avast! Distributed Network Manager (ADNM)

Příručka administrátora

alwil software

avast! Distributed Network Manager (ADNM): Příručka administrátora

Vydáno 21. března 2005 (Rev. 1.0.3)

Obsah

1

Základy

Vítejte v avast! Distributed Network Manager, jednom z nejmocnějších nástrojů pro síťovou antivirovou správu.

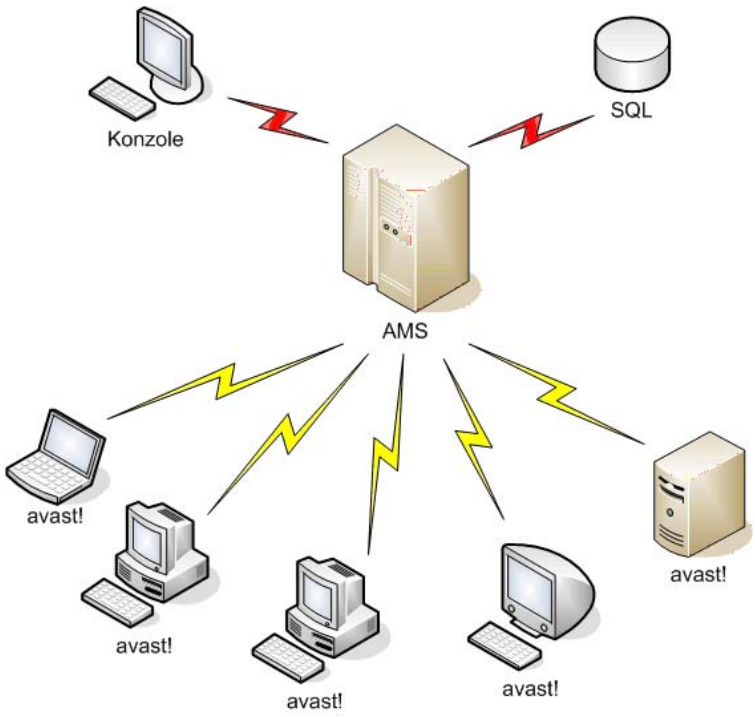
avast! Distributed Network Manager (ADNM) představuje sadu nástrojů vytvořených pro správu produktů avast! Antivirus v celé firmě.

Systém ADNM se skládá z těchto komponent:

- avast! Management Server (AMS) - srdce ADNM, které představuje základ celého systému.
- SQL Databáze - slouží jako úložiště dat pro všechna nastavení politiky, bezpečnostní nastavení a informace o klientech.
- Administrátorská konzole - program, který používají administrátoři pro správu celého systému.

Tyto tři komponenty spolupracují s produkty avast! Antivirus nasazenými na jednotlivých stanicích a serverech v síti, aby poskytly co možná nejlepší ochranu před škodlivými kódy a minimalizovaly úsilí vynakládané na jejich správu a dohled nad jejich momentálním stavem.

Mozkem celého systému je AMS (avast! Management Server).



Obrázek 1.1. Základní ADNM diagram

Spravované stroje se připojují k AMS, aby si stáhly poslední nastavení politik a reportovali svůj vlastní status a výsledky skenování. Rovněž tak Administrátorská konzole se připojuje přímo k AMS. AMS je postaven na databázi SQL – ať už se jedná o dedikovaný MS SQL Server 2000, pokud je k dispozici, nebo, pro malé až středně velké sítě, o jeho odlehčené verzi, MSDE 2000, která je standardní součástí instalačního balíku ADNM. Předpokládá se, že stroj, na němž běží AMS, má možnost připojení k Internetu prostřednictvím HTTP protokolu.

Ve větších sítí se očekává, že AMS bude instalován na dedikovaný počítač. Také je možné nasadit více AMS (každý se svou vlastní databází). Ty je možné nastavit, aby pravidelně kopírovaly své databáze, a také aby posílaly výsledky všech skenů na dedikovaný AMS, kde budou zpracovány reporty pro celou síť. Administrátoři si mohou vybrat ze dvou způsobů komunikace mezi AMS a klienty: PUSH nebo POP. Model POP je potřebný pro větší sítě a pro sítě, do nichž se připojují uživatelé občas (notebook). Každý AMS může zahrnout až desítky tisíc klientských počítačů propojených v rámci lokální sítě.

2

Instalace

2.1 Fáze plánování

Než začnete s instalací, měli byste se zamyslet nad tím, jak produkt nasadíte.

Pozornost byste měli věnovat zejména následujícím:

AMS

- Na jaký stroj nasadit AMS?
- Bude se jednat o dedikovaný počítač? Pokud ne, jaké další služby na stroji poběží? Nebudou kolidovat s AMS? Bude k dispozici dostatek prostředků, aby mohl AMS korektně pracovat?
- Používá se v síti DHCP? Může mít AMS pevnou IP adresu?
- Použijete plnohodnotnou MS SQL 2000 databázi, nebo raději její odlehčenou verzi (MSDE), jež je součástí instalace ADNM? Zvolíme-li MSDE, zvládne zpracovat veškerá data? (MSDE by měla být použita pouze v sítích, kde se počet počítačů pohybuje maximálně v řádu stovek, raději ale méně).
- Můžeme použít jen jeden AMS, nebo bude lepší použít model s více AMS? Výhodu více AMS oceníte zejména v případě více samostatných sítí LAN, propojených pomalejšími linkami.
- Vyhovuje stroj, na nějž budeme nasazovat AMS, minimálním požadavkům? Následující požadavky musí být splněny pro instalaci AMS:
  - Počítač s operačním systémem Windows NT/2000/XP/2003 a minimální pamětí 128MB RAM (256 - 512 doporučeno).
  - CPU odpovídající velikosti sítě - Pentium III nebo vyšší je doporučeno.
  - Nejméně 250MB volného místa na disku, plus dalších ~ 4GB pokud

použijete MSDE na stejném stroji.

- Připojení k Internetu HTTP protokolem.

Konzole

- Kdo bude zodpovědný za systém ADNM? Bude to jedna, nebo více osob?
- Na jaké počítače by se měly konzole instalovat?

Potřeby pro správu

- Jakým způsobem rozdělíme stroje do stromové struktury? Uděláme to geograficky? Nebo se raději budeme držet struktury sítě (např. domény Active Directory)? Nebo zkombinujeme obojí?
- Jak naimportujeme seznam počítačů do ADNM? Můžeme použít úlohu Hledání počítačů (tj. funguje správně Průzkumník sítě), nebo budeme muset použít nějakou alternativní metodu (např. import z textového souboru)?
- Budou mít všichni administrátoři stejná práva, nebo budeme mít strukturu administrátorů, kde bude mít každý administrátor zodpovědnost za něco jiného a jiná přístupová práva?

Nasazení produktů avast!

- Jak zajistíme nasazení produktů avast! na naši síť? Budeme chtít využít mechanismus nasazení ADNM (Instalační úlohy), nebo máme vlastní způsob instalace softwaru?
- Jsou v naší síti stroje s Windows 95/98/ME? Jak na ně nainstalujeme software? (Instalační úlohy pracují pouze s NT-based klienty)
- Použijeme program pro klonování disků k přípravě nových strojů? Budeme chtít zahrnout avast! do základního obrazu disku? (Pokud ano, přečtěte si prosím odpovídající kapitolu).

2.2 Fáze instalace

Po dokončení fáze plánování můžete přejít k samotné instalaci produktu.

AMS

Instalace začíná s AMS. Pro instalaci AMS jednoduše nahrajte instalační balík ADNM na počítač, kde bude AMS provozován, a spusťte program setup (setup_av_mgm.exe). Tím spustíte průvodce, který vás provede zbytkem instalace. Během ní budete požádán o zadání následujících informací:

- Cílový adresář.
- Komponenty k instalaci (buď AMS i konzole, nebo jen konzole; při instalaci AMS nechte zaškrtnuty obě součásti).
- Licenční soubor (k používání programu potřebujete licenční soubor; můžete použít přiložený DEMO licenční soubor, nebo jej nahradit vaším vlastním - ten získáte po koupi programu). Licenční soubor budete moci kdykoliv později změnit.
- Detaily databáze. Pokud se rozhodnete použít MSDE, ujistěte se, že máte zaškrtnuté políčko „Instaluj MSDE“. Pokud je toto políčko neaktivní, znamená to, že instalační program nenašel instalaci MSDE v aktuálním adresáři. Instalační balíček MSDE musí mít název „MSDE“ a musí se nacházet ve stejném adresáři jako hlavní instalátor setup_av_mgm.

Poté, co budou zkopírovány všechny soubory, budete dotázán, zda chcete vytvořit zrcadlo pro aktualizace (mirror). Velmi doporučujeme odpovědět Ano - jinak budete muset spouštět mirror sami. Odpovíte-li Ano, dojde k automatickému nastavení hodnot, takže to nebudete muset provádět později. Proces zrcadlení vyžaduje samozřejmě přístup na Internet protokolem HTTP.

Jakmile bude vytvoření mirroru hotové, musíte inicializovat SSL certifikát, který bude používán vrstvou SSL při komunikaci mezi AMS a administrátorskou konzolí. Můžete použít váš vlastní certifikát (ve formátu PEM, DER nebo PKCS#7), nebo si jej nechat vytvořit instalátorem.

Poznámka

Zadaný certifikát musí obsahovat privátní klíč, který bude použit pro šifrování komunikace mezi AMS a konzolemi.

Po dokončení instalace můžete být vyzván k restartu počítače (v závislosti na použitém operačním systému). Po restartu by měl být AMS plně funkční a jeho služby spuštěny automaticky.

Administrátorské konzole

Dalším logickým krokem je instalace administrátorské konzole (konzolí). Můžete samozřejmě používat konzoli, která byla nainstalována společně s AMS, ale není to nutné. Mnohem pohodlnější je nainstalovat konzoli přímo na administrátorův počítač a veškerou správu provádět vzdáleně. Můžete nainstalovat libovolné množství konzolí napříč sítí. Rozhodně ale není rozumné nainstalovat konzole na počítače běžných uživatelů, výsledkem čehož by mohlo být neautorizované fušování do AMS (i když tomuto jevu lze dobře zabránit použitím odpovídajících bezpečnostních opatření, jako jsou například silná hesla apod.).

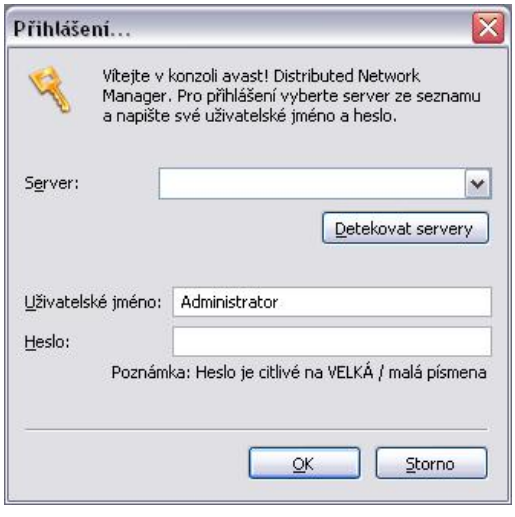
Instalace konzole je téměř shodná s instalací AMS, až na to, že při výběru komponent k instalaci nezaškrtnete políčko „Management Server“ (zaškrtnuté políčko zůstane pouze u položky „Konzole“).

Po dokončení instalace konzole můžete program okamžitě používat. Z nabídky Start zvolte ADNM Konzole. Zobrazí se přihlašovací okno. Do něj vložte název počítače, na který jste nainstaloval AMS, nebo stiskněte tlačítko Najít Servery, což způsobí nalezení všech dostupných AMS serverů v síti.

Poznámka

Výchozí přihlašovací jméno je *Administrator* a heslo je *admin*.

Doporučujeme všem uživatelům, aby výchozí heslo změnili co nejdříve po prvním přihlášení k serveru, protože ponechání výchozího hesla vede nutně ke snížení bezpečnosti celého systému.



Obrázek 2.1. Přihlašovací dialog AMS

Při prvním připojení k serveru uvidíte také varování, že SSL certifikát používaný serverem je pro klienta neznámý a tudíž podezřelý. To je normální a můžete bez obav zvolit „Povolit a Uložit“, čímž daný certifikát permanentně

schválíte. Tím zamezíte zobrazování dalších varovných hlášení do doby, než se certifikát AMS změní.

Jakmile dojde k úspěšnému spojení se serverem, budete mít k dispozici všechny možnosti konzole. Následující kapitola vás seznámí se základním konceptem konzole a popíše, jak používat ADNM k zajištění optimální ochrany celé sítě.

3

Konzole - První kroky

3.1 Základní koncept konzole

Konzole je organizována do adresářů, které fungují jako skladiště pro různé spravované objekty. Nejdůležitější ADNM objekty jsou tyto:

- **Úlohy.** Úlohy jsou základním stavebním kamenem ADNM. Úloha je popis nějakého úkolu, tj. definice toho, co se má provést. V případě ADNM je úloha také spojena s počítači, na kterých by měla běžet, a s časovým plánem jejího spuštění. V ADNM je mnoho typů úloh, ale základní rozdělení může být na Klientské úlohy a Serverové úlohy.

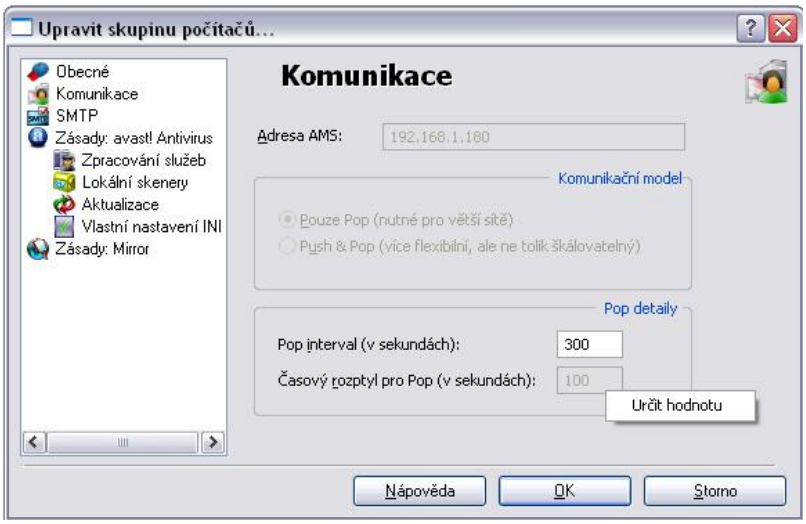
  - Klientské úlohy, to jsou ty, které běží na klientských počítačích (pracovních stanicích, serverech - zkrátka na strojích, na nichž jsou nasazeny produkty avast!). To zahrnuje skenování na vyžádání a aktualizační úlohy.

  - Naopak Serverové úlohy běží přímo na AMS. Typicky se jedná o úlohy zpracovávající reporty a úlohy pro údržbu databáze.

- **Seance.** Po spuštění úlohy se vytvoří její seance. Seance je objekt, který definuje podrobný běh úlohy. Např. pokud je úloha A spuštěna pětkrát, vytvoří se pět seancí, přičemž každá z nich zpracovává výsledky jednoho každého spuštění. Pro některé úlohy obsahuje seance pouze základní informace o jejím stavu; pro jiné může obsahovat velké množství výsledků (např. výsledky skenování na vyžádání), nebo dokonce binární data (např. reporty). Existují také dvě speciální, předdefinované seance mající zvláštní význam. „On-Access Skener“ seance udržuje všechny výsledky všech on-access skenů v síti. Seance „Lokální skenery“ zase udržuje výsledky všech testů spouštěných na vyžádání (tj. těch, které nebyly spuštěny prostřednictvím ADNM úloh).

- **Počítače.** Složka počítače (v konzoli nazvaná „Katalog Počítačů“) pracuje jako skladiště všech strojů spravovaných v síti. Má stromovou strukturu, můžete si tedy vytvořit tolik podsložek, kolik se vám hodí pro optimální organizaci. Nesmějí existovat žádné duplicity, tj. každý počítač má ve

stromu svojí pevnou pozici (pro přesun počítačů ve struktuře můžete používat metodu táhni a pusť). V Katalogu Počítačů se nastavuje veškerá bezpečnostní politika: každá složka může mít politiku nastavenou jinak. Politiky se dědí podle stromové struktury, ale stejně tak mohou být změněny na kterékoliv úrovni. Vytváření stromové struktury proto věnujte velkou pozornost.



