Konfigurace

Mechanismus antivirové ochrany je integrován přímo v aplikaci **Kerio MailServer**. Abyste aktivovali antivirovou ochranu **Kerio MailServeru** pomocí testovacího jádra AVG, spus te administrací konzoli programu Kerio. V navigační struktuře na levé straně okna této aplikace zvolte položku **Filtrování obsahu** ve vlně **Konfigurace**.



Na hlavním panelu aplikace se zobrazí dialogové okno **Filtrování obsahu**. V rámci tohoto okna je možné volit ze tří nabídek:

- **Filtr spamu**
- **Antivirus**
- **Filtrování příloh**

6.1.1. Antivirus

Na této záložce můžete zapnout nebo vypnout antivirovou kontrolu pomocí **AVG pro Kerio MailServer**. Pro aktivaci aplikace zvolte položku **Použít externí antivirový program** a vyberte možnost **AVG E-mail Server** z menu externího softwaru:



Antiviry

Použít integrovaný antivirový modul McAfee®

Použít externí antivirový program AVG Email Server Edition Volby

V následující části můžete specifikovat pravidla pro akce provedené v rámci detekce infikované zprávy nebo filtrování příloh:

Je-li ve zprávě nalezen virus

Zahodit zprávu

Doručit zprávu bez viru (resp. bez přílohy obsahující virus)

Přeposlat originální zprávu (včetně virů) správci na adresu:

Přeposlat filtrovanou zprávu správci na adresu:

Umožňuje definovat akce provedené při detekci viru nebo v rámci procesu filtrování příloh:

- **Zahodit zprávu** – pokud je tato možnost zvolena, infikovaná/filtrovaná zpráva je zamítnuta.
- **Doručit zprávu bez viru** – pokud je tato možnost vybrána, infikovaná/filtrovaná zpráva bude zbavena přílohy a doručena adresátovi.
- **Přeposlat originální zprávu (včetně virů) správci na adresu** – zapnutí/vypnutí možnosti přeposílání infikovaných zpráv na adresu zadanou v příslušném textovém poli.
- **Přeposlat filtrovanou zprávu správci na adresu** – zapnutí/vypnutí možnosti přeposílání filtrovaných (bez přílohy) zpráv na adresu zadanou v příslušném textovém poli.

Nemůže-li být některá příloha zkontrolována (např. šifrovaný nebo poškozený soubor)

Doručit zprávu s varováním

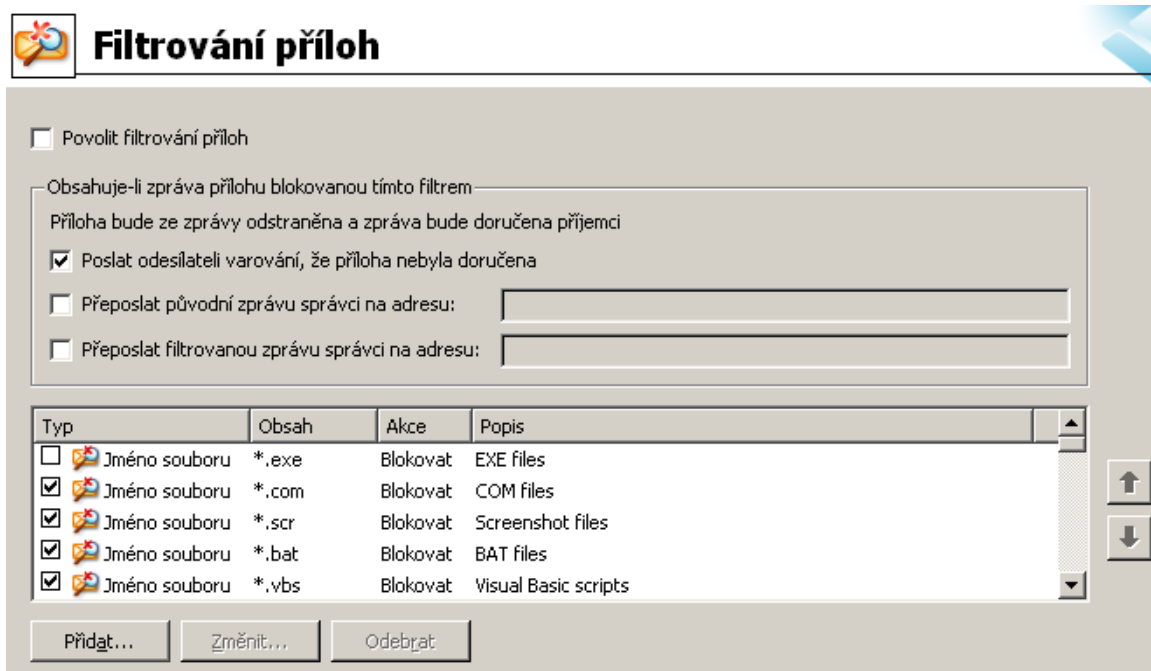
Odmítnout zprávu - považovat tuto přílohu za virus (použije se nastavení výše)

Umožňuje specifikovat akce pro soubory příloh, které nemohou být z jakéhokoli důvodu přetestovány:

- **Doručit zprávu s varováním** – zpráva (včetně přílohy) bude doručena nezkontrolovaná. Ke zprávě bude připojeno varování a uživatel bude upozorněn na to, že zpráva nebylo možno zkontrolovat, a že může obsahovat viry.
- **Odmítnout zprávu** – se zprávou bude naloženo, jako by příloha byla infikována.

6.1.2. Filtrování příloh

V nabídce *Filtrování p íloh* je seznam s definicemi p íloh pro jejich filtrování:



Filtr p íloh lze zapnout nebo vypnout pomocí položky **Povolit filtrování p íloh**. Volitelně lze upravit také následující nastavení:

- **Poslat odesílateli varování, že p íloha nebyla doručena** - odesílateli bude **Kerio Mailserverem** zasláno varování, že odeslal zprávu s infikovanou nebo nepovolenou p ílohou.
- **Přeposlat původní zprávu správci na adresu** - zpráva bude přeposlána v původním tvaru, tedy i s infikovanou nebo zakázanou p ílohou, na zadanou emailovou adresu. Nezáleží na tom, zda bude uvedena lokální nebo externí adresa.
- **Přeposlat filtrovanou zprávu správci na adresu** - zpráva bez infikované nebo zakázané p ílohy bude, kromě níže vybraných akcí, také přeposlána na zadanou emailovou adresu. Toho lze využít například pro ověření správné funkce antivirové kontroly a filtru p íloh.

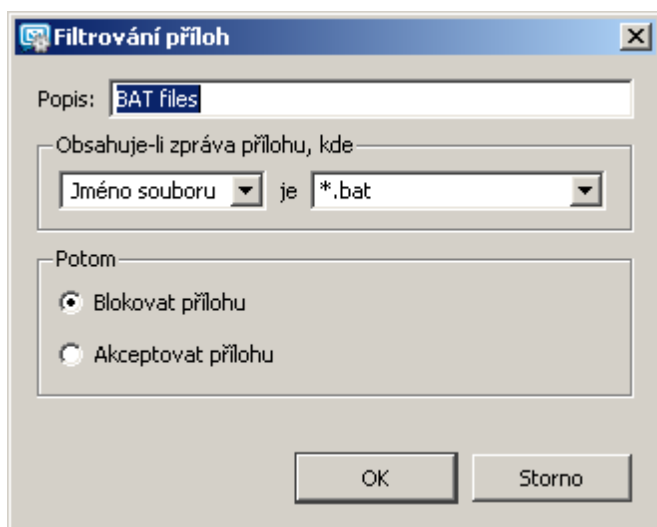
V seznamu p íloh/p íloh jsou u každého prvku obsažena tři pole:

- **Typ** – specifikace druhu p ílohy dané p íponou zadanou v poli **Obsah**. Možné typy jsou *Jméno souboru* nebo *MIME typ*. V příslušném poli můžete také zahrnout/vyloučit daný typ p ílohy do/z filtru.
- **Obsah** – zde můžete definovat p íponu filtrovaných p íloh. Pro zápis lze využít zástupné znaky operačního systému (*například `*.doc.*` pro jakýkoli soubor s p íponou `.doc` a libovolnou další za ním*).
- **Akce** – definice akce, která má být provedena s danou p ílohou. Možné akce jsou **Akceptovat** (příjmout p ílohu) a **Blokovat** (bude provedena akce definovaná nad seznamem

zakázaných příloh).