Obrázek 3.1. Vlastnosti Skupiny Počítačů se dědí shora, ale mohou být přepsány na jakékoliv úrovni.

- **Management Servery** Zde jsou uloženy všechny management servery. Ve výchozí situaci se tu nachází pouze jeden - ten, ke kterému jste právě připojen. Pro větší sítě ale může být nutné mít nasazených několik AMS. Situaci, kdy je použito více AMS, se podrobně věnuje jiná kapitola.

- **Uživatelé.** ADNM má velmi dobrý systém uživatelů a jejich práv. Složka Uživatelé obsahuje seznam všech uživatelů (administrátorů), kteří mají různé možnosti a omezení přístupu k AMS. Různí uživatelé mají různá práva. Uživatelé mohou být spojeni do uživatelských skupin, zobrazených jako podsložky složky Uživatelé. Ve skutečnosti by měl být každý uživatel v nějaké skupině, tj. není možné vytvořit uživatele v kořenové složce Uživatelé. Skupina určuje pouze základní práva - mnohem podrobnější přiřazování práv lze uskutečnit změnou ACL (access control lists) pro každý ADNM objekt (úlohy, počítače, seance, objekty plánovače...).

- **Varování.** Tady můžete definovat varování (nebo oznámení), rozesílané při nalezené viru.. Potom můžete přiřazovat objekty Varování skenovacím úlohám, takže kdykoliv je nalezen virus, bude objekt použit k upozornění na problém odpovědné osoby.

- **Plánovač.** Složka Plánovač obsahuje události plánovače, určující, kdy má

být jaká úloha spouštěna. Jedná se o alternativní způsob jak editovat plánování - druhým způsobem je definice pravidel plánování ve vlastnostech úlohy.

- **Instalační balíčky.** Protože Instalační úlohy běží v tichém módu (bez zásahu uživatele), je nutné předem nastavit jejich požadované vlastnosti. Instalační balíčky se používají k definici instalací (nastavení instalace), které potom budou k dispozici pro Instalační úlohy k nasazení na klienty. Možnosti jsou: jaký produkt se bude instalovat, do jakého adresáře, počet služeb apod.

- **Události.** Toto je prohlížeč událostí ADNM. Do logu se během operací na AMS a agentech zapisuje spousta důležitých informací. K dispozici jsou až neuvěřitelné možnosti filtrování poskytující snadnou navigaci.

Poznámka

Vemte prosím na vědomí, že konzole není automaticky obnovována. Chcete-li tedy sledovat příslušné změny v čase, musíte obnovení provést ručně (buď stisknutím klávesy F5, nebo použitím odpovídajícího tlačítka v nabídce).

3.2 První kroky po instalaci

Typická série kroků, které by měly být provedeny po instalaci nového AMS, je následující:

- Změnit heslo Administrátorského účtu (to můžete provést v adresáři Uživatelé/Administrátoři editací vlastností objektu Administrátor).

- Vytvořit Katalog počítačů. Více informací naleznete v samostatné kapitole.

- Přizpůsobit stromovou strukturu Katalogu počítačů vaším potřebám. Standardně Katalog počítačů respektuje systém pracovních skupin/domén nalezených v síti. To ovšem není vždy ideální způsob způsob organizace z hlediska správy ADNM. V tomto kroku vyladíte stromovou strukturu, např. vytvořením vlastních skupin počítačů se specifickými požadavky (např. stroje patřící vedení firmy).

- V Katalogu počítačů nastavit odpovídající politiky editací vlastností skupin počítačů. Začněte kořenovým adresářem a pokračujte po větvích.

- Vytvořit nové uživatelské účty ve složce Uživatelé a nastavit jim odpovídající práva k objektům ADNM v okně „Práva Objektů“ (dostupným po kliknutí pravým tlačítkem na kterémkoliv objektu ADNM).

- Začít nasazovat produkty avast! Antivirus na klienty (viz následující kapitola).

4

Vytvoření Katalogu Počítačů

Klíčovým aspektem komfortní správy je efektivní organizace Katalogu Počítačů. Čím lépe navrhnete Katalog, tím snadněji se vám bude přiřazovat bezpečnostní politika a tím lepší bude výkon celého ADNM. Proto je třeba věnovat jeho vytvoření zvýšenou pozornost.

V základě existují dvě rozdílné metody vytváření Katalogu, které mohou být vzájemně kombinovány. První metoda využívá speciální druh serverové úlohy, konkrétně úlohy Hledání počítačů, k automatickému vytvoření katalogu. Druhá metoda spočívá v importování informací z externího zdroje (souboru). Položky katalogu můžete také vytvořit přímo, využitím grafického rozhraní konzole, což je ovšem zdlouhavý úkol, pokud chcete vložit více než jen několik málo strojů.

4.1 Použití úlohy Hledání počítačů

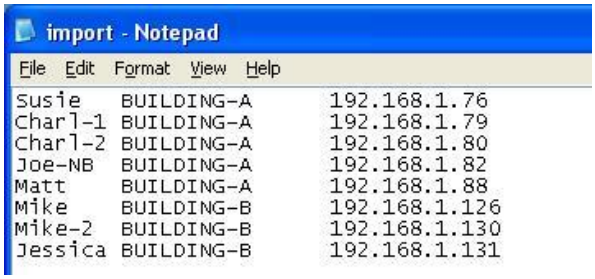
Použití úlohy Hledání počítačů je pravděpodobně nejsnazší a nejpohodlnější způsob vytvoření Katalogu. Zvolte Úlohy/Serverové úlohy/úlohy Hledání počítačů a v této složce vytvořte novou úlohu (ve většině případů můžete ponechat všechny volby na svých výchozích hodnotách). Potom úlohu spusťte. Tím se vytvoří nová seance pro zmíněnou úlohu, jako obyčejně. Úloha se dotáže Active Directory a/nebo NT LAN Manažera na seznam počítačů v síti a vloží je do Katalogu - buď do kořenového adresáře nebo do individuálních složek vytvořených tak, aby odpovídaly struktuře domény/pracovní skupiny v organizaci. Tato úloha zabere nějaký čas, takže budete muset počkat, než skončí. Její momentální stav můžete sledovat ve vlastnostech seance. Znovu si prosím uvědomte, že zobrazení není automaticky obnovované, takže budete muset obnovovat ručně. Jakmile se úloha dokončí, Katalog Počítačů by měl být naplněn všemi počítači, které byly nalezeny (a opět - nezapomeňte pohled na Katalog obnovit, abyste viděl nové položky).

4.2 Importování počítačů z externího zdroje

V některých případech nebude možné úlohu Hledání počítačů použít (např. proto, že na síti neběží Active Directory a/nebo nefunguje procházení počítači). Potom je ideální využít schopnosti ADNM a importovat stroje z externího

zdroje. Zejména můžete importovat seznam počítačů do Katalogu z jednoduchého textového souboru.

Textový soubor má poměrně jednoduchou strukturu. Každý řádek představuje jeden počítač a má tři sloupce. Sloupce jsou odděleny tabulátorem. První sloupec udává název počítače tak, jak by se měl objevit v Katalogu. Druhý sloupec představuje jméno domény nebo pracovní skupiny, do které počítač patří. A konečně sloupec třetí je interpretován jako IP adresa počítače (a proto by měl být ve formátu xx.xx.xx.xx, kde xx jsou čísla mezi 0 a 255). Tento sloupec je volitelný, hodnotu tedy specifikovat nemusíte, pokud nechcete.



Obrázek 4.1. Importování počítačů do Katalogu z textového souboru

Jakmile je textový soubor připraven, (ať už vytvořen ručně v textovém editoru nebo exportován z jiné aplikace), vše co musíte udělat, je předat jej ADNM. Přesuňte se do kterékoliv složky v Katalogu Počítačů a z nabídky zvolte Importovat Počítače.

4.3 Prohlížení Katalogu Počítačů

ADNM poskytuje množství zajímavých detailů o všech spravovaných strojích, souvisejících jak s avastem, tak se systémovou konfigurací. Tyto informace mohou být využity administrátory k analyzování problémů a také dávají lepší přehled o celé struktuře sítě..

Uložené informace zahrnují název počítače a domény/pracovní skupiny, IP adresu, typ CPU, velikost RAM, operační systém (a service packy), časovou zónu, místo na disku zabrané adresářem TEMP a další. Tyto informace jsou obnovovány při každé komunikaci s klientem.

⊟ Obecné	
Jméno	ARCTURUS
Komentář:	
Nalezen	únor, 6 (neděle)
⊟ Hardware	
Název CPU	x86 Family 6 Model 8 Stepping 3, MMX, ~729Mhz
Počet CPU	2
Fyzická paměť	383,5 M
⊟ Nastavení komponent	
Doména	ASW
Název skupiny	Root
IP adresa	192.168.1.220
Operační systém	Windows XP
Dostupné jednotky	A;C;D;E;F;G;I
Velikost Temp adresáře	103,0 MB
Časová zóna	GMT+1
⊟ Agent ADNM	
Poslední komunikace	Dnes v 15:03:11
GUID agenta	88e0a0d4-5df7-46ba-8b14-6cd05e84b7d4
Nainstalované produkty	avast! NetClient Edition
⊟ avast!	
Poslední virus	
Verze	4.6.293.0
Čas vytvoření VPS	Včera v 10:00:00
verze VPS	0507-0, 15.02.2005
Nainstalovaní poskytovatelé	STANDARD,MAIL,OUTLOOK,NS,JSCRIPT,IM,P2P,<Unknown>
Běžící poskytovatelé	STANDARD,MAIL,NS,JSCRIPT,IM,P2P,<Unknown>
Poskytovatelé čekající na spuštění	OUTLOOK

Obrázek 4.2. Základní info o spravovaném stroji v Katalogu Počítačů

Konzole rovněž označuje jednotlivé počítače v Katalogu ikonou. Každý počítač má jednu z následujících ikon:

 **Zelený počítač.** Ikona signalizuje zdravý stav počítače. Zejména že počítač nebyl v poslední době zavirován (nebyly na něm nalezeny žádné viry) a že aktivně komunikuje s AMS (např. že není vypnutý).

 **Červený počítač.** Ikona signalizuje infekci. Nedávno byl na počítači nalezen virus. Počítač zůstane „červeným“, dokud jej administrátor ručně neoznačí jako čistý (použitím volby „Označit počítač jako čistý“).

 **Šedý počítač.** Tato ikona signalizuje, že počítač v poslední době nekomunikoval s AMS (dobu, po které bude počítač označen šedě, může být nastavena v globálních nastaveních AMS; výchozí hodnotou je 20 minut). To, že je počítač označen šedě, neznačí samo o sobě nic špatného. Např. vypnuté počítače se označí jako šedé velmi brzy. Šedou ikonou se také označují počítače, na nichž není nainstalován avast! agent (např. nově objevené počítače).

 **Počítače se symbolem klíče.**Tato ikona upozorňuje na nedostatečný počet licencí definovaný v licenčním souboru. To znamená, že Katalog obsahuje větší počet počítačů, než na kolik byla zakoupena licence na ADNM. Výběr počítačů, na něž se nedostává licencí, je prováděn AMS náhodně, ale preferují se počítače, které ještě nekomunikovaly se serverem (tedy ty, které by

byly normálně označeny jako šedé).

5

Nasazení produktů avast!

Existuje pět hlavních metod, jak nasadit produkty avast! v síti:

- Použitím Instalační úlohy v ADNM pro automatickou instalaci na klienty. Vemte prosím v potaz, že tato metoda funguje pouze na strojích s Windows NT/2000/XP/2003.
- Použitím log-on skriptu nebo podobného způsobu ke spuštění (bezobslužné) instalace na cílových strojích.
- Použitím MSI balíčků.
- Použitím metody klonování disků.
- Ručním spuštěním instalace na cílových strojích a dokončením průvodce instalací.

První způsob je obyčejně nejjednodušší a nejvíce doporučený.

Poznámka

Před instalací klientů se ujistěte, že splňují minimální systémové požadavky. Zejména se ujistěte, že jsou nainstalovány MDAC (ODBC) a Jet ovladače a že správně fungují. To je obyčejně případ Windows ME, 2000, XP and 2003, kde jsou stabilní verze MDAC vestavěny do systému. U starších operačních systémů (jako je Windows 98 nebo Windows NT 4.0) byste se měl ujistit, že jsou MDAC/Jet ovladače aktuální (MDAC verze 2.5 nebo vyšší, Jet 4.0 SP4 nebo vyšší. Nezapomeňte, že od verze MDAC 2.6 jsou k dispozici dva oddělené downloady (pro MDAC a pro Jet). Poslední verze těchto ovladačů můžete získat na stránkách Microsoftu http://www.microsoft.com/downloads.

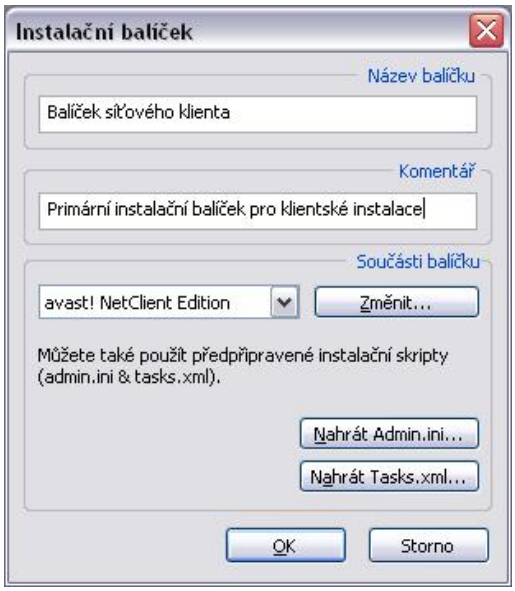
Poznámka

Pokud je na klientských strojích spuštěn firewall (např. na Windows XP SP2 je integrovaný firewall standardně zapnutý), některé funkce ADNM nemusí pracovat korektně. Např. Sdílení Souborů a Tiskáren musí být ve firewallu

povoleno, aby fungovala vzdálená instalace (jinak nebude mít instalátor šanci nahrát instalační balíčky na klienty). Více informací naleznete v sekci *ADNM a lokální firewally* v kapitole *Pokročilá témata*. V případě firewallu vestavěného do Windows XP lze naštěstí nastavit jeho pravidla hromadně v Group Policies.

5.1 Automatická (Push) Instalace

Pro přípravu instalačního balíčku jděte do složky „Instalační balíčky" a zvolte „Vytvořit balíček...". Vyberte, jaký balíček chcete připravit: avast! Network Client je verze avastu určená pro pracovní stanice (víceméně shodná s avastem Professional Edition); avast! Network Server je verze avastu určená pro servery (ekvivalent k avast! Server Edition + pluginy); a avast! Mirror je sekundární mirror agent, který může být použit k vyvážení aktualizací (viz dále).



Obrázek 5.1. Editor instalačních balíčků

Potom klikněte na tlačítko „Upravit", abyste mohl nastavit vlastnosti instalace. Zobrazí se stejný průvodce jako při interaktivní instalaci. Nastavte vlastnosti instalace a nezapomeňte změny uložit. Zvláštní pozornost věnujte názvu účtu, pod nímž bude služba avastu běžet.

Poznámka

Tento účet musí mít práva lokálního administrátora a také by měl mít přístup ke všem síťovým prostředkům (alespoň pro čtení).

Zejména si uvědomte, že:

- účet musí být platný na všech strojích, na kterých chcete tento instalační

balíček použít.

- pokud tomuto účtu změníte později heslo, budete muset zařídit změnu této informace pro všechny služby na všech počítačích (což nemusí být zrovna snadný úkol).

Proto je vhodné tomuto heslu nastavit atribut „Nevyprší nikdy“.