- **Popis** – krátký popis dané přílohy.

Položka seznamu může být odstraněna pomocí tlačítka **Odebrat**. Při přidání položky je možné po stisknutí tlačítka **Přidat...** Stejně tak lze editovat existující záznam po stisknutí tlačítka **Změnit...** Objeví se toto okno:



- V poli **Popis** zadejte krátký popis druhu dané přílohy.
- V poli **Obsahuje-li zpráva přílohu, kde** můžete vybrat typ přílohy (*Jméno souboru* nebo *MIME typ*). V dalším poli také můžete zvolit příponu z připravené nabídky, nebo zadat příponu vlastní.

V poli **Potom** můžete rozhodnout, zda danou přílohu blokovat nebo přijmout.

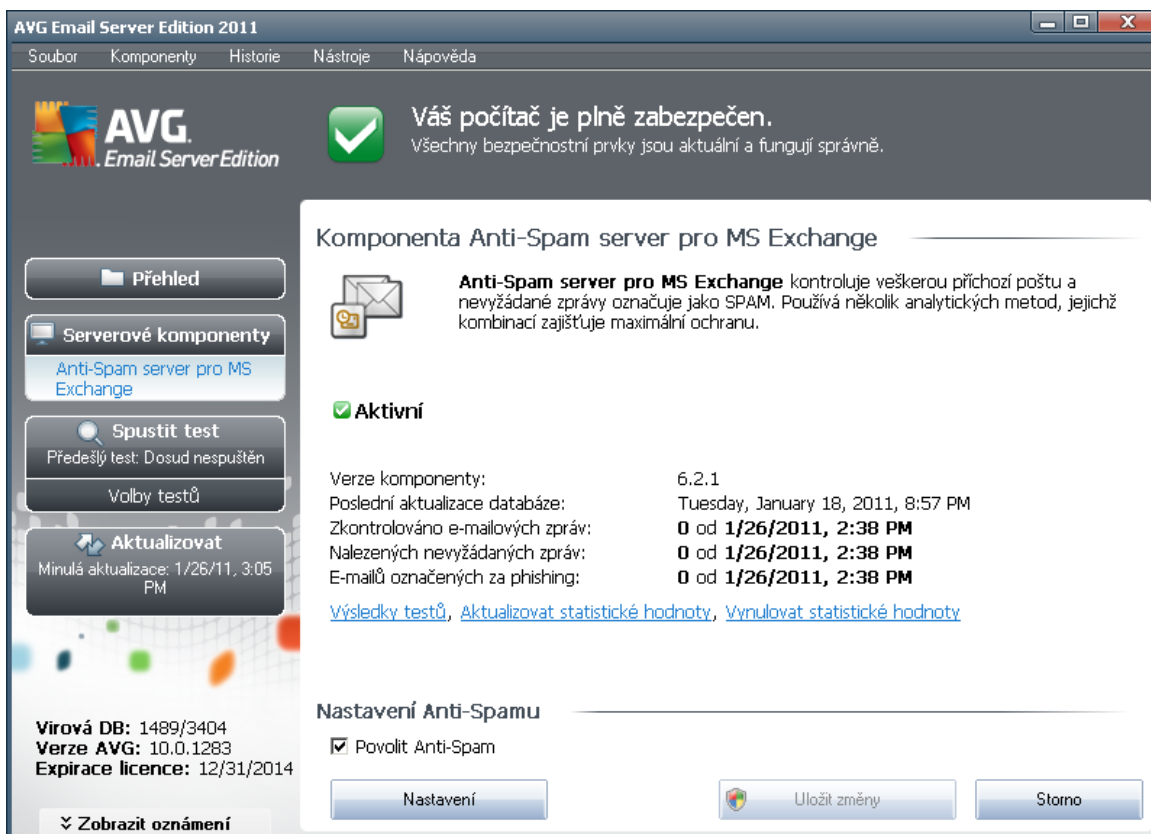
7. Nastavení komponenty Anti-Spam

7.1. Anti-Spam princip

Termínem *spam* označujeme nevyžádanou elektronickou poštu, převážně reklamního charakteru, jež je jednorázově hromadně rozesílána obrovskému počtu adresátů, čímž zahlcuje jejich poštovní schránky. Termín *spam* se nevztahuje na oprávněný e-mail komerčního charakteru, k jehož přijetí dal zákazník svůj souhlas. Spam je nejen nepříjemný a obtížný, ale je také hlavním zdrojem virů nebo distributorem textu urážlivého charakteru.

Komponenta **Anti-Spam** kontroluje veškerou příchozí poštu a nežádoucí zprávy označuje jako *spam*. K detekci spamu v jednotlivých zprávách používá několik analytických metod a zaručuje tedy maximální úroveň ochrany proti nevyžádané poště.

7.2. Anti-Spam rozhraní

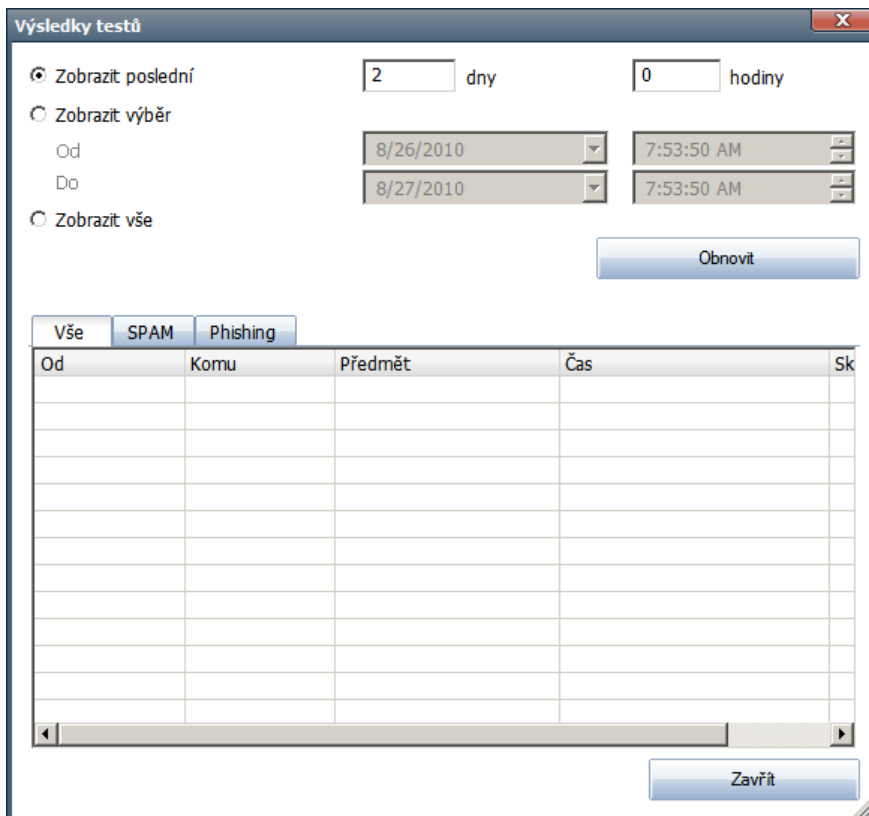


The screenshot shows the AVG Email Server Edition 2011 interface. At the top, there is a menu bar with 'Soubor', 'Komponenty', 'Historie', 'Nástroje', and 'Nápověda'. Below the menu, there is a status bar indicating 'Váš počítač je plně zabezpečen.' (Your computer is fully secured). The main content area is titled 'Komponenta Anti-Spam server pro MS Exchange'. It includes a description of the component, a status indicator 'Aktivní' (Active), and a table of test results. The table shows the version (6.2.1), the last database update (Tuesday, January 18, 2011, 8:57 PM), and the results of three tests: 'Zkontrolováno e-mailových zpráv' (Checked emails), 'Nalezených nevyžádaných zpráv' (Found unwanted emails), and 'E-mailů označených za phishing' (Emails marked as phishing), all showing '0' results from 1/26/2011, 2:38 PM. There are also links for 'Výsledky testů', 'Aktualizovat statistické hodnoty', and 'Vynulovat statistické hodnoty'. At the bottom, there is a 'Nastavení Anti-Spamu' section with a checkbox for 'Povolit Anti-Spam' (checked) and buttons for 'Nastavení', 'Uložit změny', and 'Storno'. On the left side, there are buttons for 'Přehled', 'Serverové komponenty', 'Spustit test', 'Aktualizovat', and 'Zobrazit oznámení'.