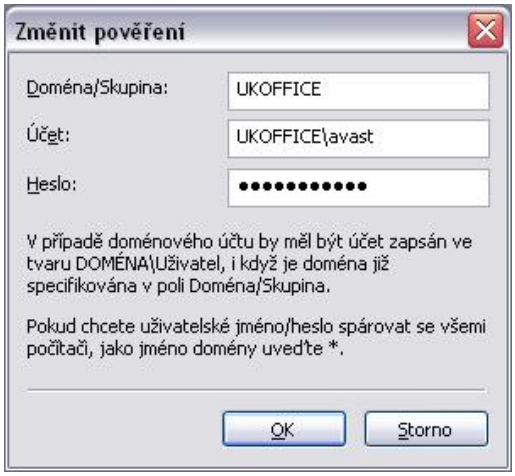
Jakmile je instalační balíček hotov, pokračujte vytvořením instalační úlohy. Přesuňte se do složky Úlohy/Klientské úlohy/Instalační úlohy a zvolte „Vytvořit novou...“. Na stránce Instalace vyberte balíček, který jste vytvořil.

Dále pokračujte stránkou Přihlašovací Účty. Tady můžete přiřadit všechna uživatelská jména a hesla, která budou použita při přihlašování ke vzdáleným strojům a umísťování balíčků. Pokud nejsou stroje součástí domény, zadejte místo ní název pracovní skupiny. Pro všechny domény/pracovní skupiny můžete (jako poslední možnost) použít zástupný znak *.

Poznámka

Pokud jsou stroje v doméně a používáte doménový účet, nezapomeňte uvést uživatelské jméno ve formátu DOMÉNA\uživatelské jméno. Např. pokud je název domény UKOFFICE a účet, který chcete použít se nazývá „avast“, zadáte do pole doména „UKOFFICE“ a do pole uživatelské jméno „UKOFFICE\avast“ (pokud neuvedete název domény v názvu účtu, bude tento interpretován jako lokální, nikoliv doménový účet).

Přiřazení jsou čtena shora dolů a jejich posloupnost můžete změnit tlačítky „Nahoru“ a „Dolů“. Aby instalační úloha proběhla korektně, je důležité zadat tyto informace správně a kompletně. V opačném případě nebudou některé stroje obslouženy díky chybě při přihlašování.



Obrázek 5.2. Definice účtů

Obrázek 5.3. Stránka přihlašovacích účtů v editoru Instalační úlohy ADNM

Na poslední stránce konfigurace (Počítače) můžete specifikovat stroje, na kterých by měla tato úloha běžet. Můžete také specifikovat skupiny počítačů - ty by měly být v případě statických skupin uvedeny v hranatých závorkách (např. [Skupina1]) a v případě dynamických skupin v závorkách kulatých.

Jakmile je úloha připravena, vše co musíte udělat je spustit ji a sledovat její stav (nezapomeňte okno obnovit, abyste viděl změny). Můžete ji spustit na skupině počítačů uvedených na stránce Počítače (prostým poklepáním na úlohu), nebo ji přesunout do jiné skupiny počítačů a spustit ji tam (tato metoda - táhni a pusť - je použitelná se všemi úlohami ADNM, nikoliv pouze s úlohami instalačními). Můžete také naplánovat spouštění úlohy periodicky.

5.2 Ruční instalace

Pokud není možné z nějakého důvodu použít Automatickou Instalaci popsanou v minulé sekci, budete muset nasadit produkty avast! v síti ručně. Pro zjednodušení tohoto procesu doporučujeme umístit instalační balíček do nějakého sdíleného síťového adresáře, abyste jej nemusel kopírovat na každý počítač zvlášť. K tomu stačí překopírovat adresář InstPkgs, který podsložkou adresáře, v němž je nainstalován AMS. Tato složka obsahuje všechny soubory potřebné k instalaci jakéhokoliv podporovaného produktu. Složka také obsahuje soubor setup.exe který se používá ke spuštění instalace. Program by měl být spuštěn s následujícími parametry:

setup.exe /client /createprogress /sfx /sfxstorage "package-folder"

(v případě instalování na pracovní stanice), nebo

setup.exe /server /createprogress /sfx /sfxstorage "package-folder"

(v případě instalování na server), kde package-folder nahradíte úplnou cestou k adresáři s instalačními balíčky. Pokud se v daném adresáři právě nacházíte, můžete tuto cestu nahradit "." (včetně uvozovek).

Abyste nemusel obejít každý stroj v síti a manuálně spouštět instalační program, můžete použít některou z následujících metod:

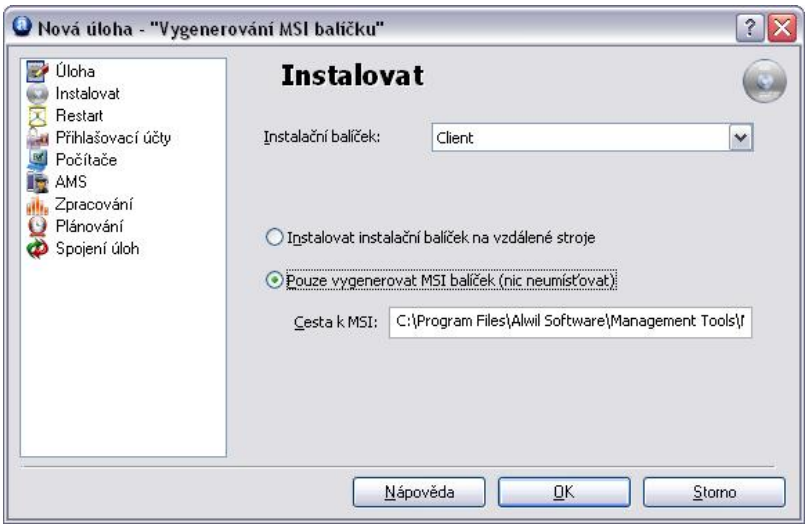
- Umístit instalační příkaz do logon skriptu. Tato metoda je poměrně efektivní, ale má jednu nevýhodu - na počítačích s NT-based Windows se mohou vyskytnout problémy díky nedostatečným uživatelským právům. To je způsobeno tím, že login skript se obyčejně pouští s právy uživatele, který se zrovna přihlašuje, a ve většině případů nemají uživatelé práva administrátora (jež instalační program vyžaduje). Toto není naštěstí případ Windows 95/98/ME.

- Rozeslat uživatelům e-mail obsahující odkaz na instalační program umístěný ve sdíleném adresáři na serveru, spolu s podrobnými instrukcemi, jak na odkaz kliknout a co v průvodci instalací zvolit. Tato metoda je také poměrně efektivní (pokud nejsou uživatelé úplné lamy :-)), která ovšem bohužel neřeší problém s uživatelskými právy, zmíněný výše.

- Zabalit instalační soubory do MSI balíčku a tento nějakým způsobem rozdistribuovat.

5.3 Instalace pomocí MSI balíčků

Rozhodnete-li se nasadit produkty avast! pomocí MSI (Microsoft Installer) balíčků, budete tyto balíčky muset nejprve připravit (vytvořit). Toho dosáhnete vytvořením instalační úlohy, kde na stránce Instalace zvolíte "Generovat MSI (nic neinstalovat)". V tomto módu jsou cílové stroje, definované na stránce Počítače, ignorovány. Spuštěním úlohy dojde k vytvoření souboru MSI.



Obrázek 5.4. Instalační úloha může být také použita k vygenerování MSI balíčku

S vytvořeným MSI souborem můžete použít váš oblíbený nástroj (jako je Microsoft Systems Management Server nebo ActiveDirectory Group Policy) k umístění instalací na klienty, nebo využít některou proceduru popsanou dříve v sekci Ruční Instalace.

5.4 Instalace klonováním disků

Ve větších organizacích je obvyklé instalovat (připravovat) nové počítače metodou klonování disků. To je obzvlášť vhodné v případech, kdy máme velké množství strojů se stejnou hardwarovou konfigurací. Na trhu je množství speciálních nástrojů, jako např. Symantec Ghost, které klonování zjednodušují.

Metoda klonování spočívá obyčejně v přípravě jednoho stroje („master“) (např. nainstalování operačního systému a potřebných aplikací a provedení odpovídajících nastavení), následném zachycení obsahu disku takového stroje (na úrovni sektorů) a přenesení obsahu na libovolný počet cílových počítačů.

Obecně lze klonovat stroje s nainstalovaným produktem avast!. Budou zachována všechna nastavení a komunikační kanál s AMS bude fungovat. Nicméně některé věci musí být změněny (jako např. GUID agenta, což je jedinečný identifikátor používaný k autorizaci k AMS). Z těchto důvodů obsahuje instalace všech verzí avastu speciální nástroj. Ten se nazývá aswImgPr.exe a jedná se o velmi jednoduchou command-line aplikaci s jediným účelem: připravit instalaci avastu na "master" počítači ke klonování.

Poznámka

V době mezi spuštěním aswImgPr.exe a vytvořením obrazu disku by nemělo

dojít k restartu; v opačném případě bude nutné spustit aswImgPr.exe znovu.

5.5 Odinstalace

Každý slušný program nabízí možnost deinstalace a ADNM není výjimkou. Rozhodnete-li se odstranit avast! z vaší sítě, můžete použít Odinstalační úlohu. Odinstalační úloha je speciální druh úlohy (naleznete ji v konzoli ve složce Instalační úlohy), která slouží k jedinému účelu: odinstalování všech spravovaných produktů z vybraných strojů. Úlohu můžete spustit buď na všech spravovaných strojích, nebo pouze na některých.

Poznámka

Někdy se může stát, že Odinstalační úloha zůstane ve stavu "Spuštěna", ačkoliv již byla dokončena (tedy i když byl software odinstalován z klientských strojů). To je způsobeno skutečností, že odinstalovaný agent nemůže již reportovat svůj konečný stav AMS.

6

Používání ADNM

6.1 Spravování politiky antiviru

Primárním určením ADNM je efektivní správa antivirových programů nainstalovaných v síti. Tato kapitola vás provede nejobvyklejšími činnostmi, se kterými se budete při správě bezpečnosti sítě setkávat den co den.

6.1.1 Základy správy Katalogu Počítačů

Většina nastavení souvisejících se správou je specifikována ve vlastnostech skupin Katalogu Počítačů. V ADNM se zásady nenastavují pro jednotlivé počítače, ale pro skupiny. Pokud potřebujete mít stroj se speciálním nastavením, měl byste pro něj nejprve vytvořit samostatnou skupinu (obyčejně podskupinu skupiny, v níž počítač původně byl).

Každá skupina má svou vlastní sadu zásad. Standardně se tyto zásady dědí z rodičovské skupiny. Mohou být nicméně předefinovány na jakékoliv úrovni.

Pokud není některá ze zásad politiky definována, zobrazí se ve vlastnostech skupiny jako šedá (nedostupná). Jelikož ve výchozím nastavení není přepsána žádná zásada, jsou šedé všechny možnosti ve vlastnostech skupin, kromě skupiny kořenové. Chcete-li nějakou zásadu změnit, klikněte na ovládací prvek pravým tlačítkem a zvolte "Určit hodnotu". Ovládací prvek se stane dostupným a může být použit k určení hodnoty. Pokud se později rozhodnete danou zásadu nedefinovat, klikněte na ni opět pravým tlačítkem a zvolte "Zdědit od rodiče".

Obrázek 6.1. Přepisování politiky rodičovské skupiny. Nabídka "Určit hodnotu" je vyvolána pravým tlačítkem myši.

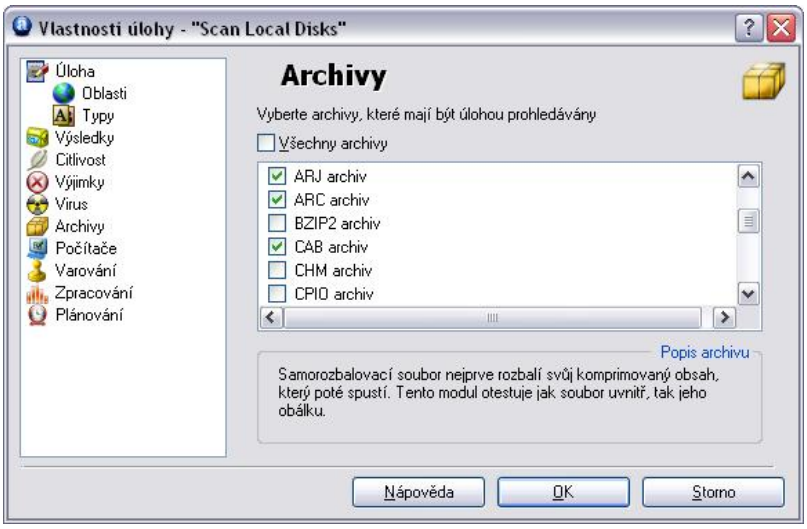
Dialog Vlastnosti obsahuje nastavení zásad pro všechny podporované spravované produkty, ať už jsou nainstalovány na klientských strojích, nebo ne. Pokud je např. na počítači nainstalován pouze "mirror" (který také patří do spravovaných produktů), nastavení zásad pro produkt avast! Antivirus nebude mít žádný efekt, zatímco zásady nastavené pro Mirror ano.

Většina zásad je nastavena přímo jako vlastnosti Skupiny Počítačů. Důležitou výjimkou jsou on-access testovací úlohy, tj. nastavení rezidentních úloh. Ty jsou uloženy ve vlastnostech skupiny pouze jako odkazy na objekty on-access skenovacích úloh. To znamená, že pokud chcete změnit nastavení rezidentní úlohy pro daný stroj, musíte nejprve vytvořit novou on-access úlohu a tu následně přiřadit zvolené skupině počítačů. To v důsledku znamená, že nastavení rezidentních úloh nelze dědit v rámci Katalogu.

6.1.2 Používání skenování na vyžádání

ADNM nabízí komfortní způsoby skenování na vyžádání na klientských strojích. Skenovací proces je definován vytvořením On-demand skenovací úlohy. Tyto úlohy naleznete ve stejnojmenné složce, pod složkou Úlohy na straně klienta.

Editor úloh nabízí velké množství nastavení, která mohou být různě upravována. To zahrnuje oblasti k testování, definice výsledků, které budou poslány na AMS nebo nastavení skenování uvnitř archivů. Úloha také pochopitelně určuje počítače, na nichž se bude spouštět.



Obrázek 6.2. Vlastnosti skenovacích úloh na vyžádání (on-demand).

Jakmile je úloha připravena, můžete jí buď okamžitě spustit, nebo její spuštění naplánovat (např. aby se spouštěla pravidelně). Pokud spustíte úlohu okamžitě použitím tlačítka "Spustit Úlohu", bude spuštěna na počítačích definovaných ve vlastnostech této úlohy. Jestliže použijete metodu táhni a pusť a přesunete úlohu do nějaké skupiny v Katalogu Počítačů, bude spuštěna na počítačích v této skupině a výchozí seznam počítačů uvedený ve vlastnostech úlohy bude ignorován.

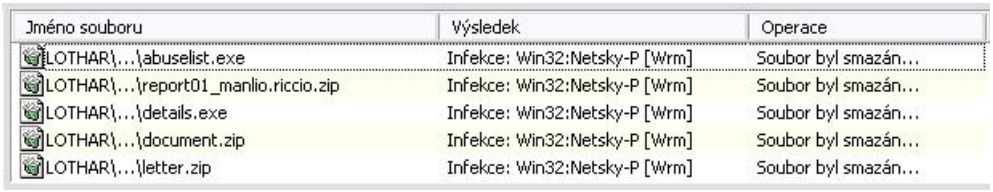
Více informací o plánování on-demand úloh naleznete v kapitole "Plánování běžných testů".

6.1.3 Sledování výsledků skenování

Každá skenovací úloha (jak on-demand, tak on-access) může generovat výsledky související s infekcí. Ty jsou ukládány do databáze pro pozdější nahlédnutí, generování reportů nebo přímé prohlížení.

Výsledky úlohy jsou uloženy v seanci úlohy. Seance představuje danou (běžící) instanci dané úlohy, zakončenou jejími výsledky. Seance naleznete ve složkách Klientské seance a Serverové seance.