V dialogu komponenty Anti-Spam server pro MS Exchange jsou dostupné následující ovládací prvky:

- **Výsledek test**

Otevře nový dialog s přehledem výsledků testů:



Od	Komu	Předmět	Čas	Sk

Zde můžete zkontrolovat zprávy označené buď jako SPAM (nevyžádaná pošta) nebo pokus o Phishing (získání osobních údajů, identity, bankovních údajů atp.).

Ve výchozím nastavení jsou zobrazeny pouze výsledky za poslední dva dny. Interval pro zobrazení můžete změnit tímto volbami:

- **Zobrazit poslední** - vložte preferovaný počet dní a hodin.
- **Zobrazit výběr** - zvolte libovolný časový a datumový rozsah.
- **Zobrazit vše** - zobrazí výsledky za celé období.

Tlačítkem **Obnovit** znovu načítáte výsledky testů.

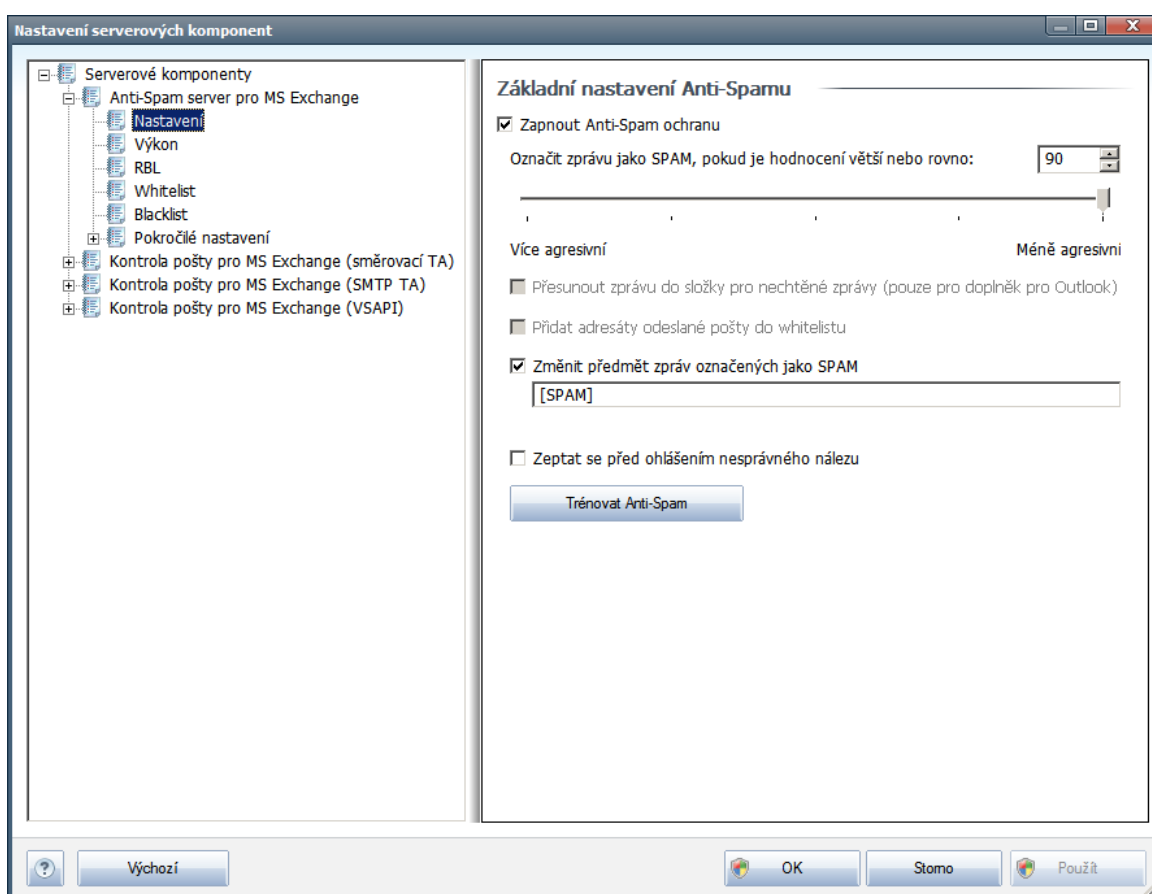
- **Aktualizovat statistické hodnoty** - aktualizuje statistiky uvedené v dialogu.
- **Vynulovat statistické hodnoty** - vynuluje všechny statistiky.

Sekce **Nastavení Anti-Spamu** obsahuje jediné zaškrtnací políčko **Povolit Anti-Spam**. Zrušením jeho zaškrtnutí vypnete antispamovou ochranu vašeho počítače (deaktivujete celou komponentu). Pro její opětovné zapnutí použijte buď toto opět zaškrtnací políčko v tomto dialogu, anebo obdobné políčko v [nastavení komponenty Anti-Spam](#).

V rozhraní jsou k dispozici tato ovládací tlačítka:

- **Nastavení** - otevře [nastavení komponenty Anti-Spam](#).
- **Zpět** - vrátí vás do výchozího uživatelského rozhraní AVG (přehled serverových komponent).

7.3. Anti-Spam nastavení



V dialogu **Základní nastavení Anti-Spamu** můžete označením položky **Zapnout Anti-Spam ochranu** celkově povolit i zakázat funkci komponenty **Anti-Spam**.

V tomto dialogu také můžete definovat, jak chcete nastavit úroveň ochrany proti spamu - více i méně agresivní. Na základě několika dynamických testovacích technik pak filtr komponenty **Anti-Spam** přiřadí každé zprávě určitou skóre (například podle toho, nakolik se obsah zprávy blíží textu, který lze považovat za spam). Hodnotu úrovně citlivosti pro označení spamu lze nastavit buď pomocí vepsání číselné hodnoty (50 až 90) do příslušného pole nebo pomocí posuvníku.

Přehled úrovní ochrany, jež odpovídají jednotlivým hodnotám:

- **Hodnota 90** - Většina příchozí pošty bude normálně doručena, aniž by byla označena jako



[spam](#). Snadno identifikovatelný [spam](#) bude odfiltrován, ale poměrně velká část spamových zpráv se přesto do vaší schránky dostane.