Konzole zobrazuje výsledky seance v tabulce. Každý výsledek (soubor) se nachází na jednom řádku, spolu s plným názvem souboru (včetně názvu stroje, na němž sídlí), názvem viru (pokud se jedná o infikovaný soubor) a akcí, kterou s daným souborem avast! provedl.



Jméno souboru	Výsledek	Operace
LOTHAR\...\abuselist.exe	Infekce: Win32:Netsky-P [Wrm]	Soubor byl smazán...
LOTHAR\...\report01_manlio.riccio.zip	Infekce: Win32:Netsky-P [Wrm]	Soubor byl smazán...
LOTHAR\...\details.exe	Infekce: Win32:Netsky-P [Wrm]	Soubor byl smazán...
LOTHAR\...\document.zip	Infekce: Win32:Netsky-P [Wrm]	Soubor byl smazán...
LOTHAR\...\letter.zip	Infekce: Win32:Netsky-P [Wrm]	Soubor byl smazán...

Obrázek 6.3. Výsledky skenovací úlohy

6.1.4 Výchozí nastavení spravovaných produktů

Ve výchozím nastavení jsou spravované verze avastu nastavené tak, aby byly odolné vůči zásahům uživatelů počítačů. To znamená, že žádný uživatel kromě administrátora by neměl být schopen měnit funkčnost a/nebo nastavení antiviru. Pokud má uživatel na daném počítači práva administrátora, je samozřejmě obtížné zabránit tomu, aby např. ukončil službu avastu a vyřadil tak rezidentní ochranu. To je další z důvodů, proč není obvykle vhodné poskytovat obyčejným uživatelům administrátorská práva.

Rezidentní ochrana (ikona v systémové liště) je pouze zobrazena, ale klikání na ní nevede k zobrazení žádné nabídky nebo dialogu. Předpokládá se, že normální uživatelé by neměli mít práva měnit jakékoliv nastavení, proto je odpovídající grafické rozhraní blokováno.

Všechny součásti avastu jsou zároveň přednastaveny tak, aby pracovaly v "tichém režimu", tj. aby nevyžadovaly žádnou akci od uživatele, ale aby je prováděly automaticky. Výchozí akcí je "přesunout do truhly, a selže-li, smazat". Jedinou výjimkou jsou lokální skenery (rozšíření Průzkumníka, Jednoduché Ovládání atd.), které jsou vždy interaktivní - neboť se předpokládá, že se uživatel pokouší spustit tyto programy s očekáváním okamžitého, interaktivního výsledku (např. ruční ověření, že soubory na disketě nejsou zavirovány). A jelikož je skenování vyvoláno samotným uživatelem, není považováno za součást společné politiky a proto je rozhodnutí, co s nalezeným virem, ponecháno na uživateli.

6.1.5 Vlastní nastavení INI

Některá nastavení (zásady) nemohou být nastavena přímo prostřednictvím vlastností Skupiny Počítačů, protože pro ně nejsou definovány žádné prvky grafického rozhraní. To se týká hlavně nastavení, která mají pro většinu uživatelů minimální význam. Většina takových nastavení může být změněna editací souboru avast4.ini na klientských počítačích.

ADNM značně usnadňuje nastavování těchto vlastností prostřednictvím vzdálené (dávkové) editace souborů avast4.ini. Ve skutečnosti se položky INI

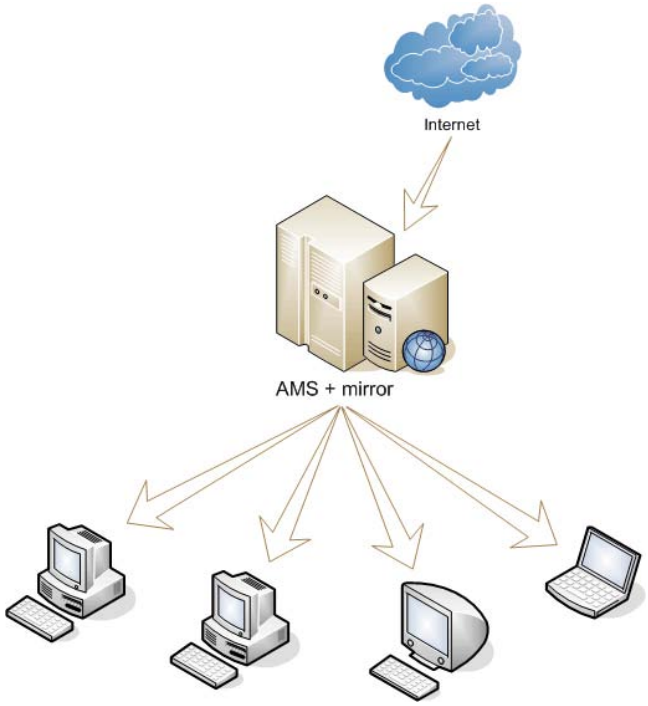
souboru stávají součástí vlastností Skupiny Počítačů (včetně dědění atd.). Nastavení INI souboru mohou být vložena na stránce "Vlastní Nastavení INI" ve vlastnostech Skupiny. Syntaxe je stejná jako v případě skutečných INI souborů - tj. názvy sekcí jsou v hranatých závorkách a jednotlivé položky jsou specifikovány ve formátu položka=hodnota (každá na samostatném řádku).

6.2 Aktualizace v ADNM

Systém ADNM nabízí flexibilní možnosti správy aktualizací. To se týká jak aktualizací virové databáze, tak celého programu.

ADNM používá tzv. aktualizační mirrory, zajišťující efektivní mechanismy aktualizací na všech strojích v síti (i na těch, které nemají přímý přístup na Internet). Mirrory také značně snižují zatížení sítě, protože místo toho, aby si jeden každý počítač v síti stahoval aktualizace z Internetu, jsou tyto staženy pouze na mirror a následně rozdistribuovány lokálně.

Obyčejně je jeden mirror na AMS a to je jediný mirror v síti (nebo - v případě více AMS - se nachází mirror na každém AMS a jsou to jediné mirrory v síti). Všechny spravované stroje si stahují aktualizace z mirroru na AMS (tedy pokud je připojení k AMS dostupné, což nemusí v některých případech být, např. v případě uživatelů notebooků; více informací o občas se připojujících (roaming) uživatelích naleznete na konci kapitoly).



Obrázek 6.4. Nejjednodušší scénář aktualizací přes mirror. Jediný mirror v síti je na samotném AMS.

Základní parametry aktualizací pro počítač lze nastavit editací vlastností skupiny v Katalogu Počítačů. Ty zahrnují interval auto-aktualizací a zdroj aktualizací.

Obrázek 6.5. Konfigurační stránka aktualizací skupin počítačů.

Aktualizační úlohy

Pro aktualizace na vyžádání existuje speciální typ úlohy: aktualizační úloha. Pro vytvoření aktualizační úlohy se přesuňte do složky Aktualizační úlohy a zvolte Nová Úloha. Zvolte Aktualizace v políčku Typ úlohy a na stránce Počítače vyberte cílové stroje pro tuto úlohu. Můžete také určit, jakým způsobem se bude program chovat v případech, kdy bude pro dokončení aktualizace vyžadován restart klientského počítače.

Zvláštní požadavky pro aktualizace

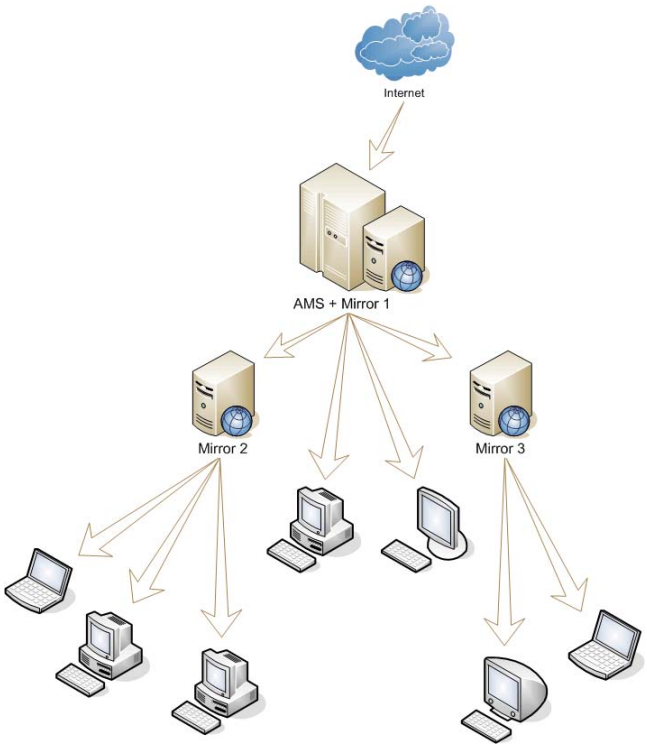
Model jediného mirroru by měl vyhovovat většině typů sítí. Nabízí rozumnou škálovatelnost pro sítě čítající stovky strojů a rozhodně se nejsnadněji spravuje. V některých případech ale nemusí vyhovovat. Např. pokud

- se jedná o rozsáhlou síť s tisíci počítači, nebo
- stroj s AMS nemá přístup na Internet (nedoporučeno), nebo
- existuje požadavek na otestování jednotlivých aktualizací na skupině strojů před jejich uvolněním do celé sítě.

6.2.1 Nasazení mirrorů druhé úrovně

Pokud scénář jediného mirroru nevyhovuje požadavkům vaší sítě, je možné nasadit libovolný počet mirrorů druhé úrovně. Všechny tyto mirrory jsou

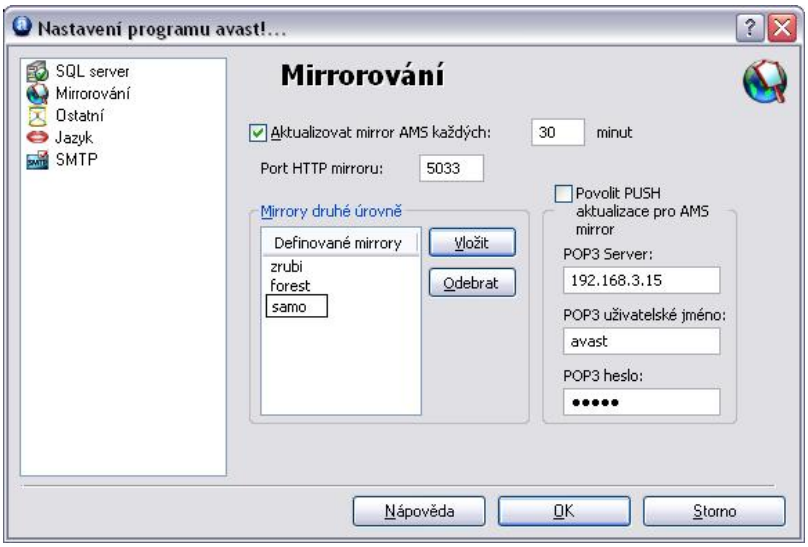
ekvivalentní (tj. klientské stroje si náhodně vybírají, z jakého z nich budou aktualizovat) a jejich primární cíl je vyvážit zatížení serveru (protože v případě, kdy je jedním AMS spravováno velké množství počítačů, může mít AMS mirror problém obsloužit všechny tyto klienty). Jak již bylo řečeno, každý mirror by měl být schopen obsloužit přibližně stovky klientů.



Obrázek 6.6. Konfigurace mirrorů druhé úrovně

Před použitím mirrorů druhé úrovně je musíte nejprve nainstalovat na cílové stroje. Mirrory jsou brány jako další spravovaný produkt v ADNM. Jejich příprava je tedy uskutečněna stejně jako nasazení klientů avast! Antivirus: vytvořením instalačního balíčku a následném použití některé z metod probíraných v předchozí kapitole (typicky se použije instalační úloha).

Jakmile je mirror nainstalován, je připraven k použití. Mirrory druhé úrovně musí být registrovány v AMS. Toho lze docílit použitím dialogu Nastavení v konzoli. Zde je třeba zapsat do seznamu všechny mirrory druhé úrovně, které se používají. Můžete použít např. IP adresy (pokud jsou pevné), nebo DNS názvy, jak je vidět na následujícím obrázku.



Obrázek 6.7. Konfigurace mirrorů druhé úrovně

Zbývá sdělit klientům, aby používaly mirrory druhé úrovně namísto AMS mirroru. Toho lze docílit změnou politiky skupiny, tj. různé skupiny počítačů mohou mít různá nastavení. Někteří klienti tedy mohou aktualizovat z mirrorů druhé úrovně, zatímco další budou aktualizovat ze samotného AMS. Odpovídající nastavení je na stránce "Aktualizace" pod "Zásady: avast! Antivirus".

Mirrory druhé úrovně mají také několik možností nastavení - kromě jiných věcí lze nastavit časový interval synchronizace mirroru. Tato nastavení naleznete na stránce "Zásady: Mirror" ve vlastnostech skupiny počítačů.

Obrázek 6.8. Vlastnosti produktu "mirror" (mirrory druhé úrovně)

Mirrorovací úlohy

Pro synchronizace mirrorů druhé úrovně existuje speciální typ úlohy: mirrorovací úloha. Mirrorovací úlohy jsou uloženy ve složce Aktualizačních

úloh. Pro vytvoření mirrorovací úlohy se přesuňte do složky Aktualizační úlohy a zvolte Nová Úloha. V poli Typ Úlohy zvolte Mirrorovací a na stránce Počítače specifikujte stroje mirrorů druhé úrovně pro tuto úlohu. Úloha nebude mít žádný efekt na strojích, kde není žádný mirror nainstalovaný.

Použití dvoufázových aktualizací

V některých organizacích (zejména v těch, kde je otázka bezpečnosti na prvním místě) je požadováno, aby veškeré aktualizace, distribuované na počítače v síti, byly nejprve ověřeny na několika testovacích strojích. Pokud jsou výsledky testů vyhodnoceny jako OK, mohou být aktualizace umístěny na ostatní stroje. Tento požadavek může být poměrně snadno implementován použitím funkce ADNM mirrorů druhé úrovně:

- Mirrory druhé úrovně mají vypnutou auto-synchronizaci, a
- AMS mirror je využíván pouze testovacími stroji.

V tomto případě, pokud je na našich Internetových serverech uvolněna nová aktualizace, dojde k následujícímu:

1. AMS mirror se sesynchronizuje s naším Internetovým serverem, stáhne nové balíčky a publikuje je klientům.
2. Skupina testovacích strojů (těch, které jsou nastaveny, aby aktualizovaly přímo z AMS mirroru) stáhne novou verzi. Žádné další stroje v tuto chvíli neaktualizují, neboť na mirrorech druhé úrovně nejsou žádné nové soubory.
3. Testeři vyzkouší, zda nová aktualizace funguje korektně.
4. Pokud je všechno OK, spustí se mirrorovací úloha na mirrorech druhé úrovně. To způsobí nakopírování nových souborů na mirrory druhé úrovně.
5. Všechny počítače v síti spustí stahování a instalaci nové (ověřené) aktualizace.

6.2.2 Aktualizace mobilních uživatelů

ADNM je vytvořen tak, aby byl schopen vyhovět požadavkům na aktualizace i pro mobilní uživatele. Základní myšlenka je celkem jednoduchá: Pokud je k dispozici AMS (nebo mirror druhé úrovně), použij jej pro aktualizaci. V opačném případě aktualizuj z Internetu.

Ačkoliv to může vypadat až triviálně, jedná se o velmi efektivní záležitost. Mobilní uživatelé, kteří jsou zčásti připojeni do sítě společnosti (ať už přímo, nebo vzdáleně přes VPN) a zčásti ne (ale většinou stále mají přístup na Internet), vždy aktualizují z nejlepšího zdroje, díky čemuž probíhá aktualizační proces rychle a hladce. Jediná situace, kdy k aktualizaci nedojde, je v případě nedostupnosti jak firemní sítě, tak sítě Internet - to ovšem asi nikoho nepřekvapí.

6.2.3 Použití PUSH Aktualizací

AMS mirror může být také nastaven, aby používal PUSH synchronizaci (neplést s automatickou (push) instalací klientů). PUSH aktualizace v ADNM pracují úplně stejně jako v avast! Professional Edition: prostřednictvím e-mailů.