- **Hodnota 80-89** - E-mailové zprávy, u nichž se dá předpokládat charakter [spamu](#), budou odfiltrovány. Je možné, že omylem dojde i k odfiltrování některých zpráv, jež nejsou spamového charakteru.
- **Hodnota 60-79** - Toto nastavení je již považováno za poměrně agresivní konfiguraci. E-mailové zprávy, které mohou být považovány za [spam](#), budou odfiltrovány. Současně však dojde k poměrně velkému odchytu zpráv, které nejsou spamového charakteru, ale na základě určitých znaků mohou být takto vyhodnoceny.
- **Hodnota 50-59** - Velmi agresivní konfigurace. Nespamové e-mailové zprávy budou ve většině případů odfiltrovány spolu se zprávami pozitivně detekovanými jako [spam](#). **Tato konfigurace už není doporučena pro běžné uživatele.**

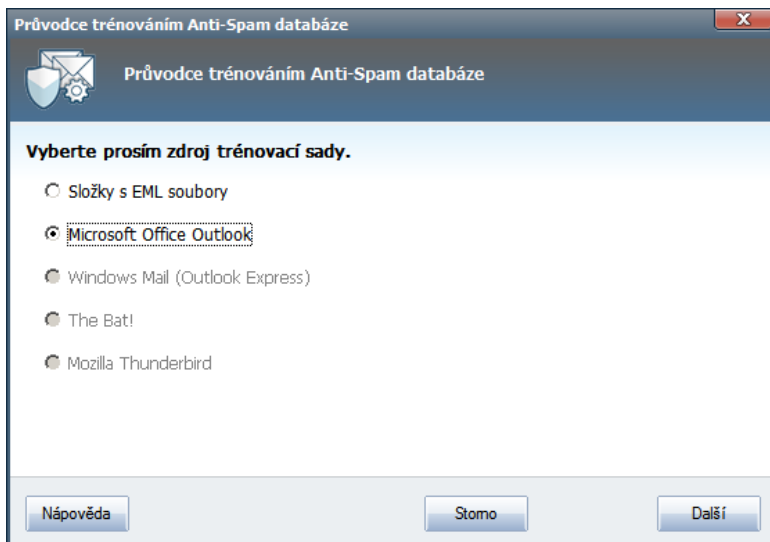
V dialogovém okně můžete dále nastavit, jak se má zacházet s e-mailovými zprávami pozitivně detekovanými jako [spam](#):

- **Změnit předem nastavení zprávy u zpráv označených jako spam** - označením této položky zvolíte aktivujete textové pole, v němž máte možnost editovat text, kterým si přejete označovat zprávy detekované jako [spam](#) - tento text pak bude automaticky vepsán do předem nastavení každé detekované e-mailové zprávy.
- **Zeptat se před ohlášením nesprávného nálezu** - pokud jste během instalace potvrdili svou účast v Programu zlepšování produktu (program slouží ke shromáždění nejnovějších informací o výřech, spywaru i škodlivých webových stránkách a vylepšování ochrany pro všechny naše uživatele), povolili jste odesílání reportů o detekovaných hrozbách do AVG. Tato hlášení jsou odesílána automaticky. Pokud si však přejete mít možnost zkontrolovat, že detekovaná zpráva má být skutečně klasifikována jako spam, označte položku Zeptat se před ohlášením nesprávného dotazu a před odesláním reportu vám bude zobrazen dotazovací dialog vyžadující vaše potvrzení.

Tlačítko **Trénovat Anti-Spam** otevírá [Průvodce trénováním Anti-Spam databáze](#). Popis jednotlivých kroků průvodce najdete v [samostatné kapitole](#).

7.3.1. Průvodce trénováním Anti-Spam databáze

V prvním dialogovém okně **Průvodce trénováním Anti-Spam databáze** je nutno vybrat zdroj e-mailových zpráv, které chcete pro trénink použít. K trénování se obvykle používají zprávy, které byly anti-spamovou ochranou mylně označeny jako spam, nebo naopak nevyžádané zprávy, které prošly anti-spamovou ochranou bez povšimnutí.



Na výběr jsou následující možnosti:

- **Konkrétní e-mailový program** - pokud používáte některý z uvedených e-mailových programů (*MS Outlook, Outlook Express, The Bat!, Mozilla*), jednoduše vyberte příslušnou možnost.
- **Složky s EML soubory** - používáte-li jiný e-mailový program, než které jsou v dialogu uvedeny, pak je vhodné nejdříve požadované zprávy uložit do nějakého adresáře na disk (ve formátu *.eml*), nebo se ujistit, že víte, kam váš e-mailový program zprávy ukládá. Poté zvolte možnost **Složky s EML soubory**, v dalším kroku budete moci zadat umístění těchto složek.

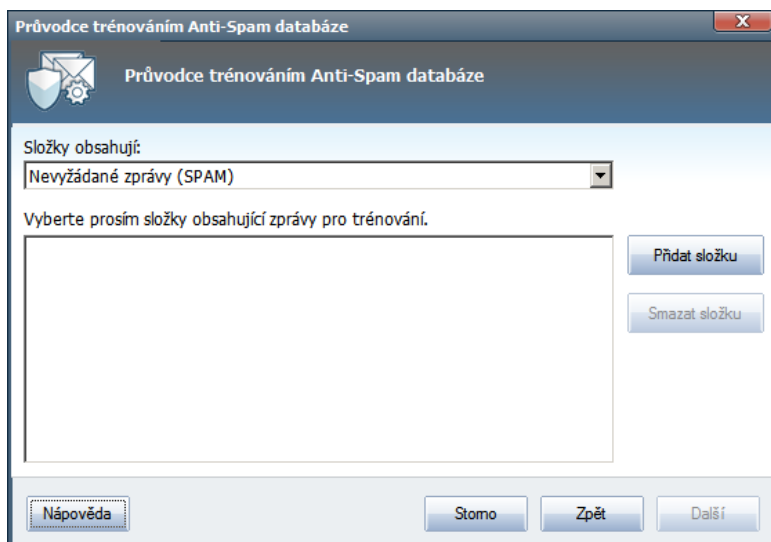
Chcete-li průběh trénování co nejvíce urychlit a zjednodušit, doporučujeme e-mailové zprávy dopředu vytřídit tak, aby ve zvolené složce byly umístěny pouze ty zprávy, které chcete použít pro trénink - žádané a nevyžádané zvlášť. Nicméně není to nutné, protože před zahájením samotného trénování budete mít možnost zprávy filtrovat.

Jakmile je zvolena požadovaná možnost, stiskněte tlačítko **Následující** a přejděte k dalšímu kroku.

7.3.2. Výběr složky se zprávami

Zobrazení dialogu v tomto kroku průvodce závisí na vaší předchozí volbě.

Volba složky s EML soubory



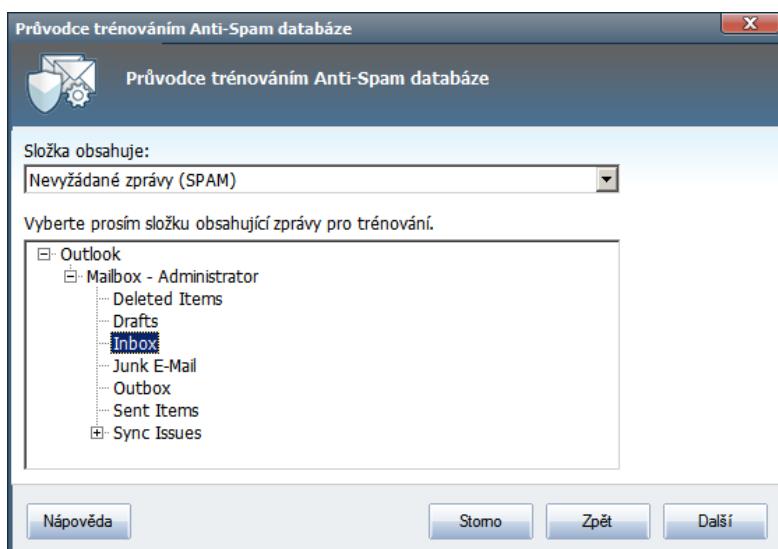
V tomto dialogu volíte složku se zprávami, které chcete pro trénování použít. Stisknete tlačítko **Přidat složku** a určete umístění adresářových souborů (uloženými e-maily). Cesta k vybranému adresáři pak bude zobrazena v dialogu. Pro odebrání složky ze seznamu použijte tlačítko **Smazat složku** po jejím označení.

V rozbalovací nabídce **Složka obsahuje** zadejte, jaké zprávy se ve vybrané složce nacházejí - zda vyžádané (tzv. *HAM*), nebo nevyžádané (*SPAM*). V dalším dialogu budete moci zprávy ve složce filtrovat, takže složka nemusí obsahovat pouze e-maily určené k trénování.