Tradičně si každý instalovaný program čas od času kontroluje, jestli není k dispozici nová verze. Ovšem PUSH aktualizace jsou vyvolány naším serverem - a to okamžitě po tom, co je nová aktualizace uvolněna; výsledkem je rychlá odezva AMS mirroru a provedení potřebné synchronizace. Systém je postaven na protokolu SMTP, tj. na běžných e-mailových zprávách.

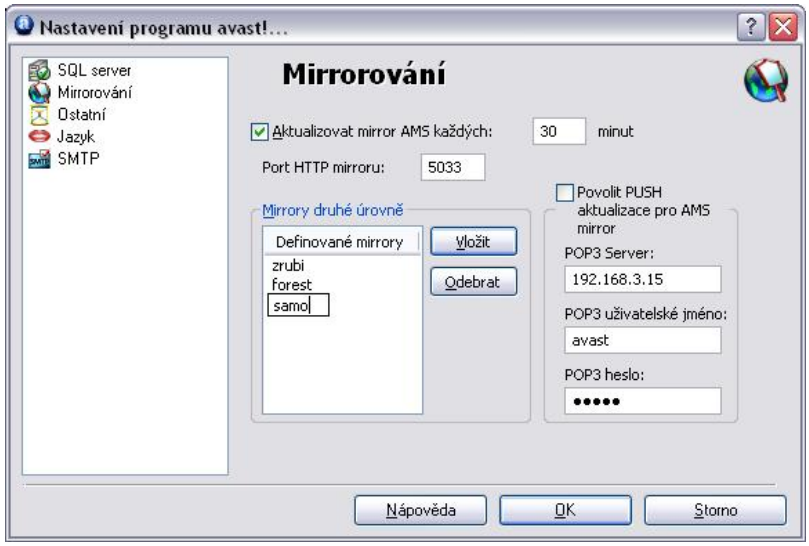
Celý systém PUSH aktualizací je chráněn asymetrickou šifrou a je odolný proti neautorizovanému zneužití.

6.2.3.1 Nastavení Push Aktualizací pro AMS Mirror

Před nastavením PUSH aktualizací pro AMS mirror se nejprve přihlašte k odběru novinek na adrese http://www.avast.com/cze/subscription_service.html vyplněním e-mailové adresy. Velkým zákazníkům s vlastním mail serverem doporučujeme pro tento účel nastavit zvláštní e-mailový účet.

Po registrování adresy otevřete hlavní dialog Vlastností AMS, jděte na stránku Mirrorování a vyplňte detaily účtu. Konfigurační stránka podporuje změnu pouze nejzákladnějších parametrů (název POP3 serveru, uživatelské jméno a heslo). Pro vyladění nastavení budete muset změnit některé položky v sekci [InetWDMirror] v souboru <ADMM>\DATA\avast4.ini na AMS. Např. hodnota PushDaemonInterval udává interval v minutách, v němž se kontrolují nové zprávy (výchozí hodnota je 3; interval můžete nastavit na 1 minutu pro maximální efektivitu PUSH aktualizací). Další důležitou hodnotou je položka PushDaemonDeleteMessages (0 nebo 1), která udává, zda se mají zprávy po jejich stažení ze serveru smazat, nebo ponechat. Výchozí hodnota je 0 (nechat zprávy na serveru). Pokud použijete výchozí hodnotu, je dobré čas od času smazat zprávy z mailboxu ručně (minimálně jednou ročně - závisí to též na

objemu spamu).



Obrázek 6.9. Určení detailů POP3 serveru pro PUSH aktualizace.

6.3 Sledování Logů ADNM

Pro zajištění celkového zdraví sítě je třeba průběžně sledovat položky logů, které jsou posílány klienty nebo jsou zapisovány samotným AMS. To se většinou provádí prostřednictvím složky Události v konzoli (některé položky se do této složky nelogují. Podívejte se prosím do sekce Monitorování AMS Logů v kapitole Pokročilá Témata pro více informací).

Kliknutím na složku událostí se zobrazí všechny události uložené v databázi (nefiltrované). Jsou tam také tři podsložky:

- Klientské události. Tato složka obsahuje všechny události zaslané spravovanými klienty. Může také obsahovat některá varovná/chybová hlášení, takže je užitečné tento adresář pravidelně sledovat.

- Serverové události. Tato složka shromažďuje události generované AMS (s výjimkou specifických událostí, které jsou z tohoto pohledu vyfiltrovány). To obsahuje jednoduchý audit - položky dokumentující, kdy byl server zastaven/spuštěn, kdy byl vytvořen nový objekt atd.

- Vlastní filtr událostí. Tato složka vám umožňuje definovat vlastní masku, takže můžete přesně určit události, které chcete vidět. Možnosti filtrování jsou: podle dílčího řetězce, podle typu, podle kategorie a podle času.

Události nemohou být smazány z logu přímo. Staré položky mohou být odstraněny prostřednictvím úlohy Údržba Databáze (použitím volby Smazat Události Starší Než ... Dnů). Pro více informací o úlohách týkajících se Údržby

DB se prosím podívejte do odpovídající kapitoly.

6.4 Licencování v ADNM

ADNM poskytuje velmi flexibilní model licencování. Všechny kontroly licencí jsou prováděny na serveru. To znamená, že všechny spravované stroje používají jeho licenci. Není třeba distribuovat licenční soubor klientům (ve skutečnosti není licenční soubor na klientských strojích vůbec přítomen - tím je zabráněno možnému zcizení tohoto souboru). Pokud licence na serveru vyprší, stane se tak automaticky také na všech klientech.

Ve většině případů toto chování pracuje správně. Nicméně existují situace, kdy tento způsob nemůže být použit, např. v případě, kdy nějaké stroje nejsou permanentně připojeny k serveru (např. laptopy). V ADNM je speciální mechanismus ošetřující tyto situace. Jmenovitě u notebooků je vyžadováno, aby se připojily k serveru minimálně jednou za 21 dnů (3 týdny; tato hodnota je zakódována do programu a nelze ji změnit). Po této době přestanou spravované produkty na klientském stroji fungovat (včetně aktualizací virové databáze), a to do okamžiku, kdy dojde opět ke spojení se serverem, který poskytne platnou licenci.

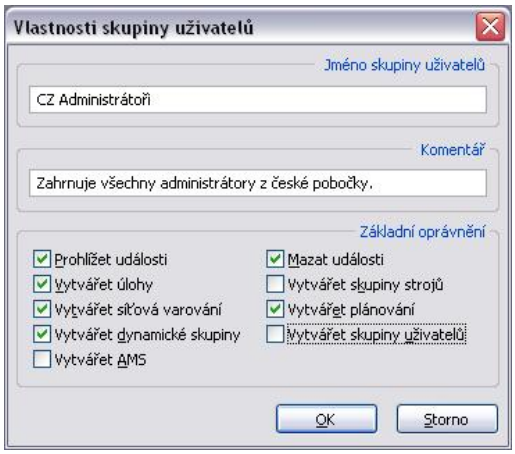
Poznámka

Pokud se vyskytne potřeba vzít stroj z dosahu AMS na dobu delší než 21 dní, je nutné na počítač zkopírovat licenční soubor (ručně).

6.5 Správa Uživatelů v ADNM

ADNM podporuje plnohodnotný systém uživatelů a jejich práv. Na AMS může být vytvořeno libovolné množství uživatelských účtů. Uvědomte si prosím, že tyto účty nemají vůbec nic společného s účty Windows domén/skupin.

Uživatelé jsou uloženi ve zvláštních složkách - ve Skupinách Uživatelů. Ve výchozím nastavení existují dva uživatelé a dvě skupiny uživatelů: účet Administrátora (ve skupině Administrátoři) a účet Host (ve skupině Hosté). Tyto dva účty mají zvláštní význam a neměly by být měněny (jediná věc, která by změněna být měla, je heslo Administrátorova účtu). Účet Administrátora má neomezený přístup ke všem objektům ADNM. Účet Hosta má velmi omezená práva a víceméně nemůže měnit (nebo ani číst) žádné objekty. Heslo pro účet Hosta je prázdné a nemůže být změněno.



Obrázek 6.10. Editor uživatelských skupin

Každý objekt v ADNM (úloha, plánovač, varování, instalační balíček atd.) má svůj Access Control List (ACL). ACL určuje přístupová práva k objektu. Existují čtyři úrovně přístupu: čtení, zápis, mazání a spuštění. Je tu také speciální typ přístupu - 'Úplné Řízení', který spojuje všechny čtyři typy přístupu. Jakýkoliv účet nebo skupina může být zahrnuta do ACL objektu, s jakoukoliv úrovní přístupu (jedinou výjimkou jsou členové skupiny Administrátorů, kteří mají vždy Úplné Řízení na všechny objekty).

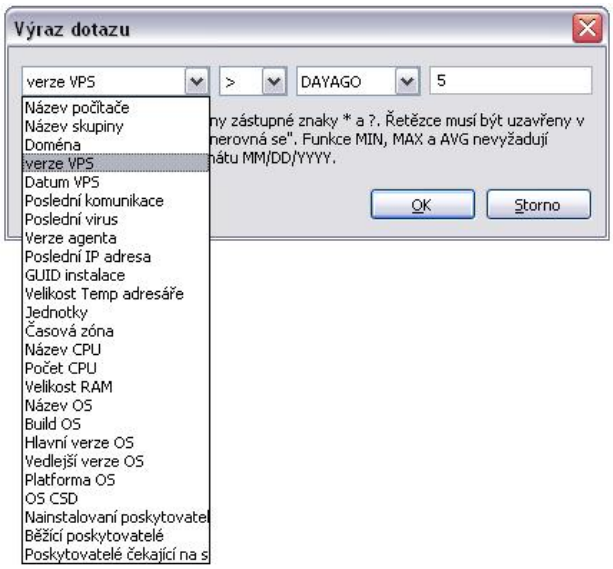
Tento robustní systém uživatelských práv usnadňuje administraci (zejména ve větších společnostech s mnoha pobočkami s vlastními administrátory). Typický způsob nastavení uživatelů by mohl spočívat ve vytvoření účtů pro každého administrátora, který bude pracovat s ADNM, ale omezit jeho/její pravomoc pouze na počítače/objekty, které spadají pod jeho správu. To znamená, že pokud je administrátor např. zodpovědný za správu LAN_A, vytvoříte zvláštní skupinu počítačů pro LAN_A v Katalogu Počítačů a účtu zmíněného administrátora přiřadíte úplný přístup k této skupině. Pro tuto skupinu byste měl také vytvořit zvláštní úlohy (tedy úlohy, jež budou běžet pouze na této skupině) a omezit přístup ke všem ostatním úlohám. Tímto způsobem můžete mít tolik poboček/lokálních administrátorů, kolik potřebujete, přičemž každý bude moci pracovat pouze uvnitř své vlastní oblasti (části Katalogu Počítačů).

6.6 Používání Dynamických Skupin Počítačů

Dynamické skupiny počítačů poskytují mocnou metodu vyhledávání, správy a další kategorizace Katalogu Počítačů. Můžete si jí představit jako vysoce výkonný filtr Katalogu Počítačů, ale ve skutečnosti toho umí mnohem více.

Každá dynamická skupina je vytvořena nastavením výrazů a logických operátorů. Příkladem výrazu je "computer_name = NEMESIS" a příkladem logického operátoru je AND nebo OR. Výrazy zahrnují operátory jako

rovná-se, menší-než, větší-než a také může obsahovat funkce, jako Min, MAX nebo AVERAGE.



Obrázek 6.11. Editor výrazů dynamických skupin. Výrazy mohou být spojeny pomocí AND a OR a seskupiny pomocí závorek.

Následující parametry jsou podporovány pro vytváření výrazů:

- **Název počítače** (typ: řetězec). Název počítače, jak je uložen v Katalogu.
- **Název skupiny** (typ: řetězec). Název (statické) skupiny, ve které je počítač uložen v Katalogu.
- **Doména** (typ: řetězec). Název domény Windows nebo pracovní skupiny, v níž počítač sídlí.
- **Verze VPS** (typ: řetězec se třemi tečkami). Verze současného VPS souboru (virové databáze), nainstalovaného na počítači.
- **Časová značka VPS** (typ: řetězec). Datum uvolnění současného VPS souboru (virové databáze), nainstalovaného na počítači.
- **Poslední komunikace** (typ: řetězec). Datum a čas posledního kontaktu se strojem.
- **Poslední virus** (typ: řetězec). Název posledního viru nalezeného na počítači.
- **Verze agenta** (typ: řetězec se třemi tečkami). Verze avast! agenta nainstalovaného na stroji (ve formátu x.x.x.x, např. 4.1.102.0).
- **Poslední IP adresa** (typ: řetězec se třemi tečkami). Poslední IP adresa,

kterou stroj použil při kontaktu se serverem.

- **Instalační GUID** (typ: řetězec). GUID (globally-unique-identifier) agenta nainstalovaného na stroji.

- **Nainstalovaný avast! NetClient** (typ: logická hodnota, t.j. 0 nebo 1). Logická hodnota určující, zda je na stroji nainstalován avast! NetClient Edition.

- **Nainstalovaný avast! NetServer** (typ: logická hodnota, t.j. 0 nebo 1). Logická hodnota určující, zda je na stroji nainstalován avast! NetServer Edition.

- **Nainstalovaný Mirror** (typ: logická hodnota, t.j. 0 nebo 1). Logická hodnota určující, zda je na stroji nainstalovaný produkt "mirror druhé úrovně".

- **Stroj je nutné restartovat** (typ: logická hodnota, t.j. 0 nebo 1). Logická hodnota určující, zda agent na stroji čeká na restart (např. z důvodu nekompletní aktualizace).

- **Místo v Temp adresáři** (typ: celé čéslo). Celkové volné místo v adresáři TEMP daného stroje, v megabytech.

- **Disky** (typ: řetězec). Seznam logických jednotek na stroji, oddělených středníkem (např. "A;C;D").

- **Časové pásmo** (typ: celé číslo). Časové pásmo stroje (posunutí počtu minut oproti GMT).

- **Název CPU** (typ: řetězec). Název procesoru nainstalovaného na stroji, jak jej prezentuje systém.

- **Počet CPU** (typ: celé číslo). Počet procesorů nainstalovaných ve stroji.

- **Velikost RAM** (typ: celé číslo). Velikost operační paměti nainstalované ve stroji, v megabytech.

- **Název OS** (typ: řetězec). Název operačního systému, který běží na stroji, např. "Windows XP".

- **Hlavní verze OS** (typ: celé číslo). Hlavní číslo verze operačního systému, běžícího na stroji. Např. retail verze Windows XP má tuto hodnotu nastavenou na 5.

- **Vedlejší verze OS** (typ: celé číslo). Vedlejší číslo verze operačního systému

běžícího na stroji, např. retail verze Windows XP má tuto hodnotu nastavenu na 1.

- **Build OS** (typ: celé číslo). Číslo "buildu" operačního systému, např. retail verze Windows XP má tuto hodnotu nastavenu na 2600.

- **Platforma OS** (typ: celé číslo). ID platformy operačního systému. Windows 9x/ME mají tuto hodnotu 1, Windows používající technologii NT 2.

- **CSD OS** (typ: řetězec). Název service packu, např. "Service Pack 3".

- **Nainstalovaní poskytovatelé** (typ: řetězec). Seznam rezidentních poskytovatelů (modulů) avastu nainstalovaných na počítači. Poskytovatelé jsou označeni podle jejich krátkých jmen (např. STANDARD jako Standardní Štít, MAIL jako Internet Mail a OUTLOOK jako Outlook/Exchange) a jsou odděleni čárkou.

- **Běžící poskytovatelé** (typ: řetězec). Seznam rezidentních poskytovatelů (modulů), běžících na stroji.

- **Čekající poskytovatelé** (typ: řetězec). Seznam rezidentních poskytovatelů (modulů), jejichž momentální status je "čeká na spuštění subsystému".

"Řetězec se třemi tečkami" znamená řetězec ve formátu "a.b.c.d". Používá se pro čísla verzí, stejně jako pro IP adresy. Všechny hodnoty řetězce mohou používat zástupný znak *, např. maska NEM* vyhovuje řetězcům NEMO a NEMESIS, ale nikoliv NEON. Poslední komunikace a časová značka VPS používají datum ve formátu MM/DD/YYYY.

Podporovány jsou následující operátory:

- Rovný-čemu, **=**.

- Nerovný-čemu, **!=**.

- Menší-než, **<**.

- Větší-než, **>**.

- Menší-než-nebo-rovný-čemu, **<=**.

- Větší-než-nebo-rovný-čemu, **>=**.

Podporovány jsou následující funkce:

- **MIN**. Tato funkce vrací počítač(e) s minimální hodnotou parametru. Nemá

žádné operandy.

- **MAX**. Tato funkce vrací počítač(e) s maximální hodnotou parametru. Nemá žádné operandy.
- **AVG**. Tato funkce vrací počítač(e) s průměrnou hodnotou parametru. Nemá žádné operandy.
- **DAYSAGO**. Tato funkce vrací počítač(e), u nichž se parametr (který musí být časový) vyskytl nejpozději před N dny. Operand určuje hodnotu N.
- **HOURSAGO**. Tato funkce vrací počítač(e), u nichž se parametr (který musí být časový) vyskytl nejpozději před N dny. Operand určuje hodnotu N.
- **MINUTESAGO**. Tato funkce vrací počítač(e), u nichž se parametr (který musí být časový) vyskytl nejpozději před N minutami. Operand určuje hodnotu N.

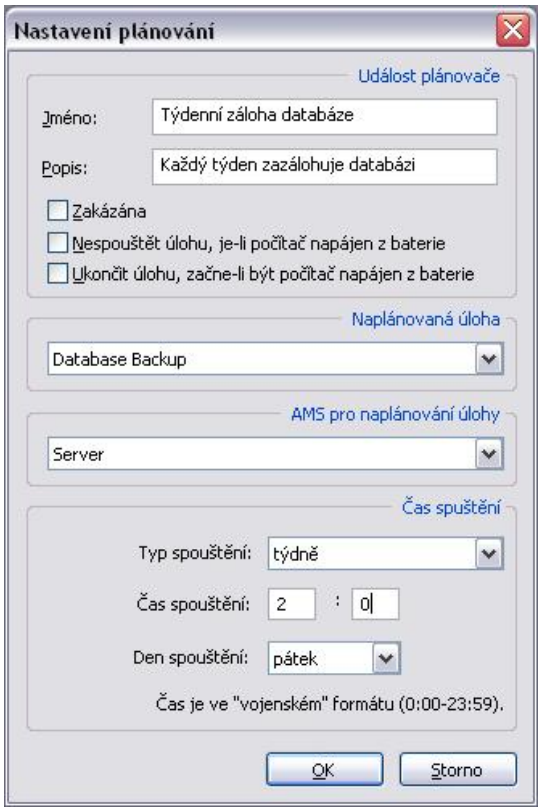
Logické operátory pro spojení více výrazů jsou jen dva: **OR** a **AND**. Definice dynamické skupiny může být vytvořena mnoha výrazy spojenými těmito logickými operátory.

6.7 Další užitečné úkony

6.7.1 Plánování pravidelných testů

Pro zvýšení bezpečnosti je vhodné naplánovat pravidelné testy všech pevných disků na všech spravovaných strojích. Nejdůležitějším prvkem ochrany je samozřejmě rezidentní skener, není ale nad jistotu, že se přes něj opravdu nic nedostalo.

Obyčejně stačí naplánovat skenování jednou za týden. Spouštění testů nastavte na dobu, kdy se počítače nepoužívají, protože probíhající sken může podstatně zpomalit počítač a uživatelé jej nemohou žádným způsobem zastavit. Vhodnou dobou je čas oběda, víkend nebo noc (pokud necháváte počítače přes noc zapnuté). Vlastnost vypršení úlohy určuje, jak dlouho tato zůstane ve frontě (to se týká všech klientských úloh, nejen testovacích). Pokud je např. nastavena na 6 hodin a sken je naplánován na 02:00, bude-li počítač zapnut před 08:00 úloha se spustí, bude-li ale zapnut po 08:00, úloha se nespustí (v seanci úlohy bude indikován time-out). To je pohodlný způsob jak zabránit úlohám, které mají běžet např. v noci, ve spouštění v pracovní době a snižovaly tak produktivitu uživatelů.



Obrázek 6.12. Plánovač úloh

6.7.2 Nasazení ochrany na nové počítače

Ve většině sítí počítače přicházejí a odcházejí. Efektivní správa sítě, která se často mění, může být noční můrou. ADNM naštěstí obsahuje mechanismus, který administrátorům pomáhá automaticky nasadit avast! na nové stroje.

Dosažení tohoto cíle dá trochu práce, ale jedná se o zajímavý příklad toho, jak lze využít několika schopností ADNM k dosažení pokročilé funkčnosti. Jmenovitě použijeme následující komponenty:

- Úlohy "Hledání počítačů"
- Instalační úlohy a s nimi svázané instalační balíčky
- Dynamické skupiny počítačů
- Řetězení úloh
- Plánování úloh

Začneme přípravou instalačního balíčku pro produkt avast! NetClient (pokud jsme tak již neučinili). Dále vytvoříme instalační úlohu a přiřadíme jí instalační balíček. Zajistěte, aby vložené parametry domén/skupin byly opravdu platné a umožňovaly tak instalaci produktu na všech počítačích v síti. Dále vytvoříme

dynamickou skupinu pro všechny počítače bez nainstalovaného agenta. To lze udělat několika způsoby, ale nejpřímější volbou je použití jednoduchého výrazy "Verze agenta je rovná nule". Použijeme tuto dynamickou skupinu jako cíl pro instalační úlohu. Zbývá vytvořit úlohu hledání počítačů a použít funkci Řetězení úloh tak, abychom zajistili spuštění instalační úlohy (vytvořené v minulém kroku) poté, co bude úloha hledání počítačů úspěšně dokončena. Nakonec naplánujeme úlohu hledání počítačů (např. denně), čímž celý proces zautomatizujeme.

7

Reportování v ADNM

ADNM nabízí mocné schopnosti reportování, jaké u jiného srovnatelného produktu na trhu nenaleznete. Můžete použít široký výběr z užitečných reportů z informací, které získává AMS od klientů, a exportovat je do mnoha oblíbených formátů. Reporty můžete dokonce automaticky rozesílat týmu administrátorů nebo vedení.

Reportování, ostatně skoro jako vše ostatní, je v ADNM realizováno prostřednictvím určitých úloh. Reportovací úlohy jsou seskupeny ve zvláštní složce v konzoli, v kategorii Serverové úlohy.

Obrázek 7.1. Reportovací úlohy ve stromu konzole

7.1 Reporty ADNM

ADNM obsahuje okolo dvaceti předdefinovaných reportů, popsaných níže.

7.1.1 Přehled strojů v síti

Tento report ukazuje všechny počítače v síti. Existuje ve dvou základních verzích. První typ pouze podává přehled a počítačích s informací, do které skupiny patří, jaký operační systém na nich běží a jaké spravované produkty jsou na nich nainstalovány. Druhý možný typ reportu obsahuje všechny zmíněné informace plus detailní informace o počítačích v síti. Uvědomte si, že tento report může být velmi rozsáhlý a obyčejně je dobré snížit jeho velikost aplikováním dalších filtrů. Možnosti filtrování zahrnují masku názvu skupiny a

masku názvu počítače. Můžete také určit řazení údajů podle názvu skupiny/počítače v sestupném či vzestupném pořadí.

Obrázek 7.2. Přehled strojů v síti

7.1.2 Přehled strojů v síti s ohledem na avast!

Tento report vytváří přehled všech strojů v síti se zvláštním ohledem na počítače, které mají nainstalovaný avast! klient. Tento report může být generovaný ve zkrácené či kompletní variantě s detailními informacemi o každém počítači. Nastavení tohoto reportu jsou stejná jako u předešlého. Skládá se také z výsečového diagramu, ze kterého může administrátor snadno zjistit, na kterých počítačích je avast! nainstalován a na kterých nikoliv.

Obrázek 7.3. Přehled strojů v síti s ohledem na avast!

7.1.3 Přehled strojů v síti podle verze avastu

Tímto vytváříme přehledný report (s výsečovým diagramem a tabulkovým zobrazením), který zobrazuje všechny verze avastu, jež jsou nainstalovány na počítačích v síti. Report může také zahrnovat stroje bez nainstalovaného avastu, takže může být použit také k ověření celkového stavu antivirové ochrany v síti.

7.1.4 Stroje v síti podle verze VPS

Tento report se podobá předchozímu, ale namísto verze avastu je zde klíčem verze virové databáze (VPS souboru). I zde je možné zahrnout do reportu počítače, na nichž není avast! nainstalován, filtrovat stroje podle masky domény apod.

7.1.5 Přehled strojů v síti podle poslední komunikace

Jedná se o v tabulce uvedený výpis všech strojů v síti, které jsou seřazeny podle času, kdy naposledy reportovali svůj stav AMS. Užitečné pro zjišťování problémů s komunikací, stejně jako pro hledání zombie-počítačů (tj. strojů

zahrnutých v konzoli, které již ale nejsou součástí sítě). Jako ostatní reporty přehledů sítě, i tento nabízí dostatečné možnosti úprav dle konkrétních představ.

7.1.6 Top N viry

Tento report zobrazuje Top N viry (za využití výsečového a sloupcového diagramu), detekované za určité časové období, zahrnujíc informace o jejich celkovém počtu a datu první a poslední detekce. Můžete upravit parametr N, který určuje počet záznamů, jenž bude zahrnut do reportu (např. Top 5, Top 10 apod.). I když tento parametr není omezen, doporučujeme nepoužívat čísla větší než 20, neboť takový report se může stát poněkud nepřehledným.

Obrázek 7.4. Report Top N viry

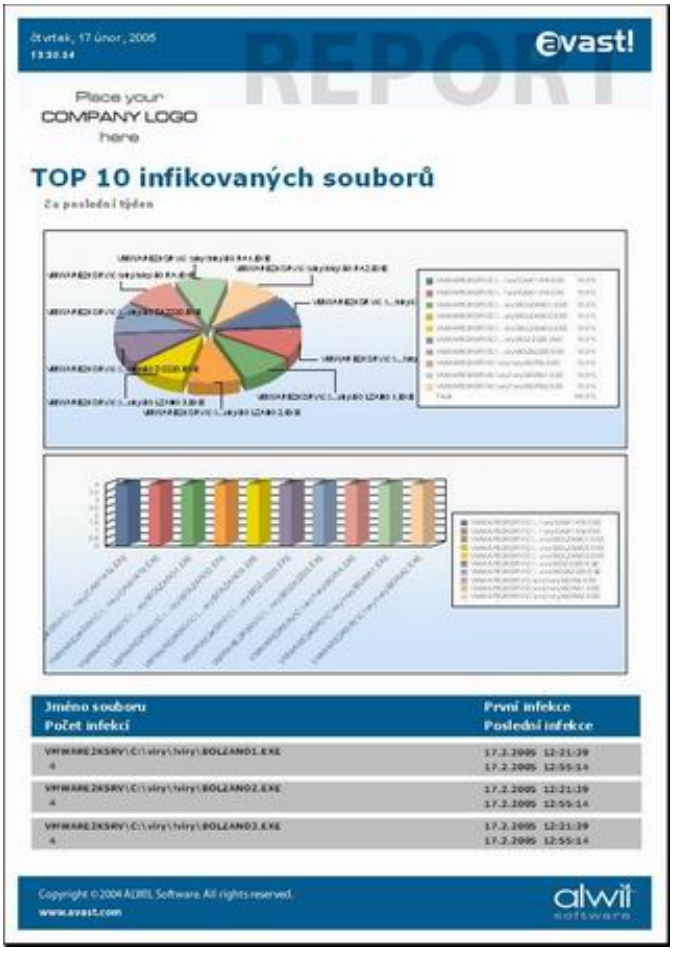
7.1.7 Akce s Top N viry

Tento report je velmi podobný předchozímu, ale zobrazuje akce, které byly provedeny s Top N viry, nikoliv tedy viry samotné. Výběr dat zobrazených v reportu může být určen časovým úsekem, maskou názvu viru a - jako obvykle -

parametrem N. Opět - nedoporučujeme nastavovat hodnotu parametru N větší než 15.

7.1.8 Top N infikovaných souborů

Tento report ukazuje Top N infikovaných souborů ve formě výsečového a sloupcového diagramu, doprovázeném obsáhlým seznamem těchto souborů, spolu s jejich počtem a časovými informacemi. Názvy infikovaných souborů začínají názvem počítače, na kterém byl virus detekován. Můžete upravit parametr N, který určuje počet položek zahrnutých v reportu. I když není tento parametr omezen, nedoporučujeme zadávat větší hodnoty než 15 - 20, jinak se report může stát méně čitelným. Dalším konfiguračním parametrem je časové rozpětí (včetně vlastního rozpětí), pro které se infikované soubory zahrnou do reportu.



Obrázek 7.5. Report Top N infikovaných souborů

7.1.9 Top N infikovaných počítačů

Tento report zobrazuje přehled (výsečový diagram a tabulku) Top N nejvíce

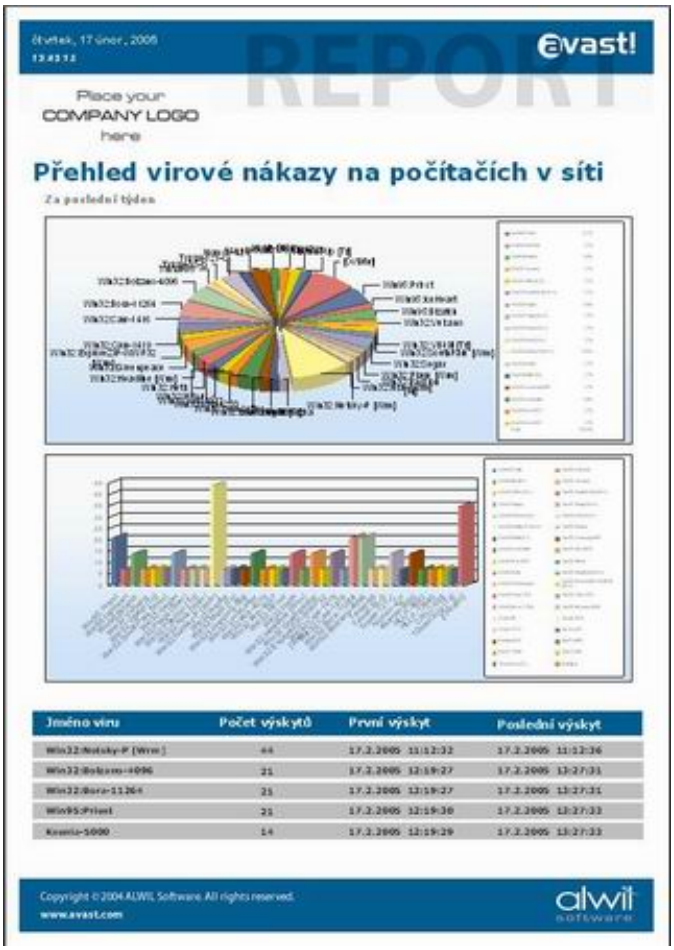
infikovaných počítačů v síti. Můžete určit, zda má report v tabulce obsahovat také detailní informace o počítačích. Je možné upravit parametr N, který určuje, kolik položek bude do reportu zahrnuto. A zase - nedoporučujeme zadávat hodnoty vyšší než 15 - 20. Jako obvykle můžete definovat masku skupiny či domény a časový úsek.

7.1.10 Přehled zdrojů infekce

Tento report vytváří přehlednou tabulku, která ukazuje relativní četnost zdrojů infekce (mail, pevný disk, výměnné médium, síť, skript). Můžete určit časovou hodnotu, pro kterou bude report generován. Report také obsahuje výsečový diagram pro snažší představu.