Chcete-li pokračovat, stisknete tlačítko **Následující** a pokračujete k části [Způsob filtrování zpráv](#).

Volba konkrétního e-mailového programu

Pokud jste vybrali kterýkoli e-mailový program, zobrazí se nový dialog se složkami.





Poznámka: V případě Microsoft Office Outlook bude nejprve potřeba zvolit MS Office Outlook profil.

V rozbalovací nabídce **Složka obsahuje** zadejte, jaké zprávy se ve vybrané složce nacházejí - zda vyžádané (tzv. *HAM*), nebo nevyžádané (*SPAM*). V dalším dialogu budete moci zprávy ve složce filtrovat, takže složka nemusí obsahovat pouze e-maily určené k trénování. V hlavní sekci dialogu je zobrazen navigační strom příslušného e-mailového programu. Vyberte složku obsahující e-maily k trénování a označte ji.

Stiskem tlačítka **Následující** pokračujte k části [Způsob filtrování zpráv](#).

7.3.3. Způsob filtrování zpráv

V tomto dialogu můžete zvolit možnosti filtrování zpráv ve vybrané složce:

Jste-li si jisti, že složka obsahuje pouze zprávy, které chcete použít k trénování, a žádné další, zvolte možnost **Všechny zprávy (nepoužít filtr)**.

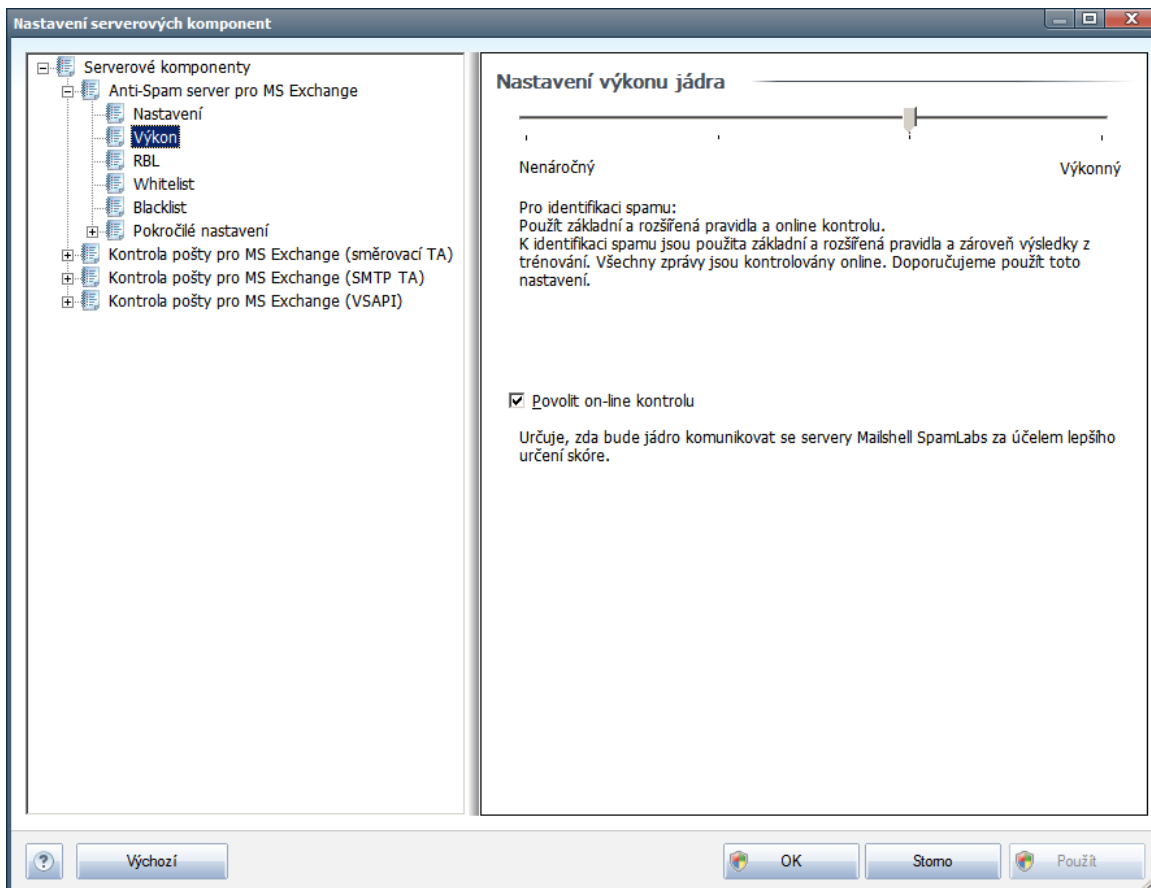
Pokud si nejste jisti, jaké zprávy složka obsahuje, a chcete, aby se průvodce u každé z nich zeptal, zda ji chcete nebo nechcete použít k trénování, pak zvolte možnost **Dotazovat se na každou zprávu**.

Chcete-li zprávy filtrovat pokračujte s **Způsobem filtrování**, zvolte položku **Použít filtr**. Do textových polí můžete pak můžete doplnit slovo (jméno), část slova nebo více slov, která se mají vyhledávat v polích "Odesílatel" a "Předmět" v hlavičce zprávy. Všechny e-maily, které budou tímto kritériím přesně vyhovovat, budou bez dalších dotazů použity k trénování.

Pozor: Vyplníte-li obě textová pole (Předmět obsahuje: a Od obsahuje:), budou k trénování použity i zprávy, které vyhoví jen jedné z obou podmínek!

Jakmile máte vybránu příslušnou možnost filtrování, stiskněte tlačítko **Následující**. V následujícím informativním dialogu potvrdíte svou volbu opět tlačítkem **Následující**. Poté bude zahájeno trénování zpráv podle zvolených kritérií.

7.4. Výkon



Dialog **Nastavení výkonu jádra** (odkazovaný položkou **Výkon**) nabízí možnost konfigurace parametru výkonu komponenty **Anti-Spam**. Polohou posuvníku určete úroveň testovacího výkonu na ose **Nenáročný** / **Výkonný** režim.