7.1.11 Přehled infekce sítě

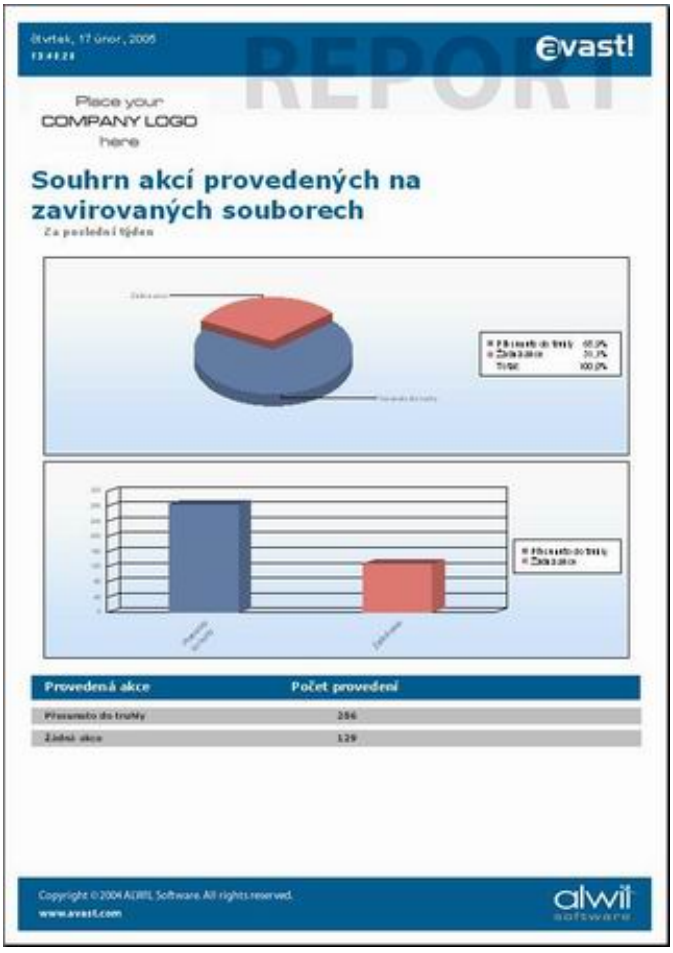
Report Přehled infekce sítě je podobný reportu Top N viry. Narozdíl od něho ale ukazuje seznam všech virů, které byly nalezeny v síti (ne pouze Top N). Pokud je počet virů příliš velký, takže se report stává nepřehledným, doporučujeme zredukovat seznam virů aplikováním masky nebo zúžit časové rozpětí, pro které se bude report generovat.



Obrázek 7.6. Report Přehled infekce sítě

7.1.12 Přehled akcí s viry

Výsledkem tohoto reportu je tabulkové a grafické znázornění akcí, jež byly provedeny s infikovanými soubory (smazán, opraven, přesunut do virové truhly atd.). Opět můžete nastavit časový úsek, pro nějž bude report generován.



Obrázek 7.7. Report Přehled akcí s viry

7.1.13 Přehled změn logických disků

Tento report je poněkud odlišný, neboť se nevztahuje přímo k antivirové ochraně. Místo toho zobrazuje přehled změn mapování logických jednotek na spravovaných počítačích (např. připojení USB disku, mapování síťových jednotek atd.). Report můžete upravit specifikací časového období.

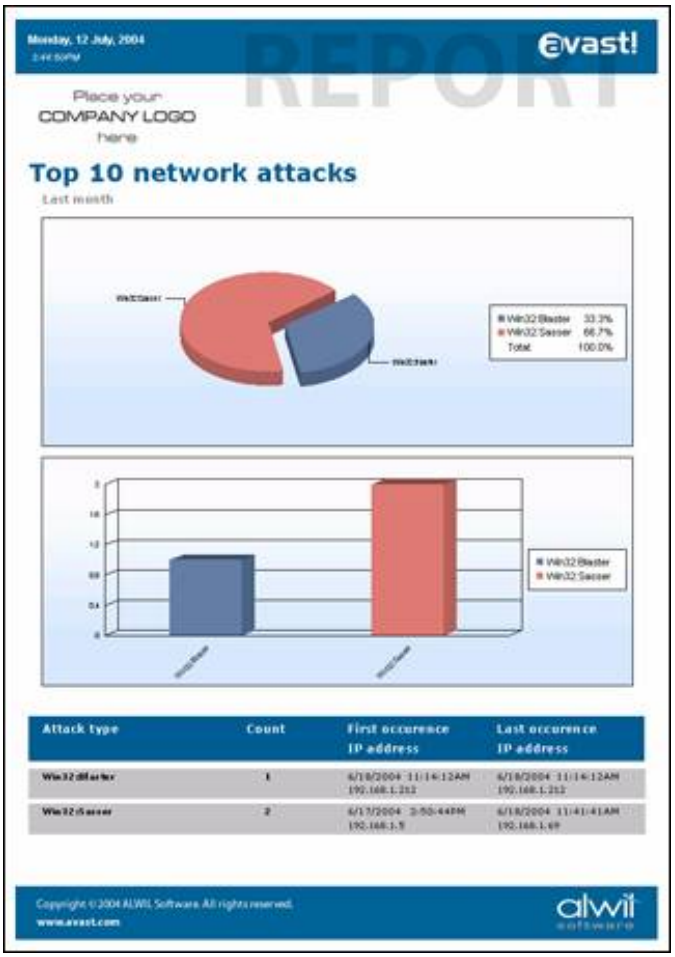
7.1.14 Top N napadených počítačů

Tento report zobrazuje seznam Top N počítačů, které byli nejčastěji napadeny

(neúspěšně) síťovým červem, detekovaným poskytovatelem Síťový štít. I zde můžete určit parametr N stejně jako časový úsek, ze kterého budou data zahrnuta do reportu. Z důvodu lepší přehlednosti je tento report generován ve formě výsečového diagramu, sloupcového grafu a tabulky.

7.1.15 Top N síťových útoků

Report Top N síťových útoků zobrazuje přehled síťových útoků detekovaných rezidentním poskytovatelem Síťový štít. Opět můžete definovat parametr N, který určí, kolik útoků bude zahrnuto, stejně jako časové období, ve kterém byly útoky detekovány. Report také obsahuje vyčerpávající informace o útocích, včetně IP adres ze kterých přišly a časových údajů. Pro zvýšení přehlednosti obsahuje report také výsečový diagram a sloupcový graf.

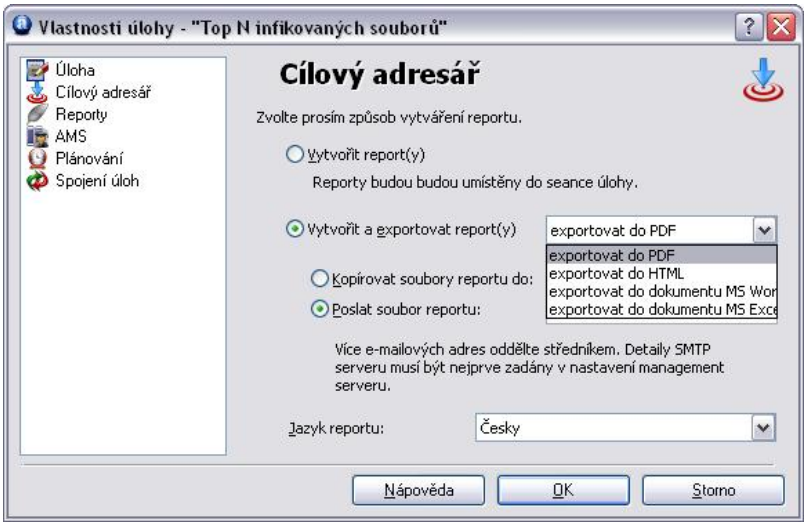


Obrázek 7.8. Report Top N síťových útoků

7.2 Výstupy reportů

Reporty mohou být generovány buď přímo do seance úlohy (kde je lze prohlížet a/nebo tisknout prostřednictvím integrovaného prohlížeče reportů),

nebo mohou být exportovány mimo databázi. Výstupy reportů zahrnují soubory (možné na sdíleném síťovém disku) a e-mail. Formáty exportů zahrnují PDF, HTML, DOC a XLS. Všechny tyto parametry lze nastavit ve vlastnostech reportovací úlohy.



Obrázek 7.9. Vlastnosti reportovací úlohy

7.3 Použití vlastního loga společnosti

Jak můžete vidět na screenshotu reportu výše, ADNM vám umožňuje umístit do všech generovaných reportů vlastní logo. Taková úprava může pomoci prosazovat identitu společnosti (zejména na výtiscích), stejně jako pomoci administrátorům, kteří spravují více než jednu síť, rychle rozlišit reporty generované pro jednotlivé AMS.

Pro definování vlastního loga použijte stránku Ostatní v dialogu globálních nastavení. Podporované jsou formáty png, jpg a bmp. Obrázek může mít libovolnou velikost, doporučujeme ale zachovat poměr stran 5:14, jinak se projeví roztažení. Také je doporučeno nepoužívat velké obrazové soubory, neboť obrázek bude součástí každého vygenerovaného reportu a pokud bude jeho velikost velká, zabere také zbytečně velké místo v databázi.

8

Údržba AMS

8.1 Údržba databáze

Díky tomu, že je ADNM postaveno na SQL databázi, vyžaduje pravidelnou údržbu. Za těmito účely existuje v ADNM speciální typ serverových úloh - úlohy údržby DB. S úlohou Údržba DB můžete provádět následující:

- Provádět zálohu databáze.
- Provádět pročištění databáze

Je vysoce doporučeno naplánovat pravidelné zálohování databáze. Zálohu ADNM databáze můžete začlenit do zálohovací strategie celé vaší sítě. Doporučený způsob je buď využít váš vlastní zálohovací software k přímému zálohování SQL serveru (pokud to podporuje - podívejte se prosím do dokumentace k vašemu zálohovacímu programu), nebo použít úlohu údržby DB přímo v ADNM pro zálohu databáze do souboru a následně zálohovat tento soubor pomocí standardních metod.

Vyčištění databáze se používá k odstranění starých záznamů z databáze. Můžete se rozhodnout, jak staré záznamy bude udržovat. Jakmile - pochopitelně - smažete staré záznamy, nebude možné např. generovat reporty ze starších záznamů, takže je důležité správně rozhodnout, kolik záznamů potřebujete. Vyčištění databáze je důležité jako prevence před jejím nekonečným růstem. Úloha Údržba DB nabízí také možnost smazání takzvaných osiřelých záznamů, což může zredukovat velikost databáze.

8.2 Nástroj údržby AMS

V ADNM je rovněž několik věcí, které není možné provést prostřednictvím konzole, ale musí být provedeny přímo na serveru. Za těmito účely je k dispozici speciální program zvaný „Nástroj údržby AMS“, který poskytuje prostředky k dosažení většiny těchto úkolů.

Nástroj údržby AMS může být použit zejména k provedení těchto úkolů:

- Změna licenčního souboru.
- Změna serverového SSL certifikátu.
- Obnovení databáze (naopak zálohování databáze může být vyvoláno použitím úloh správy databáze z administrátorské konzole, včetně jejího pravidelného naplánování). **Poznámka:** obnovením databáze dojde ke zničení jejího současného obsahu. Je proto vhodné vytvořit novou zálohu databáze těsně před tím, než provedete obnovení.
- Kontrola správnosti databáze.
- Smazání a znovuvytvoření databáze. To proveďte v případě, že chcete začít úplně od začátku. **Poznámka:** smazáním nebo znovuvytvořením databáze dojde ke ztrátě jejího předchozího obsahu. Než tedy přistoupíte k těmto operacím, zálohujte.
- Změna detailů připojení databáze. Tuto možnost použijte např. v případě, kdy chcete přesunout databázi na jiný SQL server, nebo aktualizovat z MSDE na plný SQL server. Měli byste vytvořit zálohu, změnit detaily připojení databáze a nakonec obnovit databázi ze zálohy).

Obrázek 8.1. Hlavní okno Nástroje údržby AMS

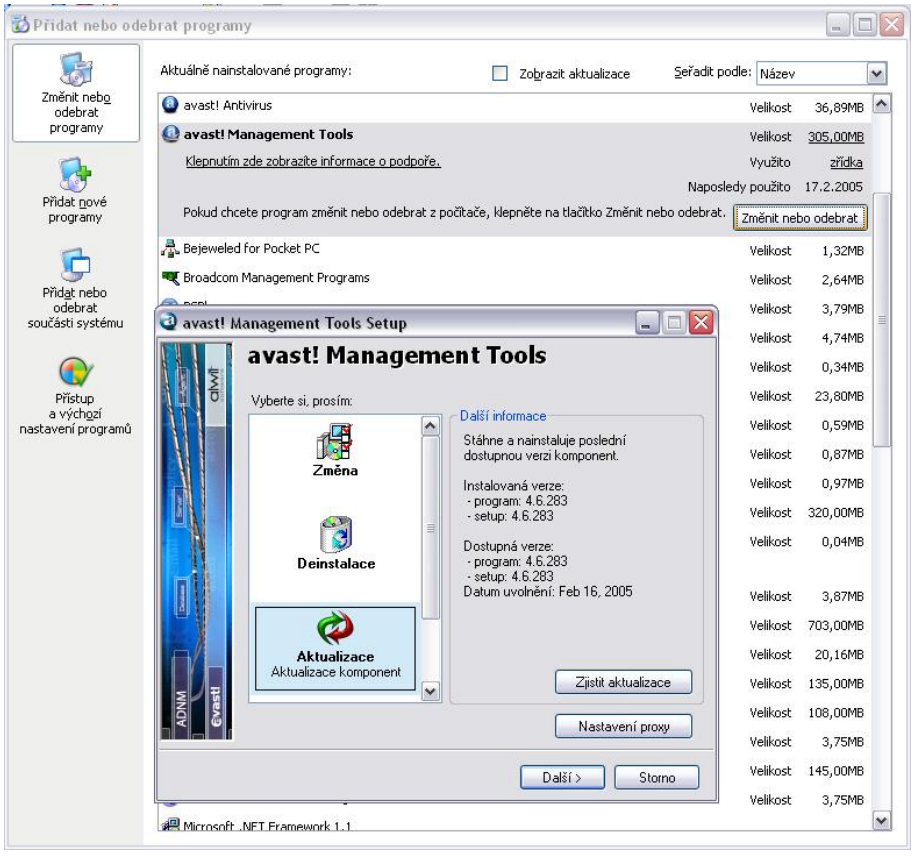
Nástroj údržby databáze naleznete v menu START pod položkou ADNM. Jak už bylo řečeno, nemůže být spuštěn vzdáleně, ale měl by fungovat správně přes vzdálené připojení plochy (remote desktop) nebo připojením přes terminálový server.

8.3 Změna nastavení proxy

Jelikož ADNM poskytuje mirrorování aktualizací, je důležité mít správně nastaveny detaily proxy serveru. Tyto detaily jsou zpočátku nastaveny při instalaci AMS, ale někdy může být nezbytné je změnit. Pro změnu nastavení proxy serveru AMS postupujte následovně: otevřete Ovládací panely, Přidat/Odebrat programy, zvolte "avast! Management Tools". Klikněte na tlačítka Změnit/Odebrat. Objeví se okno, kde jedna z možností je i změna nastavení proxy serveru.

8.4 Aktualizace AMS/Konzole

Zajištění pravidelných aktualizací lokálních klientů (antivirových agentů) je sice nejdůležitější, ale není na škodu udržovat aktuální také AMS a konzoli(e). Aktualizace pro AMS a konzole jsou vydávány po několika měsících. Uvolňovány jsou vždy ve stejném čase a se stejným číslem verze. Tato sekce vás provede procesem aktualizace AMS a konzole.



Obrázek 8.2. Aktualizování AMS a/nebo konzole

Varování

Aktualizace AMS je poněkud složitější úlohou, protože zahrnuje také aktualizaci SQL databáze. Pokud došlo ke změně formátu databáze (tabulky, uložené procedury atd.), vyžaduje to také převedení dat do nového formátu. Při aktualizaci dojde obyčejně k určitému prostoji a rovněž může být vyžadován restart serveru. Je proto rozumné naplánovat aktualizaci na víkend nebo alespoň na mimopracovní dobu.