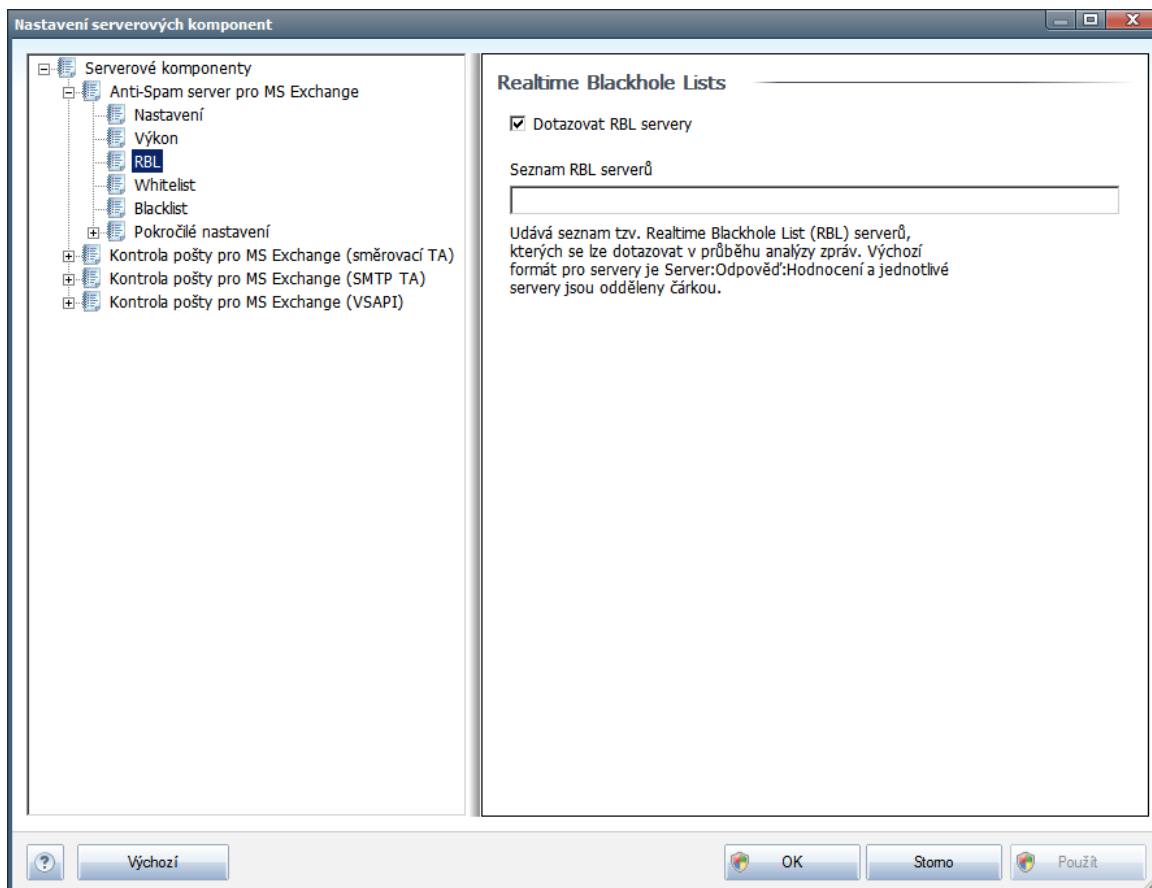
- **Výkonný režim** spotřebuje velký objem paměti. Během testovacího procesu budou k identifikaci [spamu](#) použity následující parametry: pravidla a spamové databáze, základní a pokročilá nastavení, IP adresy spammerů a spamové databáze.
- **Nenáročný režim** znamená, že během testovacího procesu nebudou k identifikaci [spamu](#) použita žádná pravidla. Identifikace [spamu](#) bude založena výhradně na porovnání s testovacími daty. Tento režim pro běžné používání nedoporučujeme, nastavení lze doporučit výhradně u počítačů s velmi nízkou úrovní hardwarového vybavení.

Položka **Povolit on-line kontrolu** je ve výchozím nastavení označena a určuje, že pro přesnější detekci [spamu](#) bude k testování použita i komunikace se servery společnosti [Mailshell](#), a během testování budou testovaná data porovnávána s databází této společnosti v online režimu.

Obecně doporučujeme podržet výchozí nastavení, pokud nemáte skutečný důvod pro tuto konfiguraci. Změnu parametru nastavení výkonu jádra lze doporučit výhradně znalým a zkušeným uživatelům!

7.5. RBL

Položka **RBL** otevírá editační dialog **Realtime Blackhole Lists**.



V tomto dialogu máte možnost povolit funkci **Dotazovat RBL servery**.

RBL (*Realtime Blackhole List*) server je DNS server s rozsáhlou databází známých odesílatelů **spamu**. Při zapnutí této funkce budou všechny příchozí zprávy v reálném čase porovnávány s RBL databází a při nalezení shody označeny jako **spam**.

Databáze RBL serverů obsahují skutečně nejnovější a nejaktuálnější záznamy o existujících centrech **spamu** a díky porovnávání e-mailových zpráv proti těmto databázím lze dosáhnout maximální úrovně ochrany před nevyžádanou poštou. Tato vlastnost se hodí zejména pro uživatele, kteří dostávají velké množství spamových zpráv, jež nemohou být detekovány pouze na základě pravidel definovaných jádrem komponenty Anti-Spam.

Položka **Seznam RBL serverů** vám dále umožní nastavit adresy konkrétních serverů, na nichž jsou tyto spamové databáze umístěny. Ve výchozím nastavení budou zprávy kontrolovány proti databázím na dvou RBL serverech. Doporučujeme ponechat toto nastavení, pokud nemáte skutečný důvod jej změnit - editace konfigurace RBL je vhodná jen pro skutečně znalé uživatele!

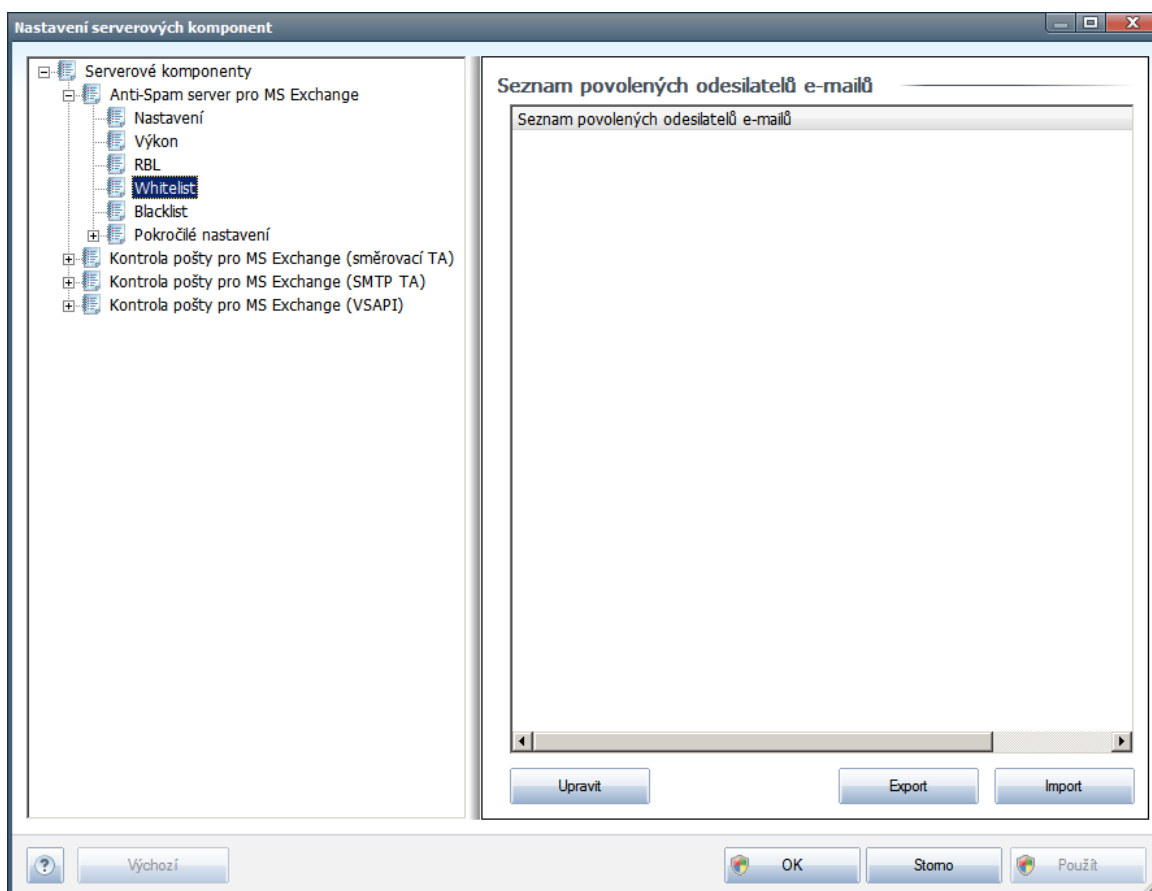
Poznámka: Zapnutí této služby může na některých operačních systémech a konfiguracích zpomalit

proces p íjmu pošty, protože každá jednotlivá zpráva musí být prov ěna proti databázi RBL serveru.

Touto službou nedochází k odesílání žádných osobních nebo citlivých dat!

7.6. Whitelist

Položka **Whitelist** otevírá dialog se seznamem emailových adres a doménových jmen, u nichž víte, že pošta z těchto adres/domén doručena nikdy nebude mít charakter [spamu](#):



V editačním rozhraní máte možnost sestavit seznam odesílatelů, u nichž předpokládáte, že vám nikdy nepošlou poštu, kterou lze považovat za [spam](#) (nevyžádanou poštu). Můžete také sestavit seznam kompletních doménových jmen (například [avg.com](#)), o nichž víte, že negenerují nevyžádanou poštu.