Při aktualizaci AMS a konzole postupujte následovně:

1. Zavřete všechny spuštěné konzole.

2. Aktualizujte AMS. Otevřete Ovládací panely (přímo na AMS), zvolte Přidat/Odebrat Programy a označte "avast! Management Tools". Klikněte na tlačítko Změnit/Odebrat. Otevře se okno, kde jedna z nabízených možností je Aktualizace. Zvolte ji a klikněte na Další. Můžete nejprve zkusit tlačítko Zjistit aktualizace, čímž se vám zobrazí informace o číslech verzí (současná verze a nejnovější verze dostupná ke stažení). Jakmile aktualizace skončí, můžete být vyzván k restartu serveru. Tlačítkem OK potvrďte a nechte server zrestartovat.

3. Aktualizujte všechny konzole. Postupujte stejně jako při aktualizace AMS, ale tentokrát na stroji (strojích), na kterých jsou nainstalovány konzole.

Poznámka

Nespouštějte prosím žádnou z konzolí do doby, než bude aktualizace dokončena, tj. mezi aktualizací AMS a aktualizací konzolí. V opačném případě se objeví neshoda verzí a program nebude pracovat správně.

4. Volitelně proveďte programové aktualizace všech síťových agentů za použití Aktualizačních úloh. Tím zajistíte, že všechny součásti systému budou zcela aktuální.

9

Pokročilá témata

9.1 Monitorování AMS logů

Kromě událostí zapisovaných přímo do databáze - viditelných v klientských a serverových log souborech, které si můžete prohlédnout ve složce Události v administrátorské konzoli - loguje AMS také určité události do zvláštních log souborů. Tyto logy se používají zejména při řešení problémů. Nejsou zapisovány do databáze, protože spojení s databází nemusí být funkční.

Většina logů je uložena ve složce adnm\data\log. K jejich prohlížení můžete použít Poznámkový blok (Notepad) nebo jakýkoliv jiný textový program. Nejdůležitější z nich jsou především Error.log a Warning.log. Logy lze prohlížet také přímo z konzole, za použití položky nabídky Zobrazit / Ukázat AMS Logy. Konzole otevírá log soubory ve vašem výchozím webovém prohlížeči, takže si je můžete mimo jiné také přidat do Oblíbených, chcete-li. Prohlížení z konzole funguje samozřejmě pouze pokud se můžete připojit k AMS, tzn. služba AMS běží - což v případě problémů nemusí vždy platit.

Log soubory pro mirror se ukládají do složky adnm\mirror\logs, a instalační/aktualizační položky AMS zase do logu adnm\setup\setup.log. Oba mohou být také otevřeny volbou Zobrazit / Ukázat AMS Logy.

9.2 Jak se klienti dívají po AMS

ADNM byl projektován tak, aby správně fungoval i v sítích s nespolehlivým spojením, se stále se měnícím hardware a jinými problémy, ztěžujícími administraci. Jedním z klíčových prvků tohoto návrhu je, že agenti nasazení na spravovaných strojích se vždy snaží najít použitelný AMS. Klienti mohou stroj chránit i v případě dlouhých výpadků spojení s AMS.

Toto je algoritmus, jaký agenti používají při hledání AMS:

1. Agent použije předdefinovaný server. Pokud toto selže, tak

2. zkouší použít posledním známou funkční adresu serveru. Selže-li, pak

3. zkouší nalézt server v síti posíláním paketů (broadcast) a čekáním na odpověď. Selže-li, pak

4. zkouší se připojit ke stroji s pevně zapsaným názvem avastms.

9.3 Přemístění AMS na jiný stroj

Jelikož klienti používají více různých metod k nalezení aktivního AMS (jak je popsáno v předchozí sekci), je poměrně snadné přenést AMS na jiný stroj, zejména pokud používáte plný SQL server a nemusíte přesouvat databázi, ale pouze samotný AMS. Stejnou proceduru použijete také v případě, kdy dojde k problému s hardware na AMS, nebo pokud chcete vyměnit hardware za silnější stroj.

Při přemísťování AMS (pouze AMS, nikoliv databáze) na jiný stroj postupujte podle následujících kroků:

1. Nainstalujte AMS na nový stroj. V okamžiku, kdy budete dotázáni na detaily SQL serveru, zadejte údaje, které právě používá starý server.

2. Jakmile je instalace dokončena, zastavte službu AMS na starém stroji (Ovládací panely / Nástroje pro správu / Služby, avast! Management Server).

3. Za použití konzole se připojte k novému serveru,

   - Ve vlastnostech odpovídající skupiny v Katalogu počítačů změňte adresu AMS serveru a

   - počkejte, než dojde k POP timeoutu na klientských strojích (5 - 15 minut, pokud jste toto nastavení neměnil v globálních nastaveních AMS).

   - Ověřte, že se klienti v síti přesouvají na nový server, tzn. že se aktualizuje položka Čas posledního připojení.

4. Pokud na novém serveru vše správně funguje, volitelně odinstalujte AMS ze starého stroje.

Při přemísťování AMS včetně databáze na jiný stroj postupujte podle těchto kroků:

1. Proveďte zálohu databáze na starém serveru.

2. Nainstalujte AMS na nový stroj. Při dotazu na detaily SQL serveru

použijte buď MSDE, nebo vyplňte informace o spojení pro novou databázi.

3. Jakmile instalace skončí, spusťte Nástroj údržby AMS (ze složky ADNM v nabídce START) a obnovte databázi ze zálohy provedené v kroku 1.

4. Ukončete službu AMS na starém stroji (Ovládací panely / Nástroje pro správu / Služby, avast! Management Server).

5. Za použití konzole se připojte k novému serveru,

   - Ve vlastnostech odpovídající skupiny v Katalogu počítačů změňte adresu AMS serveru a

   - počkejte, než dojde k POP timeoutu na klientských strojích (5 - 15 minut, pokud jste toto nastavení neměnil v globálních nastaveních AMS).

   - Ověřte, že se klienti v síti přesouvají na nový server, tzn. že se aktualizuje položka Poslední Připojený.

6. Pokud na novém serveru vše správně funguje, volitelně odinstalujte AMS ze starého stroje.

Pokud se klienti nepřipojují k novému serveru, zkuste následující:

- Zkuste stroji s AMS přiřadit DNS jméno avastsm. Klienti by měli toto speciální jméno rozpoznat a začít se ke stroji připojovat.

- Zkuste na klientech ručně změnit jméno AMS. Přihlaste se tedy jako administrátor, otevřete soubor avast\data\avast4.ini, a změňte položku ServerAddress= na adresu nového AMS. Smažte řádek s položkou LastServerAddress=xxx. Potom spusťte Editor registru, přesuňte se do HKLM\Software\ALWIL Software\avast\4.0\SS a smažte hodnoty ServerAddress a LastServerAddress. Nakonec restartujte službu "avast! NetAgent".

9.4 Model s více AMS

Za některých okolností nemusí jediný AMS postačovat. V těchto případech vám ADNM nabízí možnost instalovat více AMS ve stejné síti. Jedná se o něco jiného než je běžný případ, kdy jsou jednotlivé segmenty sítě od sebe zcela odděleny a vy jednoduše instalujete samostatný AMS pro každý segment zvlášť. Více AMS je organizováno ve stromové struktuře. Každý AMS je odpovědný za svou vlastní podskupinu klientských strojů. Veškeré zásady jsou uloženy

(replikovány) na všech AMS, ale každý AMS udržuje výsledky úloh pouze od svých vlastních klientů - kromě kořenového AMS, který posléze ukládá výsledky ze všech klientů. Díky tomu lze na kořenovém AMS reportovat celopodnikovou síť.

Při instalaci ADNM v modelu s více AMS postupujte prosím následovně:

1. Nainstalujte zvlášť všechny AMS, typicky jeden pro každou LAN, a rozhodněte, který z nich bude kořenový ("rodič"). Obyčejně, ale nikoliv nezbytně, to bývá ten v hlavním sídle společnosti.

Poznámka

Žádný z počítačů by neměl být v jednom okamžiku v přímém dosahu více než jednoho AMS. "Přímým dosahem" máme na mysli dosah UDP paketů. Typicky se jedná o jeden síťový segment. V opačném případě si jednotlivé AMS mohou navzájem "krást" klienty.

Každý AMS musí používat svůj vlastní SQL server. Je rozumnější použít plný SQL server na kořenovém AMS a MSDE na podřazených AMS, neboť podřazené AMS budou většinou zpracovávat menší množství dat.

2. Na každém použitém MSDE serveru povolte síťový listener. Ve výchozím nastavení je MSDE instalován ve zvláštním módu, jež zakazuje veškerou síťovou komunikaci. To z důvodu bezpečnostních rizik, jež jsou se síťovými listenery spojeny. Např. notoricky známý červ “SQL Slammer” zneužil chyby v SQL/MSDE, čímž v roce 2002 došlo k velkému poškození tisíců serverů na celém světě. Nicméně při použití modelu s více AMS je nutné, aby spolu jednotlivé databázové servery byly schopny komunikovat, protože jsou mezi nimi přenášena data prostřednictvím replikace SQL DB. Pro povolení síťových listenerů postupujte prosím následovně pro každý AMS s MSDE:

   - Spusťte následující program: %ProgramFiles%\Microsoft SQL Server\80\Tools\Binn\svrnetconn.exe

   - Objeví se dialogové okno. Přesuňte “Named Pipes” a “TCP/IP” z “Disabled Protocols” do “Enabled Protocols”.

   - Uložte změny tlačítkem OK, zastavte služby “MSSQL$AVAST” a “avast! Management Server” a opět je spusťte. Obě musí být před znovuspuštěním zastaveny.

3. Připojte se ke každému podřazenému AMS, tj. ke všem kromě toho, který

jste zvolil za kořenový, a v nabídce Soubor zvolte "Přihlásit ke kořenovému AMS." Do políčka "Kořenový AMS" vepište adresu kořenového AMS. Do polí Uživatelské jméno AMS a Heslo zadejte odpovídající údaje pro kořenový AMS (doporučujeme použít administrátorský účet). Pole Název serveru a Komentář určují, jak se tento podřazený serverový objekt bude prezentovat ve složce "Spravované servery". Pole Adresa LAN a Adresa WAN by měly obsahovat IP adresy tohoto podřazeného AMS. LAN adresa je typicky NATována; WAN adresa je vnější adresa. Pokud není vnější přístup požadován, použijte NAT adresu v obou polích. A konečně pole SQL server by mělo obsahovat úplný název lokálního SQL serveru včetně instance, např. NEMESIS\AVAST.

4. Připojte se ke kořenovému AMS a vytvořte replikační úlohu. Replikační úlohy jsou uloženy ve složce Úlohy správy databáze. Naplánujte ji, např. aby se spouštěla každou noc. Vezměte prosím v potaz, že musí existovat funkční spojení mezi jednotlivými AMS SQL databázemi, jinak nebude replikační úloha správně pracovat. Prvotní replikace může být také spuštěna okamžitě (na vyžádání) přímým spuštěním replikační úlohy. Nemá smysl spouštět replikační úlohu na jiném serveru než kořenovém.

Reportovací úlohy a úlohy Hledání počítačů se obyčejně spouští pouze na kořenovém AMS. Důvodem je, že reporty těchto úloh se týkají celopodnikové sítě (jsou vytvářeny ze všech spravovaných strojů ze všech AMS), a úlohy Hledání počítačů by neměly vytvářet nechtěné duplikace. Úlohy Hledání počítačů by se měly na podřazených AMS spouštět pouze tehdy, pokud neexistuje žádné křížení v Okolních počítačích (Network Neighborhood) nebo v Active Directory, tj. nebudou nalezeny žádné duplicity strojů.

Za zmínku také stojí, že replikační úloha poskytuje velmi omezené reportování chyb. Pro důkladnou kontrolu stavu replikačního procesu byste měl použít SQL Enterprise Manager tool. Podívejte se po něm na kořenovém AMS SQL Serveru, který obvykle nepoužívá MSDE, ale plný SQL s Enterprise Managerem.

9.5 Přístup na AMS zvenčí

Někdy můžete chtít umožnit přístup na AMS z vnějšku sítě. To může být užitečné pro roaming uživatele bez VPN přístupu, např. bez přímého přístupu na AMS, nebo pro mimopodnikovou administraci, jako například konzole běžící mimo LAN. Aby toto fungovalo, je třeba provést několik změn na síťovém obvodu (firewallu); zejména je třeba povolit následující:

Pro přístup na AMS ze vzdálené konzole

- Otevřít porty tcp/16102 a udp/6000 na firewallu (bráně) a přesměrovat je na AMS.
- V konzoli použít veřejnou (WAN) IP adresu brány jako adresu AMS.

Pro přístup vzdálených agentů na AMS

- Otevřít porty tcp/16111 a udp/6000 na firewallu (bráně), a přesměrovat je na AMS. (Aktualizace budou stahovány přímo z Internetu, neboť není možné vytvořit na bráně směrování pro http listener mirroru.)
- Nastavit klienty, aby jako adresu AMS používali veřejnou (WAN) IP adresu. Jedním ze způsobů, jak toto nastavit, je použít utilitku aswChAms.exe, která je součástí instalace spravovaných produktů avast!.

Uvědomte si prosím, že příkaz Použij hned nebude pracovat s klienty mimo LAN. Tyto stroje nemůže AMS adresovat, proto neexistuje žádný způsob, jak jim vnutit aktualizace zásad. To samé se týká situace, kdy je na agentech aktivní firewall. Pro zprovoznění funkce Použij hned i s nainstalovaným firewallem je nutné povolit provoz na portu tcp/16109 na každém z klientů.

Varování

Vytvoření díry ve vašem firewallu může být skutečně nebezpečné, neboť dojde ke snížení bezpečnosti systému. Prosím, používejte tuto volbu opatrně.

9.6 Co je kde

- Výchozí složka pro instalaci AMS/konzole je

%ProgramFiles%\ALWIL Software\Management Tools

- Výchozí složka pro instalaci avastu je

%ProgramFiles%\ALWIL Software\Avast

- AMS je hostován v systémové službě "avast! Management Server", která je implementována spouštěcím souborem avEngine.exe. Většina práce je prováděná v knihovně aswNeser.dll.

- Proces správcovské konzole se nazývá asaAdmin.exe. Nástroj údržby AMS je obsažen v AmsTool.exe.

- Na Windows NT/2000/XP/2003 je agent hostován v systémové službě "avast! NetAgent" obsažené v souboru AvAgent.exe. Všechny skeny na vyžádání (on-demand), naplánované z AMS, běží také v kontextu tohoto procesu. Většinu práce agenta je prováděno v knihovnách aswComun.dll a avClient.dll, které se natahují do do procesu AvAgent.

- Na Windows NT/2000/XP/2003 je rezidentní (on-access) skener a generátor VRDB hostován v systémové službě "avast! Antivirus" obsažené v souboru aswServ.exe.

- Poštovní skener (poskytovatel Internet Mail) je implementován souborem aswMaiSv.exe. Skenování MS Outlooku je realizováno knihovnou aswOutXt.dll, která se natahuje přímo do procesu Outlook.

- Virová databáze je obsažena v souboru <avast>\data\400.vps.

- Hlavním konfiguračním souborem je <avast>\data\avast4.ini. Uvědomte si prosím, že nastavení jsou čtena nejprve z *Bezpečného úložiště avast! (avast! Secure Storage)* - zašifrovaného úložiště dat v klíči registru HKEY_LOCAL_MACHINE\Software\ALWIL Software\avast\4.0\SS. Pokud chcete změnit spravovaný klíč v avast4.ini a máte administrátorská práva, musíte smazat přidruženou položku z Bezpečného úložiště před tím, než změníte hodnotu v INI souboru. V opačném případě bude hodnota klíče načtena přímo z Bezpečného úložiště a aktualizovaná hodnota v INI souboru bude ignorována.

- Instalační soubory pro spravované produkty jsou na AMS ve složce <adnm>\InstPkgs. Tento adresář je naplněný po startu služby Management Server a potom po každé úspěšné operaci mirroru.