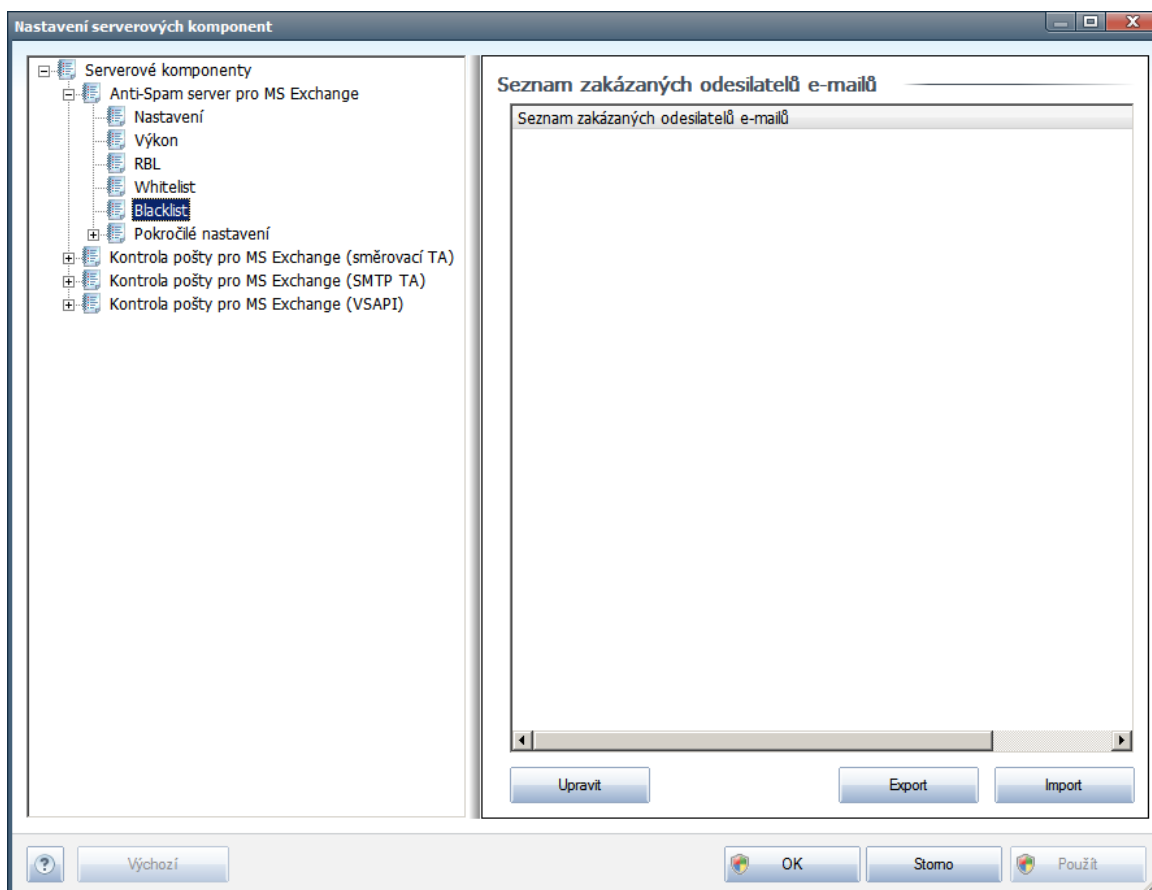
Jakmile budete mít připraven tento seznam adres a domén, můžete je zadat do **Whitelistu** dvěma způsoby: pomocí vložením jednotlivých adres nebo jednorázovým importem celého seznamu. K dispozici jsou vám tato ovládací tlačítka:

- **Upravit** - stiskem tohoto tlačítka otevřete dialog, v němž můžete manuálně přidávat adresy ze seznamu (můžete také použít jednorázovou metodu "kopírovat a vložit"). Adresy/doménová jména vkládejte po jednom na každý řádek.

- **Import** - pokud již máte seznam adres/doménových jmen uložený v textovém souboru, můžete jej snadno importovat za použití tohoto tlačítka. Import lze provést buď z textového souboru (musí být ve formátu prostého textu a obsah musí být rozdělen tak, že každý řádek obsahuje pouze jedinou položku - adresu nebo doménové jméno), z WAB souboru přímo z adresáře Windows nebo Microsoft Office Outlooku.
- **Export** - pokud budete z libovolného důvodu chtít seznam adres/doménových jmen exportovat, můžete export provést pomocí tohoto tlačítka. Veškeré záznamy budou uloženy ve formátu prostého textu.

7.7. Blacklist

Položka **Blacklist** otevírá dialog se seznamem emailových adres a doménových jmen, která mají být zablokována pro příjem jakékoliv pošty. To znamená, že pošta odeslaná z kterékoliv uvedené adresy nebo domény bude vždy označena jako [spam](#):



V editačním rozhraní máte možnost sestavit seznam odesílatelů, u nichž předpokládáte, že poštu, kterou vám posílají, lze považovat za [spam](#) (nevyžádaná pošta). Můžete také sestavit seznam kompletních doménových jmen (například *spammingcompany.com*), u nichž je předpoklad, že budou generovat nevyžádanou poštu. Pošta odeslaná z kterékoliv uvedené adresy bude pak detekována jako [spam](#).



Jakmile budete mít připraven tento seznam adres a domén, můžete je zadat do **Blacklistu** dvěma způsoby: pomocí vložením jednotlivých adres nebo jednorázovým importem celého seznamu. K dispozici jsou vám tato ovládací tlačítka:

- **Upravit** - stiskem tohoto tlačítka otevřete dialog, v němž můžete manuálně přidávat adresy ze seznamu (můžete také použít jednorázovou metodu "kopírovat a vložit"). Adresy/doménová jména vkládejte po jednom na každý řádek.
- **Import** - existující e-mail adresy můžete snadno importovat za použití tohoto tlačítka. Import lze provést buď z textového souboru (musí být ve formátu prostého textu a obsah musí být rozdelen tak, že každý řádek obsahuje pouze jednu položku - adresu nebo doménové jméno), z WAB souboru přímo z adresáře Windows nebo Microsoft Office Outlooku.
- **Export** - pokud budete z libovolného důvodu chtít seznam adres/doménových jmen exportovat, můžete export provést pomocí tohoto tlačítka. Veškeré záznamy budou uloženy ve formátu prostého textu.

7.8. Pokročilé nastavení

Obecně doporučujeme podržet výchozí nastavení, pokud nemáte skutečný důvod pro tuto konfiguraci změnit. Změnu parametrů nastavení výkonu jádra lze doporučit výhradně znalým a zkušeným uživatelům!

Pokud se přesto domníváte, že je nutné změnit konfiguraci komponenty Anti-Spam na úrovni vysoce pokročilého nastavení, pokračujte prosím podle instrukcí uvedených přímo v uživatelském rozhraní. Obecně platí, že v každém dialogu máte možnost zapnout jednu konkrétní funkci komponenty Anti-Spam a její popis je uveden přímo v dialogu:

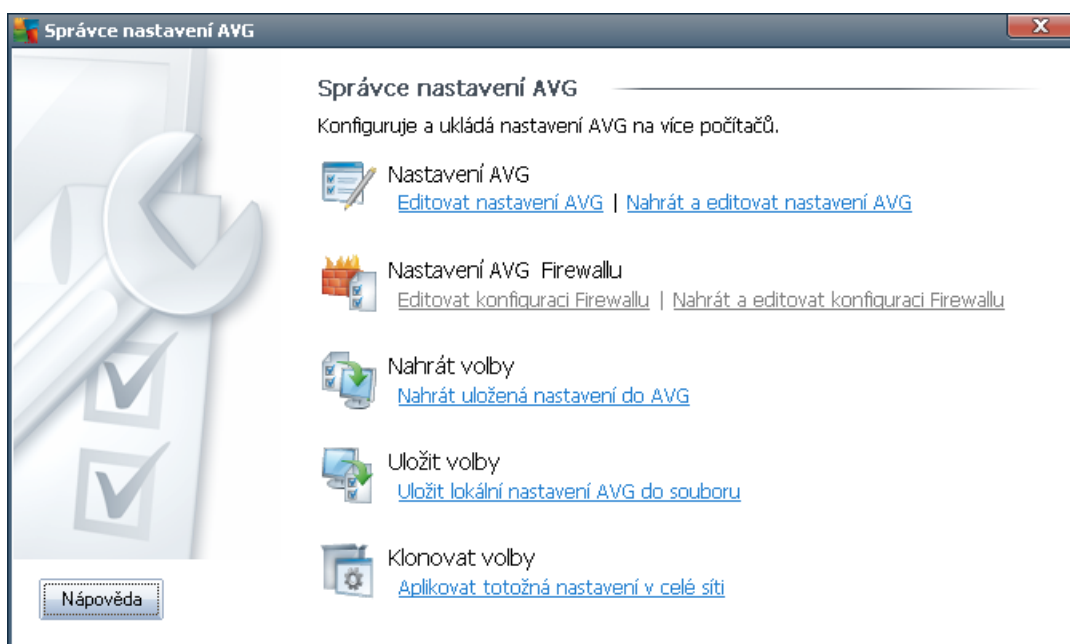
- **Paměť** - fingerprint, reputace domén, LegitRepute
- **Trénování** - počet slovních záznamů, práh pro samotrénování, váha
- **Filtrování** - seznam jazyků, seznam zemí, povolené IP adresy, blokové IP adresy, blokové země, blokové znakové sady, falešní odesílatelé
- **RBL** - RBL servery, multidetekce, práh, časový limit, maximum IP adres
- **Internetové připojení** - časový limit, ...

8. Manažer nastavení AVG

Manažer nastavení AVG je nástroj určený zejména pro menší síť. Umožňuje kopírovat, upravovat a distribuovat konfiguraci AVG, kterou lze následně uložit na přenosné médium (např. USB flash disk) a aplikovat ručně na vybrané stanice.

Tento nástroj je volitelnou součástí instalace AVG a lze jej spustit z Windows nabídky Start skrze:

Všechny programy/AVG 2011/Manažer nastavení AVG



• Nastavení AVG

- **Editovat nastavení AVG** - otevře dialog pro změnu nastavení vaší lokální instalace AVG. Všechny změny provedené v tomto dialogu se projeví v lokální instalaci AVG.
- **Nahrát a editovat nastavení AVG** - pokud již máte k dispozici dříve uložený soubor s konfigurací AVG (.pck), použijte tento odkaz pro jeho otevření a následné úpravy. Otevře se otevírací dialog pro nastavení AVG a provedené změny budou po stisku tlačítka **OK** nebo **Použít**, uloženy do přenosného souboru.

• Nastavení AVG Firewallu

Tato sekce by vám umožnila provádět změny v nastavení Firewallu vaší lokální instalace AVG, popřípadě upravovat nastavení Firewallu v již připraveném souboru s konfigurací AVG (.pck). Protože však váš AVG Email Server 2011 nezahrnuje komponentu Firewall, jsou oba odkazy zobrazeny šedě a nejsou aktivní.

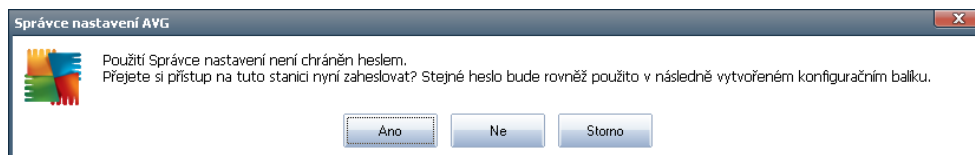
• Nahrát volby

- **Nahrát uložená nastavení do AVG** - tímto odkazem lze otevřít soubor s konfigurací AVG (.pck) a aplikovat jej na lokální instalaci AVG.



• Uložit volby

- **Uložit lokální nastavení AVG do souboru** - tento odkaz použijte k uložení konfigurace místní instalace AVG do souboru (.pck). Pokud jste nenastavili heslo pro Povolené akce, zobrazí se následující dialog:



Zvolte **Ano**, pokud si nyní přejete nastavit heslo pro přístup k Povoleným položkám. Tlačítkem **Ne** vytvoříte hesla nepískáte a budete moci pokračovat v uložení konfigurace do souboru.

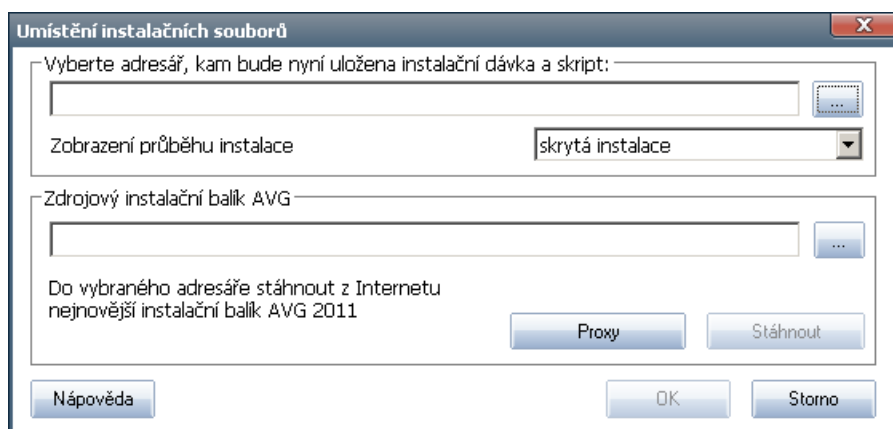
• Klonovat volby

- **Aplikovat totožná nastavení v celé síti** - tento odkaz umožní vytvořit instalační balík se stejným nastavením, jako má místní instalace AVG.

Proces klonování zahrnuje většinu nastavení AVG s výjimkou následujících položek:

- ✓ *Nastavení jazyka*
- ✓ *Nastavení zvuk*
- ✓ *Seznam povolených položek a PUP výjimky komponenty Identity protection*

Nejprve zvolte složku, do které si přejete instalovat skript uložit:



Z nabídky zvolte jednu z možností:

- ✓ *Skrytá instalace* - na stanici nebude aktuálně přihlášenému uživateli zobrazeno žádné informační okno týkající se procesu instalace.
- ✓ *Zobrazit průběh instalace* - instalace nebude vyžadovat žádnou interakci



uživatele, nicméně bude moci průběh instalace sledovat.

- ✓ *Zobrazit průvodce instalací* - instalace průvodce bude na stanici viditelný a aktuálně přihlášený uživatel bude muset potvrdit všechny kroky ručně.

Tlačítkem **Stáhnout** lze spustit stahování nejnovějšího instalačního balíku AVG přímo ze stránek výrobce do vybraného adresáře. Alternativně můžete do zvolené složky instalační balík nakopírovat ručně.

Pro nastavení proxy serveru pro připojení k síti zvolte tlačítko **Proxy** a vyplňte požadované údaje.

Kliknutím na tlačítko **OK** zahájíte proces klonování instalace. Po zahájení se vám může zobrazit odtáhnout dialog pro zadání hesla pro přístup k povoleným položkám (viz výše). Jakmile proces skončí, ve zvoleném adresáři by se vám měl nacházet mj. také soubor **AvgSetup.bat**. Spuštěním tohoto souboru dojde k instalaci AVG s vybraným nastavením.



9. FAQ a technická podpora

V případě problému s AVG se pokuste vyhledat řešení na webu [AVG \(http://www.avg.cz\)](http://www.avg.cz) v sekci **FAQ**.

Pokud na svůj dotaz nenajdete uspokojivou odpověď, obraťte se prosím na oddělení technické podpory AVG prostřednictvím kontaktního formuláře dostupného ze systémového menu volbou položky **Nápověda / Odborná pomoc online**.